SIAM J. COMPUT.
Vol. 39, No. 7, pp. 3336–3402

A COMPLEXITY DICHOTOMY FOR PARTITION FUNCTIONS WITH MIXED SIGNS*

LESLIE ANN GOLDBERG†, MARTIN GROHE‡, MARK JERRUM§, AND MARC THURLEY‡

Abstract. *Partition functions*, also known as *homomorphism functions*, form a rich family of graph invariants that contain combinatorial invariants such as the number of k-colorings or the number of independent sets of a graph and also the partition functions of certain "spin glass" models of statistical physics such as the Ising model. Building on earlier work by Dyer and Greenhill [*Random Structures Algorithms*, 17 (2000), pp. 260–289] and Bulatov and Grohe [*Theoret. Comput. Sci.*, 348 (2005), pp. 148–186], we completely classify the computational complexity of partition functions. Our main result is a dichotomy theorem stating that every partition function is either computable in polynomial time or #P-complete. Partition functions are described by symmetric matrices with real entries, and we prove that it is decidable in polynomial time in terms of the matrix whether a given partition function is in polynomial time or #P-complete. While in general it is very complicated to give an explicit algebraic or combinatorial description of the tractable cases, for partition functions described by Hadamard matrices (these turn out to be central in our proofs) we obtain a simple algebraic tractability criterion, which says that the tractable cases are those "representable" by a quadratic polynomial over the field $\mathbb{F}_2$.

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

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

DOI. 10.1137/090757496

1. Introduction.

We study the complexity of a family of graph invariants known as *partition functions* or *homomorphism functions* (see, for example, [12, 20, 21]). Many natural graph invariants can be expressed as homomorphism functions, among them the number of k-colorings, the number of independent sets, and the number of nowhere-zero k-flows of a graph. The functions also appear as the partition functions of certain "spin-glass" models of statistical physics, such as the Ising model or the q-state Potts model.

Let $A \in \mathbb{R}^{m\times m}$ be a symmetric real matrix with entries $A_{i,j}$. The *partition function* Z_A associates with every graph $G = (V, E)$ the real number

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

We refer to the row and column indices of the matrix, which are elements of $[m] := \{1, \ldots, m\}$, as *spins*. We use the term *configuration* to refer to a mapping $\xi : V \to [m]$ assigning a spin to each vertex of the graph. To avoid difficulties with models of real

*Received by the editors April 29, 2009; accepted for publication (in revised form) May 19, 2010; published electronically August 5, 2010. This work was partly funded by the EPSRC grant "The complexity of counting in constraint satisfaction problems" and by the Deutsche Forschungsgemeinschaft within the research training group "Methods for Discrete Structures" (GRK 1408).

http://www.siam.org/journals/sicomp/39-7/75749.html

†Department of Computer Science, University of Liverpool, Liverpool L69 3BX, UK (L.A. Goldberg@liverpool.ac.uk).

‡Institut für Informatik, Humboldt-Universität zu Berlin, 10099 Berlin, Germany (grohe@informatik.hu-berlin.de, thurley@informatik.hu-berlin.de).

§School of Mathematical Sciences, Queen Mary, University of London, Mile End Road, London E1 4NS, UK (m.jerrum@qmul.ac.uk).

number computation, throughout this paper we restrict our attention to algebraic numbers.[1] Let $\mathbb{R}_{\mathbb{A}}$ denote the set of algebraic real numbers.

Our main result is a dichotomy theorem stating that for every symmetric matrix $A \in \mathbb{R}_{\mathbb{A}}^{m\times m}$ the partition function Z_A is either computable in polynomial time or #P-hard. This extends earlier results by Dyer and Greenhill [8], who proved the dichotomy for 0-1 matrices, and Bulatov and Grohe [6], who proved it for nonnegative matrices. Therefore, in this paper we are mainly interested in matrices with both positive and negative entries.

Motivation. The main motivation for this work is understanding the complexity of computation for problems within #P (and problems reducible to #P) and in particular understanding the boundary between tractable and intractable. An easy modification of Ladner's theorem [17] shows that there is no clean boundary between tractable and intractable within the whole of #P in the sense that, if FP (the class of polynomial-time computable functions) is unequal to #P, then there is an infinite hierarchy in between. However, *partition functions* present a wide class of problems, containing many natural and interesting examples, for which dichotomy theorems do hold.

Examples. In the following, let $G = (V, E)$ be a graph with N vertices. Consider the matrices

$$S = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \quad \text{and} \quad C_3 = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}.$$

It is not hard to see that $Z_S(G)$ is the number of independent sets of a graph G and $Z_{C_3}(G)$ is the number of 3-colorings of G. More generally, if A is the adjacency matrix of a graph H, then $Z_A(G)$ is the number of homomorphisms from G to H. Here we allow H to have loops and parallel edges; the entry $A_{i,j}$ in the adjacency matrix is the number of edges from vertex i to vertex j.

Let us turn to matrices with negative entries. Consider

$$H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{1.1}$$

Then $\frac{1}{2}Z_{H_2}(G) + 2^{N-1}$ is the number of induced subgraphs of G with an even number of edges. Hence up to a simple transformation, Z_{H_2} counts induced subgraphs with an even number of edges. To see this, observe that for every configuration $\xi : V \to [2]$ the term $\prod_{\{u,v\}\in E} A_{\xi(u),\xi(v)}$ is 1 if the subgraph of G induced by $\xi^{-1}(2)$ has an even number of edges and -1 otherwise. Note that H_2 is the simplest nontrivial Hadamard matrix. Hadamard matrices will play a central role in this paper. Another simple example is the matrix

$$U = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}.$$

It is a nice exercise to verify that for connected G the number $Z_U(G)$ is 2^N if G is Eulerian and 0 otherwise.

[1] There is a problem with the treatment of real numbers in [6], but all results stated in [6] are valid for algebraic real numbers. We use a standard representation of algebraic numbers by polynomials and standard Turing machines as our underlying model of computation. See [9, 23] for a more detailed discussion of this issue.

A less obvious example of a counting function that can be expressed in terms of a partition function is the number of nowhere-zero k-flows of a graph. It can be shown that the number of nowhere-zero k-flows of a graph G with N vertices is $k^{-N} \cdot Z_{F_k}(G)$, where F_k is the $k \times k$ matrix with $(k-1)$'s on the diagonal and -1's everywhere else. This is a special case of a more general connection between partition functions for matrices A with diagonal entries d and off diagonal entries c and certain values of the Tutte polynomial. This well-known connection can be derived by establishing certain contraction-deletion identities for the partition functions. For example, it follows from [24, equation (3.5.4)] and [22, equations (2.26) and (2.9)].

Complexity. Like the complexity of graph polynomials [2, 14, 16, 19] and constraint satisfaction problems [1, 3, 4, 5, 10, 13, 15], which are both closely related to our partition functions, the complexity of partition functions has already received quite a bit of attention. Dyer and Greenhill [8] studied the complexity of counting homomorphisms from a given graph G to a fixed graph H without parallel edges. (Homomorphisms from G to H are also known as H*-colorings* of G.) They proved that the problem is in polynomial time if every connected component of H is either a complete graph with a loop at every vertex or a complete bipartite graph, and the problem is #P-hard otherwise. The two polynomial-time cases are very easy to see; in both cases, a trivial algorithm suffices. The interesting thing about the result of Dyer and Greenhill is that they manage to show that the problem is #P-hard in every other case. Note that this result gives a complete classification of the complexity of computing Z_A for symmetric 0-1 matrices A since every such matrix can be viewed as the adjacency matrix of an undirected graph H. Bulatov and Grohe [6] extended this result to symmetric nonnegative matrices. To state the result, it is convenient to introduce the notion of a *block* of a matrix A. To define the blocks of A, it is best to view A as the adjacency matrix of a graph with weighted edges; then each nonbipartite connected component of this graph corresponds to one block, and each bipartite connected component corresponds to two blocks. A formal definition will be given below. Bulatov and Grohe [6] proved that computing the function Z_A is in polynomial time if the row rank of every block of A is 1 and $\#P$-hard otherwise. Their theorem is stated formally below. The problem for matrices with negative entries was left open. In particular, Bulatov and Grohe asked for the complexity of the partition function Z_{H_2} for the matrix H_2 introduced in (1.1). Note that H_2 is a matrix with one block of row rank 2. As we shall see, Z_{H_2} is computable in polynomial time. Hence the complexity classification of Bulatov and Grohe does not extend to matrices with negative entries. Nevertheless, we obtain a dichotomy, and this is our main result.

Results and outline of the proofs. Our main theorem is the following.

THEOREM 1.1 (Dichotomy Theorem). *Let $A \in \mathbb{R}_{\mathbb{A}}^{m \times m}$ be a symmetric matrix. Then the function Z_A either can be computed in polynomial time or is #P-hard. Also, there is a polynomial-time computable predicate on symmetric matrices A such that Z_A is computable in polynomial time if the predicate holds, and Z_A is #P-hard otherwise.*

Let us call a matrix A *tractable* if Z_A can be computed in polynomial time and *hard* if computing Z_A is #P-hard. Then the Dichotomy Theorem states that every symmetric matrix with entries in $\mathbb{R}_{\mathbb{A}}$ is either tractable or hard. The classification of matrices into tractable and hard matrices can be made explicit, but is very complicated and does not give any real insights. Very roughly, a matrix A is tractable if each of its blocks can be written as a tensor product of a positive matrix of row rank 1 and a tractable Hadamard matrix. Unfortunately, the real classification is not

that simple, but for now let us focus on tractable Hadamard matrices. Recall that a Hadamard matrix is a square matrix H with entries from $\{-1,1\}$ such that $H \cdot H^T$ is a diagonal matrix. Let $H \in \{-1,1\}^{n\times n}$ be a symmetric $n \times n$ Hadamard matrix with $n = 2^k$. Let $\rho : \mathbb{F}_2^k \to [n]$ be a bijective mapping, which we call an *index mapping*. We say that a multivariate polynomial $h(X_1, \ldots, X_k, Y_1, \ldots, Y_k)$ over $\mathbb{F}_2$ *symmetrically represents* H *with respect to* ρ if, for all $\mathbf{x} = (x_1, \ldots, x_k)$, $\mathbf{y} = (y_1, \ldots, y_k) \in \mathbb{F}_2^k$, it holds that

$$h(x_1, \ldots, x_k, y_1, \ldots, y_k) = 1 \iff H_{\rho(\mathbf{x}),\rho(\mathbf{y})} = -1.$$

For example, the $\mathbb{F}_2$-polynomial $h_2(X_1, Y_1) = X_1 \cdot Y_1$ symmetrically represents the matrix H_2 with respect to the index mapping $\rho(x_1) = x_1 + 1$. The $\mathbb{F}_2$-polynomial $h_4(X_1, X_2, Y_1, Y_2) = X_1 \cdot Y_2 \oplus X_2 \cdot Y_1$ symmetrically represents the matrix

$$H_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

with respect to the index mapping $\rho(x_1, x_2) = 2 \cdot x_1 + x_2 + 1$. The qualifier "symmetrically" in "symmetrically represents" indicates that the same index mapping is applied to both $\mathbf{x}$ and $\mathbf{y}$. We will need to consider asymmetric representations later. Note that we can represent a matrix $H \in \{-1,1\}^{n\times n}$ by an $\mathbb{F}_2$-polynomial in this way only if n is a power of 2. In this case, for every index mapping ρ there is a unique $\mathbb{F}_2$-polynomial symmetrically representing h with respect to ρ. We say that H has a *quadratic representation* if there is an index mapping ρ and an $\mathbb{F}_2$-polynomial h of degree at most 2 that symmetrically represents H with respect to ρ. Our dichotomy theorem for Hadamard matrices is as follows.

THEOREM 1.2 (complexity classification for Hadamard matrices). *A symmetric Hadamard matrix H is tractable if it has a quadratic representation and hard otherwise.*

Hence, in particular, the matrices H_2 and H_4 are tractable. The tractability part of Theorem 1.2 is an easy consequence of the fact that counting the number of solutions of a quadratic equation over $\mathbb{F}_2$ (or any other finite field) is in polynomial time (see [11, 18]). The following symmetric Hadamard matrix has no quadratic representation and so is hard:

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & 1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & -1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & -1 \\ -1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 \end{pmatrix}.$$

The difficulty in proving the hardness part is that the degree of a polynomial representing a Hadamard matrix is not invariant under the choice of the index mapping ρ. However, for *normalized* Hadamard matrices, that is, Hadamard matrices whose first row and column consist entirely of +1s, we can show that either they are hard or they can be written as an iterated tensor product of the two simple Hadamard matrices H_2 and H_4. This gives us a canonical index mapping and hence a

canonical representation by a quadratic $\mathbb{F}_2$-polynomial. Unfortunately, we could not find a direct reduction from arbitrary to normalized Hadamard matrices. To get a reduction, we first need to work with a generalization of partition functions. If we view the matrix A defining a partition function as an edge-weighted graph, then this is the natural generalization to graphs with edge and vertex weights. Let $A \in \mathbb{R}_{\mathbb{A}}^{m\times m}$ be a symmetric matrix and $D \in \mathbb{R}_{\mathbb{A}}^{m\times m}$ a diagonal matrix, which may be viewed as assigning the weight $D_{i,i}$ to each vertex i. We define the *partition function* $Z_{A,D}$ by

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

for every graph $G = (V, E)$. As a matter of fact, we need a further generalization that takes into account that vertices of even and odd degrees behave differently when it comes to negative edge weights. For a symmetric matrix $A \in \mathbb{R}_{\mathbb{A}}^{m\times m}$ and two diagonal matrices $D, O \in \mathbb{R}_{\mathbb{A}}^{m\times m}$ we let

$$Z_{A,D,O}(G) = \sum_{\xi:V\to[m]} \prod_{\{u,v\}\in E} A_{\xi(u),\xi(v)} \cdot \prod_{\substack{v\in V\\ \deg(v) \text{ is even}}} D_{\xi(v),\xi(v)} \cdot \prod_{\substack{v\in V\\ \deg(v) \text{ is odd}}} O_{\xi(v),\xi(v)}$$

for every graph $G = (V, E)$. We call $Z_{A,D,O}$ the *parity-distinguishing partition function* (pdpf) defined by A, D, O. We show that the problem of computing $Z_{A,D,O}(G)$ is always either polynomial-time solvable or #P-hard, and we call a triple (A, D, O) *tractable* or *hard* accordingly. Obviously, if $D = O = I_m$ are identity matrices, then we have $Z_A = Z_{A,D} = Z_{A,D,O}$.

Returning to the outline of the proof of Theorem 1.2, we can show that, for every Hadamard matrix H, either H is hard or there is a normalized Hadamard matrix H' and diagonal matrices D', O' such that computing Z_H is polynomial-time equivalent to computing $Z_{H',D',O'}$. Actually, it turns out that we may assume D' to be an identity matrix and O' to be a diagonal matrix with entries $0, 1$ only. For the normalized matrix H' we have a canonical index mapping, and we can use this to represent the matrices D' and O' over $\mathbb{F}_2$ (in a sense to be explained later). Then we obtain a tractability criterion that essentially says that (H', D', O') is tractable if the representation of H' is quadratic and that of O' is linear in the sense that, under the canonical index mapping of H', the subset of indices for which O' is 1 forms a linear subspace. There is no analogous condition on D' because it is an identity matrix.

For the proof of the Dichotomy Theorem, Theorem 1.1, we actually need an extension of Theorem 1.2 that states a dichotomy for parity-distinguishing partition functions $Z_{A,D,O}$, where A is a "bipartization" of a Hadamard matrix (this notion will be defined later). The proof sketched above can be generalized to give this extension. Then to prove the Dichotomy Theorem, we first reduce the problem of computing Z_A to the problem of computing Z_C for the connected components C of A. The next step is to eliminate duplicate rows and columns in the matrix, which can be done at the price of introducing vertex weights. Using the classification theorem for nonnegative matrices and some gadgetry, from there we get the desired reduction to parity-distinguishing partition functions for bipartizations of Hadamard matrices.

Let us finally mention that our proof shows that the Dichotomy Theorem holds not only for simple partition functions Z_A but also for vertex-weighted and parity-distinguishing partition functions.

Preliminaries. Let $A \in \mathbb{R}_{\mathbb{A}}^{m\times n}$ be an $(m \times n)$-matrix. The entries of A are denoted by $A_{i,j}$. The ith row of A is denoted by $A_{i,*}$ and the jth column by $A_{*,j}$. By

abs(A) we denote the matrix obtained from A by taking the absolute value of each entry in A.

Let I_m be the $m \times m$ identity matrix and, for every $\Lambda \subseteq [m]$, let $I_{m;\Lambda}$ be the $m \times m$ matrix that is all zero except that $I_{j,j} = 1$ for $j \in \Lambda$.

The *Hadamard* product C of two $m \times n$ matrices A and B, written $C = A \circ B$, is the $m \times n$ componentwise product in which $C_{i,j} = A_{i,j} B_{i,j}$. $-A$ denotes the Hadamard product of A and the matrix in which every entry is -1.

We write $\langle u, v \rangle$ to denote the inner product (or dot product) of two vectors in $\mathbb{R}_{\mathbb{A}}^n$.

Recall that the *tensor product* (or *Kronecker product*) of an $r \times s$ matrix B and a $t \times u$ matrix C is an $rt \times su$ matrix $B \otimes C$. For $k \in [r]$, $i \in [t]$, $\ell \in [s]$, and $j \in [u]$, we have $(B \otimes C)_{(k-1)t+i,(\ell-1)u+j} = B_{k,\ell} C_{i,j}$. It is sometimes useful to think of the product in terms of rs "blocks" or "tiles" of size $t \times u$.

$$B \otimes C = \begin{pmatrix} B_{11}C & \dots & B_{1s}C \\ \vdots & \ddots & \vdots \\ B_{r1}C & \dots & B_{rs}C \end{pmatrix}.$$

For index sets $I \subseteq [m]$, $J \subseteq [n]$, we let $A_{I,J}$ be the $(|I| \times |J|)$-*submatrix* with entries $A_{i,j}$ for $i \in I$, $j \in J$. The matrix A is *indecomposable* if there are no index sets $I \subseteq [m]$, $J \subseteq [n]$ such that $(I, J) \neq (\emptyset, \emptyset)$, $(I, J) \neq ([m], [n])$, and $A_{i,j} = 0$ for all $(i, j) \in \big(([m] \setminus I) \times J\big) \cup \big(I \times ([n] \setminus J)\big)$. Note that, in particular, an indecomposable matrix has at least one nonzero entry. The *blocks* of a matrix are the maximal indecomposable submatrices. For every symmetric matrix $A \in \mathbb{R}^{n \times n}$ we can define a graph G with vertex set $[n]$ and edge set $\big\{\{i, j\} \bigm| A_{i,j} \neq 0\big\}$. We call the matrix A *bipartite* if the graph G is bipartite. We call A *connected* if the graph G is connected. The *connected components* of A are the maximal submatrices $A_{C,C}$ such that $G[C]$, the subgraph of G induced by $C \subseteq [n]$, is a connected component. If the connected component $G[C]$ is not bipartite, then $A_{C,C}$ is a block of A. If the connected component $G[C]$ is bipartite and contains an edge, then $A_{C,C}$ has the form $\left(\begin{smallmatrix} 0 & B \\ B^T & 0 \end{smallmatrix}\right)$, where B is a block of A. Furthermore, all blocks of A arise from connected components in this way.

For two counting problems f and g, we write $f \leq g$ if there is a polynomial time Turing reduction from f to g. If $f \leq g$ and $g \leq f$ hold, we write $f \equiv g$. For a symmetric matrix A and diagonal matrices D, O of the same size, EVAL(A, D, O) (EVAL(A, D), EVAL(A)) denotes the problem of computing $Z_{A,D,O}(G)$ ($Z_{A,D}(G)$, $Z_A(G)$, resp.) for an input graph G (which need not be a simple graph; it may have loops and/or multiedges).

We can now formally state the result of Bulatov and Grohe that we use.

THEOREM 1.3 (Bulatov and Grohe). *Let A be a symmetric matrix with nonnegative entries in $\mathbb{R}_{\mathbb{A}}$.*

1. *If A is connected and not bipartite, then* EVAL(A) *is in polynomial time if the row rank of A is at most* 1*; otherwise* EVAL(A) *is #P-hard.*
2. *If A is connected and bipartite, then* EVAL(A) *is in polynomial time if the row rank of A is at most* 2*; otherwise* EVAL(A) *is #P-hard.*
3. *If A is not connected, then* EVAL(A) *is in polynomial time if each of its connected components satisfies the corresponding condition stated in* (1) *or* (2)*; otherwise* EVAL(A) *is #P-hard.*

2. Hadamard matrices. The main focus of this section is on proving Theorem 2.2 below which is a strengthened version of Theorem 1.2. Suppose that H is an $n \times n$ Hadamard matrix (which is not necessarily symmetric) and that Λ^R and Λ^C

are subsets of $[n]$. It will be useful to work with the *bipartization* M, Λ of H, Λ^R, and Λ^C which we define as follows. Let $m = 2n$, and let M be the $m \times m$ matrix defined by the following equations for $i, j \in [n]$: $M_{i,j} = 0$, $M_{i,n+j} = H_{i,j}$, $M_{n+i,j} = H_{j,i}$, and $M_{n+i,n+j} = 0$. The matrix M can be broken into four "tiles" as follows:

$$M = \begin{pmatrix} 0 & H \\ H^T & 0 \end{pmatrix}.$$

Let $\Lambda = \Lambda^R \cup \{n + j \mid j \in \Lambda^C\}$. Note that the matrix $I_{m;\Lambda}$ can be decomposed naturally in terms of the tiles $I_{n;\Lambda^R}$ and $I_{n;\Lambda^C}$:

$$I_{m;\Lambda} = \begin{pmatrix} I_{n;\Lambda^R} & 0 \\ 0 & I_{n;\Lambda^C} \end{pmatrix}.$$

We identify a set of conditions on H, Λ^R, and Λ^C that determine whether or not the problem $\mathrm{EVAL}(M, I_m, I_{m;\Lambda})$ can be computed in polynomial time. We will see how this implies Theorem 1.2. The reason that we work with the problem $\mathrm{EVAL}(M, I_m, I_{m;\Lambda})$ is that M is a symmetric matrix, whereas H is not necessarily symmetric. If H is symmetric and $\Lambda^R = \Lambda^C$, then essentially the same set of conditions determines whether or not the problem $\mathrm{EVAL}(H, I_n, I_{n;\Lambda^R})$ can be computed in polynomial time. The only extra condition that we need for this is that our representation (defined below) is consistent on the rows and columns of H. Therefore, we add this stipulation in the conditions that we develop below.

The group condition. For an $n \times n$ matrix H and a row index $l \in [n]$, let

$$G(H, l) := \{H_{i,*} \circ H_{l,*} \mid i \in [n]\} \cup \{-H_{i,*} \circ H_{l,*} \mid i \in [n]\}.$$

The *group condition for H* is as follows:

(CG) For all $l \in [n]$, both $G(H, l) = G(H, 1)$ and $G(H^T, l) = G(H^T, 1)$.

The group condition gets its name from the fact that the condition implies that $G(H, l)$ is an Abelian group (see Lemma 7.1). As all elements of this group have order 2, the group condition gives us some information about the order of such matrices, as the following lemma (which we prove later in section 7) shows.

LEMMA 2.1. *Let H be an $n \times n$ Hadamard matrix. If H satisfies* (GC)*, then $n = 2^k$ for some integer k.*

Note than in general, the number of rows and columns of a Hadamard matrix need not be a power of 2. For example, there are 12×12 Hadamard matrices.

The representability conditions. We describe Hadamard matrices H satisfying (GC) by $\mathbb{F}_2$-polynomials. By Lemma 2.1 these matrices have order $n = 2^k$. We extend our notion of "symmetric representation": Let $\rho^R : \mathbb{F}_2^k \to [n]$ and $\rho^C : \mathbb{F}_2^k \to [n]$ be index mappings (i.e., bijective mappings) and $X = (X_1, \ldots, X_k)$ and $Y = (Y_1, \ldots, Y_k)$. A polynomial $h(X, Y)$ over $\mathbb{F}_2$ *represents H with respect to ρ^R and ρ^C* if for all $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^k$ it holds that

$$h(\mathbf{x}, \mathbf{y}) = 1 \iff H_{\rho^R(\mathbf{x}), \rho^C(\mathbf{y})} = -1.$$

So a symmetric representation is just a representation with $\rho^R = \rho^C$. We say that the set Λ^R is *linear with respect to ρ^R* if there is a linear subvectorspace $L^R \subseteq \mathbb{F}_2^k$ such that $\rho^R(L^R) = \Lambda^R$. Note that, if Λ^R is linear, then $|\Lambda^R| = 2^l$ for some $l \leq k$. We may therefore define a *coordinatization of Λ^R (with respect to ρ^R)* as a linear map $\phi^R : \mathbb{F}_2^l \to \mathbb{F}_2^k$ such that $\phi^R(\mathbb{F}_2^l) = L^R$, that is, Λ^R is just the image of the

concatenated mapping $\rho^R \circ \phi^R$. We define the notion of linearity of Λ^C with respect to ρ^C and the coordinatization of Λ^C with respect to ρ^C similarly. For a permutation $\pi \in S_k$ we use the shorthand $X_\pi \cdot Y := \bigoplus_{i=1}^k X_{\pi(i)} \cdot Y_i$.

The following conditions stipulate the representability (R) of H by $\mathbb{F}_2$-polynomials, the linearity (L) of the sets Λ^R and Λ^C, and the appropriate degree restrictions on the associated polynomials (D).

(R) There are index mappings $\rho^R : \mathbb{F}_2^k \to [n]$ and $\rho^C : \mathbb{F}_2^k \to [n]$ and a permutation $\pi \in S_k$ such that (with respect to ρ^R and ρ^C) the matrix H is represented by a polynomial of the form

$$h(X,Y) = X_\pi \cdot Y \oplus g^R(X) \oplus g^C(Y). \tag{2.1}$$

Moreover, if Λ^R is nonempty, then $\rho^R(0) \in \Lambda^R$. Similarly, if Λ^C is nonempty, then $\rho^C(0) \in \Lambda^C$. Finally, if H is symmetric and $\Lambda^R = \Lambda^C$, then $g^R = g^C$ and $\rho^R = \rho^C$.

(L) Λ^R and Λ^C are linear with respect to ρ^R and ρ^C, respectively.

(D) Either Λ^R is empty or there is a coordinatization ϕ^R of Λ^R with respect to ρ^R such that the polynomial $g^R \circ \phi^R$ has degree at most 2. Similarly, either Λ^C is empty or there is a coordinatization ϕ^C of Λ^C with respect to ρ^C such that the polynomial $g^C \circ \phi^C$ has degree at most 2. Finally, if H is symmetric and $\Lambda^R = \Lambda^C$ is nonempty, then $\phi^R = \phi^C$.

Actually, it turns out that condition (D) is invariant under the choice of the coordinatizations ϕ^R, ϕ^C. However, the conditions are not invariant under the choice of the representation ρ^R, ρ^C, and this is a major source of technical problems.

Before we can apply the conditions (R), (L), and (D), we deal with one technical issue. Let H be an $n \times n$ Hadamard matrix, and let $\Lambda^R, \Lambda^C \subseteq [n]$ be subsets of indices. Let M, Λ be the bipartization of H, Λ^R, and Λ^C.

If H is symmetric and $\Lambda^R = \Lambda^C$, then we say that H is *positive* for Λ^R (and Λ^C) if there is an entry $H_{i,i} = +1$ such that $i \in \Lambda^R$ or $\Lambda^R = \emptyset$. In the remaining case (if H is not symmetric or $\Lambda^R \neq \Lambda^C$), we say that H is *positive* for Λ^R and Λ^C if there is an entry $H_{i,j} = +1$ such that

1. $i \in \Lambda^R$ or $\Lambda^R = \emptyset$, and
2. $j \in \Lambda^C$ or $\Lambda^C = \emptyset$.

Note that, if H is not positive for Λ^R and Λ^C, then $-H$ is positive for Λ^R and Λ^C. Since $Z_{M,I_m,I_{m;\Lambda}}(G) = (-1)^{|E(G)|} Z_{-M,I_m,I_{m;\Lambda}}(G)$, the problems $\mathrm{EVAL}(M, I_m, I_{m;\Lambda})$ and $\mathrm{EVAL}(-M, I_m, I_{m;\Lambda})$ have equivalent complexity, so we lose no generality by restricting our attention to the positive case, which is helpful for a technical reason.

