Dichotomy for Graph Homomorphisms with Complex Values on Bounded Degree Graphs

Jin-Yi Cai, Artem Govorov
Department of Computer Sciences
University of Wisconsin-Madison
Madison, USA
Email: jyc@cs.wisc.edu, hovarau@cs.wisc.edu

***Abstract*—The complexity of graph homomorphisms has been a subject of intense study [1], [2], [3], [4], [5], [6], [7], [8]. The partition function $Z_{\mathbf{A}}(\cdot)$ of graph homomorphism is defined by a symmetric matrix $\mathbf{A}$ over $\mathbb{C}$. We prove that the complexity dichotomy of [7] extends to bounded degree graphs. More precisely, we prove that either $G \mapsto Z_{\mathbf{A}}(G)$ is computable in polynomial-time for every G, or for some $\Delta > 0$ it is #P-hard over (simple) graphs G with maximum degree $\Delta(G) \leq \Delta$. The tractability criterion on $\mathbf{A}$ for this dichotomy is explicit, and can be decided in polynomial-time in the size of $\mathbf{A}$. We also show that the dichotomy is effective in that either a P-time algorithm for, or a reduction from #SAT to, $Z_{\mathbf{A}}(\cdot)$ can be constructed from $\mathbf{A}$, in the respective cases.**

***Keywords*-graph homomorphism; complexity dichotomy; counting problems; bounded degree graphs; Vandermonde Argument**

I. Introduction

Given two graphs G and H, a graph homomorphism (GH) 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 [9], [10]. In 1967, Lovász [9] 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. More generally, one considers weighted graphs H where every edge of H is given a weight, represented by a symmetric matrix $\mathbf{A}$, and the partition function $Z_{\mathbf{A}}(G)$ in (1) is defined [11]. The number of homomorphisms from G to H is the special case where all edges of H have weight 1, and $\mathbf{A}$ is the 0-1 adjacency matrix of H. This partition function $Z_{\mathbf{A}}(G)$ provides an elegant framework to express a wide variety of *graph properties*. These partition functions are also widely studied in statistical physics representing spin systems [12], [13], [14], [15], [16], [17], [18].

We recap the standard definition. Our graphs G and H are undirected (unless otherwise specified). G is allowed to have multiple edges but no loops; it is *simple* if it has neither. H can have loops, multiple edges, and more generally, edge weights. We allow edge weights to be arbitrary complex numbers.[1] Let $\mathbf{A} = (A_{i,j})$ be an $m \times m$ symmetric matrix with entries $A_{i,j} \in \mathbb{C}$, we define

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

for every undirected graph $G = (V, E)$.

The complexity of the partition function $Z_{\mathbf{A}}(\cdot)$ has been shown to obey a dichotomy: Depending on $\mathbf{A}$, the computation $G \mapsto Z_{\mathbf{A}}(G)$ is either in polynomial time or #P-hard. This has been proved for progressively more general matrices $\mathbf{A}$: In [1], [2], Dyer and Greenhill first proved this complexity dichotomy for symmetric $\{0, 1\}$-matrices $\mathbf{A}$. In this case, $Z_{\mathbf{A}}(G)$ counts the number of graph homomorphisms without weight. Bulatov and Grohe [3], [4], [5] proved this for $Z_{\mathbf{A}}(\cdot)$ where $\mathbf{A}$ is any nonnegative symmetric matrix. This was extended by Goldberg, Grohe, Jerrum and Thurley [19] to all real symmetric matrices. Finally, Cai, Chen and Lu [7] generalized this to all complex symmetric matrices. Every subsequent complexity dichotomy subsumes the previous one as a special case. In each case, an explicit tractability criterion on $\mathbf{A}$ is given such that if $\mathbf{A}$ satisfies the criterion then $Z_{\mathbf{A}}(\cdot)$ is computable in P-time, otherwise it is #P-hard.

In [1] Dyer and Greenhill established a stronger fact: if a $\{0, 1\}$-matrix $\mathbf{A}$ fails the tractability condition then $Z_{\mathbf{A}}(\cdot)$ is #P-complete even when restricted to bounded degree graphs. We note that the complexity of GH for bounded degree graphs is particularly interesting as much work has been done on the approximate complexity of GH focusing on bounded degree graphs and approximate algorithms are achieved for them [20], [21], [22], [23], [24], [25], [26], [27], [28]. Beyond the 0-1 case, Govorov, Cai and Dyer [8] proved that the #P-hardness part of the Bulatov-Grohe dichotomy for nonnegative weights holds for bounded degree graphs. The tractability criterion in the nonnegative case is block-rank-1, which is relatively simple but not applicable in the complex case. The tractability criterion in the complex case (or even in the real case with mixed signs) is a lot

This paper is supported by NSF CCF-1714275. A full version is available at https://arxiv.org/abs/2004.06620.

Artem Govorov is the author's preferred spelling of his name, rather than the official spelling Artsiom Hovarau.

[1] To be computable in the strict Turing model, they are algebraic complex numbers.

2575-8454/20/$31.00 ©2020 IEEE
DOI 10.1109/FOCS46700.2020.00106

more involved. This is due to the presence of cancellation which leads to additional tractable cases. In this paper we finally extend the full complexity dichotomy for complex weights [7] to the bounded degree case.

Theorem 1. *Let* $\mathbf{A}$ *be a symmetric and algebraic complex matrix. Then either* $G \mapsto Z_{\mathbf{A}}(G)$ *can be computed in polynomial time on arbitrary graphs* G*, or for some* $\Delta > 0$ *depending on* $\mathbf{A}$*, it is #P-hard on graphs* G *of maximum degree at most* Δ*.*

The dichotomy criterion on $\mathbf{A}$ is the same as in [7]. This complexity dichotomy has an explicit form, and given $\mathbf{A}$, it is decidable in polynomial time (in the size of $\mathbf{A}$) whether $\mathbf{A}$ satisfies the criterion. However, there is a more demanding sense in which the dichotomy of [7] is not constructive. When $\mathbf{A}$ satisfies the criterion, then an explicit polynomial-time algorithm for $G \mapsto Z_{\mathbf{A}}(G)$ is given; but when $\mathbf{A}$ does not satisfy the criterion, it is only proved that a polynomial time reduction from #SAT to $Z_{\mathbf{A}}(\cdot)$ *exists* and not given constructively. In this paper we remedy this situation and prove that the dichotomy in Theorem 1 can be made fully constructive.

By the standard definition of GH, the input graph G can have multiple edges (but no loops). Our P-time algorithm for $G \mapsto Z_{\mathbf{A}}(G)$ in the tractable case of Theorem 1 works for graphs with multiple edges and loops. More importantly, we prove that in the #P-hard case, we may restrict to *simple* graphs G (i.e., no multiple edges and no loops) in addition to being of bounded degree.

Theorem 2. *The complexity dichotomy criterion in Theorem 1 is P-time decidable in the size of* $\mathbf{A}$*. If* $\mathbf{A}$ *satisfies the criterion, then* $G \mapsto Z_{\mathbf{A}}(G)$ *is computable in P-time by an explicit algorithm for any* G *(allowing multiple edges and loops). Otherwise,* $Z_{\mathbf{A}}(G)$ *is #P-hard for bounded degree simple graphs* G*, and a P-time reduction from #SAT to* $Z_{\mathbf{A}}(\cdot)$ *can be constructed from* $\mathbf{A}$*.*

The proof in [7] does not work for bounded degree graphs G. The main structure of the proof in [7] is a long sequence of successively stringent conditions which a matrix $\mathbf{A}$ must satisfy, or else it is proved that $Z_{\mathbf{A}}(\cdot)$ is #P-hard. This process continues until the conditions on $\mathbf{A}$ imply that $Z_{\mathbf{A}}(\cdot)$ is computable in polynomial time. In each stage, assuming $\mathbf{A}$ satisfies the condition of that stage, the matrix $\mathbf{A}$ (or another matrix $\mathbf{A}'$ which has a better form, but $Z_{\mathbf{A}'}(\cdot)$ is equivalent to $Z_{\mathbf{A}}(\cdot)$ in complexity) is passed on to the next stage. The condition often gives some structural information that allows for a better representation of $\mathbf{A}$, which is not available otherwise.

However, close to the beginning of [7] there is an equivalence of $Z_{\mathbf{A}}(\cdot)$ to another counting problem called $\mathsf{COUNT}(\mathbf{A})$. This equivalence allows us to substitute $\mathbf{A}$ with a "purified" matrix $\underline{\mathbf{A}}$ which defines an "equivalent" problem $Z_{\underline{\mathbf{A}}}(\cdot)$, but $\underline{\mathbf{A}}$ has desirable structural properties without which the proof in [7] cannot continue. Unfortunately, the proof of this equivalence does not work for bounded degree graphs. We also remark that the method in [8] extending the Bulatov-Grohe dichotomy for nonnegative weights to bounded degree graphs also does not work here. However, we adapt a construction from [8] in this paper.

In addition to this crucial construction, the main idea in this paper is *algebraic* instead. We will introduce a new notion called *multiplicative-block-rank*-1, and a related notion called *modular-block-rank*-1. These are weaker notions than the *block-rank*-1 condition that was widely used in all previous dichotomies. We establish a fundamental implication that if a complex matrix $\mathbf{A}$ is not multiplicative-block-rank-1, then $Z_{\mathbf{A}}(\cdot)$ is #P-hard for bounded degree graphs.

We estabslish an important technical fact about the long proof in [7]. In every stage either we prove the matrix $\mathbf{A}$ must satisfy some additional conditions, or we actually get an explicit construction of a graph fragment which defines a matrix that is *non-multiplicative-block-rank*-1. Then we show that in each case, this property of non-multiplicative-block-rank-1 can be *transferred* from any subsequent stage to the previous stage. Here is a high-level outline of our proof:

For the purification step we cannot simply substitute $\mathbf{A}$ by its purified form and move to the next stage. Instead we will keep both $\mathbf{A}$ and its purified form $\underline{\mathbf{A}}$, and pass both to subsequent stages. It is only with respect to the purified form $\underline{\mathbf{A}}$ we can use combinatorial gadget constructions to conclude that the matrix has desirable properties. However, with a purely algebraic argument we nevertheless "transfer" these conclusions to the unpurified $\mathbf{A}$. These algebraic arguments are in terms of properties of polynomials, exponential polynomials, and properties of finitely generated subfields of $\mathbb{C}$. Ultimately most of the algebraic arguments rely on a simple algebraic fact which we call the *Vandermonde Argument*. Then we show in each step how to "transfer" the property of non-multiplicative-block-rank-1 of a later stage to the previous stage. This task is accomplished by three meta-arguments, (Meta_1), (Meta_2) and (Meta_3). These formulate our transfer procedure.

For the dichotomy of Goldberg et al. [6] for real symmetric matrices $\mathbf{A}$, it is proved in [8] that its #P-hardness part can be made to hold for simple graphs. This uses interpolation with stretchings. For the dichotomy in [7] and our Theorem 1 over complex symmetric matrices $\mathbf{A}$, this trick does not work. While real symmetric matrices can always be diagonalized, for complex symmetric matrices this is not true, and more importantly, the Jordan normal form may contain nontrivial nilpotent blocks, i.e., blocks of size greater than one and corresponding to eigenvalue 0.

In this paper, we overcome this difficulty by not proving a reduction from the case of bounded degree graphs to the

case of bounded degree *and* simple graphs. Instead we use a transfer argument of the property of non-multiplicative-block-rank-1 constructions. In order to prove it, we will heavily make use of the results from [29].

II. Preliminaries

For a symmetric matrix $\mathbf{A} \in \mathbb{C}^{n\times n}$, we use $H = H_{\mathbf{A}} = (V, E)$ to denote the undirected graph: $V = [n]$ and $ij \in E$ iff $A_{i,j} \neq 0$. We say $\mathbf{A}$ is *bipartite* if H is bipartite; otherwise, $\mathbf{A}$ is *non-bipartite*. We say $\mathbf{C}$ is the *bipartization* of a matrix $\mathbf{F}$ if $\mathbf{C} = \left(\begin{smallmatrix} \mathbf{0} & \mathbf{F} \\ \mathbf{F}^{\mathsf{T}} & \mathbf{0} \end{smallmatrix}\right)$.

Let $\mathbf{A} \in \mathbb{C}^{m\times m}$ be a symmetric matrix and $\mathfrak{D} = \{\mathbf{D}^{[\![i]\!]}\}_{i=0}^{\infty}$ a sequence of diagonal matrices in $\mathbb{C}^{m\times m}$. The problem $\mathrm{EVAL}(\mathbf{A}, \mathfrak{D})$ is: Given an undirected graph $G = (V, E)$, compute

$$Z_{\mathbf{A},\mathfrak{D}}(G) = \sum_{\xi: V\to[m]} \prod_{w\in V} D_{\xi(w)}^{[\![\deg(w)]\!]} \prod_{(u,v)\in E} A_{\xi(u),\xi(v)}. \quad (2)$$

The problem $\mathsf{EVAL}(\mathbf{A})$ is the special case where every $\mathbf{D}^{[\![i]\!]} = \mathbf{I}_m$. $\mathrm{EVAL}^{(\Delta)}(\mathbf{A})$ denotes this problem when restricted to graphs G with maximum degree $\Delta(G) \leq \Delta$.

In this paper, a crucial object is an *edge gadget*. An edge gadget Γ is simply a graph (V, E) with two distinguished (ordered) vertices $u^*, v^* \in V$.

Definition 3. *Let $\mathbf{A} \in \mathbb{C}^{m\times m}$ be a symmetric matrix and let $\Gamma = (V, E)$ be an edge gadget with distinguished vertices u^*, v^* (in this order). The edge weight matrix $M_{\Gamma,\mathbf{A}} \in \mathbb{C}^{m\times m}$, or signature, of Γ in the framework $\mathrm{EVAL}(\mathbf{A})$ is defined to be, for $i, j \in [m]$,*

$$M_{\Gamma,\mathbf{A}}(i,j) = \sum_{\substack{\xi:\, V\to[m] \\ \xi(u^*)=i,\ \xi(v^*)=j}} \mathrm{wt}_{\Gamma,\mathbf{A}}(\xi)$$

$$\textit{where} \quad \mathrm{wt}_{\Gamma,\mathbf{A}}(\xi) = \prod_{(u,v)\in E} A_{\xi(u),\xi(v)}.$$

We say a matrix $\mathbf{A} \in \mathbb{C}^{m\times n}$ is *rectangular* if its rows and columns can be permuted (separately) so that it becomes a block-diagonal matrix where each block is a matrix with no zero elements, with possibly one block being an all-0 matrix. (For a symmetric $\mathbf{A}$ the permutations are the same for rows and columns.) We say $\mathbf{A}$ is *block-rank*-1 if $\mathbf{A}$ is rectangular and every (nonzero) block of $\mathbf{A}$ has rank one.

Theorem 4 (Bulatov and Grohe [3])**.** *Let $\mathbf{A}$ be a symmetric matrix with nonnegative entries. Then $\mathrm{EVAL}(\mathbf{A})$ is in polynomial time if $\mathbf{A}$ is block-rank-1, and is #P-hard otherwise.*

The Hadamard power $\mathbf{A}^{\odot k}$ is the matrix $(A_{i,j}^k)$, taking the kth power entrywise.