We can now state the theorem which is proved in this section.

THEOREM 2.2. *Let H be an $n \times n$ Hadamard matrix, and let $\Lambda^R, \Lambda^C \subseteq [n]$ be subsets of indices. Let M, Λ be the bipartization of H, Λ^R, and Λ^C, and let $m = 2n$. If H is positive for Λ^R and Λ^C, then $\mathrm{EVAL}(M, I_m, I_{m;\Lambda})$ is polynomial-time computable if and only if H, Λ^R, and Λ^C satisfy the group condition* (GC) *and conditions* (R), (L), *and* (D). *Otherwise $\mathrm{EVAL}(M, I_m, I_{m;\Lambda})$ is #P-hard. If H is not positive for Λ^R and Λ^C, then $\mathrm{EVAL}(M, I_m, I_{m;\Lambda})$ is polynomial-time computable if and only if $-H$, Λ^R, and Λ^C satisfy the group condition* (GC) *and conditions* (R), (L), *and* (D). *Otherwise $\mathrm{EVAL}(M, I_m, I_{m;\Lambda})$ is #P-hard. There is a polynomial-time algorithm that takes input H, Λ^R, and Λ^C and decides whether $\mathrm{EVAL}(M, I_m, I_{m;\Lambda})$ is polynomial-time computable or #P-hard.*

The theorem is proved using a sequence of lemmas. Proof sketches of these lemmas will be given in this section, and full proofs will be given later in section 7.

LEMMA 2.3 (Group Condition Lemma). *Let H be an $n \times n$ Hadamard matrix and let $\Lambda^R, \Lambda^C \subseteq [n]$ be subsets of indices. Let M, Λ be the bipartization of H, Λ^R, and Λ^C, and let $m = 2n$. If H does not satisfy* (GC)*, then* EVAL$(M, I_m, I_{m;\Lambda})$ *is* #P*-hard. There is a polynomial-time algorithm that determines whether H satisfies* (GC)*.*

Proof sketch. For any integer p and a symmetric nonnegative matrix $C^{[p]}$, which depends upon H, the proof uses gadgetry to transform an input to EVAL$(C^{[p]})$ into an input to EVAL$(M, I_m, I_{m;\Lambda})$. The fact that H does not satisfy (GC) is used to show that, as long as p is sufficiently large with respect to M, then $C^{[p]}$ has a block of rank greater than one. By Theorem 1.3 (due to Bulatov and Grohe), EVAL$(C^{[p]})$ is #P-hard, so EVAL$(M, I_m, I_{m;\Lambda})$ is #P-hard.

LEMMA 2.4 (Polynomial Representation Lemma). *Let H be an $n \times n$ Hadamard matrix and $\Lambda^R, \Lambda^C \subseteq [n]$ subsets of indices. Suppose that H satisfies* (GC) *and that H is positive for Λ^R and Λ^C. Then the representability condition* (R) *is satisfied, and there is a polynomial-time algorithm that computes the representation.*

Proof sketch. The representation is constructed inductively. First, permutations are used to transform H into a normalized matrix $\hat{H}$, that is, a Hadamard matrix $\hat{H}$ whose first row and column consist entirely of +1s, which still satisfies (GC). We then show that there is a permutation of $\hat{H}$ which can be expressed as the tensor product of a simple Hadamard matrix (either H_2 or H_4) and a smaller normalized symmetric Hadamard matrix H'. By induction, we construct a representation for H' and use this to construct a representation for the normalized matrix $\hat{H}$ of the form $X_\pi \cdot Y$ for a permutation $\pi \in S_k$. We use this to construct a representation for H.

LEMMA 2.5 (Linearity Lemma). *Let H be an $n \times n$ Hadamard matrix and $\Lambda^R, \Lambda^C \subseteq [n]$ subsets of indices. Let M, Λ be the bipartization of H, Λ^R, and Λ^C, and let $m = 2n$. Suppose that* (GC) *and* (R) *are satisfied. Then the problem* EVAL$(M, I_m, I_{m;\Lambda})$ *is* #P*-hard unless the linearity condition* (L) *holds. There is a polynomial-time algorithm that determines whether* (L) *holds.*

Proof sketch. For a symmetric nonnegative matrix C, which depends upon H, the proof uses gadgetry to transform an input to EVAL$(C, I_m, I_{m;\Lambda})$ into an input of EVAL$(M, I_m, I_{m;\Lambda})$. By (R), there are bijective index mappings $\rho^R : \mathbb{F}_2^k \to [n]$ and $\rho^C : \mathbb{F}_2^k \to [n]$ and a permutation $\pi \in S_k$ such that (with respect to ρ^R and ρ^C) the matrix H is represented by a polynomial of the appropriate form, according to (2.1). Let τ^R be the inverse of ρ^R and τ^C be the inverse of ρ^C. Let $L^C = \tau^C(\Lambda^C)$ and $L^R = \tau^R(\Lambda^R)$. We show that either EVAL$(C, I_m, I_{m;\Lambda})$ is #P-hard or (L) is satisfied. In particular, the assumption that EVAL$(C, I_m, I_{m;\Lambda})$. is not #P-hard means that its blocks all have rank 1 by Theorem 1.3 (due to Bulatov and Grohe). We use this fact to show that L^R is a linear subspace of Λ^R and that L^C is a linear subspace of Λ^C. To show that L^R is a linear subspace of Λ^R, we use L^R to construct an appropriate linear subspace and compare Fourier coefficients to see that it is, in fact, L^R itself.

LEMMA 2.6 (Degree Lemma). *Let H be an $n \times n$ Hadamard matrix and $\Lambda^R, \Lambda^C \subseteq [n]$ subsets of indices. Let M, Λ be the bipartization of H, Λ^R, and Λ^C, and let $m = 2n$. Suppose that* (GC)*,* (R)*, and* (L) *are satisfied. Then* EVAL$(M, I_m, I_{m;\Lambda})$ *is* #P*-hard unless the degree condition* (D) *holds. There is a polynomial-time algorithm that determines whether* (D) *holds.*

Proof sketch. For any (even) integer p and a symmetric nonnegative matrix $C^{[p]}$, which depends upon H, the proof uses gadgetry to transform an input to EVAL$(C^{[p]})$ into an input to EVAL$(M, I_m, I_{m;\Lambda})$. Using the representation of H, a coordinatization ϕ^R with respect to Λ^R, and a coordinatization ϕ^C with respect to Λ^C, some of the entries $C^{[p]}_{a,b}$ of the matrix $C^{[p]}$ may be expressed as sums, over elements in

$\mathbb{F}_2^\ell$, for some ℓ, of appropriate powers of -1. We study properties of polynomials $g(X_1,\ldots,X_k) \in \mathbb{F}_2[X_1,\ldots,X_k]$, discovering that the number of roots of a certain polynomial $g_{\alpha,\beta,\gamma}(X_1,\ldots,X_k)$, which is derived from $g(X_1,\ldots,X_k)$, depends upon the degree of g. From this we can show that if (D) does not hold, then there is an even p such that EVAL($C^{[p]}$) is #P-hard.

Proof of Theorem 2.2. By the equivalence of the problems EVAL$(M, I_m, I_{m;\Lambda})$ and EVAL$(-M, I_m, I_{m;\Lambda})$ we can assume that H is positive for Λ^R and Λ^C. The hardness part follows directly from the lemmas above. We shall give the proof for the tractability part. Given H, Λ^R, and Λ^C satisfying (GC), (R), (L), and (D), we shall show how to compute $Z_{M,I_m,I_{m;\Lambda}}(G)$ for an input graph G in polynomial time.

Note first that $Z_{M,I_m,I_{m;\Lambda}}(G) = 0$ unless G is bipartite. If G has connected components $G_1,\ldots G_c$, then

$$Z_{M,I_m,I_{m;\Lambda}}(G) = \prod_{i=1}^{c} Z_{M,I_m,I_{m;\Lambda}}(G_i).$$

Therefore, it suffices to give the proof for connected bipartite graphs. Let $G = (V, E)$ be such a graph with vertex bipartition $U \dot\cup W = V$. Let $V_o \subseteq V$ be the set of odd-degree vertices in G and let $U_o = W \cap V_o$ and $W_o = W \cap V_o$ be the corresponding subsets of U and W. Let $U_e = U \setminus U_o$ and $W_e = W \setminus W_o$. We have

$$\begin{aligned} Z_{M,I_m,I_{m;\Lambda}}(G) &= \sum_{\xi:V\to[m]} \prod_{\{u,w\}\in E} M_{\xi(u),\xi(w)} \prod_{v\in V_o} (I_{m;\Lambda})_{\xi(v),\xi(v)} \\ &= \sum_{\substack{\xi:V\to[m]\\ \xi(V_o)\subseteq\Lambda}} \prod_{\{u,w\}\in E} M_{\xi(u),\xi(w)}. \end{aligned}$$

As G is bipartite and connected, this sum splits into $Z_{M,I_m,I_{m;\Lambda}}(G) = Z^{\rightarrow} + Z^{\leftarrow}$ for values

$$Z^{\rightarrow} = \sum_{\substack{\xi:U\to[n]\\ \xi(U_o)\subseteq\Lambda^R}} \sum_{\substack{\zeta:W\to[n]\\ \zeta(W_o)\subseteq\Lambda^C}} \prod_{\substack{\{u,w\}\in E\\ u\in U}} H_{\xi(u),\zeta(w)}$$

and

$$Z^{\leftarrow} = \sum_{\substack{\xi:U\to[n]\\ \xi(U_o)\subseteq\Lambda^C}} \sum_{\substack{\zeta:W\to[n]\\ \zeta(W_o)\subseteq\Lambda^R}} \prod_{\substack{\{u,w\}\in E\\ u\in U}} H_{\zeta(w),\xi(u)}.$$

We will show how to compute $Z^{\rightarrow}$. The computation of the value $Z^{\leftarrow}$ is similar.

Fix configurations $\xi : U \to [n]$ and $\zeta : W \to [n]$, and let ρ^R, ρ^C be the index mappings and h the $\mathbb{F}_2$-polynomial representing H, as given in condition (R). Let τ^R be the inverse of ρ^R, and let τ^C be the inverse of ρ^C. Let $L^R = \tau^R(\Lambda^R)$ and $L^C = \tau^C(\Lambda^C)$. Then ξ and ζ induce a configuration $\varsigma : V \to \mathbb{F}_2^k$ defined by

$$\varsigma(v) := \begin{cases} \tau^R(\xi(v)) & \text{if } v \in U, \\ \tau^C(\zeta(v)) & \text{if } v \in W, \end{cases}$$

which implies for all $u \in U$, $w \in W$ that $h(\varsigma(u), \varsigma(w)) = 1$ if and only if $H_{\xi(u),\zeta(w)} = -1$. Let ϕ^R and ϕ^C be coordinatizations of Λ^R and Λ^C with respect to ρ^R and ρ^C

satisfying (L) and (D). We can simplify

$$\begin{aligned} Z^{\rightarrow} &= \sum_{\substack{\xi:U\to[n]\\ \xi(U_o)\subseteq\Lambda^R}} \sum_{\substack{\varsigma:W\to[n]\\ \varsigma(W_o)\subseteq\Lambda^C}} \prod_{\substack{\{u,w\}\in E\\ u\in U}} (-1)^{h(\tau^R(\xi(u)),\tau^C(\varsigma(w)))} \\ &= \sum_{\substack{\varsigma:V\to\mathbb{F}_2^k\\ \varsigma(U_o)\subseteq L^R\\ \varsigma(W_o)\subseteq L^C}} (-1)^{\bigoplus_{\{u,w\}\in E:u\in U} h(\varsigma(u),\varsigma(w))}. \end{aligned}$$

Define, for $a \in \mathbb{F}_2$, sets

$$s_a := \left| \left\{ \varsigma : V \to \mathbb{F}_2^k \mid \varsigma(U_o) \subseteq L^R,\ \varsigma(W_o) \subseteq L^C,\ \bigoplus_{\substack{\{u,w\}\in E\\ u\in U}} h(\varsigma(u),\varsigma(w)) = a \right\} \right|. \tag{2.2}$$

Then $Z^{\rightarrow} = s_0 - s_1$. Therefore, it remains to show how to compute the values s_a. Define, for each $v \in V$, a tuple $X^v = (X_1^v, \ldots, X_k^v)$ and let h_G be the $\mathbb{F}_2$-polynomial

$$h_G := \bigoplus_{\substack{\{u,w\}\in E\\ u\in U}} h(X^u, X^w) = \bigoplus_{\substack{\{u,w\}\in E\\ u\in U}} (X^u)_\pi \cdot X^w \oplus \bigoplus_{u\in U_o} g^R(X^u) \oplus \bigoplus_{w\in W_o} g^C(X^w). \tag{2.3}$$

Here the second equality follows from the definition of the polynomial h given in condition (R) and the fact that the terms $g^R(X^u)$ and $g^C(X^w)$ in the definition of h appear exactly $\deg(u)$ and $\deg(w)$ many times in h_G. Therefore, these terms cancel for all even degree vertices.

Let $\mathrm{var}(h_G)$ denote the set of variables in h_G, and for mappings $\chi : \mathrm{var}(h_G) \to \mathbb{F}_2$ we use the expression $\chi(X^v) := (\chi(X_1^v), \ldots, \chi(X_k^v))$ as shorthand and define the $\mathbb{F}_2$-sum $h_G(\chi) := \bigoplus_{\{u,w\}\in E:u\in U} h(\chi(X^u), \chi(X^w))$. We find that s_a can be expressed by

$$s_a = \left| \left\{ \chi : \mathrm{var}(h_G) \to \mathbb{F}_2 \mid \begin{array}{ll} \chi(X^u) \in L^R & \text{for all } u \in U_o, \\ \chi(X^w) \in L^C & \text{for all } w \in W_o, \end{array} \ h(\chi) = a) \right\} \right|. \tag{2.4}$$

By (2.4) we are interested only in those assignments χ of the variables of h_G which satisfy $\chi(X^u) \in L^R$ and $\chi(X^w) \in L^C$ for all $u \in U_o$ and $w \in W_o$. With $|\Lambda^R| = 2^{\ell^R}$ and $|\Lambda^C| = 2^{\ell^C}$ for some appropriate ℓ^R, ℓ^C, we introduce variable vectors $Y^u = (Y_1^u, \ldots, Y_{\ell^R}^u)$ and $Z^w = (Z_1^w, \ldots, Z_{\ell^C}^w)$ for all $u \in U_o$ and $w \in W_o$. If $u \in U_o$ or $w \in W_o$, then we can express the term $(X^u)_\pi \cdot X^w$ in h_G in terms of these new variables. In particular, recall that ϕ^R and ϕ^C are coordinatizations of Λ^R and Λ^C with respect to ρ^R and ρ^C satisfying (L) and (D). Let

$$\begin{aligned} h''_G = &\bigoplus_{\substack{\{u,w\}\in E\\ u\in U_o, w\in W_o}} (\phi^R(Y^u))_\pi \cdot \phi^C(Z^w) \oplus \bigoplus_{\substack{\{u,w\}\in E\\ u\in U_e, w\in W_e}} (X^u)_\pi \cdot X^w \\ &\oplus \bigoplus_{\substack{\{u,w\}\in E\\ u\in U_e, w\in W_o}} (X^u)_\pi \cdot \phi^C(Z^w) \oplus \bigoplus_{\substack{\{u,w\}\in E\\ u\in U_o, w\in W_e}} (\phi^R(Y^u))_\pi \cdot X^w. \end{aligned}$$

Let

$$h'_G = h''_G \oplus \bigoplus_{u\in U_o} g^R(\phi^R(Y^u)) \oplus \bigoplus_{w\in W_o} g^C(\phi^C(Z^w)). \tag{2.5}$$

We therefore have

$$s_a = |\{\chi : \mathrm{var}(h'_G) \to \mathbb{F}_2 \mid h'_G(\chi) = a)\}| \,. \tag{2.6}$$

By condition (D), the polynomials $g^R \circ \phi^R$ and $g^C \circ \phi^C$ are of degree at most 2, and therefore h'_G is a polynomial of degree at most 2. Furthermore, we have expressed s_a as the number of solutions to a polynomial equation over $\mathbb{F}_2$. Therefore, the proof now follows by the following well-known fact.

FACT 2.7. *The number of solutions to polynomial equations of degree at most* 2 *over* $\mathbb{F}_2$ *can be computed in polynomial time.*

This is a direct consequence of Theorems 6.30 and 6.32 in [18] (see also [11]). ∎

3. The general case. In this section we will prove Theorem 1.1. Before we can give the proof some further results have to be derived, which will then enable us to extend Theorems 1.2 and 2.2. It will be convenient to focus on connected components. This is expressed by the following lemma, which will be proved later in section 8.

LEMMA 3.1. *Let A be a symmetric real-valued matrix with components $A_1, \ldots, A_c$. Then the following hold:*

1. *If* EVAL(A_i) *is* #P*-hard for some $i \in [c]$, then* EVAL(A) *is* #P*-hard.*
2. *If* EVAL(A_i) *is* PTIME *computable for all $i \in [c]$, then* EVAL(A) *is* PTIME *computable.*

Recall that for each connected symmetric matrix A there is a block B such that either $A = B$ or, up to permutation of the rows and columns, $A = \left(\begin{smallmatrix} 0 & B \\ B^T & 0 \end{smallmatrix}\right)$. We call B the block *underlying* A. For such connected A we furthermore see that either the evaluation problem is #P-hard or we can reduce it to the evaluation problem on bipartizations of Hadamard matrices. This is expressed in the following lemma, which will be proved later in section 8.

LEMMA 3.2. *Suppose that A is a symmetric connected matrix. Then either* EVAL(A) *is* #P*-hard or the following hold.*

1. *If A is not bipartite, then there is a symmetric $r \times r$ Hadamard matrix H and a set $\Lambda^R \subseteq [r]$ such that*
$$\mathrm{EVAL}(A) \equiv \mathrm{EVAL}(H, I_r, I_{r;\Lambda^R}).$$
2. *If A is bipartite, then there is an $r \times r$ Hadamard matrix H, sets $\Lambda^R, \Lambda^C \subseteq [r]$, and a bipartization M, Λ of H, Λ^R, and Λ^C such that*
$$\mathrm{EVAL}(A) \equiv \mathrm{EVAL}(M, I_{2r}, I_{2r;\Lambda}).$$

Furthermore, it can be decided in time polynomial in the size of A which of the three alternatives (#P*-hardness,* (1)*, or* (2)*) holds.*

We are now able to prove the main theorem.

Proof of Theorem 1.1. Given a symmetric matrix $A \in \mathbb{R}_{\mathbb{A}}^{m \times m}$, by Lemma 3.1 we may assume that the matrix A is connected. By Lemma 3.2, Theorem 2.2, and Corollary 7.14 the problem EVAL(A) is either polynomial-time computable or #P-hard. The existence of a polynomial time algorithm for deciding which of the two possibilities holds, given a matrix A, follows directly by these results. ∎

4. Outline of the paper. The rest of the paper is organized as follows. Section 5 describes some generalizations of the partition function evaluation problem, including related work and open problems. The remaining sections contain the proofs of the lemmas which have been stated without proof. In particular, section 6 develops some technical tools which we will use. Section 7 proves the lemmas that are stated in section 2. Finally, section 8 proves the lemmas that are stated in section 3.

5. Related work. There are several natural directions in which the work in this paper could be extended. First, the matrix A could be extended to include algebraic *complex* numbers and not merely algebraic real numbers. This extension has been carried out, subsequent to this paper, in an impressive 111-page paper by Cai, Chen, and Lu [7]. The work could also be extended by allowing the matrix A to be *asymmetric*. A recent breakthrough by Bulatov [4] establishes the existence of a dichotomy theorem for counting satisfying assignments in constraint satisfaction. This implies that a dichotomy exists for the case in which A is a 0-1 matrix (which is not necessarily symmetric)—in this case computing the partition function corresponds to counting homomorphisms to a directed graph, in particular to the directed graph with adjacency matrix A. Bulatov's dichotomy is not known to be *effective* in the sense that it is not known to be decidable given a matrix A whether it is tractable or not. An effective dichotomy was given by Dyer, Goldberg, and Paterson [10] for the special case in which the directed graph with adjacency matrix A is *acyclic* but no effective dichotomy is currently known for the case of general 0-1 matrices A. A generalization of Bulatov and Grohe's dichotomy for symmetric nonnegative matrices to symmetric nonnegative functions of *arbitrary arity* was given recently by Dyer, Goldberg, and Jerrum [9]. However, nothing is known about how to handle functions of larger arity in the presence of mixed signs.

6. Technical tools.

6.1. Stretchings and thickenings. We introduce some fundamental relations which will be used in most of our reductions. Let $G = (V, E)$ be a graph. The *s-stretch* of G is the graph S_sG obtained from G by replacing each edge by a path on s edges. The *t-thickening* of G is the graph T_tG obtained from G by replacing each edge by t parallel edges. Let $A^{(t)}$ denote the matrix obtained from A by taking each of its entries to the power of t.

LEMMA 6.1 (see [8]). *For a symmetric matrix $A \in \mathbb{R}_{\mathbb{A}}^{m\times m}$ and a diagonal $m \times m$ matrix D we have, for all $s, t \in \mathbb{N}$,*

$$\mathrm{EVAL}(A(DA)^{s-1}, D) \le \mathrm{EVAL}(A, D) \quad \textit{and} \quad \mathrm{EVAL}(A^{(t)}, D) \le \mathrm{EVAL}(A, D).$$

These reducibilities hold as

$$Z_{A(DA)^{s-1},D}(G) = Z_{A,D}(S_sG) \quad \textit{and} \quad Z_{A^{(t)},D}(G) = Z_{A,D}(T_tG).$$

6.1.1. Twin reduction. We need some extensions of Lemma 3.5 in [8]. For a symmetric $m \times m$ matrix A we say that two rows $A_{i,*}$ and $A_{j,*}$ are *twins* if and only if $A_{i,*} = A_{j,*}$. This induces an equivalence relation on the rows (and by symmetry on the columns) of A. Let $I_1, \ldots, I_n$ be a partition of the row indices of A according to this relation. The *twin-resolvent* of A is the matrix defined, for all $i, j \in [n]$, by

$$\mathcal{T}(A)_{i,j} := A_{\mu,\nu} \text{ for some } \mu \in I_i, \nu \in I_j.$$

The definition of the classes I_i implies that $A_{\mu,\nu} = A_{\mu',\nu'}$ for all $\mu, \mu' \in I_i$, and $\nu, \nu' \in I_j$ and therefore the matrix $\mathcal{T}(A)$ is well defined.

The above definition furthermore gives rise to a mapping $\tau : [m] \to [n]$ defined by $\mu \in I_{\tau(\mu)}$; that is, τ maps $\mu \in [m]$ to the class I_j it is contained in. Therefore, we have $\mathcal{T}(A)_{\tau(i),\tau(j)} = A_{i,j}$ for all $i, j \in [m]$. We call τ the *twin-resolution mapping* of A.

LEMMA 6.2 (Twin Reduction Lemma). *Let A be a symmetric $m \times m$ matrix and D a diagonal $m \times m$ matrix of vertex weights. Let $I_1, \dots, I_n$ be a partition of the row indices of A according to the twin-relation. Then*

$$Z_{A,D}(G) = Z_{\mathcal{T}(A),\Delta}(G) \text{ for all graphs } G,$$

where Δ is a diagonal $n \times n$ matrix defined by $\Delta_{i,i} = \sum_{\nu \in I_i} D_{\nu,\nu}$ for all $i \in [n]$.

Proof. Let τ be the twin-resolution mapping of A. Then

$$\begin{aligned} Z_{A,D}(G) &= \sum_{\xi: V \to [m]} \prod_{\{u,v\} \in E} A_{\xi(u),\xi(v)} \prod_{v \in V} D_{\xi(v),\xi(v)} \\ &= \sum_{\xi: V \to [m]} \prod_{\{u,v\} \in E} \mathcal{T}(A)_{\tau\circ\xi(u),\tau\circ\xi(v)} \prod_{v \in V} D_{\xi(v),\xi(v)}, \end{aligned}$$

where the second equality follows from the definition of τ. As for all $\xi : V \to [m]$ we have $\tau \circ \xi : V \to [n]$, we can partition the ξ into classes according to their images under concatenation with τ, and we obtain

$$\begin{aligned} Z_{A,D}(G) &= \sum_{\psi: V \to [n]} \sum_{\substack{\xi: V \to [m] \\ \tau\circ\xi = \psi}} \prod_{\{u,v\} \in E} \mathcal{T}(A)_{\psi(u),\psi(v)} \prod_{v \in V} D_{\xi(v),\xi(v)} \\ &= \sum_{\psi: V \to [n]} \prod_{\{u,v\} \in E} \mathcal{T}(A)_{\psi(u),\psi(v)} \left(\sum_{\substack{\xi: V \to [m] \\ \tau\circ\xi = \psi}} \prod_{v \in V} D_{\xi(v),\xi(v)} \right). \end{aligned}$$

Fix some $\psi : V \to [n]$. For $\xi : V \to [m]$ we have $\tau \circ \xi = \psi$ if and only if $\psi^{-1}(\{i\}) = \xi^{-1}(I_i)$ for all $i \in [n]$. Define $V_i := \psi^{-1}(\{i\})$ for all $i \in [n]$ which yields a partition of V. Thus

$$\begin{aligned} \sum_{\substack{\xi: V \to [m] \\ \tau\circ\xi = \psi}} \prod_{v \in V} D_{\xi(v),\xi(v)} &= \sum_{\substack{\xi: V \to [m] \\ \forall\, i \in [n]:\, \xi(V_i) \subseteq I_i}} \prod_{v \in V} D_{\xi(v),\xi(v)} \\ &= \prod_{i=1}^{n} \sum_{\xi_i: V_i \to I_i} \prod_{v \in V_i} D_{\xi(v),\xi(v)} \\ &= \prod_{i=1}^{n} \prod_{v \in V_i} \sum_{\nu \in I_i} D_{\nu,\nu} \\ &= \prod_{v \in V} \Delta_{\psi(v),\psi(v)}. \end{aligned}$$

Hence

$$Z_{A,D}(G) = \sum_{\psi: V \to [n]} \prod_{\{u,v\} \in E} \mathcal{T}(A)_{\psi(u),\psi(v)} \prod_{v \in V} \Delta_{\psi(v),\psi(v)} = Z_{\mathcal{T}(A),\Delta}(G). \qquad \square$$

6.2. Basic tractability and #P-hardness. The following lemma is a straightforward extension of Theorem 6 in [6].

LEMMA 6.3. *Let $A \in \mathbb{R}_{\mathbb{A}}^{m \times m}$ be a symmetric matrix and D a diagonal $m \times m$ matrix. If each component of A either has row rank 1 or is bipartite and has rank 2, then* EVAL(A, D) *is polynomial-time computable.*

Proof. Let $G = (V, E)$ be a given graph with components $G_1, \ldots, G_c$ and let $A_1, \ldots, A_l$ be the components of A and $D_1, \ldots, D_l$ the submatrices of D corresponding to these components. Then

$$Z_{A,D}(G) = \prod_{i=1}^{c} \sum_{j=1}^{l} Z_{A_j,D_j}(G_i).$$

Therefore the proof follows straightforwardly from the special case of connected G and A. Assume therefore that both G and A are connected.

We will prove the following claim, which holds for directed graphs.

Claim 1. *Let $B^{m\times m}$ be a (not necessarily symmetric) matrix of row rank 1 and D' a diagonal matrix. Then for every directed graph G the value*

$$Z^*_{B,D'}(G) = \sum_{\xi:V\to[m]} \prod_{(u,v)\in E} B_{\xi(u),\xi(v)} \prod_{v\in V} D'_{\xi(v),\xi(v)}$$

can be computed in polynomial time.

Proof. Let $G = (V, E)$ be a directed graph and for every vertex $v \in V$ denote by $\mathrm{outdeg}(v)$ and $\mathrm{indeg}(v)$ the number of outgoing and incoming edges incident with v. There are vectors $a, b \in \mathbb{R}^m_{\mathbb{A}}$ such that $B = ab^T$. Then, for every configuration $\xi : V \to [m]$,

$$\prod_{(u,v)\in E} B_{\xi(u),\xi(v)} = \prod_{(u,v)\in E} a_{\xi(u)} b_{\xi(v)} = \prod_{v\in V} a^{\mathrm{outdeg}(v)}_{\xi(v)} b^{\mathrm{indeg}(v)}_{\xi(v)},$$

and therefore

$$\begin{aligned} Z^*_{B,D'}(G) &= \sum_{\xi:V\to[m]} \prod_{(u,v)\in E} B_{\xi(u),\xi(v)} \prod_{v\in V} D'_{\xi(v),\xi(v)} \\ &= \sum_{\xi:V\to[m]} \prod_{v\in V} a^{\mathrm{outdeg}(v)}_{\xi(v)} b^{\mathrm{indeg}(v)}_{\xi(v)} D'_{\xi(v),\xi(v)} \\ &= \prod_{v\in V} \sum_{i=1}^{m} a^{\mathrm{outdeg}(v)}_{i} b^{\mathrm{indeg}(v)}_{i} D'_{i,i}. \end{aligned}$$

The terms in the last line can be evaluated in polynomial time. This completes the proof of the claim.

With this claim we are now able to prove the lemma. Recall that A is connected and symmetric. If A is nonbipartite, then A has rank 1. For a given connected graph G let G' be a directed graph obtained from G by orienting its edges arbitrarily. We have $Z_{A,D}(G) = Z^*_{A,D}(G')$, and the value $Z^*_{A,D}(G')$ can be computed by Claim 1.

Otherwise, if A is bipartite, then we have (up to permutation of the rows/columns of A)

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

for a block B of rank 1. Let A' be the matrix

$$A' = \begin{pmatrix} 0 & B \\ 0 & 0 \end{pmatrix}$$

which has rank 1 because B has rank 1. Note, furthermore, that $Z_{A,D}(G) = 0$ unless G is bipartite. Assume therefore that $G = (U, W, E)$ is a bipartite graph and let the graphs G_{UW}, G_{WU} be obtained from G by directing all edges from U to W (W to U, resp.). Then

$$Z_{A,D}(G) = Z_{A',D}(G_{UW}) + Z_{A',D}(G_{WU}),$$

and the terms of the right-hand side are polynomial-time computable by Claim 1. ∎

The following #P-hardness result will be the basis of all our proofs of intractability.

LEMMA 6.4. *Given a symmetric matrix A of order n and diagonal $n \times n$ matrices D, O such that D is a nonsingular matrix of nonnegative integers, if* $\mathrm{abs}(A)$ *contains a block of row rank at least* 2*, then* $\mathrm{EVAL}(A, D, O)$ *is #P-hard.*

Proof. Observe that by 2-thickening we have $\mathrm{EVAL}(A^{(2)}, D) \leq \mathrm{EVAL}(A, D, O)$. We can form a matrix A' from $A^{(2)}$ by *introducing twins according to* D, that is, doing the inverse operation of Lemma 6.2. More precisely, let $n_i := D_{i,i}$ for all $i \in [n]$ and define $m := \sum_{i=1}^{n} n_i$. To define the $m \times m$ matrix A' we consider its row and column indices as pairs and define

$$A'_{(\kappa,i),(\lambda,j)} := A^{(2)}_{\kappa,\lambda} \text{ for all } \kappa, \lambda \in [n],\ i \in n_\kappa,\ j \in n_\lambda. \tag{6.1}$$

By the definition of A' we see that application of the Twin Reduction Lemma, Lemma 6.2, to A' yields

$$Z_{A'}(G) = Z_{A^{(2)},D}(G) \text{ for every graph } G,$$

and thus $\mathrm{EVAL}(A') \equiv \mathrm{EVAL}(A^{(2)}, D)$. By (6.1) the matrix A' contains a block of row rank at least 2 if and only if $A^{(2)}$ does, which in turn is the case if and only if $\mathrm{abs}(A)$ contains such a block. The proof now follows from Theorem 1.3 (due to Bulatov and Grohe). ∎

6.3. Interpolation lemma. In the next chapters we will make extensive use of the following lemma, which is an analogue of the interpolation technique used, for example, in [8].

LEMMA 6.5. *Let $x_1, \ldots, x_n \in \mathbb{R}_{>0}$ be pairwise distinct and let $\mathcal{P}$ and $\mathcal{N}$ be two finite multisets of real numbers with $|\mathcal{P}| = |\mathcal{N}| = n$. Then the following are equivalent:*

(1) $\mathcal{P} = \mathcal{N}$.

(2) *There is an ordering of the elements in $\mathcal{P}$ and $\mathcal{N}$ such that, for some infinite increasing sequence $\{p\}$, we have*

$$\sum_{a_i \in \mathcal{P}} x_i^p a_i = \sum_{b_i \in \mathcal{N}} x_i^p b_i.$$

Proof. The forward direction is trivial. Hence, assume that (2) holds but not (1). With the given ordering of $\mathcal{P}$ and $\mathcal{N}$ we have $\mathcal{P} = \{a_1, \ldots, a_n\}$ and $\mathcal{N} = \{b_1, \ldots, b_n\}$. We may assume that there is no $i \in [n]$ such that $a_i = b_i$ because, otherwise, we might delete this pair from $\mathcal{P}$ and $\mathcal{N}$. Hence, let $k \in [n]$ be such that $x_k = \max_{i \in [n]} x_i$. Assume without loss of generality that $a_k > b_k$; then, for a constant $c \neq 0$ and for every p in the sequence,

$$\begin{aligned} 0 = \sum_{a_i \in \mathcal{P}} x_i^p a_i - \sum_{b_i \in \mathcal{N}} x_i^p b_i &= x_k^p (a_k - b_k) + \sum_{i \in [n] \setminus \{k\}} x_i^p (a_i - b_i) \\ \iff 0 = c + \sum_{i \in [n] \setminus \{k\}} &\left(\frac{x_i}{x_k}\right)^p (a_i - b_i). \end{aligned}$$

By $\lim_{p\to\infty} \sum_{i\in[n]\setminus\{k\}} (\frac{x_i}{x_k})^p (a_i - b_i) = 0$, this yields a contradiction. ∎

LEMMA 6.6. *Let $x_1, \ldots, x_n \in \mathbb{R}_{>0}$ be pairwise distinct and let $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{R}^n$ and $\mathbf{b} = (b_1, \ldots, b_n) \in \mathbb{R}^n$. If $\mathbf{a} \neq \mathbf{b}$, then there is a $p_0 \in \mathbb{N}$ such that the equation*

$$\sum_{i=1}^{n} x_i^p a_i = \sum_{i=1}^{n} x_i^p b_i$$

does not hold for any $p \geq p_0$.

Proof. We will prove the following. For each $I \subseteq [n]$ there is a $p_I \in \mathbb{N}$ such that for all $p \geq p_I$, if

$$\sum_{i\in I} x_i^p (a_i - b_i) = 0, \tag{6.2}$$

then $a_i = b_i$ for all $i \in I$. We will give the proof by induction on the cardinality of I. For empty I there is nothing to be shown. Assume therefore that $I \neq \emptyset$, let $k \in I$ be such that $x_k = \max_{i\in I} x_i$, and define $I' = I \setminus \{k\}$.

CLAIM 2. *There is a $p_k \in \mathbb{N}$ such that for all $p \geq p_k$, if (6.2) is satisfied, then $a_k = b_k$.*

Proof. Assume for contradiction that $a_k \neq b_k$ but (6.2) holds for all $p \in \mathbb{N}$. This implies

$$0 = (a_k - b_k) + \sum_{i\in I'} \left(\frac{x_i}{x_k}\right)^p (a_i - b_i). \tag{6.3}$$

As $i \in I'$ with $a_i = b_i$ do not contribute to the above sum, we may further assume that $a_i \neq b_i$ for all $i \in I'$. If $I' = \emptyset$, we already have a contradiction. If otherwise $I' \neq \emptyset$, let k' be such that $x_{k'} = \max_{i\in I'} x_i$. We find that

$$\left| \sum_{i\in I'} \left(\frac{x_i}{x_k}\right)^p (a_i - b_i) \right| \leq \left(\frac{x_{k'}}{x_k}\right)^p \sum_{i\in I'} |a_i - b_i|.$$

In particular, (6.3) does not hold if $(\frac{x_{k'}}{x_k})^p \sum_{i\in I'} |a_i - b_i| < |a_k - b_k|$, which, as $x_k > x_{k'}$, is the case for all

$$p > \frac{\log|a_k - b_k| - \log\sum_{i\in I'} |a_i - b_i|}{(\log x_{k'} - \log x_k)},$$

in contradiction to our assumption.

By the induction hypothesis there is a $p_{I'}$ such that for all $p \geq p_{I'}$,

$$\sum_{i\in I'} x_i^p (a_i - b_i) = 0$$

implies $a_i = b_i$ for all $i \in I'$. Let p_k be defined as in Claim 2. Then the proof follows with $p_I = \max\{p_k, p_{I'}\}$. ∎

7. The proofs for section 2.

7.1. Notation and preliminaries. For $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n) \in \mathbb{R}^n$, by $\langle x, y \rangle$ we denote the inner product $\sum_{i=1}^n x_i y_i$ of x and y. It may be a source of confusion that we work over two different fields, $\mathbb{R}$ and $\mathbb{F}_2$. Addition in $\mathbb{F}_2$ is denoted by $\oplus$, and for $\alpha = (\alpha_1, \ldots, \alpha_n)$, $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{F}_2^k$, $\alpha \cdot \beta$ is the dot product $\bigoplus_{i=1}^k \alpha_i \beta_i$. Similarly, for $\pi \in S_k$, $\alpha_\pi \cdot \beta$ denotes $\bigoplus_{i=1}^k \alpha_{\pi(i)} \beta_i$. $\alpha \oplus \beta$ denotes the element $(\alpha_1 \oplus \beta_1, \ldots, \alpha_k \oplus \beta_k)$ in $\mathbb{F}_2^k$. Also, for $\pi \in S_k$, $\alpha_\pi \oplus \beta$ denotes the element $(\alpha_{\pi(1)} \oplus \beta_1, \ldots, \alpha_{\pi(k)} \oplus \beta_k)$. Similar notation applies to variables, so if $X = (X_1, \ldots, X_k)$ and $Y = (Y_1, \ldots, Y_k)$, then $X_\pi \cdot Y$ denotes $\bigoplus_{i=1}^k X_{\pi(i)} Y_i$. For $I \subseteq [k]$, let $X \setminus I$ be the tuple containing, in order, all variables in $\{X_1, \ldots, X_k\}$ other than those with indices in I. For example, $X \setminus \{2, 3\}$ denotes the tuple $(X_1, X_4, \ldots, X_k)$.

7.2. The group condition.

LEMMA 7.1. *Let H be an $n \times n$ Hadamard matrix. If H satisfies* (GC)*, then $G(H, 1)$ forms an Abelian group under the Hadamard product.*

Proof. Commutativity and associativity follow from the definition of the Hadamard product. To show closure, we consider two elements in $G(H, 1)$ and show that their Hadamard product is also in $G(H, 1)$. First, consider $H_{i,*} \circ H_{1,*}$ and $H_{j,*} \circ H_{1,*}$. Their Hadamard product is $H_{i,*} \circ H_{1,*} \circ H_{j,*} \circ H_{1,*} = H_{i,*} \circ H_{j,*}$, which is in $G(H, j)$ by the definition of $G(H, j)$ and therefore in $G(H, 1)$ by (GC). Similarly, we find that the product of $-H_{i,*} \circ H_{1,*}$ and $H_{j,*} \circ H_{1,*}$ is in $G(H, 1)$ and also the product of $-H_{i,*} \circ H_{1,*}$ and $-H_{j,*} \circ H_{1,*}$ is in $G(H, 1)$. From closure, it follows that the product of $H_{1,*} \circ H_{1,*}$ and itself is in $G(H, 1)$ and this row (the all ones row) is the identity element in the group. ∎

Proof of Lemma 2.1. By Lemma 7.1, $G(H, 1)$ forms an Abelian group under the Hadamard product. All elements of this group have order 2, and thus it follows from elementary algebra that the order of the group is a power of 2. Furthermore, the nonsingularity of H implies that for all $i \neq j$ the elements $H_{i,*} \circ H_{1,*}$, $-H_{i,*} \circ H_{1,*}$, $H_{j,*} \circ H_{1,*}$, and $-H_{j,*} \circ H_{1,*}$ are all distinct. Hence we have that $|G(H, 1)|$ equals twice the number of rows of H. ∎

Proof of Lemma 2.3*, the Group Condition Lemma.* It is clear from the definition of the group condition that there is a polynomial time algorithm that determines whether H satisfies (GC). We focus on the #P-hardness result. Let EVALeven(A) denote the problem of computing $Z_A(G)$ for an input graph G in which every vertex of G has even degree.

Let H, n, M, Λ, and m be defined as in the statement of the lemma. Let p be an even number. We will show how to transform any graph G into a graph G_p with all even-degree vertices so that $Z_{C^{[p]}}(G) = Z_M(G_p)$ for a matrix $C^{[p]}$ which we will define below. The definition of $C^{[p]}$ depends upon M but not upon G. Thus, we will have $\mathrm{EVAL}(C^{[p]}) \leq \mathrm{EVALeven}(M) \leq \mathrm{EVAL}(M, I_m, I_{m;\Lambda})$.

To finish the proof, we will show that, as long as p is sufficiently large with respect to M (and H does not satisfy (GC)), then $\mathrm{EVAL}(C^{[p]})$ is #P-hard.

We start by giving the transformation from $G = (V, E)$ into $G_p = (V_p, E_p)$:

$$
\begin{aligned}
V_p &:= V \cup \{v_e, v_{e^\alpha}, v_{e,1} \ldots, v_{e,p} \mid e \in E\}, \\
E_p &:= \quad \{\{u, v_{e,1}\}, \ldots, \{u, v_{e,p}\} \mid e = \{u, v\} \in E\} \\
&\quad \cup \{\{v, v_{e,1}\}, \ldots, \{v, v_{e,p}\} \mid e = \{u, v\} \in E\} \\
&\quad \cup \{\{v_{e,1}, v_e\}, \ldots, \{v_{e,p}, v_e\} \mid e \in E\} \\
&\quad \cup \{\{v_{e,1}, v_{e^\alpha}\}, \ldots, \{v_{e,p}, v_{e^\alpha}\} \mid e \in E\}.
\end{aligned}
$$

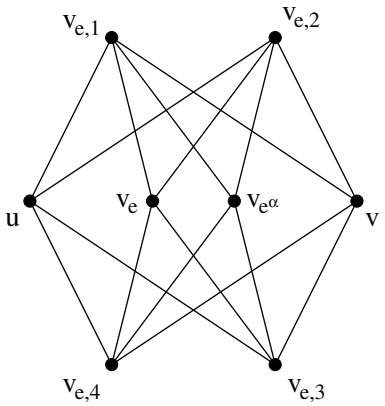

FIG. 7.1. *The gadget for* $p = 4$.

Essentially, every edge $e = \{u, v\}$ in G is replaced by a distinct gadget. Figure 7.1 illustrates this gadget for $p = 4$. Since p is even, it is clear that all vertices of G_p have even degree.

Let us now construct the matrix $C^{[p]}$. Let Γ denote the graph with vertices u and v and a single edge between them. Clearly, to satisfy $Z_{C^{[p]}}(\Gamma) = Z_M(\Gamma_p)$, $C^{[p]}_{i,j}$ should be equal to the contribution to $Z_M(\Gamma_p)$ corresponding to those configurations ξ with $\xi(u) = i$ and $\xi(v) = j$. Thus,

$$C^{[p]}_{i,j} = \sum_{a=1}^{m} \sum_{b=1}^{m} \left(\sum_{c=1}^{m} M_{i,c} M_{j,c} M_{a,c} M_{b,c} \right)^p, \tag{7.1}$$

where a denotes the choice of spin for v_e, b denotes the choice of spin for v_{e^α}, and c denotes the choice of spin for a vertex $v_{e,\ell}$. Then $Z_{C^{[p]}}(\Gamma) = Z_M(\Gamma_p)$ and also $Z_{C^{[p]}}(G) = Z_M(G_p)$ for any graph G because the contribution for any edge Γ of G is exactly captured by the gadget Γ_p in G_p.

To finish the proof we must show that, as long as p is sufficiently large with respect to M, then EVAL($C^{[p]}$) is #P-hard. From the definition of M, we see that, for $i \in [n]$, $j \in \{n+1, \ldots, 2n\}$, we have $C^{[p]}_{i,j} = C^{[p]}_{j,i} = 0$. Also, for all $i, j \in [n]$, we have the following:

$$C^{[p]}_{i,j} = \sum_{a=1}^{n} \sum_{b=1}^{n} \langle H_{i,*} \circ H_{j,*}, H_{a,*} \circ H_{b,*} \rangle^p \text{ and}$$

$$C^{[p]}_{n+i,n+j} = \sum_{a=1}^{n} \sum_{b=1}^{n} \langle H_{*,i} \circ H_{*,j}, H_{*,a} \circ H_{*,b} \rangle^p.$$

Now, for all $i, j \in [n]$ and $x \in \{0, \ldots, n\}$ let $s^{[x]}_{i,j}$ be the number of pairs (a, b) such that $|\langle H_{i,*} \circ H_{j,*}, H_{a,*} \circ H_{b,*} \rangle| = x$, and similarly let $s^{[x]}_{n+i,n+j}$ be the number of pairs (a, b) such that $|\langle H_{*,i} \circ H_{*,j}, H_{*,a} \circ H_{*,b} \rangle| = x$. Then for all $i, j \in [n]$ we have

$$C^{[p]}_{i,j} = \sum_{x=0}^{n} s^{[x]}_{i,j} x^p \text{ and } C^{[p]}_{n+i,n+j} = \sum_{x=0}^{n} s^{[x]}_{n+i,n+j} x^p, \tag{7.2}$$

because p is even.

The pair $(a,b)=(i,j)$ contributes 1 toward $s^{[n]}_{i,j}$ and 1 toward $s^{[n]}_{n+i,n+j}$, so, for all $i,j\in[n]$, we have $C^{[p]}_{i,j}>0$ and $C^{[p]}_{n+i,n+j}>0$ (remember that p is even).

Since H is Hadamard, $s^{[n]}_{i,i}=n$ for every $i\in[n]$ and, for every $x\in\{1,\ldots,n-1\}$, $s^{[x]}_{i,i}=0$, so $C^{[p]}_{i,i}=n^{p+1}$. Also, since H is Hadamard, $HH^T=nI$, so H^T/n is the right inverse, and hence also the left inverse, of H, so $(1/n)H^TH=I$, so H^T is also Hadamard. It follows that $s^{[n]}_{n+i,n+i}=n$ and, for every $x\in\{1,\ldots,n-1\}$, $s^{[x]}_{n+i,n+i}=0$, so $C^{[p]}_{n+i,n+i}=n^{p+1}$.

We will prove that EVAL$(C^{[p]})$ is #P-hard for some sufficiently large even p. We will assume for contradiction that, for every even p, EVAL$(C^{[p]})$ is not #P-hard. Equation (7.1) indicates that $C^{[p]}$ is symmetric, so by Lemma 6.4 (due to Bulatov and Grohe), for every even p, both blocks of $C^{[p]}$ have rank 1. This means that every principal 2×2 submatrix in the blocks has a zero determinant. So, for $i,j\in[n]$, we have $(C^{[p]}_{i,i})^2-(C^{[p]}_{i,j})^2=0$ and $(C^{[p]}_{n+i,n+i})^2-(C^{[p]}_{n+i,n+j})^2=0$, so

$$C^{[p]}_{i,j}=C^{[p]}_{i,i}\text{ and }C^{[p]}_{n+i,n+j}=C^{[p]}_{n+i,n+i}. \tag{7.3}$$

Since (7.2) and (7.3) hold for all even p and all $i,j\in[n]$, Lemma 6.5 allows us to deduce that, for all $i,j\in[n]$ and $x\in\{0,\ldots,n\}$, $s^{[x]}_{i,j}=s^{[x]}_{i,i}$ and $s^{[x]}_{n+i,n+j}=s^{[x]}_{n+i,n+i}$. Thus, for all $i,j\in[n]$,

$$s^{[1]}_{i,j}=\cdots=s^{[n-1]}_{i,j}=s^{[1]}_{n+i,n+j}=\cdots=s^{[n-1]}_{n+i,n+j}=0\text{ and }s^{[n]}_{i,j}=s^{[n]}_{n+i,n+j}=n. \tag{7.4}$$

From the statement of the lemma, we assume that H does not satisfy (GC). There are two similar cases.

Case 1. Suppose there are $i,j\in[n]$ such that $G(H,i)\neq G(H,j)$. Fix such a pair i,j. Fix $a\in[n]$ such that $H_{a,*}\circ H_{i,*}$ is not in $G(H,j)$. Now consider any $b\in[n]$. If it were the case that $|\langle H_{a,*}\circ H_{i,*},\ H_{b,*}\circ H_{j,*}\rangle|=n$, then we would know that either $H_{a,v}H_{i,v}=H_{b,v}H_{j,v}$ for all v or $H_{a,v}H_{i,v}=-H_{b,v}H_{j,v}$ for all v. Either of these would imply $H_{a,*}\circ H_{i,*}\in G(H,j)$, which is not the case. So we conclude that $|\langle H_{a,*}\circ H_{i,*},\ H_{b,*}\circ H_{j,*}\rangle|<n$.

Furthermore, there is some $b\in[n]$ such that $|\langle H_{a,*}\circ H_{i,*},\ H_{b,*}\circ H_{j,*}\rangle|\neq 0$. Otherwise,

$$\{H_{1,*}\circ H_{j,*},\ldots,H_{n,*}\circ H_{j,*},H_{a,*}\circ H_{i,*}\}$$

would be a set of $n+1$ linearly independent vectors, which is impossible.

But this implies that for some $x\in[n-1]$ we have $s^{[x]}_{i,j}\neq 0$, contradicting (7.4).

Case 2. Suppose there are $i,j\in[n]$ such that $G(H^T,i)\neq G(H^T,j)$. As in Case 1, we can deduce that $|\langle H^T_{a,*}\circ H^T_{i,*},\ H^T_{b,*}\circ H^T_{j,*}\rangle|<n$. Furthermore, there is some $b\in[n]$ such that $|\langle H^T_{a,*}\circ H^T_{i,*},\ H^T_{b,*}\circ H^T_{j,*}\rangle|\neq 0$. But this implies that for some $x\in[n-1]$ we have $s^{[x]}_{n+i,n+j}\neq 0$, contradicting (7.4). ∎

7.3. Polynomial representation. For an $n\times n$ matrix H and a row index $l\in[n]$, let $R(H):=\{H_{i,*}\mid i\in[n]\}$. The *extended group condition for H* is as follows:

(EGC) $R(H)$ is an Abelian group under the Hadamard product.

The following lemmas are useful preparation for the proof of Lemma 2.4, the Polynomial Representation Lemma. We say that a Hadamard matrix is *normalized* if its first row and column consist entirely of +1's.

LEMMA 7.2. *Let H be a normalized $n \times n$ Hadamard matrix. If $G(H,1)$ is closed under the Hadamard product, then $R(H)$ is closed under the Hadamard product.*

Proof. Fix $i, j \in [n]$. Since $G(H,1)$ is closed under the Hadamard product, and $H_{i,*} \circ H_{1,*} \in G(H,1)$ and $H_{j,*} \circ H_{1,*} \in G(H,1)$, we have $H_{i,*} \circ H_{j,*} \in G(H,1)$. Thus, there is an $\ell \in [n]$ such that either $H_{i,*} \circ H_{j,*} = H_{\ell,*} \circ H_{1,*} = H_{\ell,*}$ (using the fact that the first row of H is all ones) or $H_{i,*} \circ H_{j,*} = -H_{\ell,*} \circ H_{1,*} = -H_{\ell,*}$. The latter is equivalent to $H_{i,*} \circ H_{\ell,*} = -H_{j,*}$. And since $H_{j,1} = 1$ (since the first column of H is positive), this implies that one of $H_{i,1}$ and $H_{\ell,1}$ is negative, which is a contradiction. We conclude that $H_{i,*} \circ H_{j,*} = H_{\ell,*}$. ∎

COROLLARY 7.3. *Let H be a normalized $n \times n$ Hadamard matrix. If H satisfies the group condition, then H satisfies the extended group condition.*

Proof. Suppose that H satisfies the group condition. By Lemma 7.1, $G(H,1)$ is an Abelian group under the Hadamard product. The identity is the all ones row, which is in $R(H)$, and every element is its own inverse. Closure of $R(H)$ follows from Lemma 7.2. ∎

LEMMA 7.4. *Suppose that B is an $r \times r$ matrix with entries in $\{-1,+1\}$ and that C is a $t \times t$ matrix with entries in $\{-1,+1\}$. Suppose that the tensor product $H = B \otimes C$ is a Hadamard matrix. Then B and C are Hadamard. If H is symmetric, then so are B and C. If H and B are normalized and H satisfies* (EGC)*, then B and C satisfy* (EGC) *and C is normalized.*

Proof. Since H is Hadamard, we know that for any such $k \in [r]$ and distinct i and i' in $[t]$, the inner product $\langle H_{(k-1)t+i,*}, H_{(k-1)t+i',*} \rangle$ is zero. But this inner product is

$$\begin{aligned}\sum_{\ell \in [r]} \sum_{j \in [t]} H_{(k-1)t+i,(\ell-1)t+j} H_{(k-1)t+i',(\ell-1)t+j} &= \sum_{\ell \in [r]} \sum_{j \in [t]} B_{k,\ell} C_{i,j} B_{k,\ell} C_{i',j} \\ &= \sum_{\ell \in [r]} B_{k,\ell}^2 \langle C_{i,*}, C_{i',*} \rangle \\ &= r \langle C_{i,*}, C_{i',*} \rangle,\end{aligned}$$

so C is Hadamard. Similarly, for any distinct $k, k' \in [r]$ and any $i \in [t]$,

$$\begin{aligned}0 = \langle H_{(k-1)t+i,*}, H_{(k'-1)t+i,*} \rangle &= \sum_{\ell \in [r]} \sum_{j \in [t]} H_{(k-1)t+i,(\ell-1)t+j} H_{(k'-1)t+i,(\ell-1)t+j} \\ &= \sum_{\ell \in [r]} \sum_{j \in [t]} B_{k,\ell} C_{i,j} B_{k',\ell} C_{i,j} \\ &= \sum_{j \in [t]} C_{i,j}^2 \langle B_{k,*}, B_{k',*} \rangle \\ &= t \langle B_{k,*}, B_{k',*} \rangle,\end{aligned}$$

so B is Hadamard. If H is symmetric, then it is easy to see that B and C are symmetric as well. Also, if H and B are normalized, then it is easy to see that C is normalized as well.

Suppose now that H and B are normalized and H satisfies (EGC). We first show that C satisfies (EGC). Then we will finish by showing that B satisfies (EGC).

To show that $R(C)$ is an Abelian group under the Hadamard product, we just need to show closure. (Commutativity and associativity come from the definition of the Hadamard product, the identity element is the row of all ones, and every element

is its own inverse.) Since $R(H)$ is closed under the Hadamard product, we know that, for any distinct $i, i' \in [t]$, $H_{i,*} \circ H_{i',*} \in R(H)$. But the first t elements of this row are $H_{i,1}H_{i',1}, \ldots, H_{i,t}H_{i',t} = B_{1,1}C_{i,1}B_{1,1}C_{i',1}, \ldots, B_{1,1}C_{i,t}B_{1,1}C_{i',1}$, which is equal to $C_{i,*} \circ C_{i',*}$. This shows that $C_{i,*} \circ C_{i',*} \in G(C, 1)$. Now use Lemma 7.2 to show that $R(C)$ is closed under the Hadamard product.