Definition 5. *We say $\mathbf{A} \in \mathbb{C}^{m\times n}$ is multiplicative-block-rank-1 (mult-brk-1) if there exists a $k \geq 1$ such that $\mathbf{A}^{\odot k}$ is block-rank-1. It is modular-block-rank-1 (mod-brk-1) if the matrix $(|A_{i,j}|)_{i,j=1}^{m,n}$ obtained from $\mathbf{A}$ by taking the complex norm entrywise is block-rank-1.*

Clearly, being block-rank-1 $\Longrightarrow$ mult-brk-1 $\Longrightarrow$ mod-brk-1 $\Longrightarrow$ rectangular. We will often use the implication: every non-mod-brk-1 matrix is non-mult-brk-1.

Definition 6. *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*

$$a/(g_1^{k_1} \cdots g_d^{k_d}) \textit{ is a root of unity.}$$

Lemma 7. *Every set $\mathscr{A}$ of nonzero algebraic numbers has a generating set.*

The purification matrix $\underline{\mathbf{A}}$ of $\mathbf{A}$ is constructed by taking $\mathscr{A}$ to be the non-zero entries of $\mathbf{A}$, replacing each entry of $\mathbf{A}$ of the form $a = \xi g_1^{k_1} \cdots g_d^{k_d}$ by $\xi p_1^{k_1} \cdots p_d^{k_d}$, where ξ is a root of unity and p_i is the ith smallest prime. The following lemma only applies to unbounded degree graphs.

Lemma 8. $\mathsf{EVAL}(\underline{\mathbf{A}}) \equiv \mathsf{EVAL}(\mathbf{A})$. *If $\mathbf{A} \in \mathbb{C}^{m\times m}$ is not mult-brk-1, then $\mathrm{EVAL}(\mathbf{A})$ is #P-hard.*

The following simple lemma underlies a lot of our algebraic reasonings in this paper. There are several other similar statements in the full paper; we call these the *Vandermonde Argument*.

Lemma 9. *Let $m \geq 0$, $g(x_1, \ldots, x_m) = \sum_{(i_1,\ldots,i_m)\in I} a_{i_1,\ldots,i_m} \prod_{j=1}^m x_j^{i_j} \in \mathbb{C}[x_1, \ldots, x_m]$ and $\lambda_1, \ldots, \lambda_m \in \mathbb{C}$. If $g(\lambda_1^k, \ldots, \lambda_m^k) = 0$ for $1 \leq k \leq |I|$, then $g(\overline{\lambda_1}, \ldots, \overline{\lambda_m}) = 0$.*

Corollary 10. *Let $m \geq 0$, $g_i(x_1, \ldots, x_m) \in \mathbb{C}[x_1, \ldots, x_m]$ where $1 \leq i \leq n$, let $g(x_1, \ldots, x_m) = \prod_{i=1}^n g_i(x_1, \ldots, x_m)$. Let $\lambda_1, \ldots, \lambda_m \in \mathbb{C}$. Assume $g_i(\overline{\lambda_1}, \ldots, \overline{\lambda_m}) \neq 0$ for all $1 \leq i \leq n$. Then for some $1 \leq k \leq |I|$, here $|I|$ is the number of terms in g, we have $g_i(\lambda_1^k, \ldots, \lambda_m^k) \neq 0$ for all $1 \leq i \leq n$.*

Lemma 11. *Let $m \geq 0$, $b_1, \ldots, b_m \in \mathbb{C}$, let $\{g_1, \ldots, g_d\}$, where $d \geq 0$, be a generating set for the set of nonzero entries of $(b_1, \ldots, b_m)$, and let $(c_1, \ldots, c_m)$ be the purification of $(b_1, \ldots, b_m)$ obtained by going from $(g_1, \ldots, g_d)$ to d smallest primes $(p_1, \ldots, p_d)$. Let*

$$f(x_1, \ldots, x_m) = \sum_{(i_1,\ldots,i_m)\in I} a_{i_1,\ldots,i_m} \prod_{j=1}^m x_j^{i_j} \in \mathbb{C}[x_1, \ldots, x_m].$$

If $f(c_1, \ldots, c_m) \neq 0$, then $f(b_1^\ell, \ldots, b_m^\ell) \neq 0$ for some $1 \leq \ell \leq |I|$.

III. A High-Level Description of the Proof of Theorem 1

The first preliminary step in the proof of the dichotomy theorem in [7] is to reduce the problem to connected

components. This uses the so-called first pinning lemma. But the proof for this lemma is non-constructive. Instead we use another technique that is based on transforming gadgets.

An important theorem in this paper is Theorem 14 which shows that if a complex symmetric matrix $\mathbf{A}$ is not mult-brk-1 then $\mathrm{EVAL}(\mathbf{A})$ remains #P-hard even restricted to bounded degree graphs. Indeed, extending Theorem 14 we can show that if we have an edge gadget Γ with a signature matrix $M_{\Gamma,\mathbf{A}}$ that is not mult-brk-1, then for some $\Delta > 0$, the problem $\mathrm{EVAL}^{(\Delta)}(\mathbf{A})$ is #P-hard. Using this gadget-based approach, we prove that if $\mathbf{A}$ has connected components $\{\mathbf{A}_i\}_{i\in[s]}$, then

1) Either $\mathsf{EVAL}(\mathbf{A}_i)$ is polynomial-time computable for every i, and this implies that $\mathsf{EVAL}(\mathbf{A})$ is also polynomial-time computable;
2) Or for some $i \in [s]$, we have an edge gadget Γ such that $M_{\Gamma,\mathbf{A}_i}$ is not mult-brk-1, from which we can get an edge gadget Γ' such that $M_{\Gamma',\mathbf{A}}$ is not mult-brk-1, and therefore we get #P-hardness for $\mathrm{EVAL}^{(\Delta)}(\mathbf{A})$, for some $\Delta > 0$.

After this preliminary step, we restrict to *connected* and symmetric $\mathbf{A}$. Our tractable cases are the same as in [7] and so our description will focus on how to prove #P-hardness for bounded degree graphs. As in [7] the difficulty starts with 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 given matrix $\mathbf{A}$ and the gadget such that $Z_{\mathbf{A}^*}(G) = Z_{\mathbf{A}}(G^*)$, for all undirected graphs G. This gives a reduction from $\mathsf{EVAL}(\mathbf{A}^*)$ to $\mathsf{EVAL}(\mathbf{A})$. If the gadget has bounded degree k, it also gives a reduction from $\mathsf{EVAL}^{(\Delta)}(\mathbf{A}^*)$ to $\mathsf{EVAL}^{(k\Delta)}(\mathbf{A})$ for any $\Delta \geq 0$. If the gadget were to produce nonnegative matrices $\mathbf{A}^*$, then one could apply Theorem 4 and its extension to bounded degree graphs [8] to $\mathbf{A}^*$.

However, for complex matrices $\mathbf{A}$, any graph gadget will only produce a matrix $\mathbf{A}^*$ whose entries are polynomials of the entries of $\mathbf{A}$, as they are obtained by arithmetic operations $+$ and $\times$. But no nonconstant polynomials on $\mathbb{C}$ are non-negative valued. Pointedly, *conjugation* is not an arithmetic operation. However, it is clear that for roots of unity, one *can* produce conjugation by multiplication.

Thus, as in [7] we wish to replace our matrix $\mathbf{A}$ by its purification matrix. It is here the proof in [7] fundamentally does not go through for bounded degree graphs. An essential observation of this paper is that, in each of the steps in the proof of [7] we in fact can prove the following: Either the matrix $\mathbf{A}$ satisfies some additional conditions, or we can produce an edge gadget Γ such that $M_{\Gamma,\mathbf{A}}$ is not mult-brk-1. We state three meta-arguments ($Meta_1$), ($Meta_2$) and ($Meta_3$) to formalize this ability to transfer such gadgets from one step of the proof to a previous step. Thus in the last step (when $\mathbf{A}$ does not satisfy all the tractability conditions) we have such a gadget whose signature matrix is not mult-brk-1, then we can get such a gadget in the initial setting, and then invoke the extension to Theorem 14.