Similarly, to show that $R(B)$ is closed under the Hadamard product, note that for any distinct $k, k' \in [r]$, $H_{(k-1)t+1,*} \circ H_{(k'-1)t+1,*} \in R(H)$. But the elements of this row are

$$H_{(k-1)t+1,(\ell-1)t+j}H_{(k'-1)t+1,(\ell-1)t+j}$$

for $\ell \in [r]$, $j \in [t]$, and taking those with $\ell = 1$ (which occur as the first t elements along the row), we get $B_{k,1}C_{1,j}B_{k',1}C_{1,j}$. Thus, the subrow of these elements is the Hadamard product of $B_{k,*}$ and $B_{k',*}$. This shows that $B_{k,*} \circ B_{k',*} \in G(B, 1)$. Now use Lemma 7.2 to show that $R(B)$ is closed under the Hadamard product. ∎

Given an $n \times n$ matrix H and permutations Σ and Π in S_n, let $H_{\Sigma,\Pi}$ denote the matrix with $(H_{\Sigma,\Pi})_{i,j} = H_{\Sigma(i),\Pi(j)}$.

LEMMA 7.5. *Let H be a normalized $n \times n$ Hadamard matrix with $n \geq 2$ that satisfies* (GC). *Then there are permutations Σ, Π in S_n with $\Sigma(1) = 1$ and $\Pi(1) = 1$ and a normalized Hadamard matrix H' satisfying* (GC) *such that $H_{\Sigma,\Pi} = H_2 \otimes H'$. Σ, Π, and H' can be constructed in polynomial time.*

Proof. By Lemma 2.1 we know n is a power of 2, say, $n = 2^{k+1}$. The lemma is trivial for $k = 0$ since $H = H_2$ and Σ and Π can be taken to be the identity. So suppose $k \geq 1$. Let $\nu = 2^k$.

Part 1. Choose Σ' and Π' in S_n with $\Sigma'(1) = 1$ and $\Pi'(1) = 1$ so that $(H_{\Sigma',\Pi'})_{\nu+1,\nu+1} = -1$.

Σ' and Π' may be constructed as follows: H is Hadamard, so some entry $H_{i,j} = -1$. The indices i and j are not 1 because H is normalized. Let Σ' be the transposition $(i, \nu + 1)$ and let Π' be the transposition $(j, \nu + 1)$.

Part 2C. Choose π in S_n with $\pi(1) = 1$ and $\pi(\nu + 1) = \nu + 1$ so that, for $\ell \in [\nu]$,

$$(H_{\Sigma',\Pi''})_{\nu+1,\ell} = +1 \text{ and } (H_{\Sigma',\Pi''})_{\nu+1,\nu+\ell} = -1, \tag{7.5}$$

where Π'' denotes the composition of first Π' and then π.

π may be constructed as follows. We construct a sequence of permutations $\pi_1, \ldots, \pi_\nu$, where π_1 is the identity and we let $\pi = \pi_\nu$. Let H^j denote $H_{\Sigma',\pi_j\Pi'}$. For $j \in \{2, \ldots \nu\}$, we define π_j as follows. If $H^{j-1}_{\nu+1,\nu+j} = -1$, then $\pi_j = \pi_{j-1}$. Otherwise, there is a $1 < \ell < \nu + 1$ with $H^{j-1}_{\nu+1,\ell} = -1$. So π'_j is the composition of first applying π'_{j-1} and then transposing $\nu+j$ and ℓ. To see that such an ℓ exists, note that H is Hadamard, so $\langle H_{1,*}, H_{\nu+1,*}\rangle = 0$. But $H_{1,*}$ is positive, so $H_{\nu+1,*}$ has exactly ν ones. $\ell > 1$ because $\pi_{j-1}\Pi'(1) = 1$.

Part 2R. Choose σ in S_n with $\sigma(1) = 1$ and $\sigma(\nu + 1) = \nu + 1$ so that, for $\ell \in [\nu]$,

$$(H_{\Sigma'',\Pi''})_{\ell,\nu+1} = +1 \text{ and } (H_{\Sigma'',\Pi''})_{\nu+\ell,\nu+1} = -1, \tag{7.6}$$

where Σ'' denotes the composition of first Σ' and then σ.

The construction of σ is symmetric to the earlier construction of π.

Since $\sigma(\nu+1) = \nu+1$, we have $(H_{\Sigma',\Pi''})_{\nu+1,\ell} = (H_{\Sigma',\Pi''})_{\sigma(\nu+1),\ell} = (H_{\Sigma'',\Pi''})_{\nu+1,\ell}$ for every $\ell \in [n]$, so (7.5) and (7.6) give

$$(H_{\Sigma'',\Pi''})_{\nu+1,\ell} = (H_{\Sigma'',\Pi''})_{\ell,\nu+1} = +1 \text{ and } (H_{\Sigma'',\Pi''})_{\nu+1,\nu+\ell} = (H_{\Sigma'',\Pi''})_{\nu+\ell,\nu+1} = -1. \tag{7.7}$$

Part 3C. Choose π' in S_n with $\pi'(1) = 1$ and $\pi'([\nu]) = [\nu]$ so that, for $j, \ell \in [\nu]$,

$$(H_{\Sigma'',\Pi})_{\ell,j} = (H_{\Sigma'',\Pi})_{\ell,\nu+j} \text{ and } (H_{\Sigma'',\Pi})_{\nu+\ell,j} = -(H_{\Sigma'',\Pi})_{\nu+\ell,\nu+j}, \tag{7.8}$$

where Π denotes the composition of first Π'' and then π'.

π' is constructed as follows. Note that H satisfies (EGC) by Corollary 7.3; hence $H_{\Sigma'',\Pi''}$ satisfies (EGC) (permuting does not change (ECG)). Start with $\pi'(1) = 1$ and $\pi'(\nu+1) = \nu+1$. Note that, for $j = 1$, we have, by normalization and (7.6),

$$\begin{aligned} &\forall \ell \in [\nu], (H_{\Sigma'',\Pi''})_{\ell,\pi'(j)} = (H_{\Sigma'',\Pi''})_{\ell,\pi'(\nu+j)} \\ &\quad \text{and } (H_{\Sigma'',\Pi''})_{\nu+\ell,\pi'(j)} = -(H_{\Sigma'',\Pi''})_{\nu+\ell,\pi'(\nu+j)}, \end{aligned} \tag{7.9}$$

Now for $j \in \{2, \ldots, \nu\}$ we define $\pi'(j)$ and $\pi'(\nu+j)$ to satisfy (7.9) as follows. Choose any $i \in [\nu]$ such that $\pi'^{-1}(i)$ is undefined and set $\pi'(j) = i$. By (EGC) there is a unique i' with

$$(H_{\Sigma'',\Pi''})_{i,*} \circ (H_{\Sigma'',\Pi''})_{\nu+1,*} = (H_{\Sigma'',\Pi''})_{i',*}. \tag{7.10}$$

Also, i' is not in $[\nu]$ since by (7.10) $(H_{\Sigma'',\Pi''})_{i,\nu+1}(H_{\Sigma'',\Pi''})_{\nu+1,\nu+1} = (H_{\Sigma'',\Pi''})_{i',\nu+1}$, and the left-hand side is -1 by (7.6). Finally, $\pi'^{-1}(i')$ is undefined since no other i satisfies (7.10). So set $\pi'(\nu+j) = i'$.

Part 3R. Choose σ' in S_n with $\sigma'(1) = 1$ and $\sigma'([\nu]) = [\nu]$ so that, for $j, \ell \in [\nu]$,

$$(H_{\Sigma,\Pi})_{\ell,j} = (H_{\Sigma,\Pi})_{\nu+\ell,j} \text{ and } (H_{\Sigma,\Pi})_{\ell,\nu+j} = -(H_{\Sigma,\Pi})_{\nu+\ell,\nu+j}, \tag{7.11}$$

where Σ denotes the composition of first Σ'' and then σ'.

The construction of σ' is symmetric to the (earlier) construction of π'.

Now, since $\sigma'([\nu]) = [\nu]$, (7.8) implies

$$(H_{\Sigma'',\Pi})_{\sigma(\ell),j} = (H_{\Sigma'',\Pi})_{\sigma(\ell),\nu+j} \text{ and } (H_{\Sigma'',\Pi})_{\sigma(\nu+\ell),j} = -(H_{\Sigma'',\Pi})_{\sigma(\nu+\ell),\nu+j}$$

or, equivalently,

$$(H_{\Sigma,\Pi})_{\ell,j} = (H_{\Sigma,\Pi})_{\ell,\nu+j} \text{ and } (H_{\Sigma,\Pi})_{\nu+\ell,j} = -(H_{\Sigma,\Pi})_{\nu+\ell,\nu+j}. \tag{7.12}$$

By (7.11) and (7.12) we can take H' to be the first ν rows and columns of $H_{\Sigma,\Pi}$, and then we have $H_{\Sigma,\Pi} = H_2 \otimes H'$. ∎

LEMMA 7.6. *Let H be a normalized symmetric $n \times n$ Hadamard matrix with $n \geq 2$ that has an entry -1 on the diagonal and satisfies* (GC). *Then there is a permutation Σ in S_n with $\Sigma(1) = 1$ and a normalized symmetric Hadamard matrix H' satisfying* (GC) *such that $H_{\Sigma,\Sigma} = H_2 \otimes H'$. Σ and H' can be constructed in polynomial time.*

Proof. In the proof of Lemma 7.5 note that we can ensure that $\Pi = \Sigma$. If $H_{a,a} = -1$, then $i = j = a$ in part 1. ∎

Define H_4 as follows:

$$H_4 = \begin{pmatrix} + & + & + & + \\ + & + & - & - \\ + & - & + & - \\ + & - & - & + \end{pmatrix}.$$

LEMMA 7.7. *Let H be a normalized symmetric $n \times n$ Hadamard matrix with $n > 2$. Suppose that H has a positive diagonal and satisfies* (GC). *Then there is a*

permutation $\Sigma \in S_n$ *with* $\Sigma(1) = 1$ *and a normalized symmetric Hadamard matrix* H' *satisfying* (GC) *such that* $H_{\Sigma,\Sigma} = H_4 \otimes H'$. Σ *and* H' *can be constructed in polynomial time.*

Proof. By Lemma 2.1 we know that n is a power of 2, say, $n = 2^{k+2}$. The lemma is trivial for $k = 0$ since $H = H_4$ and Σ can be taken to be the identity. So suppose that $k \geq 1$. Let $\nu = 2^k$.

Part 1. Choose Σ' in S_n with $\Sigma'(1) = 1$ and $\Sigma'(\nu+1) = \nu+1$ so that, for $j \in [2\nu]$,

$$(H_{\Sigma',\Sigma'})_{\nu+1,j} = +1 \text{ and } (H_{\Sigma',\Sigma'})_{\nu+1,2\nu+j} = -1. \tag{7.13}$$

Σ' is constructed as follows. We construct a sequence of permutations $\sigma_0, \ldots, \sigma_{2\nu}$, where σ_0 is the identity and we let $\Sigma' = \sigma_{2\nu}$. Let H^j denote H_{σ_j,σ_j}. For $j \in \{1, \ldots 2\nu\}$, we define σ_j as follows. If $H^{j-1}_{\nu+1,2\nu+j} = -1$, then $\sigma_j = \sigma_{j-1}$. Otherwise, there is a $1 < \ell < 2\nu + 1$ with $\ell \neq \nu + 1$ with $H^{j-1}_{\nu+1,\ell} = -1$. So σ_j is the composition of first applying σ_{j-1} and then transposing $2\nu + j$ and ℓ. To see that such an ℓ exists, note that $H_{\nu+1,*}$ has exactly 2ν ones. However, since H is normalized and has a positive diagonal, $H_{\nu+1,1} = H_{\nu+1,\nu+1} = +1$, so $H^{j-1}_{\nu+1,1} = H^{j-1}_{\nu+1,\nu+1} = +1$.

Observation. Since $H_{\Sigma',\Sigma'}$ is Hadamard, $(H_{\Sigma',\Sigma'})_{2\nu+1,*}$ has 2ν positive entries (since its dot product with row 1 is 0). Also, half of these are in the first 2ν columns (since its dot product with row $\nu + 1$ is 0).

Part 2. Choose σ' in S_n with $\sigma'(1) = 1$, $\sigma'(\nu + 1) = \nu + 1$, $\sigma'(2\nu + 1) = 2\nu + 1$, and $\sigma'([2\nu]) = [2\nu]$ so that, for $j \in [\nu]$,

$$\begin{aligned}(H_{\Sigma'',\Sigma''})_{2\nu+1,j} = (H_{\Sigma'',\Sigma''})_{2\nu+1,2\nu+j} = +1 \\ \text{and } (H_{\Sigma'',\Sigma''})_{2\nu+1,\nu+j} = (H_{\Sigma'',\Sigma''})_{2\nu+1,3\nu+j} = -1,\end{aligned} \tag{7.14}$$

where Σ'' is the composition of Σ' and then σ'.

σ' is constructed as follows. We construct a sequence of permutations $\sigma'_1, \ldots, \sigma'_{2\nu}$, where σ'_1 is the identity and we let $\sigma' = \sigma'_{2\nu}$. Let H^j denote $H_{\sigma'_j\Sigma',\sigma'_j\Sigma'}$. Note that $H^1_{2\nu+1,\nu+1} = -1$ by (7.13) and symmetry of H^1. For $j \in \{2, \ldots \nu\}$, we define σ'_j as follows. If $H^{j-1}_{2\nu+1,\nu+j} = -1$, then $\sigma'_j = \sigma'_{j-1}$. Otherwise, by the observation at the end of part 1, there is a $1 < \ell < \nu + 1$ with $H^{j-1}_{2\nu+1,\ell} = -1$. So σ'_j is the composition of first applying σ'_{j-1} and then transposing $\nu + j$ and ℓ. For $j \in \{\nu + 1, \ldots, 2\nu\}$, we define σ_j as follows. If $H^{j-1}_{2\nu+1,2\nu+j} = -1$, then $\sigma'_j = \sigma'_{j-1}$. Otherwise, by the observation at the end of part 1, there is a $2\nu + 1 < \ell < 3\nu + 1$ with $H^{j-1}_{2\nu+1,\ell} = -1$. So σ'_j is the composition of first applying σ'_{j-1} and then transposing $2\nu + j$ and ℓ. (The reason that $\ell > 2\nu + 1$ is that the diagonal is positive.)

Note that $\Sigma''(1) = 1$. Since $\sigma'(\nu + 1) = \nu + 1$ and $\sigma'([2\nu]) = [2\nu]$,

$$(H_{\Sigma'',\Sigma''})_{\nu+1,j} = (H_{\Sigma',\Sigma'})_{\sigma'(\nu+1),\sigma'(j)} = (H_{\Sigma',\Sigma'})_{\nu+1,\sigma'(j)},$$

so (7.13) gives us

$$\forall j \in [2\nu], (H_{\Sigma'',\Sigma''})_{\nu+1,j} = +1 \text{ and } (H_{\Sigma'',\Sigma''})_{\nu+1,2\nu+j} = -1. \tag{7.15}$$

Equations (7.14) and (7.15) are summarized by the following picture, which takes into

account the symmetry of $H_{\Sigma'',\Sigma''}$:

$$H_{\Sigma'',\Sigma''} = \left(\begin{array}{ccc|ccc|ccc|ccc}
+ & \cdots & + & + & \cdots & + & + & \cdots & + & + & \cdots & + \\
\vdots & & & \vdots & & & \vdots & & & & & \\
+ & & & + & & & + & & & & & \\
\hline
+ & \cdots & + & + & \cdots & + & - & \cdots & - & - & \cdots & - \\
\vdots & & & \vdots & & & \vdots & & & & & \\
+ & & & + & & & - & & & & & \\
\hline
+ & \cdots & + & - & \cdots & - & + & \cdots & + & - & \cdots & - \\
\vdots & & & \vdots & & & \vdots & & & & & \\
+ & & & - & & & + & & & & & \\
\hline
+ & & & - & & & - & & & & & \\
\vdots & & & \vdots & & & \vdots & & & & & \\
+ & & & - & & & - & & & & &
\end{array}\right)$$

Part 3. Choose σ'' in S_n with $\sigma''(1) = 1$, $\sigma''(\nu+1) = \nu+1$, $\sigma''(2\nu+1) = 2\nu+1$, $\sigma''([\nu]) = [\nu]$, $\sigma''(\{\nu+1,\dots,2\nu\}) = \{\nu+1,\dots,2\nu\}$, and $\sigma''(\{2\nu+1,\dots,3\nu\}) = \{2\nu+1,\dots,3\nu\}$ so that, for $j \in [\nu]$, we have the following, where Σ denotes the composition of Σ'' and then σ'':

$$(H_{\Sigma,\Sigma})_{j,*} \circ (H_{\Sigma,\Sigma})_{2\nu+j,*} = (H_{\Sigma,\Sigma})_{2\nu+1,*}, \tag{7.16}$$

$$(H_{\Sigma,\Sigma})_{\nu+j,*} \circ (H_{\Sigma,\Sigma})_{3\nu+j,*} = (H_{\Sigma,\Sigma})_{2\nu+1,*}, \tag{7.17}$$

$$(H_{\Sigma,\Sigma})_{j,*} \circ (H_{\Sigma,\Sigma})_{\nu+j,*} = (H_{\Sigma,\Sigma})_{\nu+1,*}. \tag{7.18}$$

σ'' is constructed as follows. Note that H satisfies (EGC) by Corollary 7.3; hence $H_{\Sigma'',\Pi''}$ satisfies (EGC) (permuting does not change (ECG)). For $j \in [\nu]$, do the following. Let i_1 be the smallest element in $[\nu]$ such that the inverse of i_1 under σ'' is still undefined. (For $j = 1$, σ'' is still completely undefined, so we will have $i_1 = 1$.) Let i_2 be the solution to

$$(H_{\Sigma'',\Sigma''})_{i_1,*} \circ (H_{\Sigma'',\Sigma''})_{\nu+1,*} = (H_{\Sigma'',\Sigma''})_{i_2,*}. \tag{7.19}$$

This equation implies that

$$(H_{\Sigma'',\Sigma''})_{i_1,\nu+1}(H_{\Sigma'',\Sigma''})_{\nu+1,\nu+1} = (H_{\Sigma'',\Sigma''})_{i_2,\nu+1}$$

and

$$(H_{\Sigma'',\Sigma''})_{i_1,2\nu+1}(H_{\Sigma'',\Sigma''})_{\nu+1,2\nu+1} = (H_{\Sigma'',\Sigma''})_{i_2,2\nu+1}.$$

Applying (7.14) and (7.15), the left-hand side of the first of these equations is $+1$ and the left-hand side of the second of these equations is -1, so $i_2 \in \{\nu+1,\dots,2\nu\}$. Also, since no other i_1 satisfies (7.19) for this value of i_2, the inverse of i_2 under σ'' is still undefined (so there is no problem with defining it now). Let i_3 be the solution to

$$(H_{\Sigma'',\Sigma''})_{i_1,*} \circ (H_{\Sigma'',\Sigma''})_{2\nu+1,*} = (H_{\Sigma'',\Sigma''})_{i_3,*}.$$

This equation implies that

$$(H_{\Sigma'',\Sigma''})_{i_1,\nu+1}(H_{\Sigma'',\Sigma''})_{2\nu+1,\nu+1} = (H_{\Sigma'',\Sigma''})_{i_3,\nu+1}$$

and

$$(H_{\Sigma'',\Sigma''})_{i_1,2\nu+1}(H_{\Sigma'',\Sigma''})_{2\nu+1,2\nu+1} = (H_{\Sigma'',\Sigma''})_{i_3,2\nu+1}.$$

Applying (7.14) and (7.15), the left-hand side of the first of these equations is -1, and the left-hand side of the second of these equations is $+1$, so $i_3 \in \{2\nu+1,\dots,3\nu\}$ and the inverse of i_3 under σ'' is still undefined. Let i_4 be the solution to

$$(H_{\Sigma'',\Sigma''})_{i_2,*} \circ (H_{\Sigma'',\Sigma''})_{2\nu+1,*} = (H_{\Sigma'',\Sigma''})_{i_4,*}.$$

This equation implies that

$$(H_{\Sigma'',\Sigma''})_{i_2,\nu+1}(H_{\Sigma'',\Sigma''})_{2\nu+1,\nu+1} = (H_{\Sigma'',\Sigma''})_{i_4,\nu+1}$$

and

$$(H_{\Sigma'',\Sigma''})_{i_2,2\nu+1}(H_{\Sigma'',\Sigma''})_{2\nu+1,2\nu+1} = (H_{\Sigma'',\Sigma''})_{i_4,2\nu+1}.$$

Applying (7.14) and (7.15), the left-hand side of the first of these equations is -1, and the left-hand side of the second of these equations is -1, so $i_4 \in \{3\nu+1,\dots,4\nu\}$ and the inverse of i_4 under σ' is still undefined. Let $\sigma''(j) = i_1$, $\sigma''(\nu+j) = i_2$, $\sigma''(2\nu+j) = i_3$, and $\sigma''(3\nu+j) = i_4$. Note that the choices of i_1, i_2, i_3, and i_4 imply the following, which imply (7.16), (7.17), and (7.18):

$$(H_{\Sigma'',\Sigma''})_{\sigma''(j),*} \circ (H_{\Sigma'',\Sigma''})_{\sigma''(2\nu+j),*} = (H_{\Sigma'',\Sigma''})_{\sigma''(2\nu+1),*}, \tag{7.20}$$

$$(H_{\Sigma'',\Sigma''})_{\sigma''(\nu+j),*} \circ (H_{\Sigma'',\Sigma''})_{\sigma''(3\nu+j),*} = (H_{\Sigma'',\Sigma''})_{\sigma''(2\nu+1),*}, \tag{7.21}$$

$$(H_{\Sigma'',\Sigma''})_{\sigma''(j),*} \circ (H_{\Sigma,\Sigma})_{\sigma''(\nu+j),*} = (H_{\Sigma'',\Sigma''})_{\sigma''(\nu+1),*}. \tag{7.22}$$

Since $\sigma''(\nu+1) = \nu+1$, $\sigma''(2\nu+1) = 2\nu+1$, $\sigma''([\nu]) = [\nu]$, $\sigma''(\{\nu+1,\dots,2\nu\}) = \{\nu+1,\dots,2\nu\}$, and $\sigma''(\{2\nu+1,\dots,3\nu\}) = \{2\nu+1,\dots,3\nu\}$, (7.14) and (7.15) give us

$$\forall j \in [\nu], (H_{\Sigma,\Sigma})_{2\nu+1,j} = (H_{\Sigma,\Sigma})_{2\nu+1,2\nu+j} = +1$$
$$\text{and } (H_{\Sigma,\Sigma})_{2\nu+1,\nu+j} = (H_{\Sigma,\Sigma})_{2\nu+1,3\nu+j} = -1,$$

$$\forall j \in [2\nu], (H_{\Sigma,\Sigma})_{\nu+1,j} = +1 \text{ and } (H_{\Sigma,\Sigma''})_{\nu+1,2\nu+j} = -1.$$

These, together with (7.16), (7.17), and (7.18) and the symmetry of $H_{\Sigma,\Sigma}$ give us the result, where H' is the first ν rows and columns of $H_{\Sigma,\Sigma}$. ∎

LEMMA 7.8. *Let H be a normalized Hadamard matrix of order $n = 2^k$ which satisfies* (GC). *Let $X = (X_1,\dots,X_k)$, $Y = (Y_1,\dots,Y_k)$. There are index mappings $\rho^R : \mathbb{F}_2^k \to [n]$ and $\rho^C : \mathbb{F}_2^k \to [n]$ with $\rho^R(0,\dots,0) = \rho^C(0,\dots,0) = 1$ and a permutation $\pi \in S_k$ such that H is represented by the polynomial $X_\pi Y$. If H is symmetric, then $\rho^R = \rho^C$. ρ^R, ρ^C, and π can be constructed in polynomial time.*

Proof. The proof is by induction on k. The base case is $k = 1$ for which $H = H_2$. In this case, we take the index mapping ρ^R given by $\rho^R(0) = 1$ and $\rho^R(1) = 2$. $\rho^R = \rho^C$ and π is the identity.

For the inductive step, first suppose that H is not symmetric. By Lemma 7.5, there are permutations $\Sigma, \Pi \in S_n$ with $\Sigma(1) = 1$ and $\Pi(1) = 1$ and a normalized

Hadamard matrix H' satisfying (GC) such that $H_{\Sigma,\Pi} = H_2 \otimes H'$. These are constructed in polynomial time. By induction, we can construct index mappings $\rho^R_{k-1} : \mathbb{F}_2^{k-1} \to [2^{k-1}]$ and $\rho^C_{k-1} : \mathbb{F}_2^{k-1} \to [2^{k-1}]$ with $\rho^R_{k-1}(0,\ldots,0) = \rho^C_{k-1}(0,\ldots,0) = 1$ and a permutation $\pi' \in S_{k-1}$ such that H' is represented by the polynomial

$$X_{\pi'(1)}Y_1 \oplus \cdots \oplus X_{\pi'(k-1)}Y_{k-1}.$$

Now take $\rho^R(X_1,\ldots,X_k) = \Sigma(2^{k-1}X_k + \rho^R_{k-1}(X_1,\ldots,X_{k-1}))$ and $\rho^C(Y_1,\ldots,Y_k) = \Pi(2^{k-1}Y_k + \rho^C_{k-1}(Y_1,\ldots,Y_{k-1}))$, and let $\pi \in S_k$ be the permutation that maps k to itself and applies π' to $1,\ldots,k-1$.

Next, suppose that H is symmetric and that it has an entry -1 on the diagonal. Using Lemma 7.6, we proceed exactly as before except that we are guaranteed (by Lemma 7.6) that $\Pi = \Sigma$ and that H' is symmetric. Thus, by induction, we are guaranteed that $\rho^C_{k-1} = \rho^R_{k-1}$. So the construction above gives $\rho^C = \rho^R$.

Finally, suppose that H is symmetric and that it has a positive diagonal. Note that $n > 2$. By Lemma 7.7, there are a permutation $\Sigma \in S_n$ with $\Sigma(1) = 1$ and a normalized symmetric Hadamard matrix H' satisfying (GC) such that $H_{\Sigma,\Pi} = H_4 \oplus H'$. These are constructed in polynomial time. By induction, we can construct an index mapping $\rho' : \mathbb{F}_2^{k-2} \to [n]$ with $\rho'(0,\ldots,0) = 1$ and a permutation $\pi' \in S_{k-2}$ such that H' is represented by the polynomial

$$X_{\pi'(1)}Y_1 \oplus \cdots \oplus X_{\pi'(k-2)}Y_{k-2}.$$

Now take $\rho(X_1,\ldots,X_k) = \Sigma(2^{k-1}X_k + 2^{k-1}X_{k-1} + \rho'(X_1,\ldots,X_{k-2}))$ and let $\pi \in S_k$ be the permutation that transposes k and $k-1$ applies π' to $1,\ldots,k-2$. ∎

Proof of Lemma 2.4, the Polynomial Representation Lemma. Let $n = 2^k$. Since H is positive for Λ^R and Λ^C, choose a and b such that $H_{a,b} = +1$ and (1) $a \in \Lambda^R$ or $\Lambda^R = \emptyset$, (2) $b \in \Lambda^C$ or $\Lambda^C = \emptyset$, and (3) if H is symmetric and $\Lambda^R = \Lambda^C$, then $a = b$. Now let Σ be the transposition $(1,a)$ and let Π be the transposition $(1,b)$. Note that $(H_{\Sigma,\Pi})_{1,1} = +1$. Let $\widehat{H}$ be the matrix defined by

$$\widehat{H}_{i,j} = (H_{\Sigma,\Pi})_{i,j}(H_{\Sigma,\Pi})_{i,1}(H_{\Sigma,\Pi})_{1,j}.$$

Note that $\widehat{H}$ is normalized. Also, it is Hadamard, and it satisfies (GC) since $H_{\Sigma,\Pi}$ is Hadamard and satisfies (GC).

By Lemma 7.8 we can construct $\widehat{\rho}^R$, $\widehat{\rho}^C$, and π such that $\widehat{H}$ is represented by the polynomial $\widehat{h}(X,Y) := X_\pi Y$. By the definition of "represents," we have

$$\widehat{H}_{\widehat{\rho}^R(\mathbf{x}),\widehat{\rho}^C(\mathbf{y})} = -1 \iff \widehat{h}(\mathbf{x},\mathbf{y}) = 1.$$

Define $g^R(\mathbf{x}) = 1$ if $(H_{\Sigma,\Pi})_{\widehat{\rho}^R(\mathbf{x}),1} = -1$ and $g^R(\mathbf{x}) = 0$ otherwise. Define $g^C(\mathbf{y}) = 1$ if $(H_{\Sigma,\Pi})_{1,\widehat{\rho}^C(\mathbf{y})} = -1$ and $g^C(\mathbf{y}) = 0$ otherwise. Now, note that

$$(H_{\Sigma,\Pi})_{\widehat{\rho}^R(\mathbf{x}),\widehat{\rho}^C(\mathbf{y})} = -1 \iff \widehat{h}(\mathbf{x},\mathbf{y}) \oplus g^R(\mathbf{x}) \oplus g^C(\mathbf{y}) = 1.$$

Now let $\rho^R(\mathbf{x}) = \Sigma(\widehat{\rho}^R(\mathbf{x}))$ and let $\rho^C(\mathbf{y}) = \Pi(\widehat{\rho}^C(\mathbf{y}))$. Note that H is represented by $\widehat{h}(\mathbf{x},\mathbf{y}) \oplus g^R(\mathbf{x}) \oplus g^C(\mathbf{y})$ with respect to ρ^R and ρ^C.

From Lemma 7.8, $\widehat{\rho}^R(0,\ldots,0) = 1$, so $\rho^R(0,\ldots,0) = a$. So if $\Lambda^R \neq \emptyset$ then $\rho^R(0,\ldots,0) \in \Lambda^R$. Similarly, $\rho^R(1,\ldots,1) = b$, so if $\Lambda^C \neq \emptyset$, then $\rho^C(0,\ldots,0) \in \Lambda^C$.

Finally, if H is symmetric, then $H_{\Sigma,\Pi}$ is symmetric, so $\widehat{H}$ is symmetric, so Lemma 7.8 guarantees that $\widehat{\rho}^R = \widehat{\rho}^C$. Thus, if $\Lambda^R = \Lambda^C$, then $a = b$, so $\Sigma = \Pi$, so $g^R = g^C$, and $\rho^R = \rho^C$. ∎

7.4. Linearity.

Proof of Lemma 2.5*, the Linearity Lemma.* Let H be an $n \times n$ Hadamard matrix and $\Lambda^R, \Lambda^C \subseteq [n]$ subsets of indices. Let M, Λ be the bipartization of H, Λ^R, and Λ^C and let $m = 2n$. Suppose that (GC) and (R) are satisfied. Let $n = 2^k$ by Lemma 2.1. We will construct a matrix C and and a reduction $\mathrm{EVAL}(C, I_m, I_{m;\Lambda}) \leq \mathrm{EVAL}(M, I_m, I_{m;\Lambda})$. We will show that $\mathrm{EVAL}(C, I_m, I_{m;\Lambda})$ is #P-hard unless (L) is satisfied.

The reduction is as follows. Let $G = (V, E)$ be an input to $\mathrm{EVAL}(C, I_m, I_{m;\Lambda})$. We construct an input G' to $\mathrm{EVAL}(M, I_m, I_{m;\Lambda})$ as follows. Each edge $\{u, v\} \in E$ corresponds to a gadget in G' on vertex set $\{u, v, w, w', w''\}$ and edge set $\{\{u, w\}, \{v, w\}, \{w, w'\}, \{w', w''\}\}$, where w, w'', and w'' are new vertices.

Now let us construct the matrix C. Let Γ denote the graph with vertices u and v and a single edge between them. Clearly, $C_{a,b}$ is equal to the contribution to $Z_M(\Gamma')$ corresponding to those configurations ξ with $\xi(u) = a$ and $\xi(v) = b$. Thus, if c, d, and e denote the choice of spins for vertices w, w', and w'', respectively, we get

$$C_{a,b} = \sum_{c=1}^{m} M_{a,c} M_{b,c} (I_{m;\Lambda})_{c,c} \sum_{d=1}^{m} \sum_{e=1}^{m} M_{c,d} M_{d,e} (I_{m;\Lambda})_{e,e}. \tag{7.23}$$

Here we use that the vertices w, w'' have odd degree and the vertex w' has even degree.

Note that, with the above definition of C, we have $Z_{C,I_m,I_{m;\Lambda}}(G) = Z_{M,I_m,I_{m;\Lambda}}(G')$ for all G.

From the definition of bipartization, we find that $C_{a,b} = C_{b,a} = 0$ for all $a \in [n]$ and $b \in \{n+1, \ldots, 2n\}$. Furthermore, for $a, b \in [n]$,

$$\begin{aligned} C_{a,b} &= \sum_{c=1}^{n} M_{a,n+c} M_{b,n+c} (I_{m;\Lambda})_{n+c,n+c} \sum_{d=1}^{n} \sum_{e=1}^{n} M_{n+c,d} M_{d,n+e} (I_{m;\Lambda})_{n+e,n+e} \\ &= \sum_{c,e \in \Lambda^C} H_{a,c} H_{b,c} \sum_{d=1}^{n} H_{d,c} H_{d,e}. \end{aligned}$$

Now, by (R), there are bijective index mappings $\rho^R : \mathbb{F}_2^k \to [n]$ and $\rho^C : \mathbb{F}_2^k \to [n]$ and a permutation $\pi \in S_k$ such that (with respect to ρ^R and ρ^C) the matrix H is represented by the polynomial $h(X, Y) = X_\pi Y \oplus g^R(X) \oplus g^C(Y)$. Let τ^R be the inverse of ρ^R and τ^C be the inverse of ρ^C. Let $L^C = \tau^C(\Lambda^C)$ and $L^R = \tau^R(\Lambda^R)$. Also, let $\alpha^R = \tau^R(a)$, $\beta^R = \tau^R(b)$, $\gamma^C = \tau^C(c)$, $\delta^R = \tau^R(d)$, and $\varepsilon^C = \tau^C(e)$. Thus,

$$\begin{aligned} H_{a,c} H_{b,c} &= (-1)^{h(\alpha^R, \gamma^C)} \cdot (-1)^{h(\beta^R, \gamma^C)} \\ &= (-1)^{\alpha^R_\pi \cdot \gamma^C \oplus g^R(\alpha^R) \oplus g^C(\gamma^C) \oplus \beta^R_\pi \cdot \gamma^C \oplus g^R(\beta^R) \oplus g^C(\gamma^C)} \\ &= (-1)^{g^R(\alpha^R) \oplus g^R(\beta^R) \oplus \alpha^R_\pi \cdot \gamma^C \oplus \beta^R_\pi \cdot \gamma^C} \\ &= (-1)^{g^R(\alpha^R) \oplus g^R(\beta^R) \oplus \gamma^C \cdot (\alpha^R_\pi \oplus \beta^R_\pi)}. \end{aligned}$$

Similarly, we get

$$H_{d,c} H_{d,e} = (-1)^{g^C(\gamma^C) \oplus g^C(\varepsilon^C) \oplus \delta^R_\pi \cdot (\gamma^C \oplus \varepsilon^C)}.$$

So, for $a, b \in [n]$,

$$C_{a,b} = (-1)^{g^R(\alpha^R) \oplus g^R(\beta^R)} \sum_{c,e \in \Lambda^C} (-1)^{\gamma^C \cdot (\alpha^R_\pi \oplus \beta^R_\pi) \oplus g^C(\gamma^C) \oplus g^C(\varepsilon^C)} \sum_{d=1}^{n} (-1)^{\delta^R_\pi \cdot (\gamma^C \oplus \varepsilon^C)}.$$

Now note that

$$\sum_{d=1}^{n}(-1)^{\delta_\pi^R\cdot(\gamma^C\oplus\varepsilon^C)}=\sum_{\delta_\pi^R\in\mathbb{F}_2^k}(-1)^{\delta_\pi^R\cdot(\gamma^C\oplus\varepsilon^C)}=\begin{cases}n & \text{if } \gamma^C=\varepsilon^C,\\ 0 & \text{otherwise,}\end{cases}$$

so for $a,b\in[n]$,

$$\begin{aligned}C_{a,b}&=n(-1)^{g^R(\alpha^R)\oplus g^R(\beta^R)}\sum_{c\in\Lambda^C}(-1)^{\gamma^C\cdot(\alpha_\pi^R\oplus\beta_\pi^R)}\\&=n(-1)^{g^R(\alpha^R)\oplus g^R(\beta^R)}\sum_{\gamma^C\in L^C}(-1)^{\gamma^C\cdot(\alpha_\pi^R\oplus\beta_\pi^R)}.\end{aligned}\tag{7.24}$$

Similarly,

$$\begin{aligned}C_{a+n,b+n}&=\sum_{c=1}^{n}M_{a+n,c}M_{b+n,c}(I_{m;\Lambda})_{c,c}\sum_{d=1}^{n}\sum_{e=1}^{n}M_{c,d+n}M_{d+n,e}(I_{m;\Lambda})_{e,e}\\&=\sum_{c,e\in\Lambda^R}H_{c,a}H_{c,b}\sum_{d=1}^{n}H_{c,d}H_{e,d},\end{aligned}$$

so taking $\alpha^C=\tau^C(a)$, $\beta^C=\tau^C(b)$, and $\gamma^R=\tau^R(c)$, we get

$$C_{a+n,b+n}=n(-1)^{g^C(\alpha^C)\oplus g^C(\beta^C)}\sum_{\gamma^R\in L^R}(-1)^{\gamma_\pi^R\cdot(\alpha^C\oplus\beta^C)}.\tag{7.25}$$

Let $\lambda^C=|L^C|$ and $\lambda^R=|L^R|$. We will now assume that $\mathrm{EVAL}(C,I_m,I_{m;\Lambda})$ is not #P-hard. Using this assumption, we will show that L^C and L^R are linear subspaces of $\mathbb{F}_2^k$, which implies that (L) is satisfied. We give the argument for L^C. The argument for L^R is symmetric.

If L^C is empty, then it is a linear subspace of $\mathbb{F}_2^k$, so assume that it is nonempty. Condition (R) guarantees that, since Λ^C is nonempty, $\rho^C(\mathbf{0})\in\Lambda^C$. Hence, $\mathbf{0}\in L^C$.

Let $\mathcal{L}$ be the subspace of $\mathbb{F}_2^k$ spanned by L^C. $\mathcal{L}$ contains all linear combinations of elements of L^C. We will show that $L^C=\mathcal{L}$, so L^C is a linear subspace of $\mathbb{F}_2^k$.

By (7.23), the matrix C is symmetric. By (7.24), we have $C_{a,a}=n\lambda^C$ for $a\in[n]$. Thus, by Lemma 6.4 (due to Bulatov and Grohe) $C_{a,b}\in\{-n\lambda^C,0,n\lambda^c\}$ for all $a,b\in[n]$. Otherwise, $\mathrm{EVAL}(C,I_m,I_{m;\Lambda})$ is #P-hard. Let $\chi=\alpha_\pi^R\oplus\beta_\pi^R$. Since $C_{a,b}\in\{-n\lambda^C,0,n\lambda^c\}$, (7.24) implies that for every such $\chi\in\mathbb{F}_2^k$,

$$\sum_{\gamma\in L^C}(-1)^{\gamma\cdot\chi}\in\{-\lambda^C,0,\lambda^C\}.$$

Since $\mathbf{0}\in L^C$, one of the items in the summation is $(-1)^{\mathbf{0}\cdot\xi}=1$, so the outcome $-\lambda^C$ is not possible. Therefore, we get

$$\sum_{\gamma\in L^C}(-1)^{\gamma\cdot\chi}\in\{0,\lambda^C\}\quad\text{for all }\chi\in\mathbb{F}_2^k.\tag{7.26}$$

Let $\Xi_0=\{\chi\in\mathbb{F}_2^k\mid\forall\gamma\in L^C,\ \chi\cdot\gamma=0\}$. If $\chi\in\Xi_0$, then $\chi\cdot\gamma=0$ for all $\gamma\in\mathcal{L}$. Otherwise, by the linearity of $\mathcal{L}$,

$$|\{\gamma\in\mathcal{L}:\chi\cdot\gamma=0\}|=|\{\gamma\in\mathcal{L}:\chi\cdot\gamma=1\}|.$$

Thus

$$\sum_{\gamma\in\mathcal{L}}(-1)^{\chi\cdot\gamma}=\begin{cases}|\mathcal{L}| & \text{if } \chi\in\Xi_0,\\ 0 & \text{otherwise.}\end{cases}$$

Hence (the characteristic functions of) the sets L^C and $\mathcal{L}$ have the same Fourier transform, up to scaling. It follows that $\mathcal{L}=L^C$ and L^C is a linear subspace of $\mathbb{F}_2^k$, as required.

Finally, note that it is easy, in polynomial time, given H, to construct C and to determine whether, for all $a,b\in[n]$, $C_{a,b}\in\{-n\lambda^C,0,n\lambda^c\}$ and $C_{n+a,n+b}\in\{-n\lambda^R,0,n\lambda^R\}$. Also, ϕ^R and ϕ^C can be found efficiently. Thus, it is easy, in polynomial time, to determine whether (L) holds. ∎

The following fact about linear maps will be useful later.

LEMMA 7.9. *Let $\phi:\mathbb{F}_2^\ell\to\mathbb{F}_2^k$ be a linear map. There is a surjective map $f:\mathbb{F}_2^k\to\mathbb{F}_2^\ell$ and a constant $z\in\mathbb{N}$ such that*

- $f(c_1,\dots,c_k)\cdot(x_1,\dots,x_\ell)=(c_1,\dots,c_k)\cdot\phi(x_1,\dots,x_\ell)$, *and*
- $\forall(c'_1,\dots,c'_\ell)$, $z=|\{(c_1,\dots,c_k)\mid f(c_1,\dots,c_k)=(c'_1,\dots,c'_\ell)\}|$.

Proof. Let B be the $\ell\times k$ matrix defining ϕ, i.e., $\phi(x_1,\dots,x_\ell)=(x_1,\dots,x_\ell)B$. Define f by $f(c_1,\dots,c_k)=(c_1,\dots,c_k)B^T$. Then, letting $\mathbf{x}$ denote the row vector $(x_1,\dots,x_\ell)$,

$$\begin{aligned}f(c_1,\dots,c_k)\cdot(x_1,\dots,x_\ell)&=f(c_1,\dots,c_k)\mathbf{x}^T\\&=(c_1,\dots,c_k)B^T\mathbf{x}^T\\&=(c_1,\dots,c_k)(\mathbf{x}B)^T\\&=(c_1,\dots,c_k)\cdot\phi(x_1,\dots,x_\ell).\end{aligned}$$

Fix any $\mathbf{c}'\in\mathbb{F}_2^\ell$ and any $\mathbf{c}\in\mathbb{F}_2^k$ such that $f(\mathbf{c})=\mathbf{c}'$. Note that

$$f^{-1}(\mathbf{c}')=\left\{\mathbf{c}+\mathbf{x}\mid\mathbf{x}\in\mathbb{F}_2^k,\ f(\mathbf{c}+\mathbf{x})=\mathbf{c}'\right\}.$$

As f is linear, we have $f(\mathbf{c}+\mathbf{x})=f(\mathbf{c})+f(\mathbf{x})=\mathbf{c}'+f(\mathbf{x})$, so $f^{-1}(\mathbf{c}')=\left\{\mathbf{c}+\mathbf{x}\mid\mathbf{x}\in\mathbb{F}_2^k,\ f(\mathbf{x})=\mathbf{0}\right\}$. Thus, we take $z=|\{\mathbf{x}\in\mathbb{F}_2^k\mid f(\mathbf{x})=\mathbf{0}\}|$. ∎

7.5. The degree condition. Let $X=(X_1,\dots,X_k)$. Every polynomial in $g(X_1,\dots,X_k)\in\mathbb{F}_2[X_1,\dots,X_k]$ can be written as a sum of distinct monomials of the form $X_{i_1}\cdot X_{i_2},\dots,X_{i_j}$ for $1\le i_1<\cdots<i_j\le k$. Given a polynomial $g(X)$, let $\#(g(X))=|\{\alpha\in\mathbb{F}_2^k\mid g(\alpha)=1\}|$. For $\alpha,\beta,\gamma\in\mathbb{F}_2^k$, let

$$g_{\alpha,\beta,\gamma}(X)=g(\alpha\oplus X)\oplus g(\beta\oplus X)\oplus\gamma\cdot X.$$

LEMMA 7.10. *Let $g\in\mathbb{F}_2[X_1,\dots,X_k]$ be of degree at least 3. Suppose that variables X_r, X_s, and X_t are contained in a monomial of degree at least 3. Let $\beta=\mathbf{0}$ and let $\alpha\in\mathbb{F}_2^k$ be the vector which is all zero except at index r. Then there are polynomials h, $h_{r,s}$, $h_{r,t}$, and h_r such that h is not identically 0 and*

$$\begin{aligned}g_{\alpha,\beta,\gamma}(X)=X_sX_th(X\setminus\{r,s,t\})\oplus X_sh_{r,s}(X\setminus\{r,s,t\})\oplus X_th_{r,t}(X\setminus\{r,s,t\})\\\oplus h_r(X\setminus\{r,s,t\})\oplus\gamma\cdot X\end{aligned}\tag{7.27}$$

for all $\gamma\in\mathbb{F}_2^k$.

Proof. Let Z denote the tuple $X\setminus\{r,s,t\}$. Let $h'(X)$ be the sum of all monomials of g that contain X_r, X_s, and X_t. Let $h(Z)$ be the polynomial satisfying $h'(X)=$

$X_rX_sX_th(Z)$. Note that $h(Z)$ is not identically zero. Choose $h_{r,s}$, $h_{r,t}$, $h_{s,t}$, h_r, h_s, h_t, and $h_\emptyset$ so that

$$g(X) = X_rX_sX_th(Z) \oplus X_rX_sh_{r,s}(Z) \oplus X_rX_th_{r,t}(Z) \oplus X_sX_th_{s,t}(Z) \\ \oplus X_rh_r(Z) \oplus X_sh_s(Z) \oplus X_th_t(Z) \oplus h_0(Z).$$

Then for α and β as defined in the statement of the lemma, we have

$$\begin{aligned} g(\alpha \oplus X) \oplus g(\beta \oplus X) &= g(\alpha \oplus X) \oplus g(X) \\ &= ((X_r \oplus 1)X_sX_t \oplus X_rX_sX_t)\, h(Z) \\ &\quad \oplus ((X_r \oplus 1)X_s \oplus X_rX_s)h_{r,s}(Z) \\ &\quad \oplus ((X_r \oplus 1)X_t \oplus X_rX_t)h_{r,t}(Z) \oplus h_r(Z) \\ &= X_sX_th(Z) \oplus X_sh_{r,s}(Z) \oplus X_th_{r,t}(Z) \oplus h_r(Z), \end{aligned}$$

which finishes the proof. ∎

LEMMA 7.11. *Let $g(X) \in \mathbb{F}_2[X_1, \ldots, X_k]$. The following are equivalent.*

1. *g has degree at most 2.*
2. *For all α and β in $\mathbb{F}_2^k$,*
   - *there is* exactly *one $\gamma \in \mathbb{F}_2^k$ such that $\#(g_{\alpha,\beta,\gamma}(X)) \in \{0, 2^k\}$, and*
   - *for all $\gamma' \neq \gamma$, $\#(g_{\alpha,\beta,\gamma'}(X)) = 2^{k-1}$.*

Also, if g has degree greater than 2, then there are α and β in $\mathbb{F}_2^k$ for which there is no $\gamma \in \mathbb{F}_2^k$ such that $\#(g_{\alpha,\beta,\gamma}(X)) \in \{0, 2^k\}$.

Proof. Suppose that g has degree at most 2. Let $g'(X) := g(\alpha \oplus X) \oplus g(\beta \oplus X)$. Consider any degree-2 term X_rX_s in g. In g', this term becomes $(X_r \oplus \alpha_r)(X_s \oplus \alpha_s) \oplus (X_r \oplus \beta_r)(X_s \oplus \beta_s)$. Now $(X_r \oplus \alpha_r)(X_s \oplus \alpha_s) = X_rX_s \oplus X_r\alpha_s \oplus \alpha_rX_s \oplus \alpha_r\alpha_s$, so the term X_rX_s cancels in g'. We conclude that $g'(X)$ is linear in $X_1, \ldots, X_k$ and part 2 holds.

Conversely, suppose that g has degree at least 3. Suppose that variables X_r, X_s, and X_t are contained in a monomial of degree at least 3. Let $\beta = \mathbf{0}$ and let $\alpha \in \mathbb{F}_2^k$ be the vector which is all zero except at index r. By Lemma 7.10, there are polynomials h, $h_{r,s}$, $h_{r,t}$, and h_r such that h is not identically 0 and

$$g_{\alpha,\beta,\gamma}(X) = X_sX_th(X \setminus \{r,s,t\}) \oplus X_sh_{r,s}(X \setminus \{r,s,t\}) \oplus X_th_{r,t}(X \setminus \{r,s,t\}) \\ \oplus h_r(X \setminus \{r,s,t\}) \oplus \gamma \cdot X.$$

Since h is not identically 0, the term $X_sX_th(X \setminus \{r,s,t\})$ does not cancel for any choice of γ. Hence, there is no γ such that $\#(g_{\alpha,\beta,\gamma}(X)) \in \{0, 2^k\}$, part 2 does not hold. ∎

LEMMA 7.12. *Let $g \in \mathbb{F}_2[X_1, \ldots, X_k]$. There is a $\gamma \in \mathbb{F}_2^k$ such that*

$$\#(g_{\alpha,\beta,\gamma}(X)) \neq 2^{k-1}.$$

Proof. Suppose, for contradiction, that $\#(g_{\alpha,\beta,\gamma}(X)) = 2^{k-1}$ for every $\gamma \in \mathbb{F}_2^k$. We thus have, for every $\gamma \in \mathbb{F}_2^k$,

$$0 = \sum_X (-1)^{g_{\alpha,\beta,\gamma}(X)} = \sum_X (-1)^{g_{\alpha,\beta,\mathbf{0}}(X)} \cdot (-1)^{\gamma \cdot X}. \tag{7.28}$$

For $x \in \mathbb{F}_2^k$, let $v_x(\gamma) = (-1)^{\gamma \cdot x}$ and let $\overline{v_x}$ be the length-2^k vector $(v_x(00\cdots0), \ldots, v_x(11\cdots1))$. The vectors in $\{\overline{v_x}\}$ are orthogonal, so they form a basis and any vector

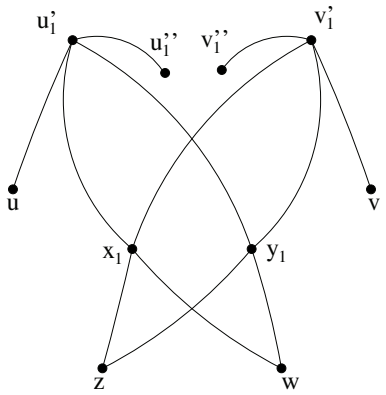

FIG. 7.2. *The lotus gadget for* $p = 1$.

in the corresponding vector space is uniquely expressible as a sum of these basis elements. In particular, the all zero vector $(0, \ldots, 0) = \sum_x c_x \overline{v_x}$ has $c_x = 0$ for all x. However, (7.28) implies $c_x = (-1)^{g_{\alpha,\beta},\mathbf{0}(x)} \in \{-1, 1\}$, which is a contradiction. ∎

COROLLARY 7.13. *Let* $g(X) \in \mathbb{F}_2[X_1, \ldots, X_k]$. *The following are equivalent.*

1. *g has degree at most* 2.
2. *For all* $\alpha \neq \beta$ *in* $\mathbb{F}_2^k$,

$$\text{there is at most one } \gamma \in \mathbb{F}_2^k \text{ such that } \#(g_{\alpha,\beta,\gamma}(X)) \in \{0, 2^k\}, \text{ and} \tag{7.29}$$

$$\text{for all } \gamma' \neq \gamma,\ \#(g_{\alpha,\beta,\gamma'}(X)) = 2^{k-1}. \tag{7.30}$$

Proof. If g has degree at most 2, then (2) holds by Lemma 7.11. Suppose that g has degree at least 3. Lemma 7.11 provides an α and β such that there is no γ such that $\#(g_{\alpha,\beta,\gamma}(X)) \in \{0, 2^k\}$. So to prove the theorem we just have to rule out the case that every γ satisfies $\#(g_{\alpha,\beta,\gamma}(X)) = 2^{k-1}$ for this choice of α and β, and this is ruled out by Lemma 7.12. ∎

Proof of Lemma 2.6*, the Degree Lemma.* Let H be an $n \times n$ Hadamard matrix and $\Lambda^R, \Lambda^C \subseteq [n]$ subsets of indices. Let M, Λ be the bipartization of H, Λ^R, and Λ^C and let $m = 2n$. Suppose that (GC), (R), and (L) are satisfied. For integers p we will construct a matrix $C^{[p]}$ and a reduction $\text{EVAL}(C^{[p]}) \leq \text{EVAL}(M, I_m, I_{m;\Lambda})$. We will show that if (D) does not hold, then there is a p such that $\text{EVAL}(C^{[p]})$ is #P-hard.

The reduction is as follows. Let $G = (V, E)$ be an input to $\text{EVAL}(C^{[p]})$. We construct an input G' to $\text{EVAL}(M, I_m, I_{m;\Lambda})$ as follows. Each edge $\{u, v\} \in E$ corresponds to a "lotus" gadget in G'. The vertex set of the gadget is $\{u, v, u_i', v_i', u_i'', v_i'', x_i, y_i, z, w \mid i \in [p]\}$. See Figure 7.2 for an illustration of the lotus gadget for $p = 1$. The gadget has the following edges for all $i \in [p]$: $\{z, x_i\}$, $\{w, x_i\}$, $\{z, y_i\}$, $\{w, y_i\}$, $\{u, u_i'\}$, $\{u_i', u_i''\}$, $\{x_i, u_i'\}$, $\{x_i, v_i'\}$, $\{v, v_i'\}$, $\{v_i', v_i''\}$, $\{y_i, u_i'\}$, and $\{y_i, v_i'\}$.

Note that the vertices of the gadget have the following degrees:

$$\begin{gathered} d(u_i'') = d(v_i'') = 1, \\ d(u_i') = d(v_i') = d(x_i) = d(y_i)) = 4, \\ d(z) = d(w) = 2p. \end{gathered}$$

Furthermore, for the "boundary" vertices u, v we have

$$d_{G'}(u) = p \cdot d_G(u), \quad d_{G'}(v) = p \cdot d_G(v).$$

We will stipulate that p is even. Then the degree of the vertices, except for the u_i'' and v_i'', is even.

Now let us construct the matrix $C^{[p]}$. Let Γ denote the graph with vertices u and v and a single edge between them. Clearly, $C^{[p]}_{a,b}$ is equal to the contribution to $Z_{M,I_m,I_{m;\Lambda}}(\Gamma')$ corresponding to those configurations ξ with $\xi(u) = a$ and $\xi(v) = b$.

By (R), there are bijective index mappings $\rho^R : \mathbb{F}_2^k \to [n]$ and $\rho^C : \mathbb{F}_2^k \to [n]$ and a permutation $\pi \in S_k$ such that (with respect to ρ^R and ρ^C) the matrix H is represented by the polynomial $h(X,Y) = X_\pi Y \oplus g^R(X) \oplus g^C(Y)$. Let τ^R be the inverse of ρ^R and τ^C be the inverse of ρ^C. Let $L^C = \tau^C(\Lambda^C)$ and $L^R = \tau^R(\Lambda^R)$. By condition (L) we know that the sizes of L^R and L^C are powers of 2. Let $|L^R| = 2^{\ell^R}$ and let $|L^C| = 2^{\ell^C}$. If Λ^R is nonempty, then let $\phi^R : \mathbb{F}_2^{\ell^R} \to \mathbb{F}_2^k$ be a coordinatization of Λ^R with respect to ρ^R. Similarly, if Λ^C is nonempty, let ϕ^C be a coordinatization of Λ^C with respect to ρ^C. Let $\phi^C = \phi^R$ if $\Lambda^C = \Lambda^R$ and this is nonempty and H is symmetric. Note that if Λ^C and Λ^R are empty, then (D) is satisfied.