To carry out this plan, we must separate out the cases where $\mathbf{A}$ is bipartite or nonbipartite. For a (nonzero) symmetric, connected and nonbipartite $\mathbf{A}$, it is mult-brk-1 iff it has the form $\mathbf{A} = (A'_{i,j}\zeta_{i,j})$ where $\mathbf{A}' = (A'_{i,j})$ is symmetric, has no zero entries and has rank 1, and $\zeta_{i,j}$ are roots of unity. For a (nonzero) symmetric, connected and bipartite $\mathbf{A}$, it is mult-brk-1 iff it is the bipartization of a rectangular matrix $\mathbf{B}$ of the form $(B'_{i,j}\zeta_{i,j})$, where $\mathbf{B}' = (B'_{i,j})$ has no zero entries and has rank 1, and $\zeta_{i,j}$ are roots of unity. Below we focus on describing the bipartite case; similar statements hold for nonbipartite matrices $\mathbf{A}$.

In the bipartite case, if $\mathbf{A}$ is mult-brk-1, it has the form $\mathbf{A} = \left(\begin{smallmatrix} \mathbf{0} & \mathbf{B} \\ \mathbf{B}^{\mathrm{T}} & \mathbf{0} \end{smallmatrix}\right)$, and $\mathbf{B}$ has the form

$$\mathbf{B} = \begin{pmatrix} \mu_1 & & & \\ & \mu_2 & & \\ & & \ddots & \\ & & & \mu_k \end{pmatrix} \begin{pmatrix} \zeta_{1,1} & \zeta_{1,2} & \cdots & \zeta_{1,m-k} \\ \zeta_{2,1} & \zeta_{2,2} & \cdots & \zeta_{2,m-k} \\ \vdots & \vdots & \ddots & \vdots \\ \zeta_{k,1} & \zeta_{k,2} & \cdots & \zeta_{k,m-k} \end{pmatrix} \begin{pmatrix} \nu_1 & & & \\ & \nu_2 & & \\ & & \ddots & \\ & & & \nu_{m-k} \end{pmatrix},$$

for some $1 \leq k < m$, in which μ_i, ν_j are nonzero, and every $\zeta_{i,j}$ is a root of unity. We prove that, for every (nonzero) symmetric, connected, and bipartite matrix $\mathbf{A} \in \mathbb{C}^{m\times m}$, either we can already prove the #P-hardness of $\mathsf{EVAL}^{(\Delta)}(\mathbf{A})$ for some $\Delta > 0$, or we may assume $\mathbf{A}$ has the above form. In the latter case we pass *both* $\mathbf{A}$ and its purification $\underline{\mathbf{A}}$ to the next step.

Continuing now with $\mathbf{A}$ and $\underline{\mathbf{A}}$, 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 EVAL problem $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ defined in the full paper, where $\mathfrak{D} = \{\mathbf{D}^{[0]}, \mathbf{D}^{[1]}, \ldots, \mathbf{D}^{[N-1]}\}$ specifies a set of vertex weights that are degree dependent $\bmod N$, for some $N \geq 1$. Matrices of the following type are called *discrete unitary* matrices:

Definition 12. *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 $i \neq j \in [m]$, we have orthogonality over $\mathbb{C}$: $\langle \mathbf{F}_{i,*}, \mathbf{F}_{j,*} \rangle = 0$ and $\langle \mathbf{F}_{*,i}, \mathbf{F}_{*,j} \rangle = 0$.*

Some of the simplest examples of discrete unitary matri-

ces are as follows:

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix},$$

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

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.

Coming back to the proof outline, we show that either there exists an edge gadget Γ such that $M_{\Gamma,\mathbf{A}}$ is not mult-brk-1 (which implies that $\mathsf{EVAL}^{(\Delta)}(\mathbf{A})$ is #P-hard for some $\Delta > 0$) or $\mathsf{EVAL}^{(\Delta)}(\mathbf{A})$ is equivalent to some $\mathsf{EVAL}^{(\Delta)}(\mathbf{C}, \mathfrak{D})$, and the pair $(\mathbf{C}, \mathfrak{D})$ satisfies some stringent conditions. In fact one can show that either $\mathsf{EVAL}^{(\Delta)}(\mathbf{A})$ is #P-hard for some $\Delta > 0$, or the pair $(\mathbf{C}, \mathfrak{D})$ has a tensor product form, and the problem $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ (and also for bounded degree graphs) can be expressed as a product of an *outer problem* $\mathsf{EVAL}(\mathbf{C}', \mathfrak{K})$ and an *inner problem* $\mathsf{EVAL}(\mathbf{C}'', \mathfrak{L})$, where $\mathsf{EVAL}(\mathbf{C}', \mathfrak{K})$ is tractable. Thus we will focus on the inner problem $\mathsf{EVAL}(\mathbf{C}'', \mathfrak{L})$, and we rename $(\mathbf{C}, \mathfrak{D})$ as the pair $(\mathbf{C}'', \mathfrak{L})$. We show that $\mathbf{C}$ is the bipartization of a discrete unitary matrix $\mathbf{F}$. In addition, there are further stringent requirements for $\mathfrak{D}$. 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 the *discrete unitary requirements*. The proof for these requirements in [7] is demanding and among the most difficult in that paper; but here we will use the meta-arguments (*Meta*$_2$) and (*Meta*$_3$) to observe that essentially the same proof can be cast in terms of transforming non-mult-brk-1 gadgets from one setting to another.

Now we assume the the pair $(\mathbf{C}, \mathfrak{D})$ satisfies the discrete unitary requirements with $\mathbf{C}$ being the bipartization of $\mathbf{F}$. Let $q > 1$ be a prime power, and let $\omega_q = e^{2\pi i/q}$.

Definition 13. *The* q-Fourier matrix $\boldsymbol{\mathcal{F}}_q$ *is a* $q \times q$ *matrix with* (x, y)*th entry* ω_q^{xy}*,* $x, y \in [0 : q-1]$.

We show that, either there exists an edge gadget Γ such that $M_{\Gamma,\mathbf{C},\mathfrak{D}}$ is not mod-brk-1 (which implies that it is not mult-brk-1 either), or after a permutation of rows and columns, $\mathbf{F}$ becomes the *tensor product* of a collection of suitable Fourier matrices:

$$\boldsymbol{\mathcal{F}}_{q_1} \otimes \boldsymbol{\mathcal{F}}_{q_2} \otimes \cdots \otimes \boldsymbol{\mathcal{F}}_{q_d},$$

where $d \geq 1$ and every q_i 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, we still get #P-hardness for $\mathsf{EVAL}^{(\Delta)}(\mathbf{C}, \mathfrak{D})$, for some $\Delta > 0$, unless $\mathbf{F}$ is the tensor product of Fourier matrices. On the other hand, the tensor product decomposition into Fourier matrices finally 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

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

Assume $q_1, \ldots, q_d$ are powers of $s \leq d$ distinct primes $p_1, \ldots, p_s$. We can also lump together all prime powers of the same prime p_i, and 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 direct product of all groups $\mathbb{Z}_{q_j}$ in the list with q_j being a power of p_i.

This canonical tensor product decomposition of $\mathbf{F}$ gives a natural way to index the rows and columns of $\mathbf{C}$ and the diagonal matrices in $\mathfrak{D}$. More exactly, for $\mathbf{x} \in \mathbb{Z}_{q_1} \times \cdots \times \mathbb{Z}_{q_d}$, 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 $(1, \mathbf{x})$.

With this canonical expression of $\mathbf{F}$ and $\mathbf{C}$, we further inquire into the structure of $\mathfrak{D}$. 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 $\mathsf{EVAL}^{(\Delta)}(\mathbf{C}, \mathfrak{D})$ is #P-hard for some $\Delta > 0$.