Let Γ_i be the subgraph of Γ' induced by $\{u, x_i, y_i, u_i', u_i''\}$. For $\alpha, \gamma, \delta \in \mathbb{F}_2^k$, let $a^R = \rho^R(\alpha)$, $c^R = \rho^R(\gamma)$, and $d^R = \rho^R(\delta)$. Let $Z^R(\alpha,\gamma,\delta)$ denote the contribution to $Z_{M,I_m,I_{m;\Lambda}}(\Gamma_i)$ corresponding to those configurations ξ with $\xi(u) = a^R$, $\xi(x_i) = c^R$, and $\xi(y_i) = d^R$, ignoring contributions due to $I_{m;\Lambda}$ for vertices u, x_i, and y_i. (We ignore these contributions because these vertices will have even degree in G', so these contributions will cancel when we use $Z(\alpha,\beta,\gamma)$.) Using $n + a'$ to denote the spin at u_i' (which must be in the range $\{n+1,\dots,2n\}$; otherwise the contribution is zero) and a'' to denote the spin at u_i'' (which must be in $[n]$), we get

$$\begin{aligned} Z^R(\alpha,\gamma,\delta) &= \sum_{a'=1}^{n}\sum_{a''=1}^{n} M_{a^R,n+a'} M_{n+a',a''} M_{c^R,n+a'} M_{d^R,n+a'} (I_{m;\Lambda})_{a'',a''} \\ &= \sum_{a''\in\Lambda^R}\sum_{a'=1}^{n} H_{a^R,a'} H_{a'',a'} H_{c^R,a'} H_{d^R,a'}. \end{aligned}$$

Plugging in the representation of H where $\rho^R(\phi^R(\mu))$ is the spin $a'' \in \Lambda^R$, we get the following:

$$Z^R(\alpha,\gamma,\delta) = (-1)^{g^R(\alpha)\oplus g^R(\gamma)\oplus g^R(\delta)} \sum_{\mu\in\mathbb{F}_2^{\ell^R}} (-1)^{g^R(\phi^R(\mu))} \sum_{\alpha'\in\mathbb{F}_2^k} (-1)^{\alpha'\cdot(\alpha_\pi \oplus \phi^R(\mu)_\pi \oplus \gamma_\pi \oplus \delta_\pi)}.$$

Note that

$$\sum_{\alpha'\in\mathbb{F}_2^k} (-1)^{\alpha'\cdot(\alpha_\pi \oplus \phi^R(\mu)_\pi \oplus \gamma_\pi \oplus \delta_\pi)} = \begin{cases} n & \text{if } \phi^R(\mu)_\pi = \alpha_\pi \oplus \gamma_\pi \oplus \delta_\pi, \\ 0 & \text{otherwise.} \end{cases}$$

Equivalently,

$$\sum_{\alpha'\in\mathbb{F}_2^k} (-1)^{\alpha'\cdot(\alpha_\pi \oplus \phi^R(\mu)_\pi \oplus \gamma_\pi \oplus \delta_\pi)} = \begin{cases} n & \text{if } \phi^R(\mu) = \alpha \oplus \gamma \oplus \delta, \\ 0 & \text{otherwise.} \end{cases}$$

Thus, $Z^R(\alpha,\gamma,\delta) = 0$ unless $\alpha \oplus \gamma \oplus \delta \in L^R$, and in this case,

$$Z^R(\alpha,\gamma,\delta) = n(-1)^{g^R(\alpha)\oplus g^R(\gamma)\oplus g^R(\delta)\oplus g^R(\alpha\oplus\gamma\oplus\delta)}. \tag{7.31}$$

Our strategy for the rest of the proof is the following: The goal is to prove that either there is a p such that EVAL($C^{[p]}$) is #P-hard or the following two conditions are satisfied.

Row condition. Either Λ^R is empty or the polynomial $g^R \circ \phi^R$ has degree at most 2.

Column condition. Either Λ^C is empty or the polynomial $g^C \circ \phi^C$ has degree at most 2.

Let us turn to the row condition first. Suppose that Λ^R is nonempty; otherwise there is nothing to prove. Let $a, b \in \Lambda^R$. Define α^R and β^R in $\mathbb{F}_2^{\ell^R}$ so that $\phi^R(\alpha^R) = \tau^R(a)$ and $\phi^R(\beta^R) = \tau^R(b)$. Note that the contribution to $Z_{M,I_m,I_m;\Lambda}(\Gamma')$ of a configuration ξ with $\xi(u) = a$ and $\xi(v) = b$ is zero unless the spins of vertices u_i', v_i', z, and w are in $\{n+1, \dots, 2n\}$ and the rest of the spins are in $[n]$. Then taking $\rho^C(\varepsilon) + n$ as the spin of z and $\rho^C(\zeta) + n$ as the spin of w, we get

$$\begin{aligned} C_{a,b}^{[p]} &= \sum_{\varepsilon,\zeta \in \mathbb{F}_2^k} \prod_{i=1}^{p} \left(\sum_{\gamma_i,\delta_i \in \mathbb{F}_2^k} Z^R(\phi^R(\alpha^R), \gamma_i, \delta_i) Z^R(\phi^R(\beta^R), \gamma_i, \delta_i) (-1)^{((\gamma_i)_\pi \oplus (\delta_i)_\pi)\cdot(\varepsilon \oplus \zeta)} \right) \\ &= \sum_{\varepsilon,\zeta \in \mathbb{F}_2^k} \left(\sum_{\gamma,\delta \in \mathbb{F}_2^k} Z^R(\phi^R(\alpha^R), \gamma, \delta) Z^R(\phi^R(\beta^R), \gamma, \delta) (-1)^{(\gamma_\pi \oplus \delta_\pi)\cdot(\varepsilon \oplus \zeta)} \right)^p. \end{aligned}$$

From (7.31) we find that if we take any γ' and δ' such that $\gamma' \oplus \delta' = \gamma \oplus \delta$, then $Z^R(\alpha, \gamma, \delta) Z^R(\beta, \gamma, \delta) = Z^R(\alpha, \gamma', \delta') Z^R(\beta, \gamma', \delta')$ for any α and β. Thus, we can simplify the expression using ψ to denote $\varepsilon \oplus \zeta$ and η to denote $\gamma \oplus \delta$.

$$\begin{aligned} C_{a,b}^{[p]} &= n \sum_{\psi \in \mathbb{F}_2^k} \left(\sum_{\gamma,\delta \in \mathbb{F}_2^k} Z^R(\phi^R(\alpha^R), \gamma, \delta) Z^R(\phi^R(\beta^R), \gamma, \delta) (-1)^{(\gamma_\pi \oplus \delta_\pi)\cdot\psi} \right)^p \\ &= n \sum_{\psi \in \mathbb{F}_2^k} \left(n \sum_{\eta \in \mathbb{F}_2^k} Z^R(\phi^R(\alpha^R), \eta, \mathbf{0}) Z^R(\phi^R(\beta^R), \eta, \mathbf{0}) (-1)^{\eta_\pi \cdot \psi} \right)^p \\ &= n^{p+1} \sum_{\psi \in \mathbb{F}_2^k} \left(\sum_{\eta \in \mathbb{F}_2^k} Z^R(\phi^R(\alpha^R), \eta, \mathbf{0}) Z^R(\phi^R(\beta^R), \eta, \mathbf{0}) (-1)^{\eta_\pi \cdot \psi} \right)^p. \end{aligned}$$

Now, by (7.31), the contribution for a given η is 0 unless $\phi^R(\alpha^R) \oplus \eta$ and $\phi^R(\beta^R) \oplus \eta$ are in L^R. But $\phi^R(\alpha^R)$ and $\phi^R(\beta^R)$ are in L^R, so by (L), the contribution for a given η is nonzero exactly when $\eta \in L^R$. Thus, we can use (7.31) to simplify, writing η as $\phi^R(\mu)$:

$$\begin{aligned} C_{a,b}^{[p]} &= n^{p+1} \sum_{\psi \in \mathbb{F}_2^k} \left(\sum_{\eta \in L^R} n^2 (-1)^{g^R(\phi^R(\alpha^R)) \oplus g^R(\phi^R(\beta^R)) \oplus g^R(\phi^R(\alpha^R) \oplus \eta) \oplus g^R(\phi^R(\beta^R) \oplus \eta) \oplus \eta_\pi \cdot \psi} \right)^p \\ &= n^{3p+1} \Big((-1)^{g^R(\phi^R(\alpha^R)) \oplus g^R(\phi^R(\beta^R))} \Big)^p \\ &\quad \times \sum_{\psi \in \mathbb{F}_2^k} \left(\sum_{\mu \in \mathbb{F}_2^{\ell^R}} (-1)^{g^R(\phi^R(\alpha^R) \oplus \phi^R(\mu)) \oplus g^R(\phi^R(\beta^R) \oplus \phi^R(\mu)) \oplus \phi^R(\mu)_\pi \cdot \psi} \right)^p. \end{aligned}$$

Since p is even, we have $((-1)^{g^R(\phi^R(\alpha^R))\oplus g^R(\phi^R(\beta^R))})^p = 1$. Using the linearity of ϕ^R and inverting π, we further simplify as follows:

$$C^{[p]}_{a,b} = n^{3p+1} \sum_{\psi\in\mathbb{F}_2^k} \left(\sum_{\mu\in\mathbb{F}_2^{\ell^R}} (-1)^{g^R(\phi^R(\alpha^R\oplus\mu))\oplus g^R(\phi^R(\beta^R\oplus\mu))\oplus\phi^R(\mu)\cdot\psi_{\pi^{-1}}} \right)^p$$
$$= n^{3p+1} \sum_{\chi\in\mathbb{F}_2^k} \left(\sum_{\mu\in\mathbb{F}_2^{\ell^R}} (-1)^{g^R\phi^R(\alpha^R\oplus\mu)\oplus g^R\phi^R(\beta^R\oplus\mu)\oplus\phi^R(\mu)\cdot\chi} \right)^p.$$

Since ϕ^R is linear, by Lemma 7.9, there are a surjective map $f : \mathbb{F}_2^k \to \mathbb{F}_2^{\ell^R}$ and a constant $\kappa^R \in \mathbb{N}$ such that $\phi^R(\mu)\cdot\chi = f(\chi)\cdot\mu$ and for any $\gamma \in \mathbb{F}_2^{\ell^R}$ the number of χ with $f(\chi) = \gamma$ is κ^R, so we can simplify:

$$C^{[p]}_{a,b} = n^{3p+1}\kappa^R \sum_{\gamma\in\mathbb{F}_2^{\ell^R}} \left(\sum_{\mu\in\mathbb{F}_2^{\ell^R}} (-1)^{g^R\phi^R(\alpha^R\oplus\mu)\oplus g^R\phi^R(\beta^R\oplus\mu)\oplus\mu\cdot\gamma} \right)^p.$$

Let

$$\widehat{C}^{[p]} = \frac{C^{[p]}}{n^{3p+1}\cdot\kappa^R}.$$

Clearly $\mathrm{EVAL}(C^{[p]}) \equiv \mathrm{EVAL}(\widehat{C}^{[p]})$. We will now show that $g^R\circ\phi^R$ has degree at most 2 or there is an even p such that $\mathrm{EVAL}(\widehat{C}^{[p]})$ is #P-hard. First note that $\widehat{C}^{[p]}$ is symmetric and

$$\widehat{C}^{[p]}_{a,a} = \sum_{\gamma\in\mathbb{F}_2^{\ell^R}} \left(\sum_{\mu\in\mathbb{F}_2^{\ell^R}} (-1)^{\mu\cdot\gamma} \right)^p = 2^{\ell^R p}.$$

For $X = (X_1,\ldots,X_{\ell^R})$ and $a,b\in\Lambda^R$ and $\gamma\in\mathbb{F}_2^{\ell^R}$, define the polynomial

$$\tilde{g}_{a,b,\gamma}(X) = g^R\circ\phi^R(\alpha^R\oplus X)\oplus g^R\circ\phi^R(\beta^R\oplus X)\oplus\gamma\cdot X.$$

For all $a,b\in\Lambda^R$ we define

$$\mathcal{C}_{a,b} := \left\{\gamma\in\mathbb{F}_2^{\ell^R} \mid \#(\tilde{g}_{a,b,\gamma}(X)) \in \left\{0, 2^{\ell^R}\right\}\right\},$$
$$\mathcal{G}_{a,b} := \left\{\gamma\in\mathbb{F}_2^{\ell^R} \mid \#(\tilde{g}_{a,b,\gamma}(X)) \notin \left\{0, 2^{\ell^R-1}, 2^{\ell^R}\right\}\right\},$$
$$\mathcal{H}_{a,b} := \left\{\gamma\in\mathbb{F}_2^{\ell^R} \mid \#(\tilde{g}_{a,b,\gamma}(X)) = 2^{\ell^R-1}\right\},$$

where $\#(\tilde{g}_{a,b,\gamma}(X))$ denotes the number of $x\in\mathbb{F}_2^{\ell^R}$ such that $\tilde{g}_{a,b,\gamma}(x) = 1$.

For every $\gamma\in\mathcal{G}_{a,b}$ define $z_{a,b,\gamma} := \sum_{\mu\in\mathbb{F}_2^{\ell^R}}(-1)^{\tilde{g}_{a,b,\gamma}(\mu)}$, which, by definition, satisfies $z_{a,b,\gamma}\neq 0$ and $|z_{a,b,\gamma}| < 2^{\ell^R}$. Let $z^{\max}_{a,b} = \max_{\gamma\in\mathcal{G}_{a,b}}|z_{a,b,\gamma}|$ and $z^{\min}_{a,b} =$

$\min_{\gamma\in\mathcal{G}_{a,b}}|z_{a,b,\gamma}|$. For $a,b\in\Lambda^R$, we can simplify the expression for $\widehat{C}^{[p]}_{a,b}$:

$$\widehat{C}^{[p]}_{a,b}=\sum_{\gamma\in\mathbb{F}_2^{\ell^R}}\left(\sum_{\mu\in\mathbb{F}_2^{\ell^R}}(-1)^{\tilde{g}_{a,b,\gamma}(\mu)}\right)^p=\left(\sum_{\gamma\in\mathcal{C}_{a,b}}2^{\ell^R p}+\sum_{\gamma\in\mathcal{G}_{a,b}}(z_{a,b,\gamma})^p+\sum_{\gamma\in\mathcal{H}_{a,b}}0\right)$$
$$=\left(|\mathcal{C}_{a,b}|2^{\ell^R p}+\sum_{\gamma\in\mathcal{G}_{a,b}}(z_{a,b,\gamma})^p\right).$$

Since p is even, $(z_{a,b,\gamma})^p$ is positive for all $\gamma\in\mathcal{G}_{a,b}$, and thus $\widehat{C}^{[p]}_{a,b}$ is nonnegative for all $a,b\in\Lambda^R$. If Λ^R is empty, then the relevant condition in (D) is satisfied, so suppose that it is nonempty. We will now show that $g^R\circ\phi^R$ has degree at most 2 or there exists an even p such that $\widehat{C}^{[p]}$ has a block of rank at least two.

Case A. *There are $a,b\in\Lambda^R$ such that $\mathcal{G}_{a,b}\neq\emptyset$.* Choose such a,b. The principal 2×2 submatrix of $\widehat{C}^{[p]}$, defined by a and b, has determinant

$$\begin{vmatrix}\widehat{C}^{[p]}_{a,a} & \widehat{C}^{[p]}_{a,b}\\ \widehat{C}^{[p]}_{b,a} & \widehat{C}^{[p]}_{b,b}\end{vmatrix}=\begin{vmatrix}2^{\ell^R p} & \widehat{C}^{[p]}_{a,b}\\ \widehat{C}^{[p]}_{a,b} & 2^{\ell^R p}\end{vmatrix}=2^{2\ell^R p}-(\widehat{C}^{[p]}_{a,b})^2. \tag{7.32}$$

If the determinant is zero, then $\widehat{C}^{[p]}_{a,b}/2^{\ell^R p}=1$. We consider two cases. If $\mathcal{C}_{a,b}=\emptyset$, then

$$\begin{aligned}\frac{\widehat{C}^{[p]}_{a,b}}{2^{\ell^R p}}&=\frac{\left(\sum_{\gamma\in\mathcal{G}_{a,b}}(z_{a,b,\gamma})^p\right)}{2^{\ell^R p}}\\ &\le\frac{|\mathcal{G}_{a,b}|(z^{\max}_{a,b})^p}{2^{\ell^R p}}\\ &\le 2^{\ell^R}\left(\frac{z^{\max}_{a,b}}{2^{\ell^R}}\right)^p\\ &\le 2^{\ell^R}\left(\frac{2^{\ell^R}-1}{2^{\ell^R}}\right)^p\qquad\qquad(\text{because } z^{\max}_{a,b}<2^{\ell^R})\\ &\le 2^{\ell^R}\cdot e^{-p/2^{\ell^R}}.\end{aligned}$$

This is less than one for all $p>\ell^R 2^{\ell^R}$. Hence the determinant (7.32) is nonzero. Furthermore, as $\mathcal{G}_{a,b}\neq\emptyset$ we have $\widehat{C}^{[p]}_{a,b}\neq 0$, and hence $\widehat{C}^{[p]}$ contains a block of rank at least two. This implies the #P-hardness of EVAL($\widehat{C}^{[p]}$) by Lemma 6.4. (Recall that $\widehat{C}^{[p]}_{a,b}$ is nonnegative since $a,b\in\Lambda^R$.)

For the other case, suppose $|\mathcal{C}_{a,b}|\ge 1$. Then

$$\begin{aligned}\frac{\widehat{C}^{[p]}_{a,b}}{2^{\ell^R p}}&=2^{-\ell^R p}\left(|\mathcal{C}_{a,b}|2^{\ell^R p}+\sum_{\gamma\in\mathcal{G}_{a,b}}(z_{a,b,\gamma})^p\right)\\ &\ge 2^{-\ell^R p}\left(|\mathcal{C}_{a,b}|2^{\ell^R p}+|\mathcal{G}_{a,b}|(z^{\min}_{a,b})^p\right)\\ &>|\mathcal{C}_{a,b}|\ge 1.\end{aligned}$$

Here, the second-to-last inequality holds, because $z^{\min}_{a,b} > 0$ and (by the precondition of Case A) $\mathcal{G}_{a,b} \neq \emptyset$. Hence again we have $\frac{\widehat{C}^{[p]}_{a,b}}{2^{\ell^R p}} \neq 1$, and the determinant (7.32) is nonzero. As in the first case, this implies the #P-hardness of EVAL($\widehat{C}^{[p]}$).

Case B. *For all $a, b \in \Lambda^R$ it holds that $\mathcal{G}_{a,b} = \emptyset$.* Then for all $a, b \in \Lambda^R$ we have

$$\widehat{C}^{[p]}_{a,b} = |\mathcal{C}_{a,b}| 2^{\ell^R p} + \sum_{\gamma \in \mathcal{G}_{a,b}} z^p_{a,b,\gamma} = |\mathcal{C}_{a,b}| 2^{\ell^R p}.$$

So the principal 2×2 submatrix of $\widehat{C}^{[p]}$ defined by a, b has determinant

$$\begin{vmatrix} \widehat{C}^{[p]}_{a,a} & \widehat{C}^{[p]}_{a,b} \\ \widehat{C}^{[p]}_{b,a} & \widehat{C}^{[p]}_{b,b} \end{vmatrix} = \begin{vmatrix} 2^{\ell^R p} & 2^{\ell^R p} |\mathcal{C}_{a,b}| \\ 2^{\ell^R p} |\mathcal{C}_{a,b}| & 2^{\ell^R p} \end{vmatrix} = 2^{2\ell^R p}(1 - |\mathcal{C}_{a,b}|^2).$$

This determinant is zero if and only if $|\mathcal{C}_{a,b}| = 1$, and the submatrix is part of a block if and only if $\mathcal{C}_{a,b} \neq \emptyset$. Hence, we have #P-hardness by Lemma 6.4 if there are $a, b \in \Lambda^R$ such that $|\mathcal{C}_{a,b}| \notin \{0, 1\}$. Assume that for all $a, b \in \Lambda^R$ we have $|\mathcal{C}_{a,b}| \in \{0, 1\}$. Define sets

$$\mathcal{I} := \left\{(a, b) \mid a \in \Lambda^R, b \in \Lambda^R, |\mathcal{C}_{a,b}| = 1, a \neq b\right\},$$
$$\mathcal{Z} := \left\{(a, b) \mid a \in \Lambda^R, b \in \Lambda^R, |\mathcal{C}_{a,b}| = 0,\ a \neq b\right\}.$$

Obviously, these form a partition of pairs of distinct elements in Λ^R. In other words, for all $a \neq b \in \Lambda^R$ there is at most one $\gamma \in \mathbb{F}_2^{\ell^R}$ such that $\#(\tilde{g}_{a,b,\gamma}(X)) \in \{0, 2^{\ell^R}\}$. Furthermore, $\mathcal{G}_{a,b} = \emptyset$ implies that for all other $\gamma' \neq \gamma$ we have $\#(\tilde{g}_{a,b,\gamma'}(X)) = 2^{\ell^R - 1}$. But Corollary 7.13 implies that in this case $g^R \circ \phi^R$ has degree at most two. This finishes Case B and hence the proof of the row condition.

For the column condition, in a symmetric way to how we defined $Z^R(\alpha, \gamma, \delta)$, we let $Z^C(\alpha, \gamma, \delta)$ denote the contribution to $Z_{M,I_m,I_m;\Lambda}(\Gamma_i)$ corresponding to those configurations ξ with $\xi(u) = n + a^C$, $\xi(x_i) = n + c^C$, and $\xi(y_i) = n + d^C$, ignoring contributions due to $I_{m;\Lambda}$ for vertices u, x_i, and y_i. Using this, we can compute $C^{[p]}_{n+a,n+b}$ for $a, b \in \Lambda^C$ and show that, if Λ^C is nonempty, then either $g^C \phi^C$ has degree at most 2 or EVAL($C^{[p]}$) is #P-hard.

Finally, we note that it is straightforward, in polynomial time, to determine whether EVAL($C^{[p]}$) is #P-hard or (D) holds. ∎

COROLLARY 7.14. *Let H be a symmetric $n \times n$ Hadamard matrix and $\Lambda^R = \Lambda^C \subseteq [n]$ identical subsets of indices. If H is positive for Λ^R and Λ^C, then* EVAL($H, I_n, I_{n;\Lambda^R}$) *is polynomial-time computable if and only if H Λ^R and Λ^C satisfy the group condition* (GC) *and conditions* (R), (L), *and* (D). *Otherwise* EVAL($H, I_n, I_{n;\Lambda^R}$) *is* #P*-hard. If H is not positive for Λ^R and Λ^C, then* EVAL($H, I_n, I_{n;\Lambda^R}$) *is polynomial-time computable if and only if $-H$ Λ^R and Λ^C satisfy the group condition* (GC) *and conditions* (R), (L), *and* (D). *Otherwise* EVAL($H, I_n, I_{n;\Lambda^R}$) *is* #P*-hard.*

Proof. By the equivalence of EVAL($H, I_n, I_{n;\Lambda^R}$) and EVAL($-H, I_n, I_{n;\Lambda^R}$) we can assume that H is positive for Λ^R and Λ^C. Let M, Λ be the bipartization of H, Λ^R, and Λ^C and let $m = 2n$. First, suppose that one of the conditions is not satisfied. By Theorem 2.2, EVAL($M, I_m, I_{m;\Lambda}$) is #P-hard. Since M is bipartite, EVAL($M, I_m, I_{m;\Lambda}$) remains #P-hard when restricted to connected bipartite instances G. But for these instances, $Z_{M,I_m,I_{m;\Lambda}}(G) = 2Z_{H,I_n,I_{n;\Lambda^R}}(G)$, so EVAL($H, I_n, I_{n;\Lambda^R}$) is #P-hard.

It remains to give the proof for the tractability part. For symmetric H and $\Lambda^R = \Lambda^C$ satisfying (GC), (R), (L), and (D), we shall show how to compute $Z_{H,I_n,I_{n;\Lambda^R}}(G)$ for an input graph G in polynomial time. Let $V_o \subseteq V$ denote the set of odd-degree vertices of G and $V_e = V \setminus V_o$. We have

$$\begin{aligned} Z_{H,I_n,I_{n;\Lambda^R}}(G) &= \sum_{\xi:V\to[n]} \prod_{\{u,v\}\in E} H_{\xi(u),\xi(v)} \prod_{v\in V_o} (I_{n;\Lambda^R})_{\xi(v),\xi(v)} \\ &= \sum_{\substack{\xi:V\to[n] \\ \xi(V^o)\subseteq\Lambda^R}} \prod_{\{u,v\}\in E} H_{\xi(u),\xi(v)}. \end{aligned}$$

Fix a configuration $\xi : V \to [n]$ and let $\rho = \rho^R = \rho^C$ be the index mapping and h the $\mathbb{F}_2$-polynomial representing H as given in condition (R). Let, furthermore, $\phi := \phi^R = \phi^C$ be the coordinatization of Λ^R as given in condition (D). Let τ be the inverse of ρ and $L = \tau(\Lambda^R)$. Then ξ induces a configuration $\varsigma : V \to \mathbb{F}_2^k$ defined by $\varsigma = \tau \circ \xi$, which implies for all $u, v \in V$ that $h(\varsigma(u), \varsigma(v)) = 1$ if and only if $H_{\xi(u),\xi(v)} = -1$. We can simplify:

(7.33)
$$Z_{H,I_n,I_{n;\Lambda^R}}(G) = \sum_{\substack{\xi:V\to[n] \\ \xi(V_o)\subseteq\Lambda^R}} \prod_{\{u,v\}\in E} (-1)^{h(\tau\circ\xi(u),\tau\circ\xi(v))} = \sum_{\substack{\varsigma:V\to\mathbb{F}_2^k \\ \varsigma(V_o)\subseteq L}} (-1)^{\bigoplus_{\{u,v\}\in E} h(\varsigma(u),\varsigma(v))}.$$

Define for each $v \in V$ a tuple $X^v = (X_1^v, \ldots, X_k^v)$ and an $\mathbb{F}_2$-polynomial

$$h_G = \bigoplus_{\{u,v\}\in E} h(X^u, X^v).$$

Let $\mathrm{var}(h_G)$ denote the set of variables in h_G and, for mappings $\chi : \mathrm{var}(h_G) \to \mathbb{F}_2$, we use the expression $\chi(X^v) := (\chi(X_1^v), \ldots, \chi(X_k^v))$ as shorthand. Define $h_G(\chi) := \bigoplus_{\{u,v\}\in E} h(\chi(X^u), \chi(X^v))$ and note that this is a sum in $\mathbb{F}_2$.

For $a \in \mathbb{F}_2$ let

$$s_a := |\{\chi : \mathrm{var}(h_G) \to \mathbb{F}_2 \mid \chi(X^v) \in L \text{ for all } v \in V_o \text{ and } h_G(\chi) = a\}|. \tag{7.34}$$

Hence, by (7.33), $Z_{H,I_n,I_{n;\Lambda^R}}(G) = s_0 - s_1$. It remains therefore to show how to compute the values s_a. Clearly,

$$h_G = \bigoplus_{\{u,v\}\in E} (X^u)_\pi X^v \oplus g(X^u) \oplus g(X^v) = \bigoplus_{\{u,v\}\in E} (X^u)_\pi X^v \oplus \bigoplus_{v\in V_o} g(X^v),$$

as the term $g(X^v)$ occurs exactly $\deg(v)$ many times in the above expression and thus these terms cancel for all even degree vertices.

By (7.34) we are interested only in those assignments χ which satisfy $\chi(X^v) \in L$ for all $v \in V_o$. With $|\Lambda^R| = 2^l$ for some appropriate l, we introduce variable vectors $Y^v = (Y_1^v, \ldots, Y_l^v)$ for all $v \in V_o$. If $u \in V_o$ or $v \in V_o$, then we can express the term $(X^u)_\pi X^v$ in h_G in terms of these new variables. In particular, let

$$h''_G = \bigoplus_{\substack{\{u,v\}\in E \\ u,v\in V_o}} (\phi(Y^u))_\pi \cdot \phi(Y^v) \oplus \bigoplus_{\substack{\{u,v\}\in E \\ u,w\in V_e}} (X^u)_\pi \cdot X^v \oplus \bigoplus_{\substack{\{u,v\}\in E \\ u\in V_o, v\in V_e}} (\phi(Y^u))_\pi \cdot X^v.$$

Let

$$h'_G = h''_G \oplus \bigoplus_{v \in V^o} \oplus g(\phi(Y^v)).$$

Then we see that

$$s_a := |\{\chi : \mathrm{var}(h'_G) \to \mathbb{F}_2 \mid h'_G(\chi) = a\}|. \tag{7.35}$$

By condition (D) $g \circ \phi$ is a polynomial of degree at most 2, and therefore h'_G is a polynomial of degree at most 2. Furthermore, we have expressed s_a as the number of solutions to a polynomial equation over $\mathbb{F}_2$. Therefore, as in the proof of Theorem 2.2, the proof now follows by Fact 2.7. □

Proof of Theorem 1.2. Let H be a symmetric $n \times n$ Hadamard matrix and $\Lambda^R = \Lambda^C = [n]$. Then H is positive for Λ^R and Λ^C. Let M, Λ be the bipartization of H, Λ^R, Λ^C.