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 use 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 $\mathcal{T}$ denote the set of r such that $\Delta_r \neq \emptyset$. We can prove that for each $r \in \mathcal{S}$, the support set Λ_r must be a direct product of cosets, $\Lambda_r = \prod_{i=1}^{s} \Lambda_{r,i}$, where $\Lambda_{r,i}$ are cosets in the Abelian groups G_i, $i = 1, \ldots, s$, corresponding 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, $\mathsf{EVAL}^{(\Delta)}(\mathbf{C}, \mathfrak{D})$ is #P-hard for some $\Delta > 0$; more precisely, there is an edge gadget Γ such that $M_{\Gamma,\mathbf{C},\mathfrak{D}}$ is not mod-brk-1.

Second, we show that for each $r \in \mathcal{S}$ (and each $r \in \mathcal{T}$ respectively), $\mathbf{D}^{[r]}$ on its support Λ_r (and Δ_r respectively), possesses a *quadratic* structure. The quadratic structure is expressed as *a set of exponential difference equations* over bases which are appropriate roots of unity of orders equal to various prime powers. We apply the meta-arguments to prove these by transforming non-mult-brk-1 gadgets from one setting to another.

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. The tractability part of the proof is almost identical to that of [7].

IV. Non-mult-brk-1 Implies Bounded Degree Hardness

We give a proof sketch of Theorem 14 in this section.

Theorem 14. *Let $\mathbf{A} \in \mathbb{C}^{m\times m}$ be a symmetric matrix. If $\mathbf{A}$ is not mult-brk-1, then for some $\Delta > 0$, the problem $\mathrm{EVAL}^{(\Delta)}(\mathbf{A})$ is #P-hard.*

In fact, Theorem 14 extends to any edge gadget Γ: If $M_{\Gamma,\mathbf{A}}$ is not mult-brk-1 or not mod-brk-1, then for some $\Delta > 0$, the problem $\mathrm{EVAL}^{(\Delta)}(\mathbf{A})$ is #P-hard.

By combining *pairwise dependent* rows and columns of $\mathbf{A}$, we can define a symmetric matrix $\mathbf{A}' \in \mathbb{C}^{s\times s}$ and a set of diagonal matrices $\mathfrak{D}$ such that $Z_{\mathbf{A}}(G) = Z_{\mathbf{A}',\mathfrak{D}}(G)$, where $\mathbf{A}'$ is a principal submatrix of $\mathbf{A}$ with *pairwise independent* rows and columns, and $\mathfrak{D} = \{\mathbf{D}^{[\![k]\!]}\}_{k=0}^{\infty}$ with each $\mathbf{D}^{[\![k]\!]}$ a diagonal matrix with diagonal entries of the form $D_i^{[\![k]\!]} = \sum_{j=1}^{m_i} \mu_{ij}^k$ for $k \geq 0$ and $1 \leq i \leq s$. If $\mathbf{A}$ is not mult-brk-1 then neither is $\mathbf{A}'$. Note that in (2) for $Z_{\mathbf{A}',\mathfrak{D}}(G)$, the vertex weight $\mathbf{D}^{[\![\deg(w)]\!]}$ depends on the degree of w; this will be a major difficulty when we "redistribute" vertex weights.

Since this holds for all G, we have $\mathrm{EVAL}^{(\Delta)}(\mathbf{A}) \equiv \mathrm{EVAL}^{(\Delta)}(\mathbf{A}', \mathfrak{D})$ for any $\Delta \geq 0$.

The graphs $G_{n,p,\ell}$: We define a gadget $\mathcal{R}_{d,n,p,\ell}$ to replace every vertex v of G with degree $d = \deg(v)$. The gadget has d external vertices with dangling edges, and has three parameters $n, p, \ell \geq 1$. Each external vertex has a dangling edge connected to a neighbor in G, and then this connection is *thickened* $\ell + 1$ times. The resulting graph is $G_{n,p,\ell}$. Within $\mathcal{R}_{d,n,p,\ell}$ itself it has a cycle of d copies of another gadget $\mathcal{P}_{n,p,\ell}$, where n is a stretching parameter, p and ℓ are two thickening parameters. In Figure 2 we show an example, a pentagon-like $\mathcal{R}_{5,3,4,3}$. Each of the $d = 5$ sides of $\mathcal{R}_{5,3,4,3}$ is a copy of $\mathcal{P}_{3,4,3}$ which is a chain of $n = 3$ subgadgets. Each subgadget consists of $p = 4$ parallel copies of the gadget depicted in Figure 1 ($\ell = 3$ with amalgamated end vertices u and v).

We will pick p and $\ell \geq 1$ depending *only* on $\mathbf{A}$ (independent of G), and let n be polynomially bounded by the size of G. Let $\mathbf{B} = (\mathbf{A}'\mathbf{D}^{[\![\ell+1]\!]}(\mathbf{A}')^{\odot\ell})^{\odot p}$. We will pick $p, \ell \geq 1$ so that $\mathbf{B}$ is nondegenerate, and all diagonal entries in $\mathbf{D}^{[\![p(\ell+1)]\!]}$ and $\mathbf{D}^{[\![(p+1)(\ell+1)]\!]}$ are nonzero. We note that $\mathbf{A}'\mathbf{D}^{[\![\ell+1]\!]}(\mathbf{A}')^{\odot\ell}$ is the signature matrix of the gadget in Figure 1.

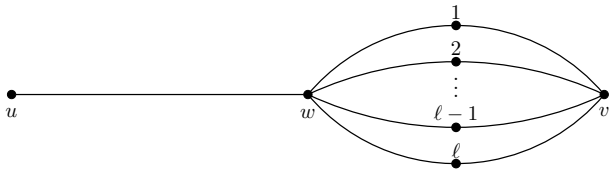

Figure 1. $\mathcal{P}_{n,p,\ell}$ is an n-chain of p-parellel copies of this gadget.

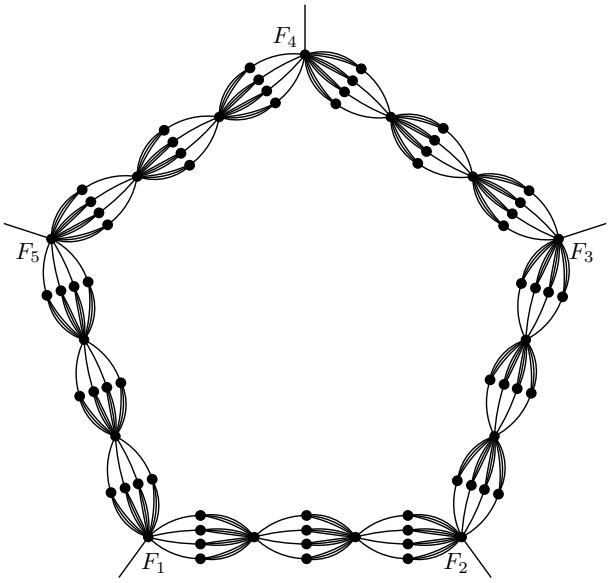

Figure 2. The gadget $\mathcal{R}_{5,3,4,3}$.