Suppose first that H has no quadratic representation. Then there are no index mapping $\rho = \rho^R = \rho^C$ and coordinatization $\phi = \phi^R = \phi^C$ such that conditions (R) and (D) are satisfied. Hence by Theorem 2.2, EVAL$(M, I_m, I_{m;\Lambda})$ is #P-hard. Since M is bipartite, EVAL$(M, I_m, I_{m;\Lambda})$ remains #P-hard when restricted to connected bipartite instances G. But for these instances, $Z_{M,I_m,I_m}(G) = 2Z_{H,I_n,I_n}(G)$, so EVAL$(H, I_n, I_n)$ is #P-hard. Suppose next that H has a quadratic representation with index mapping $\rho : \mathbb{F}_2^k \to [n]$ and polynomial $h(X, Y)$. Instead of going through Theorem 2.2, it is easier to prove the tractability of EVAL(H) directly along the lines of the proof of the tractability part of the theorem. We leave the details to the reader. This is similar to the tractability part of the proof of Corollary 7.14. □

8. The proofs for section 3.

8.1. Technical preliminaries.

LEMMA 8.1. *Let $C \in \mathbb{R}_{\mathbb{A}}^{m \times m}$ be a symmetric matrix and let Δ^+ and Δ^- be diagonal $m \times m$ matrices. Let D be the componentwise sum $D = \Delta^+ + \Delta^-$ and let $O = \Delta^+ - \Delta^-$. Let A be the tensor product*

$$A = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes C.$$

Let Δ be the $2m \times 2m$ matrix such that, for all $i \in [m]$ and $j \in [m]$, $\Delta_{i,j} = \Delta^+_{i,j}$, $\Delta_{i,m+j} = \Delta_{m+i,j} = 0$, and $\Delta_{m+i,m+j} = \Delta^-_{i,j}$. Then

$$Z_{C,D,O}(G) = Z_{A,\Delta}(G) \text{ for all graphs } G.$$

Proof. It is useful to think of A and Δ in terms of four $m \times m$ tiles as follows:

$$A = \begin{pmatrix} C & -C \\ -C & C \end{pmatrix} \text{ and } \Delta = \begin{pmatrix} \Delta^+ & 0 \\ 0 & \Delta^- \end{pmatrix}.$$

We will simplify the expression for $Z_{A,\Delta}(G)$ now. Let $\xi : V \to [2m]$ be a map such that, for some $w \in V$, $\xi(w) \in [m]$. Let ψ be the mapping such that, for all $v \in V$,

$$\psi(v) := \xi(v) + \begin{cases} m & \text{if } w = v, \\ 0 & \text{otherwise.} \end{cases}$$

Then

$$\prod_{\{u,v\}\in E} A_{\psi(u),\psi(v)} = \prod_{\{w,w\}\in E} A_{\psi(w),\psi(w)} \prod_{\substack{\{w,v\}\in E\\ v\neq w}} A_{\psi(w),\psi(v)} \prod_{\substack{\{u,v\}\in E\\ u,v\neq w}} A_{\psi(u),\psi(v)}$$
$$= \prod_{\{w,w\}\in E} A_{\xi(w),\xi(w)} \prod_{\substack{\{w,v\}\in E\\ v\neq w}} -A_{\xi(w),\xi(v)} \prod_{\substack{\{u,v\}\in E\\ u,v\neq w}} A_{\xi(u),\xi(v)},$$

which implies that

$$\prod_{\{u,v\}\in E} A_{\xi(u),\xi(v)} = (-1)^{\deg(w)} \prod_{\{u,v\}\in E} A_{\psi(u),\psi(v)},$$

where $\deg(w)$ denotes the degree of w in G (self-loops add two to this degree). Since $\prod_{v\in V} \Delta_{\xi(v),\xi(v)} = \Delta_{\xi(w),\xi(w)} \prod_{w\neq v\in V} \Delta_{\xi(v),\xi(v)}$, we have

$$Z_{A,\Delta}(G) = \sum_{\xi:V\to[2m]} \prod_{\{u,v\}\in E} A_{\xi(u),\xi(v)} \prod_{v\in V} \Delta_{\xi(v),\xi(v)}$$
$$= \sum_{\substack{\xi:V\to[2m]\\ \xi(w)\in[m]}} \prod_{\{u,v\}\in E} A_{\xi(u),\xi(v)} \left(\Delta_{\xi(w),\xi(w)} + (-1)^{\deg(w)}\Delta_{m+\xi(w),m+\xi(w)}\right)$$
$$\cdot \prod_{w\neq v\in V} \Delta_{\xi(v),\xi(v)}.$$

As this argument can be applied independently to all $w \in V$, we obtain

$$Z_{A,\Delta}(G) = \sum_{\xi:V\to[m]} \prod_{\{u,v\}\in E} A_{\xi(u),\xi(v)} \prod_{w\in V} \left(\Delta_{\xi(w),\xi(w)} + (-1)^{\deg(w)}\Delta_{m+\xi(w),m+\xi(w)}\right)$$
$$= \sum_{\xi:V\to[m]} \prod_{\{u,v\}\in E} C_{\xi(u),\xi(v)} \prod_{\substack{w\in V\\ \deg(w)\text{ even}}} D_{\xi(w),\xi(w)} \prod_{\substack{w\in V\\ \deg(w)\text{ odd}}} O_{\xi(w),\xi(w)}$$
$$= Z_{C,D,O}(G). \qquad \square$$

COROLLARY 8.2. *Let C be a symmetric $m\times m$ matrix which contains exclusively blocks of rank* 1. *Let D and O be diagonal $m\times m$ matrices. Then the problem* EVAL(C,D,O) *is polynomial-time computable.*

Proof. By Lemma 8.1 the problem EVAL(C,D,O) is polynomial-time equivalent to a problem EVAL(A,Δ) with A a matrix consisting of blocks of row-rank at most 1. Thus the statement of the corollary follows from Lemma 6.3. $\square$

8.1.1. Extended twin reduction. Unfortunately the Twin Reduction Lemma, Lemma 6.2, does not fully satisfy our needs. As we are dealing with possible negative rows, we will be in a situation where it is useful to reduce matrices even further, namely, by collapsing two rows $A_{i,*}$ and $A_{j,*}$ into one if $A_{i,*} = \pm A_{j,*}$.

To achieve this, we say that two rows $A_{i,*}$ and $A_{j,*}$ are *plus-minus-twins* (*pm-twins*) if and only if $A_{i,*} = \pm A_{j,*}$. This induces an equivalence relation on the rows (and by symmetry on the columns) of A. Let $I_1,\dots,I_k$ be a partition of the row indices of A according to this relation. For technical reasons it will be convenient to partition the sets I_i into the positive and the negative parts. That is, for every $i\in[k]$ we define a partition (P_i,N_i) of I_i such that $P_i\neq\emptyset$ and for all $\nu,\nu'\in P_i$ and $\mu,\mu'\in N_i$ we have $A_{\nu,*} = A_{\nu',*}$, $A_{\mu,*} = A_{\mu',*}$, and $A_{\nu,*} = -A_{\mu,*}$.

The *pm-twin*-resolvent of A is the matrix defined, for all $i, j \in [k]$, by

$$\mathcal{T}^{\pm}(A)_{i,j} := A_{\mu,\nu} \text{ for some } \mu \in P_i, \nu \in P_j.$$

This definition is technical and seems to be counterintuitive, as we are not taking the N_i into account. However, its motivation will become clear with the following lemma and it is still well defined, even though possibly $N_i = \emptyset$ for some $i \in [k]$.

As before, we define a mapping $\tau : [m] \to [k]$ defined by $\mu \in I_{\tau(\mu)}$; that is, τ maps $\mu \in [m]$ to the class I_j it is contained in. Therefore, we have $\mathcal{T}^{\pm}(A)_{\tau(i),\tau(j)} = \pm A_{i,j}$ for all $i, j \in [m]$. We call τ the *pm-twin-resolution mapping* of A. Define $N = N_1 \cup \cdots \cup N_k$ and $P = P_1 \cup \cdots \cup P_k$. Then, in particular,

$$\mathcal{T}^{\pm}(A)_{\tau(i),\tau(j)} = \quad A_{i,j} \text{ for all } (i,j) \in (P \times P) \cup (N \times N),$$

$$\mathcal{T}^{\pm}(A)_{\tau(i),\tau(j)} = -A_{i,j} \text{ for all } (i,j) \in (P \times N) \cup (N \times P).$$

LEMMA 8.3 (Extended Twin Reduction Lemma). *Let A be a symmetric $m \times m$ matrix and Δ a diagonal $m \times m$ matrix of vertex weights. Let $(P_1, N_1), \ldots, (P_k, N_k)$ be a partition of the row indices of A according to the pm-twin-relation.*

Then

$$Z_{A,\Delta}(G) = Z_{\mathcal{T}^{\pm}(A),D,O}(G) \text{ for all graphs } G,$$

where D and O are diagonal $k \times k$ matrices defined by

$$D_{i,i} = \sum_{\nu \in P_i} \Delta_{\nu,\nu} + \sum_{\mu \in N_i} \Delta_{\mu,\mu} \quad \text{and} \quad O_{i,i} = \sum_{\nu \in P_i} \Delta_{\nu,\nu} - \sum_{\mu \in N_i} \Delta_{\mu,\mu} \text{ for all } i \in [k].$$

Proof. Define $J_i = P_i$ and $J_{k+i} = N_i$ for all $i \in [k]$. Without loss of generality we may assume that if there is a minimal $l \in [k]$ such that $J_{k+l} = \emptyset$, then for all $j \geq l$ we have $J_{k+j} = \emptyset$ (this can be achieved by appropriate relabeling of the P_i and N_i). Let $l := k + 1$ if all J_{k+i} are nonempty. Then $J_1, \ldots, J_{k+l-1}$ are the equivalence classes of A according to the twin-relation. Therefore, the Twin Reduction Lemma, Lemma 6.2, implies that for the diagonal $(k + \ell - 1) \times (k + \ell - 1)$ diagonal matrix Δ'' defined by $\Delta''_{j,j} = \sum_{\nu \in J_j} \Delta_{\nu,\nu}$ we have

$$Z_{A,\Delta}(G) = Z_{\mathcal{T}(A),\Delta''}(G) \text{ for all graphs } G.$$

Let $n' := k + l - 1$ and note that, by the definition of the sets J_i, $\mathcal{T}(A)$ is the upper left $n' \times n'$ submatrix of the $2k \times 2k$ matrix

$$M = \begin{pmatrix} \mathcal{T}^{\pm}(A) & -\mathcal{T}^{\pm}(A) \\ -\mathcal{T}^{\pm}(A) & \mathcal{T}^{\pm}(A) \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes \mathcal{T}^{\pm}(A),$$

that is, $\mathcal{T}(A) = M_{[n'][n']}$. Define a $2k \times 2k$ diagonal matrix Δ' such that $\Delta'_{i,i} = \Delta''_{i,i}$ for all $i \in [n']$ and $\Delta'_{i,i} = 0$ for all $n' < i \leq 2k$. Then

$$Z_{M,\Delta'}(G) = Z_{\mathcal{T}(A),\Delta''}(G) \text{ for all graphs } G.$$

Moreover, by the definition of Δ'', the matrix Δ' satisfies, for all $i \in [k]$,

$$\Delta'_{i,i} = \sum_{\nu \in P_i} \Delta_{\nu,\nu} \quad \text{and} \quad \Delta'_{k+i,k+i} = \sum_{\nu \in N_i} \Delta_{\nu,\nu}. \tag{8.1}$$

Now, by Lemma 8.1, $Z_{M,\Delta'}(G) = Z_{\mathcal{T}^{\pm}(A),D',O'}$, where D' and O' are $k \times k$ matrices such that $D'_{i,i} = \Delta'_{i,i} + \Delta'_{k+i,k+i}$ and $O'_{i,i} = \Delta'_{i,i} - \Delta'_{k+i,k+i}$. But by (8.1), we see that $D' = D$ and $O' = O$. ∎

LEMMA 8.4 (Row-Column Negation Lemma). *Let C be a symmetric $m \times m$ matrix and D, O diagonal $m \times m$ matrices of vertex weights.*

Let $i \in [m]$ and define C' as the matrix obtained from C by multiplying row and column i with -1. Let O' be the matrix obtained from O by negating the diagonal entry $O_{i,i}$. Then

$$Z_{C,D,O}(G) = Z_{C',D,O'}(G) \text{ for all graphs } G.$$

Proof. Let $G = (V, E)$ be a graph and V_o, V_e the sets of odd (even) degree vertices in V. Recall that

$$Z_{C,D,O}(G) = \sum_{\xi: V \to [m]} \prod_{\{u,v\} \in E} C_{\xi(u),\xi(v)} \prod_{v \in V_e} D_{\xi(v),\xi(v)} \prod_{v \in V_o} O_{\xi(v),\xi(v)}.$$

Fix some mapping $\xi : V \to [m]$. We will prove the lemma by showing that

$$\begin{aligned} &\prod_{\{u,v\} \in E} C_{\xi(u),\xi(v)} \prod_{v \in V_e} D_{\xi(v),\xi(v)} \prod_{v \in V_o} O_{\xi(v),\xi(v)} \\ &\quad = \prod_{\{u,v\} \in E} C'_{\xi(u),\xi(v)} \prod_{v \in V_e} D_{\xi(v),\xi(v)} \prod_{v \in V_o} O'_{\xi(v),\xi(v)}. \end{aligned}$$

Define $W := \xi^{-1}(i)$ and let $W_e := V_e \cap W$ and $W_o := V_o \cap W$ denote the even and odd degree vertices in W. By the definition of O' we have

$$\prod_{v \in V_o} O'_{\xi(v),\xi(v)} = (-1)^{|W_o|} \prod_{v \in V_o} O_{\xi(v),\xi(v)}.$$

Furthermore, for all edges $\{u, v\} \in E$ we have that $C_{\xi(u),\xi(v)} = C'_{\xi(u),\xi(v)}$ if and only if either both $u, v \in W$ or both $u, v \notin W$. If exactly one of the vertices is in W, then $C_{\xi(u),\xi(v)} = -C'_{\xi(u),\xi(v)}$. Therefore, if we denote by $e(W, V \setminus W)$ the number of edges $e = \{u, v\}$ in G such that exactly one vertex is in W, we have

$$\prod_{\{u,v\} \in E} C'_{\xi(u),\xi(v)} = (-1)^{e(W,V \setminus W)} \prod_{\{u,v\} \in E} C_{\xi(u),\xi(v)}.$$

To finish the proof, we note that

$$e(W, V \setminus W) \equiv \sum_{v \in W} \deg(v) \equiv |W_o| \pmod 2. \qquad ∎$$

8.1.2. Pinning vertices. In the proof of Lemma 3.1 it will be convenient to "pin" certain vertices of the input graph G to prescribed spins. We will develop the tools which are necessary for this now. These results extend analogous techniques used in [8] and [6].

Let A be an $m \times m$ matrix and D a diagonal $m \times m$ matrix of positive vertex weights. In the following, a *labeled graph* is a triple $G = (V, E, z)$, where (V, E) is a graph and $z \in V$. For a labeled graph $G = (V, E, z)$ and a $k \in [m]$, we let

$$Z_{A,D}(k, G) = (D_{k,k})^{-1} \sum_{\substack{\xi: V \to [m] \\ \xi(z) = k}} \prod_{\{u,v\} \in E} A_{\xi(u),\xi(v)} \cdot \prod_{v \in V} D_{\xi(v),\xi(v)}.$$

The *product* GH of two labeled graphs G and H is formed by taking the disjoint union of the graphs and then identifying the labeled vertices. Let H^s denote the product of H with itself taken s times. Note that $Z_{A,D}(k, GH) = Z_{A,D}(k, G)Z_{A,D}(k, H)$ for all labeled graphs G and H.

Recall that a twin-free matrix A is a matrix such that $A_{i,*} \neq A_{j,*}$ for all row indices $i \neq j$. Furthermore, an *automorphism* of (A, D) is a bijection $\alpha : [m] \to [m]$ such that $A_{i,j} = A_{\alpha(i),\alpha(j)}$ and $D_{i,i} = D_{\alpha(i),\alpha(i)}$ for all $i \in [m]$. The following lemma follows by a result of Lovász (Lemma 2.4 in [20]).

LEMMA 8.5. *Let $A \in \mathbb{R}^{m\times m}$ be twin-free, $D \in \mathbb{R}^{m\times m}$ a diagonal matrix of positive vertex weights, and $i, j \in [m]$. If for all labeled graphs G we have*

$$Z_{A,D}(i, G) = Z_{A,D}(j, G),$$

then there is an automorphism α of (A, D) such that $j = \alpha(i)$.

We furthermore need some standard result about interpolation (see Lemma 8.6), which we use in the form as stated in [8] Lemma 3.2.

LEMMA 8.6. *Let $w_1, \ldots, w_r$ be known distinct nonzero constants. Suppose that we know the values $f_1, \ldots, f_r$ such that*

$$f_i = \sum_{j=1}^{r} c_j w_j^i \text{ for all } i \in [r].$$

Then the coefficients $c_1, \ldots, c_r$ are uniquely determined and can be computed in polynomial time.

LEMMA 8.7 (Pinning Lemma). *Let $A \in \mathbb{R}_{\mathbb{A}}^{m\times m}$ be a symmetric matrix and $\Delta \in \mathbb{R}_{\mathbb{A}}^{m\times m}$ a diagonal matrix of positive real entries. Then for every labeled graph G and every $k \in [m]$, we can compute $Z_{A,\Delta}(k, G)$ in polynomial time using an* EVAL(A, Δ) *oracle.*

Proof. Let the matrices B and D be the result of twin-reduction (Lemma 6.2) when applied to A and Δ. In particular, B is twin-free and $Z_{A,\Delta}(G) = Z_{B,D}(G)$ for all graphs G. Therefore, using the oracle, we can compute $Z_{B,D}(G)$ in polynomial time (for input G).

Consider a graph $G = (V, E)$ with a labeled vertex z and a particular spin $k \in [m]$. We will show how to compute $Z_{B,D}(k, G)$ using an oracle for $Z_{B,D}$. This suffices since, although $Z_{B,D}(k, G)$ is not the same as $Z_{A,\Delta}(k, G)$, they can be derived from each other.

Call spins $i, j \in [m]$ *equivalent* if there is an automorphism α of (B, D) such that $j = \alpha(i)$. Partition $[m]$ into equivalence classes $I_1, \ldots, I_c$ according to this definition. For every spin j in equivalence class I_i, let c_j denote the size of the equivalence class—$c_j = |I_i|$. For every equivalence class $i \in [c]$ let k_i denote a particular spin $k_i \in I_i$.

For any two equivalent spins a and a' we have $Z_{B,D}(a, F) = Z_{B,D}(a', F)$ for every graph F. Therefore,

$$Z_{B,D}(G) = \sum_{i=1}^{c} c_{k_i} Z_{B,D}(k_i, G). \tag{8.2}$$

We will now prove the following claim. The result follows by taking $S = \bigcup_{i\in[c]}\{k_i\}$.

CLAIM 3. *Given a set S of inequivalent spins and a spin $k \in S$, we can compute $Z_{B,D}(k, G)$ in polynomial time using an oracle for computing $\sum_{k\in S} c_k Z_{B,D}(k, G)$.*

Proof. The proof is by induction on $|S|$. The base case $|S| = 1$ is straightforward, so assume $|S| > 1$. We will show how to compute $Z_{B,D}(k, G)$ (for any spin $k \in S$) using an oracle for $\sum_{k\in S} c_k Z_{B,D}(k, G)$. Fix distinct spins i and j in S. By Lemma 8.5, there is a labeled graph $G_{i,j}$ such that

$$Z_{B,D}(i, G_{i,j}) \neq Z_{B,D}(j, G_{i,j}). \tag{8.3}$$

Note that the construction of $G_{i,j}$ takes $O(1)$ time since $G_{i,j}$ does not depend on any input graph G. Partition S into classes $J_1, \ldots, J_t$ such that $\nu, \nu' \in J_\mu$ if and only if $Z_{B,D}(\nu, G_{i,j}) = Z_{B,D}(\nu', G_{i,j})$. We show below how to compute $\sum_{k\in J_\mu} c_k Z_{B,D}(k, G)$ (for any $\mu \in [t]$) using an oracle for $\sum_{k\in S} c_k Z_{B,D}(k, G)$. Once we have done that, we can finish as follows. For a fixed $k \in S$, suppose $k \in J_\mu$. Note that $|J_\mu| < S$ since one of the spins i and j is not in J_μ. By induction, we can compute $Z_{B,D}(k, G)$ using the newly constructed oracle to compute $\sum_{k\in J_\mu} c_k Z_{B,D}(k, G)$.

To finish, we now show how to compute $\sum_{k\in J_\mu} c_k Z_{B,D}(k, G)$ using an oracle for $\sum_{k\in S} c_k Z_{B,D}(k, G)$. For every $\mu \in [t]$, let s_μ be a spin in J_μ. Let $w_\mu = Z_{B,D}(s_\mu, G_{i,j})$. Let

$$\begin{aligned} f_r &= \sum_{k\in S} c_k Z_{B,D}(k, GG_{i,j}^r) \\ &= \sum_{\mu\in[t]} \sum_{k\in J_\mu} c_k Z_{B,D}(k, GG_{i,j}^r) \\ &= \sum_{\mu\in[t]} \sum_{k\in J_\mu} c_k Z_{B,D}(k, G)(Z_{B,D}(k, G_{i,j}))^r \\ &= \sum_{\mu\in[t]} {w_\mu}^r \sum_{k\in J_\mu} c_k Z_{B,D}(k, G). \end{aligned}$$

Note that we can compute f_r in polynomial time using the oracle. Now by Lemma 8.6 we can recover $\sum_{k\in J_\mu} c_k Z_{B,D}(k, G)$ for every μ apart from the one with $w_\mu = 0$ (if there is a μ with $w_\mu = 0$). But we can recover this one, if it exists, by subtraction since

$$\sum_{k\in J_\mu} c_k Z_{B,D}(k, G) = \sum_{k\in S} c_k Z_{B,D}(k, G) - \sum_{\nu\neq\mu} \sum_{k\in J_\nu} c_k Z_{B,D}(k, G). \qquad \square$$

The following corollary will be helpful in the proof of Lemma 8.12.

COROLLARY 8.8. *Let $C \in \mathbb{R}_{\mathbb{A}}^{m\times m}$ be a symmetric matrix and $D, O \in \mathbb{R}_{\mathbb{A}}^{m\times m}$ diagonal matrices such that the diagonal of D is positive and that of O is nonnegative such that $D - O$ is nonnegative. Then, for every labeled graph G and every $k \in [m]$, we can compute $Z_{C,D,O}(k, G)$ in polynomial time using an* EVAL(C, D, O) *oracle.*

Proof. Let Δ^+ and Δ^- be diagonal $m \times m$ matrices with $\Delta^+_{i,i} = (D_{i,i} + O_{i,i})/2$ and $\Delta^-_{i,i} = (D_{i,i} - O_{i,i})/2$. Let

$$A = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes C.$$

Let Δ be the $2m \times 2m$ matrix such that, for all $i \in [m]$ and $j \in [m]$, $\Delta_{i,j} = \Delta^+_{i,j}$, $\Delta_{i,m+j} = \Delta_{m+i,j} = 0$, and $\Delta_{m+i,m+j} = \Delta^-_{i,j}$. Then by Lemma 8.1

$$Z_{C,D,O}(G) = Z_{A,\Delta}(G) \text{ for all graphs } G.$$

Let $I = \{i \in [2m] \mid \Delta_{i,i} \neq 0\}$. Since $D + O$ and $D - O$ are nonnegative, we have that the matrix Δ_{II} has a positive diagonal. By inspection we have

$$Z_{A,\Delta}(G) = Z_{A_{II},\Delta_{II}}(G) \text{ for all graphs } G.$$

By the Pinning Lemma, Lemma 8.7, we can compute the value $Z_{A_{II},\Delta_{II}}(k, G)$ by an algorithm with oracle access to $\mathrm{EVAL}(A_{II}, \Delta_{II})$. Now, $Z_{C,D,O}(k, G) = Z_{A_{II},\Delta_{II}}(k, G) + Z_{A_{II},\Delta_{II}}(k + m, G)$ for every $k \in [m]$. This finishes the proof. ∎

8.1.3. Tensor product decomposition. The following technical lemma will be used in the proof of Lemma 3.2.

LEMMA 8.9. *Given symmetric $r \times r$ matrices A and D and $m \times m$ matrices A', D',*

$$Z_{A\otimes A',D\otimes D'}(G) = Z_{A,D}(G) \cdot Z_{A',D'}(G) \text{ for every graph } G.$$

Proof. We consider the indices of $A \otimes A'$ and $D \otimes D'$ as pairs $(i, j) \in [r] \times [m]$ such that, e.g.,

$$(A \otimes A')_{(i,i')(j,j')} = A_{i,j} \cdot A'_{i',j'}.$$

Let $\pi : [r] \times [m] \to [r]$ and $\rho : [r] \times [m] \to [m]$ be the canonical projections; i.e., for every $(i, j) \in [r] \times [m]$ we have $\pi(i, j) = i$ and $\rho(i, j) = j$.

Thus

$$\begin{aligned}
Z_{A\otimes A',D\otimes D'}(G) &= \sum_{\xi:V\to[r]\times[m]} \prod_{uv\in E} (A \otimes A')_{\xi(u),\xi(v)} \prod_{v\in V} (D \otimes D')_{\xi(v),\xi(v)} \\
&= \sum_{\xi:V\to[r]\times[m]} \prod_{uv\in E} A_{\pi(\xi(u)),\pi(\xi(v))} A'_{\rho(\xi(u)),\rho(\xi(v))} \\
&\quad \cdot \prod_{v\in V} D_{\pi(\xi(v)),\pi(\xi(v))} D'_{\rho(\xi(v)),\rho(\xi(v))} \\
&= \sum_{\substack{\xi:V\to[r] \\ \xi':V\to[m]}} \prod_{uv\in E} A_{\xi(u),\xi(v)} A'_{\xi'(u),\xi'(v)} \prod_{v\in V} D_{\xi(v),\xi(v)} D'_{\xi'(v),\xi'(v)} \\
&= Z_{A,D}(G) \cdot Z_{A',D'}(G). \qquad \blacksquare
\end{aligned}$$

It is not hard to see that this kind of decomposition can be performed for parity-distinguishing partition functions as well, as the following lemma shows.

LEMMA 8.10. *Suppose that A' is a symmetric $m' \times m'$ matrix and D' and O' are diagonal $m' \times m'$ matrices. Suppose that A'' is a symmetric $m'' \times m''$ matrix and D'' and O'' are diagonal $m'' \times m''$ matrices. Then, for every graph G,*

$$Z_{A'\otimes A'',D'\otimes D'',O'\otimes O''}(G) = Z_{A',D',O'}(G) \cdot Z_{A'',D'',O''}(G).$$

Proof. Let $A = A' \otimes A''$, $D = D' \otimes D''$, and $O = O' \otimes O''$. We consider the indices of A, D, and O as pairs $(i, j) \in [m'] \times [m'']$ such that, for example,

$$(A)_{(i',i'')(j',j'')} = A'_{i',j'} \cdot A''_{i'',j''}.$$

Let $\pi' : [m'] \times [m''] \to [m']$ and $\pi'' : [m'] \times [m''] \to [m'']$ be the canonical projections; i.e., for every $(i, j) \in [m'] \times [m'']$ we have $\pi'(i, j) = i$ and $\pi''(i, j) = j$.