Picking p and then picking ℓ: Let $\mathbf{H} \in \mathbb{C}^{s\times s}$ be a diagonal matrix with the ith diagonal entry $H_i = \sum_{j=1}^{m_i} \mu_{ij}\overline{\mu_{ij}} > 0$ for $1 \leq i \leq s$. So $\mathbf{H}$ is positive diagonal. By an algebraic lemma, we can fix some $p \geq 1$ such that $(\mathbf{A}'\mathbf{H}\overline{\mathbf{A}'})^{\odot p}$ is nondegenerate. Also, we have $\sum_{j=1}^{m_i} \mu_{ij}^p(\overline{\mu_{ij}})^p > 0$ and $\sum_{j=1}^{m_i} \mu_{ij}^{p+1}(\overline{\mu_{ij}})^{p+1} > 0$ for $1 \leq i \leq s$. Consider the following infinite sequence of systems of conditions indexed by $\ell \geq 1$. Note that they *would* be satisfied if we formally replaced conjugation $\overline{\mu_{ij}}$ and $\overline{\mathbf{A}'}$ in the above by the ℓth powers of the respective quantities:

$$\begin{cases} \det\left((\mathbf{A}'\mathbf{D}^{[\![\ell+1]\!]}(\mathbf{A}')^{\odot\ell})^{\odot p}\right) \neq 0, \\ \sum_{j=1}^{m_i} \mu_{ij}^{p+p\ell} \neq 0, \quad 1 \leq i \leq s, \\ \sum_{j=1}^{m_i} \mu_{ij}^{(p+1)+(p+1)\ell} \neq 0, \quad 1 \leq i \leq s. \end{cases} \tag{3}$$

We use the Vandermonde Argument, Corollary 10, from Section II to pick an $\ell \geq 1$ such that each condition in the system (3) indexed by ℓ is satisfied. We now fix such an $\ell \geq 1$. From (3) we get that $\mathbf{B}$ is nondegenerate and all diagonal entries in $\mathbf{D}^{[\![p+p\ell]\!]}$ and $\mathbf{D}^{[\![p+1+(p+1)\ell]\!]}$ are nonzero, so $\mathbf{D}^{[\![p+p\ell]\!]}$ and $\mathbf{D}^{[\![p+1+(p+1)\ell]\!]}$ are nondegenerate as well.

Interpolation using $\mathbf{L}^{(n)}$: The edge gadget $\mathcal{P}_{n,p,\ell}$ has the edge weight matrix

$$\mathbf{L}^{(n)} = \underbrace{\mathbf{B}\mathbf{D}^{[\![p+p\ell]\!]}\mathbf{B}\ldots\mathbf{B}\mathbf{D}^{[\![p+p\ell]\!]}\mathbf{B}}_{\mathbf{D}^{[\![p+p\ell]\!]} \text{ appears } n-1 \geq 0 \text{ times}} = \mathbf{B}(\mathbf{D}^{[\![p+p\ell]\!]}\mathbf{B})^{n-1} \tag{4}$$

which rewrites as

$$(\mathbf{D}^{[\![p+p\ell]\!]})^{-1/2}((\mathbf{D}^{[\![p+p\ell]\!]})^{1/2}\mathbf{B}(\mathbf{D}^{[\![p+p\ell]\!]})^{1/2})^n(\mathbf{D}^{[\![p+p\ell]\!]})^{-1/2}. \tag{5}$$

In $G_{n,p,\ell}$, all the vertices that are external vertices of various $\mathcal{R}_{d,n,p,\ell}$ have degree $(p+1)(\ell+1)$ each. Their contributions to $Z_{\mathbf{A}',\mathfrak{D}}(G_{n,p,\ell})$ are not included in $\mathbf{L}^{(n)}$.

Let $\widetilde{\mathbf{B}} = (\mathbf{D}^{[\![p+p\ell]\!]})^{1/2}\mathbf{B}(\mathbf{D}^{[\![p+p\ell]\!]})^{1/2}$. Write the Jordan normal form of $\widetilde{\mathbf{B}}$ as $\widetilde{\mathbf{B}} = \mathbf{S}^{-1}\mathbf{J}\mathbf{S}$. Then $\widetilde{\mathbf{B}}^n = \mathbf{S}^{-1}\mathbf{J}^n\mathbf{S}$, so the edge weight matrix for $\mathcal{P}_{n,p,\ell}$ becomes

$$\begin{aligned}\mathbf{L}^{(n)} &= (\mathbf{D}^{[\![p+p\ell]\!]})^{-1/2}\widetilde{\mathbf{B}}^n(\mathbf{D}^{[\![p+p\ell]\!]})^{-1/2}\\ &= (\mathbf{D}^{[\![p+p\ell]\!]})^{-1/2}\mathbf{S}^{-1}\mathbf{J}^n\mathbf{S}(\mathbf{D}^{[\![p+p\ell]\!]})^{-1/2}.\end{aligned}$$

Note that $\mathbf{L}^{(n)}$ as a matrix is formally defined for any $n \geq 0$, and $\mathbf{L}^{(0)} = (\mathbf{D}^{[\![p+p\ell]\!]})^{-1}$. We denote by $\mathscr{Z}(G_{0,p,\ell})$ the value of $Z_{\mathbf{A}',\mathfrak{D}}(G_{n,p,\ell})$ when we replace $\mathbf{L}^{(0)}$ for $\mathbf{L}^{(n)}$.

Using oracle calls to get $Z_{\mathbf{A}',\mathfrak{D}}(G_{n,p,\ell})$ $(n \geq 1)$, we can get $\mathscr{Z}(G_{0,p,\ell})$ by interpolation in polynomial time. This uses the so-called exponential-polynomials (see the full paper).

Since $\mathbf{L}^{(0)}$ is a diagonal matrix, any assignment with a nonzero contribution to $\mathscr{Z}(G_{0,p,\ell})$ assigns equal value to each external vertex in a gadget $\mathcal{R}_{d,n,p,\ell}$ that corresponds to a vertex v in G. One can imagine these $\mathcal{R}_{d,n,p,\ell}$ have been replaced by a cycle of d vertices, with each cycle edge assigned $\mathbf{L}^{(0)}$; but each external vertex still has $\ell+1$ external edges, and the vertex weight is still according to $\mathbf{D}^{[\![p+1+(p+1)\ell]\!]}$. Since each vertex on a cycle gets the same value, we can contract each cycle to a single vertex. We then arrive at the $(\ell+1)$-thickening $T_{\ell+1}(G)$ of the original graph G. For each edge e of G we can further collapse its $(\ell+1)$-thickening back by assigning to e the edge weight matrix $(\mathbf{A}')^{\odot(\ell+1)}$. We still have to keep the vertex weight matrices at each vertex of $T_{\ell+1}(G)$: if a vertex in $T_{\ell+1}(G)$ has degree $d(\ell+1)$, then a vertex in G of degree d must keep the vertex weight matrix $(\mathbf{D}^{[\![p+1+(p+1)\ell]\!]}(\mathbf{D}^{[\![p+p\ell]\!]})^{-1})^d$. After this step we arrive at the original graph G.

Let $\mathfrak{P} = \{\mathbf{P}^{[\![i]\!]}\}_{i=0}^{\infty}$, where we let $\mathbf{P}^{[\![0]\!]} = \mathbf{I}_s$, and for $i > 0$, we have $P_j^{[\![i]\!]} = w_j^i$, the ith power of $w_j = \sum_{k=1}^{m_j}\mu_{jk}^{p+1+(p+1)\ell} / \sum_{k=1}^{m_j}\mu_{jk}^{p+p\ell} \neq 0$ for $1 \leq j \leq q$ (each w_j is well-defined and is nonzero by (3)). The above shows that we now can interpolate the value $Z_{(\mathbf{A}')^{\odot(\ell+1)},\mathfrak{P}}(G) = \mathscr{Z}(G_{0,p,\ell})$.

Having managed to express the vertex weight as dth powers, for degree d vertices, we can "redistribute" the vertex weight to the edge weight. For an arbitrary graph G, $Z_{(\mathbf{A}')^{\odot(\ell+1)},\mathfrak{P}}(G)$ is

$$\begin{aligned}&\sum_{\zeta:V(G)\to[s]}\prod_{z\in V(G)}P_{\zeta(z)}^{[\![\deg(z)]\!]}\prod_{(u,v)\in E(G)}(\mathbf{A}')^{\odot(\ell+1)}_{\zeta(u),\zeta(v)}\\ =&\sum_{\zeta:V(G)\to[s]}\prod_{z\in V(G)}w_{\zeta(z)}^{\deg(z)}\prod_{(u,v)\in E(G)}(\mathbf{A}')^{\odot(\ell+1)}_{\zeta(u),\zeta(v)}\\ =&\sum_{\zeta:V(G)\to[s]}\prod_{(u,v)\in E(G)}w_{\zeta(u)}w_{\zeta(v)}(\mathbf{A}')^{\odot(\ell+1)}_{\zeta(u),\zeta(v)}\\ =&\sum_{\zeta:V(G)\to[s]}\prod_{(u,v)\in E(G)}C_{\zeta(u),\zeta(v)} = Z_{\mathbf{C}}(G).\end{aligned}$$

Here $\mathbf{C}$ is an $s \times s$ matrix with the entries $C_{i,j} = (A'_{i,j})^{\ell+1}w_iw_j$ where $1 \leq i,j \leq s$. Clearly, $\mathbf{C}$ is a symmetric matrix. It follows that $\mathrm{EVAL}((\mathbf{A}')^{\odot(\ell+1)},\mathfrak{P}) \equiv \mathrm{EVAL}(\mathbf{C})$, without degree restrictions. We can show $\mathbf{C}$ is not mult-brk-1 and $\mathrm{EVAL}(\mathbf{C})$ is #P-hard (for unbounded degree graphs).

We have

$$\begin{aligned}&\mathrm{EVAL}(\mathbf{C}) \equiv \mathrm{EVAL}((\mathbf{A}')^{\odot(\ell+1)},\mathfrak{P})\\ \leq&\mathrm{EVAL}^{((p+1)(\ell+1))}(\mathbf{A}',\mathfrak{D}) \equiv \mathrm{EVAL}^{((p+1)(\ell+1))}(\mathbf{A}),\end{aligned} \tag{6}$$

so that $\mathrm{EVAL}^{(\Delta)}(\mathbf{A})$ is #P-hard for $\Delta = (p+1)(\ell+1)$.

V. Non-multiplicative-block-rank-1 from $\underline{\mathbf{A}}$ to $\mathbf{A}$

Theorem 15. *Let $\mathbf{A} \in \mathbb{C}^{m\times m}$ be a symmetric matrix, let $\underline{\mathbf{A}} \in \mathbb{C}^{m\times m}$ be the purification of $\mathbf{A}$ by going from the generating set $(g_1,\ldots,g_d)$ to primes $(p_1,\ldots,p_d)$, and let Γ be an edge gadget. If $M_{\Gamma,\underline{\mathbf{A}}}$ is not mult-brk-1 (which is true if $M_{\Gamma,\underline{\mathbf{A}}}$ is not mod-brk-1), then for some $p \geq 1$, the matrix $M_{T_p(\Gamma),\mathbf{A}} = M_{\Gamma,\mathbf{A}^{\odot p}}$ is not mult-brk-1.*

Proof: Let $\mathbf{C} = M_{\Gamma,\underline{\mathbf{A}}}$, and let $\mathbf{B}_n = M_{\Gamma,\mathbf{A}^{\odot n}}$ for $n \geq 1$. Since $\mathbf{C}$ is not mult-brk-1, there exist $1 \leq i_1 < i_2 \leq m$ and $1 \leq j_1 < j_2 \leq m$ such that the 2×2 submatrix

$$\mathbf{C}_{i_1,i_2;j_1,j_2} = \begin{pmatrix}C_{i_1,j_1} & C_{i_1,j_2}\\ C_{i_2,j_1} & C_{i_2,j_2}\end{pmatrix}$$

contains at least three nonzero entries and for every $n \geq 1$, $\mathbf{C}^{\odot n}_{i_1,i_2;j_1,j_2}$ is nondegenerate, i.e.,

$$C^n_{i_1,j_1}C^n_{i_2,j_2} - C^n_{i_1,j_2}C^n_{i_2,j_1} \neq 0. \tag{7}$$

The multiplicative group of roots of unity in the field $K = \mathbb{Q}(\{A_{i,j}\}_{i,j=1}^m)$ is a finite cyclic group. Let R be (or any positive multiple of) the order of this group. Next, let $I = \{i_1,i_2\}\times\{j_1,j_2\}$ and for each $(i,j) \in I$, consider the polynomial

$$\begin{aligned}&p_{i,j}(x_{i_1,j_1},x_{i_1,j_2},x_{i_2,j_1},x_{i_2,j_2})\\ &\quad= (\prod_{\substack{(i',j')\in I\\(i',j')\neq(i,j)}}x_{i',j'})(x^R_{i_1,j_1}x^R_{i_2,j_2} - x^R_{i_1,j_2}x^R_{i_2,j_1}).\end{aligned} \tag{8}$$

Since there are at least three nonzero entries in $\mathbf{C}_{i_1,i_2;j_1,j_2}$ and by (7), for some $(a,b) \in I$,

$$p_{a,b}(C_{i_1,j_1},C_{i_1,j_2},C_{i_2,j_1},C_{i_2,j_2}) \neq 0. \tag{9}$$

Let $\mathbf{X} = (X_{k,\ell})_{k,\ell=1}^m$ be a symmetric matrix of indeterminates in which $X_{k,\ell}$ and $X_{\ell,k}$ are identified (i.e., $X_{k,\ell} = X_{\ell,k}$) for $k,\ell \in [m]$. Consider the matrix $M_{\Gamma,\mathbf{X}}$. While we only defined $M_{\Gamma,\mathbf{X}}$ where the entries of $\mathbf{X}$ are complex numbers, the definition extends to arbitrary commutative rings. For the matrix $M_{\Gamma,\mathbf{X}}$, every edge in Γ is assigned the matrix $\mathbf{X}$, and therefore the entries of $M_{\Gamma,\mathbf{X}}$ are complex

polynomials in $\mathbf{X}$. In other words, $M_{\Gamma,\mathbf{X}} = (f_{i,j}(\mathbf{X}))_{i,j=1}^m$ for some $f_{i,j}(\mathbf{X}) \in \mathbb{C}[\mathbf{X}]$, where $i,j \in [m]$. (Here we view $\mathbf{X} = (X_{k,\ell})_{k,\ell=1}^m$ as a list of entries.) More precisely, if u^*, v^* are the distinguished vertices of Γ (in this order), then for each $i,j \in [m]$, we can write

$$f_{i,j}((X_{k,\ell})_{k,\ell=1}^m) = \sum_{\substack{\xi:V(\Gamma)\to[m] \\ \xi(u^*)=i,\xi(v^*)=j}} \prod_{(u,v)\in E(\Gamma)} X_{\xi(u),\xi(v)}.$$

Clearly, $M_{\Gamma,\mathbf{A}^{\odot n}} = (f_{i,j}(\mathbf{A}^{\odot n}))_{i,j=1}^m$ so the entries of $M_{\Gamma,\mathbf{A}^{\odot n}}$ belong to K for $n \geq 1$.

Since $\mathbf{B}_n = M_{\Gamma,\mathbf{A}^{\odot n}}$, we have $B_{n;i,j} = f_{i,j}(\mathbf{A}^{\odot n})$ for $i,j \in [m]$ and $n \geq 1$. Because $\mathbf{C} = M_{\Gamma,\underline{\mathbf{A}}}$ we also have $C_{i,j} = f_{i,j}(\underline{\mathbf{A}})$ for $i,j \in [m]$.

Let $q_{a,b}((X_{i,j})_{i,j=1}^m)$ be a complex polynomial defined as

$$q_{a,b}(\mathbf{X}) = p_{a,b}(f_{i_1,j_1}(\mathbf{X}), f_{i_1,j_2}(\mathbf{X}), f_{i_2,j_1}(\mathbf{X}), f_{i_2,j_2}(\mathbf{X})).$$

Then (9) rewrites as

$$q_{a,b}(\underline{\mathbf{A}}) \neq 0.$$

Since $\underline{\mathbf{A}}$ is the purification of $\mathbf{A}$ obtained by going from $(g_1,\ldots,g_d)$ to $(p_1,\ldots,p_d)$, by Corollary 11, we have

$$q_{a,b}(\mathbf{A}^{\odot p}) \neq 0$$

for some $p \geq 1$ (bounded by the number of terms in the expansion of $q_{a,b}(\mathbf{X})$). This is the same as

$$\begin{aligned} &p_{a,b}(B_{p;i_1,j_1}, B_{p;i_1,j_2}, B_{p;i_2,j_1}, B_{p;i_2,j_2}) \\ &= (\prod_{\substack{(i,j)\in I \\ (i,j)\neq(a,b)}} B_{p;i,j})(B^R_{p;i_1,j_1}B^R_{p;i_2,j_2} - B^R_{p;i_1,j_2}B^R_{p;i_2,j_1}) \neq 0. \end{aligned}$$

It follows that the matrix

$$\mathbf{B}_{p;i_1,i_2;j_1,j_2} = \begin{pmatrix} B_{p;i_1,j_1} & B_{p;i_1,j_2} \\ B_{p;i_2,j_1} & B_{p;i_2,j_2} \end{pmatrix}$$

has at most one zero entry (which can only be $B_{p;a,b}$), and

$$B^R_{p;i_1,j_1}B^R_{p;i_2,j_2} - B^R_{p;i_1,j_2}B^R_{p;i_2,j_1} \neq 0. \tag{10}$$

If $\mathbf{B}_{p;i_1,i_2;j_1,j_2}$ has precisely one zero entry, i.e., if $\mathbf{B}_{p;a,b} = 0$, then clearly $\mathbf{B}_p$ is not rectangular so neither is $M^{\odot R}_{\Gamma,\mathbf{A}^{\odot p}} = \mathbf{B}^{\odot R}_p$ implying that the latter is not block-rank-1. Assume $\mathbf{B}_{p;i_1,i_2;j_1,j_2}$ has no zero entries. In this case, (10) means that $\mathbf{B}^{\odot R}_{p;i_1,i_2;j_1,j_2}$ is nondegenerate and we conclude that $M^{\odot R}_{\Gamma,\mathbf{A}^{\odot p}} = \mathbf{B}^{\odot R}_p$ is not block-rank-1.

Because R is a common multiple of the orders of all roots of unity in $\mathbb{F}$, $M^{\odot R}_{\Gamma,\mathbf{A}^{\odot p}}$ is not block-rank-1 implies that $M_{\Gamma,\mathbf{A}^{\odot p}}$ is not mult-brk-1. ∎

REFERENCES

[1] M. E. Dyer and C. S. Greenhill, "The complexity of counting graph homomorphisms," *Random Struct. Algorithms*, vol. 17, no. 3-4, pp. 260–289, 2000, a preliminary version appeared in SODA 2000: 246–255.

[2] ——, "Corrigendum: The complexity of counting graph homomorphisms," *Random Struct. Algorithms*, vol. 25, no. 3, pp. 346–352, 2004.

[3] A. Bulatov and M. Grohe, "The complexity of partition functions," *Theor. Comput. Sci.*, vol. 348, no. 2-3, pp. 148–186, 2005, a preliminary version appeared in ICALP 2004: 294–306.

[4] M. Thurley, "The complexity of partition functions," Ph.D. dissertation, Humboldt Universität zu Berlin, 2009.

[5] M. Grohe and M. Thurley, "Counting homomorphisms and partition functions," in *Model Theoretic Methods in Finite Combinatorics*, ser. Contemporary Mathematics, M. Grohe and J. Makowsky, Eds., vol. 558. American Mathematical Society, 2011, pp. 243–292.

[6] L. A. Goldberg, M. Grohe, M. Jerrum, and M. Thurley, "A complexity dichotomy for partition functions with mixed signs," *SIAM J. Comput.*, vol. 39, no. 7, pp. 3336–3402, 2010.

[7] J.-Y. Cai, X. Chen, and P. Lu, "Graph homomorphisms with complex values: A dichotomy theorem," *SIAM J. Comput.*, vol. 42, no. 3, pp. 924–1029, 2013.

[8] A. Govorov, J.-Y. Cai, and M. Dyer, "A dichotomy for bounded degree graph homomorphisms with nonnegative weights," *To appear in Proceedings of the 47th International Colloquium on Automata, Languages and Programming (ICALP)*, 2020. [Online]. Available: https://arxiv.org/abs/2002.02021

[9] L. Lovász, "Operations with structures," *Acta Mathematica Hungarica*, vol. 18, pp. 321–328, 1967.

[10] P. Hell and J. Nešetřil, *Graphs and Homomorphisms*. Oxford University Press, 2004.

[11] M. Freedman, L. Lovász, and A. Schrijver, "Reflection positivity, rank connectivity, and homomorphism of graphs," *Journal of the American Mathematical Society*, vol. 20, pp. 37–51, 2007.

[12] R. J. Baxter, *Exactly Solved Models in Statistical Mechanics*. Academic Press, London, 1982.

[13] E. Ising, "Beitrag zur Theorie des Frromagnetismus," *Z. Phys.*, vol. 31, no. 1, pp. 253–258, 1925.

[14] R. B. Potts, "Some generalized order-disorder transformations," *Mathematical Proceedings of the Cambridge Philosophical Society*, vol. 48, no. 1, pp. 106–109, 1952.

[15] R. B. Potts and J. C. Ward, "The combinatrial method and the two-dimensional Ising model," *Progress of Theoretical Physics*, vol. 13, no. 1, pp. 38–46, 1955.

[16] M. Jerrum and A. Sinclair, "Polynomial-time approximation algorithms for the Ising model," *SIAM J. Comput.*, vol. 22, no. 5, pp. 1087–1116, 1993.

[17] L. Goldberg and M. Jerrum, "Approximating the partition function of the ferromagnetic Potts model," *J. ACM*, vol. 59, no. 5, pp. 25:1–25:31, 2012.

[18] L. Goldberg and H. Guo, "The complexity of approximating complex-valued Ising and Tutte partition functions," *Computational Complexity*, vol. 26, no. 4, pp. 765–833, 2017.

[19] L. Goldberg, M. Grohe, M. Jerrum, and M. Thurley, "A complexity dichotomy for partition functions with mixed signs," *SIAM Journal on Computing*, vol. 39, no. 7, pp. 3336–3402, 2010.

[20] M. E. Dyer, A. M. Frieze, and M. Jerrum, "On counting independent sets in sparse graphs," *SIAM J. Comput.*, vol. 31, no. 5, pp. 1527–1541, 2002.

[21] D. Weitz, "Counting independent sets up to the tree threshold," in *Proceedings of the 38th Annual ACM SIGACT Symposium on Theory of Computing (STOC)*, 2006, pp. 140–149.

[22] A. Sly, "Computational transition at the uniqueness threshold," in *Proceedings of the 51st Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, 2010, pp. 287–296.

[23] A. Sinclair, P. Srivastava, and M. Thurley, "Approximation algorithms for two-state anti-ferromagnetic spin systems on bounded degree graphs," in *Proceedings of the 23rd Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, 2012, pp. 941–953.

[24] L. Li, P. Lu, and Y. Yin, "Correlation decay up to uniqueness in spin systems," in *Proceedings of the 24th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, 2013, pp. 67–84.

[25] A. I. Barvinok, *Combinatorics and Complexity of Partition Functions*, ser. Algorithms and combinatorics. Springer, 2017, vol. 30.

[26] A. I. Barvinok and P. Soberón, "Computing the partition function for graph homomorphisms," *Combinatorica*, vol. 37, no. 4, pp. 633–650, 2017.

[27] H. Peters and G. Regts, "Location of zeros for the partition function of the Ising model on bounded degree graphs," *arXiv:1810.01699*, 2018. [Online]. Available: https://arxiv.org/abs/1810.01699

[28] T. Helmuth, W. Perkins, and G. Regts, "Algorithmic Pirogov-Sinai theory," in *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing (STOC)*, 2019, pp. 1009–1020.

[29] J.-Y. Cai and A. Govorov, "On a theorem of Lovász that $\hom(\cdot, H)$ determines the isomorphism type of H," in *Proceedings of the 11th Innovations in Theoretical Computer Science (ITCS)*, 2020, pp. 17:1–17:15, full version available at https://arxiv.org/abs/1909.03693.