With $V_o \subseteq V$ the set of even degree vertices and $V_e = V \setminus V_o$, we have

$$Z_{A,D,O}(G) = \sum_{\xi: V \to [m'] \times [m'']} \prod_{\{u,v\} \in E} A_{\xi(u),\xi(v)} \prod_{v \in V_e} D_{\xi(v),\xi(v)} \prod_{v \in V_o} O_{\xi(v),\xi(v)}.$$

With

$$\prod_{v \in V_e} D_{\xi(v),\xi(v)} = \prod_{v \in V_e} D'_{\pi'(\xi(v)),\pi'(\xi(v))} \prod_{v \in V_e} D''_{\pi''(\xi(v)),\pi''(\xi(v))},$$
$$\prod_{v \in V_o} O_{\xi(v),\xi(v)} = \prod_{v \in V_O} O'_{\pi'(\xi(v)),\pi'(\xi(v))} \prod_{v \in V_o} O''_{\pi''(\xi(v)),\pi''(\xi(v))},$$

and

$$\prod_{\{u,v\} \in E} A_{\xi(u),\xi(v)} = \prod_{\{u,v\} \in E} A'_{\pi'(\xi(u)),\pi'(\xi(v))} \prod_{\{u,v\} \in E} A''_{\pi''(\xi(u)),\pi''(\xi(v))},$$

we therefore have

$$\begin{aligned} Z_{A,D,O}(G) &= \left(\sum_{\psi': V \to [m']} \prod_{\{u,v\} \in E} A'_{\psi'(u),\psi'(v)} \prod_{v \in V_e} D'_{\psi'(v),\psi'(v)} \prod_{v \in V_o} O'_{\psi'(v),\psi'(v)} \right) \\ &\quad \cdot \left(\sum_{\psi'': V \to [m'']} \prod_{\{u,v\} \in E} A''_{\psi''(u),\psi''(v)} \prod_{v \in V_e} D''_{\psi''(v),\psi''(v)} \prod_{v \in V_o} O''_{\psi''(v),\psi''(v)} \right) \\ &= Z_{A',D',O'}(G) \cdot Z_{A'',D'',O''}(G). \qquad \square \end{aligned}$$

COROLLARY 8.11. *Let B' be a symmetric $m' \times m'$ block and let $D^{R'}$ and $O^{R'}$ be diagonal $m' \times m'$ matrices. Let $B'' = vv^T$ be a symmetric $m'' \times m''$ block and for v a positive vector. Let $D^{R''}$ and $O^{R''}$ be diagonal $m'' \times m''$ matrices such that $D^{R''}$ has positive diagonal and $O^{R''}$ has nonnegative diagonal. Let $D^R = D^{R'} \otimes D^{R''}$, $O^R = O^{R'} \otimes O^{R''}$, and $B = B' \otimes B''$. Furthermore, $O^{R''} = 0$ if and only if $O^{R'} = 0$. Then*

$$\mathrm{EVAL}(B, D^R, O^R) \equiv \mathrm{EVAL}(B', D^{R'}, O^{R'}).$$

Proof. For every graph G, Lemma 8.10 gives

$$Z_{B' \otimes B'', D^{R'} \otimes D^{R''}, O^{R'} \otimes O^{R''}}(G) = Z_{B', D^{R'}, O^{R'}}(G) \cdot Z_{B'', D^{R''}, O^{R''}}(G).$$

As $B'' = vv^T$ is of rank 1, Corollary 8.2 implies that $\mathrm{EVAL}(B'', D^{R''}, O^{R''})$ is polynomial-time computable. It is not hard to see that if $O^{R''} \neq 0$, then $Z_{B'', D^{R''}, O^{R''}}(G)$ is positive for all graphs G. In this case it follows straightforwardly that

$$\mathrm{EVAL}(B, D^R, O^R) \equiv \mathrm{EVAL}(B', D^{R'}, O^{R'}).$$

On the other hand, assume that $O^{R''} = 0$. This implies that $O^{R'} = 0$, and thus $Z_{B', D^{R'}, O^{R'}}(G) = 0$ for every G which contains an odd-degree vertex. For all G which contain only even-degree vertices, $Z_{B'', D^{R''}, O^{R''}}(G)$ is nonzero. The claimed reducibility follows. $\square$

LEMMA 8.12. *Let B' be an $m' \times n'$ block, $D^{R'}$ and $O^{R'}$ be diagonal $m' \times m'$ matrices, and $D^{C'}$ and $O^{C'}$ be diagonal $n' \times n'$ matrices. Let B'' be an $m'' \times n''$ block,*

$D^{R''}$ and $O^{R''}$ be diagonal $m'' \times m''$ matrices, and $D^{C''}$ and $O^{C''}$ be diagonal $n'' \times n''$ matrices. Assume that the diagonal entries of $D^{R'}, D^{C'}, D^{R''}, D^{C''}$ are positive and those of $O^{R'}, O^{C'}, O^{R''}, O^{C''}$ are nonnegative. Furthermore, we have that $O^{R'} = 0$ if and only if $O^{R''} = 0$ and that $O^{C'} = 0$ if and only if $O^{C''} = 0$. Let

$$D' = \begin{pmatrix} D^{R'} & 0 \\ 0 & D^{C'} \end{pmatrix}, \; D'' = \begin{pmatrix} D^{R''} & 0 \\ 0 & D^{C''} \end{pmatrix},$$
$$\text{and } D = \begin{pmatrix} D^{R'} \otimes D^{R''} & 0 \\ 0 & D^{C'} \otimes D^{C''} \end{pmatrix},$$

and let O and O', O'' be constructed from O^R, O^C and $O^{R'}, O^{C'}$ in the analogous way. Let A, A', A'' be the connected bipartite matrices with underlying blocks $B := B' \otimes B''$, B', and B'', respectively. Let $B'' = vw^T$ for positive vectors v, w.

If $D + O$ and $D - O$ have only nonnegative entries, then

$$\mathrm{EVAL}(A, D, O) \equiv \mathrm{EVAL}(A', D', O').$$

Proof. Note that $Z_{A,D,O}(G) = 0$ unless G is bipartite. Therefore, we will assume in the following that all graphs G are bipartite and that (U, W) is a partition of the vertex set V into two independent sets. Assume first that G is connected; the case of nonconnected graphs will be handled later. Note that A is a square matrix of order $m + n$ for $m = m'm''$ and $n = n'n''$. For diagonal $r \times r$ matrices D, O, a set $X \subseteq V$, and a configuration $\xi : X \to [r]$ define

$$\dot{\omega}_{D,O}(X, \phi) := \prod_{\substack{x \in X \\ \deg(x) \text{ even}}} D_{\xi(x),\xi(x)} \prod_{\substack{x \in X \\ \deg(x) \text{ odd}}} O_{\xi(x),\xi(x)}.$$

By the above definitions we have

$$Z_{A,D,O}(G) = \sum_{\substack{\xi : U \to [m+n] \\ \psi : W \to [m+n]}} \prod_{\{u,w\} \in E} A_{\xi(u),\psi(w)} \dot{\omega}_{D,O}(U, \xi) \dot{\omega}_{D,O}(W, \psi).$$

Therefore, since G is connected,

$$\begin{aligned} Z_{A,D,O}(G) = & \sum_{\substack{\xi : U \to [m] \\ \psi : W \to [n]}} \prod_{\{u,w\} \in E} B_{\xi(u),\psi(w)} \dot{\omega}_{D^R,O^R}(U, \xi) \dot{\omega}_{D^C,O^C}(W, \psi) \\ & + \sum_{\substack{\xi : U \to [n] \\ \psi : W \to [m]}} \prod_{\{u,w\} \in E} B_{\psi(w),\xi(u)} \dot{\omega}_{D^C,O^C}(U, \xi) \dot{\omega}_{D^R,O^R}(W, \psi). \end{aligned}$$

Define

$$Z^{\rightarrow}_{A,D,O}(G) := \sum_{\substack{\xi : U \to [m] \\ \psi : W \to [n]}} \prod_{\{u,w\} \in E} B_{\xi(u),\psi(w)} \dot{\omega}_{D^R,O^R}(U, \xi) \dot{\omega}_{D^C,O^C}(W, \psi) \tag{8.4}$$

and

$$Z^{\leftarrow}_{A,D,O}(G) := \sum_{\substack{\xi : U \to [n] \\ \psi : W \to [m]}} \prod_{\{u,w\} \in E} B_{\psi(w),\xi(u)} \dot{\omega}_{D^C,O^C}(U, \xi) \dot{\omega}_{D^R,O^R}(W, \psi). \tag{8.5}$$

That is,

$$Z_{A,D,O}(G) = Z^{\rightarrow}_{A,D,O}(G) + Z^{\leftarrow}_{A,D,O}(G). \tag{8.6}$$

For matrices A', D', O' and A'', D'', O'' we define the analogous expressions ($Z^{\leftarrow}_{A',D',O'}(G)$, etc.).

We consider the indices of $B' \otimes B''$ as pairs. That is, row indices are $(i', i'') \in [m'] \times [m'']$, and column indices become $(j', j'') \in [n'] \times [n'']$.

$$(B' \otimes B'')_{(i',i'')(j',j'')} = B'_{i',j'} \cdot B''_{i'',j''}.$$

Let $\rho' : [m'] \times [m''] \to [m']$, $\rho'' : [m'] \times [m''] \to [m'']$ and $\gamma' : [n'] \times [n''] \to [n']$, $\gamma'' : [n'] \times [n''] \to [n'']$ be the canonical projections. That is, for $(i', i'') \in [m'] \times [m'']$ we have $\rho'(i', i'') = i'$, $\rho''(i', i'') = i''$ and for $(j', j'') \in [n'] \times [n'']$ we have $\gamma'(j', j'') = j'$, $\gamma''(j', j'') = j''$. Therefore, for all $\xi : U \to [m]$ and $\psi : W \to [n]$ we have

$$\prod_{\{u,w\} \in E} B_{\xi(u),\psi(w)} = \prod_{\{u,w\} \in E} B'_{\rho' \circ \xi(u), \gamma' \circ \psi(w)} \cdot \prod_{\{u,w\} \in E} B''_{\rho'' \circ \xi(u), \gamma'' \circ \psi(w)}$$

and

$$\dot{\omega}_{D^R, O^R}(U, \xi) = \dot{\omega}_{D^{R'}, O^{R'}}(U, \rho' \circ \xi) \dot{\omega}_{D^{R''}, O^{R''}}(U, \rho'' \circ \xi),$$
$$\dot{\omega}_{D^C, O^C}(W, \psi) = \dot{\omega}_{D^{C'}, O^{C'}}(W, \gamma' \circ \psi) \dot{\omega}_{D^{C''}, O^{C''}}(W, \gamma'' \circ \psi).$$

Hence, we can rewrite (8.4):

$$\begin{aligned} Z^{\rightarrow}_{A,D,O}(G) = & \left(\sum_{\substack{\xi' : U \to [m'] \\ \psi' : W \to [n']}} \prod_{\{u,w\} \in E} B'_{\xi'(u), \psi'(w)} \dot{\omega}_{D^{R'}, O^{R'}}(U, \xi') \dot{\omega}_{D^{C'}, O^{C'}}(W, \psi') \right) \\ & \cdot \left(\sum_{\substack{\xi'' : U \to [m''] \\ \psi'' : W \to [n'']}} \prod_{\{u,w\} \in E} B''_{\xi''(u), \psi''(w)} \dot{\omega}_{D^{R''}, O^{R''}}(U, \xi'') \dot{\omega}_{D^{C''}, O^{C''}}(W, \psi'') \right) \\ = & Z^{\rightarrow}_{A',D',O'}(G) \cdot Z^{\rightarrow}_{A'',D'',O''}(G). \end{aligned}$$

By an analogous argument this extends to $Z^{\leftarrow}_{A,D,O}(G)$. We therefore have

$$Z^{\leftarrow}_{A,D,O}(G) = Z^{\leftarrow}_{A',D',O'}(G) \cdot Z^{\leftarrow}_{A'',D'',O''}(G), \tag{8.7}$$
$$Z^{\rightarrow}_{A,D,O}(G) = Z^{\rightarrow}_{A',D',O'}(G) \cdot Z^{\rightarrow}_{A'',D'',O''}(G). \tag{8.8}$$

Claim 4. *The values $Z^{\rightarrow}_{A,D,O}(G)$ and $Z^{\leftarrow}_{A,D,O}(G)$ can be computed in polynomial time for every graph G by an algorithm with oracle access to* EVAL(A, D, O).

Proof. Let $G = (U, W, E)$ be a given connected bipartite graph, and label a vertex $u \in U$. Then

$$Z^{\rightarrow}_{A,D,O}(G) = \sum_{k=1}^{m} Z_{A,D,O}(k, G),$$

and the values $Z_{A,D,O}(k, G)$ can be computed using the EVAL(A, D, O) oracle by Corollary 8.8.

The analogous argument labeling a vertex $w \in W$ yields the result for $Z^{\leftarrow}_{A,D,O}(G)$. □

We will show first that $\mathrm{EVAL}(A,D,O) \leq \mathrm{EVAL}(A',D',O')$. Let G be a given connected graph. By (8.6), (8.7), and (8.8) we have

$$\begin{aligned} Z_{A,D,O}(G) &= Z^{\rightarrow}_{A,D,O}(G) + Z^{\leftarrow}_{A,D,O}(G) \\ &= Z^{\rightarrow}_{A',D',O'}(G) Z^{\rightarrow}_{A'',D'',O''}(G) + Z^{\leftarrow}_{A',D',O'}(G) Z^{\leftarrow}_{A'',D'',O''}(G). \end{aligned}$$

By Claim 4 we can compute the values $Z^{\rightarrow}_{A',D',O'}(G)$ and $Z^{\leftarrow}_{A',D',O'}(G)$ using the $\mathrm{EVAL}(A',D',O')$ oracle. The values $Z^{\rightarrow}_{A'',D'',O''}(G)$ and $Z^{\leftarrow}_{A'',D'',O'}(G)$ can be computed by Claim 4 using the fact that $\mathrm{EVAL}(A'',D'',O'')$ is polynomial-time computable. This polynomial-time computability follows from Lemma 8.2 using the fact that the block $B'' = vw^T$ underlying A'' has rank 1.

To see that $\mathrm{EVAL}(A',D',O') \leq \mathrm{EVAL}(A,D,O)$, note that by Claim 4 we can compute

$$Z^{\rightarrow}_{A,D,O}(G) = Z^{\rightarrow}_{A',D',O'}(G) Z^{\rightarrow}_{A'',D'',O''}(G) \tag{8.9}$$

and

$$Z^{\leftarrow}_{A,D,O}(G) = Z^{\leftarrow}_{A',D',O'}(G) Z^{\leftarrow}_{A'',D'',O''}(G)$$

using an $\mathrm{EVAL}(A,D,O)$ oracle. We continue by showing how to compute $Z^{\rightarrow}_{A',D',O'}(G)$; the proof for $Z^{\leftarrow}_{A',D',O'}(G)$ will be analogous. Altogether, we will then obtain

$$Z_{A',D',O'}(G) = Z^{\rightarrow}_{A',D',O'}(G) + Z^{\leftarrow}_{A',D',O'}(G).$$

Let us see how to compute $Z^{\rightarrow}_{A',D',O'}(G)$. Note that by Claim 4, using the fact that $\mathrm{EVAL}(A'',D'',O'')$ is polynomial-time computable, we can compute $Z^{\rightarrow}_{A'',D'',O''}(G)$. If $O^{R''} \neq 0$ and $O^{C''} \neq 0$, then it is not hard to see that $Z^{\rightarrow}_{A'',D'',O''}(G)$ is positive, since D'' has positive diagonal and $B'' = vw^T$. In this case we can compute $Z^{\rightarrow}_{A',D',O'}(G)$ by (8.9).

It remains to consider the three cases where either $O^{R''} = 0$ or $O^{C''} = 0$. For simplicity, let us consider only the case that $O^{R''} = 0$ and $O^{C''} \neq 0$; the others are handled by analogous reasoning. By the condition of the lemma, we have $O^{R'} = 0$. Thus, if U contains a vertex of odd degree, then $0 = Z^{\rightarrow}_{A',D',O'}(G) = Z^{\rightarrow}_{A'',D'',O''}(G)$. If all vertices in U have even degree, then, as above, we see that $Z^{\rightarrow}_{A'',D'',O''}(G)$ is positive. Therefore, we can compute $Z^{\rightarrow}_{A',D',O'}(G)$ by (8.9).

The proof for nonconnected G follows from the above using the fact that

$$Z_{A,D,O}(G) = \prod_{i=1}^{c} Z_{A,D,O}(G_i),$$

with $G_1, \ldots, G_c$ being the connected components of G. □

8.2. The proof of Lemma 3.1.

Proof of Lemma 3.1. Let G be a given graph. Note that if $G = (V,E)$ is not connected with $G_1, \ldots, G_k$ being the components of G, then we have

$$Z_A(G) = \prod_{i=1}^{k} \sum_{j=1}^{c} Z_{A_j}(G_i).$$

This proves (2). To prove (1) note that for hardness we may restrict ourselves to connected G.

Therefore, for some $i \in [c]$ fix a component A_i of A and let $I \subseteq [m]$ be the set of row/column indices such that $A_i = A_{II}$. Let $G = (V, E)$ be a connected graph and call some vertex $z \in V$ the labeled vertex of G. Then by the connectedness of G we have

$$Z_{A_i}(G) = \sum_{k \in I} Z_A(k, G).$$

The proof now follows by the Pinning Lemma, Lemma 8.7. ∎

8.3. The proof of Lemma 3.2. In order to prove Lemma 3.2, it will be convenient to transition from partition functions to parity-distinguishing partition functions. How this translation can be performed will be described in Lemma 8.15. Once we have determined some conditions on the shape of the resulting partition functions, the proof of Lemma 3.2 will become straightforward.

Shape conditions. Given an evaluation problem EVAL(C, D, O) with D, O diagonal matrices of vertex weights and C a connected bipartite matrix with underlying block B, we define conditions on the shape of C and D, O. These conditions will be used incrementally; that is, we will rely on (C$(i+1)$) only if (C1)–(Ci) are assumed to hold.

(C1) There are $r, m, n \in \mathbb{N}$, a nonsingular $r \times r$-matrix H with entries in $\{-1, 1\}$, and vectors $v \in \mathbb{R}_{\mathbb{A}>0}^{m}$, $w \in \mathbb{R}_{\mathbb{A}>0}^{n}$ of pairwise distinct entries such that

$$B = vw^T \otimes H = \begin{pmatrix} v_1 w_1 H & \dots & v_1 w_n H \\ \vdots & \ddots & \vdots \\ v_m w_1 H & \dots & v_m w_n H \end{pmatrix}.$$

If B satisfies (C1), for convenience, we will consider the indices of the entries in B as pairs such that $B_{(\mu,i),(\nu,j)} = v_\mu w_\nu H_{i,j}$ for $\mu \in [m]$, $\nu \in [n]$, and $i, j \in [r]$. We call the submatrices $v_\mu v_\nu H$ the *tiles* of B.

The diagonal entries of the matrices D and O are vertex weights which, by the shape of C,

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

will be considered with respect to B. As B is an $rm \times rn$ matrix, we group the entries of O and D into $rm \times rm$ submatrices D^R, O^R corresponding to the rows of B and $rn \times rn$ submatrices D^C, O^C corresponding to the columns of B so as to obtain

$$D = \begin{pmatrix} D^R & 0 \\ 0 & D^C \end{pmatrix} \quad \text{and} \quad O = \begin{pmatrix} O^R & 0 \\ 0 & O^C \end{pmatrix}.$$

Furthermore, according to the tiles of B, the matrix D^R can be grouped into m *tiles* $D^{R,\mu}$ (for all $\mu \in [m]$), each of which is an $r \times r$ diagonal matrix. Analogously we group the matrix D^C into n submatrices $D^{C,\nu}$ for all $\nu \in [n]$ and we obtain

$$D^R = \begin{pmatrix} D^{R,1} & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & D^{R,m} \end{pmatrix} \quad \text{and} \quad D^C = \begin{pmatrix} D^{C,1} & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & D^{C,n} \end{pmatrix}.$$

The matrices O^R and O^C are grouped analogously. If B is symmetric, then $D^R = D^C$ and $O^R = O^C$. We define four more conditions:

(C2) D is a diagonal matrix of positive vertex weights, $O^{R,1}, O^{C,1}$, and $D+O$, and $D-O$ are nonnegative.

(C3) The matrix H is a Hadamard matrix.

(C4) For all $\mu \in [m]$, $\nu \in [n]$ there are $\alpha_\mu^R, \alpha_\nu^C$ such that $D^{R,\mu} = \alpha_\mu^R I_r$ and $D^{C,\nu} = \alpha_\nu^C I_r$.

(C5) There are sets $\Lambda^R, \Lambda^C \subseteq [r]$ such that for all $\mu \in [m]$, $\nu \in [n]$ there are β_μ^R, β_ν^C such that $O^{R,\mu} = \beta_\mu^R I_{r;\Lambda^R}$ and $O^{C,\nu} = \beta_\nu^C I_{r;\Lambda^C}$. Furthermore, $\Lambda^R = \emptyset$ ($\Lambda^C = \emptyset$, resp.) if and only if $\beta_\mu^R = 0$ for all $\mu \in [m]$ ($\beta_\nu^C = 0$ for all $\nu \in [n]$, resp.).

Before we transform a given problem EVAL(A) into the form EVAL(C, D, O) in Lemma 8.15, we will exclude some cases from our consideration. That is, we show in the following lemma that EVAL(A) is #P-hard unless the block B underlying A satisfies $\operatorname{rank}\operatorname{abs}(B) = 1$.

LEMMA 8.13. *Let A be a symmetric connected bipartite matrix with underlying block B. Then at least one of the following outcomes occurs.*

Outcome 1. EVAL(A) *is #P-hard. If B is symmetric, then* EVAL(B) *is #P-hard.*

Outcome 2. *For some $m, n \in \mathbb{N}$ there are vectors $v \in \mathbb{R}_{\mathbb{A}}^m$ and $w \in \mathbb{R}_{\mathbb{A}}^n$ satisfying $0 < v_1 < \ldots < v_m$ and $0 < w_1 < \ldots < w_n$ and permutations Σ and Π such that*

$$B_{\Sigma,\Pi} = \begin{pmatrix} v_1 w_1 S^{11} & \ldots & v_1 w_n S^{1n} \\ \vdots & \ddots & \vdots \\ v_m w_1 S^{m1} & \ldots & v_m w_n S^{mn} \end{pmatrix},$$

where, for $i \in [m]$ and $j \in [n]$, S^{ij} is a $\{-1, 1\}$-matrix of some order $m_i \times n_j$. If B is symmetric, then $\Sigma = \Pi$.

Proof. By Lemma 6.4, EVAL(A) is #P-hard unless $\operatorname{rank}\operatorname{abs}(B) = 1$. Similarly, if B is symmetric, then EVAL(B) is #P-hard unless $\operatorname{rank}\operatorname{abs}(B) = 1$.

We conclude that $\operatorname{abs}(B) = xy^T$ for some nonnegative real vectors x, y. If B is symmetric, then we can take $y = x$. To see this, suppose $\hat{x}$ and $\hat{y}$ are vectors such that $\hat{x}\hat{y}^T$ is symmetric and let $x_i = y_i = \sqrt{\hat{x}_i \hat{y}_i}$. Note that $x_i y_j = \sqrt{\hat{x}_i \hat{y}_i \hat{x}_j \hat{y}_j} = \hat{x}_i \hat{y}_j$.

Note that the vectors x and y contain no zero entries. This follows from the fact that $\operatorname{abs}(B)$ is a block because B is. Hence, if some entry of x satisfies $x_i = 0$, then $A_{i,*} = x_i x^T = 0$, and therefore B has a decomposition.

Let $v \in \mathbb{R}_{\mathbb{A}}^m$ be the vector of ascendingly ordered distinct entries of x. That is, $v_i < v_j$ for all $i < j$ and, for each x_i, there is a $j \in [m]$ such that $x_i = v_j$. Similarly, let w be the vector of ascendingly ordered distinct entries of y. ∎

LEMMA 8.14. *Let A be a symmetric $n \times n$ matrix of rank r and $I \subseteq [n]$ a set of indices with $|I| = r$. If A_{I*} has rank r, then the matrix A_{II} is nonsingular.*

Proof. As $\operatorname{rank} A_I = \operatorname{rank} A$, the rows of A with indices in $\bar{I}$ depend linearly on those from I. By symmetry this holds for the columns as well and is still true in A_I. Hence $\operatorname{rank} A = \operatorname{rank} A_{II}$. ∎

LEMMA 8.15. *Let A be a symmetric connected bipartite matrix with underlying block B_A of rank r. Then at least one of the following outcomes occurs.*

Outcome 1. EVAL(A) *is #P-hard. If B_A is symmetric, then* EVAL(B_A) *is #P-hard.*

Outcome 2. *There are a connected bipartite matrix C, whose underlying block B is size $mr \times nr$ for some m and n, and diagonal matrices D and O, which satisfy conditions* (C1) *and* (C2)*, such that*

$$\mathrm{EVAL}(C, D, O) \equiv \mathrm{EVAL}(A).$$

The matrices D and O consist of $mr \times mr$ submatrices D^R, O^R and $nr \times nr$ submatrices D^C, O^C such that

$$D = \begin{pmatrix} D^R & 0 \\ 0 & D^C \end{pmatrix} \text{ and } O = \begin{pmatrix} O^R & 0 \\ 0 & O^C \end{pmatrix}.$$

C, D, and O can be computed in time polynomial in the size of A. If B_A is symmetric, then so is B. Also $D^R = D^C$, $O^R = O^C$, and

$$\mathrm{EVAL}(B, D^R, O^R) \equiv \mathrm{EVAL}(B_A).$$

Proof. Suppose that the matrix A does not give Outcome 1 in Lemma 8.13. Let Σ and Π be the permutations from Lemma 8.13, and let Φ be the permutation on the rows of A that applies Σ to the rows of B_A and applies Π to the columns. Let $\widetilde{A} = A_{\Phi,\Phi}$. Note that $\mathrm{EVAL}(A) \equiv \mathrm{EVAL}(\widetilde{A})$. Also, the block underlying $\widetilde{A}$ is $(B_A)_{\Sigma,\Pi}$, which we denote $\widetilde{B}$. Note that $\widetilde{B}$ is symmetric if B_A is symmetric, since $\Sigma = \Pi$ in that case and $\mathrm{EVAL}(B_A) \equiv \mathrm{EVAL}(\widetilde{B})$. By Lemma 8.13 there are $m, n \in \mathbb{N}$ such that

$$\widetilde{B} = \begin{pmatrix} v_1 w_1 S^{11} & \dots & v_1 w_n S^{1n} \\ \vdots & \ddots & \vdots \\ v_m w_1 S^{m1} & \dots & v_m w_n S^{mn} \end{pmatrix}$$

for vectors $v \in \mathbb{R}_{\mathbb{A}}^m$, $w \in \mathbb{R}_{\mathbb{A}}^n$ of positive pairwise distinct reals and $\{-1, 1\}$-matrices $S^{\kappa\lambda}$ of order $m_\kappa \times n_\lambda$. Let

$$S = \begin{pmatrix} S^{11} & \dots & S^{1n} \\ \vdots & \ddots & \vdots \\ S^{m1} & \dots & S^{mn} \end{pmatrix}.$$

For convenience, we consider the indices of the entries in $\widetilde{B}$ as pairs such that $\widetilde{B}_{(\kappa,i),(\lambda,j)} = v_\kappa w_\lambda S^{\kappa\lambda}_{i,j}$ for $(\kappa, \lambda) \in [m] \times [n]$ and $(i, j) \in [m_\kappa] \times [n_\lambda]$. Entries and submatrices of S will be treated in the same way.

First we shall see that we may assume that either every pair of rows (or columns) of S is orthogonal or they are (possibly negated) copies of each other.

Claim 5. *Outcome* 1 *occurs unless for all $\kappa, \lambda \in [m]$ and $i \in [m_\kappa]$, $j \in [m_\lambda]$*

$$\begin{array}{l} \text{either } \langle S^{\kappa\nu}_{i,*}, S^{\lambda\nu}_{j,*} \rangle = 0 \text{ for every } \nu \in [n] \\ \text{or there is an } s \in \{-1, +1\} \text{ such that } S^{\kappa\nu}_{i,*} = s S^{\lambda\nu}_{j,*} \text{ for every } \nu \in [n]. \end{array} \tag{8.10}$$

The analogues hold for the columns of S: for all $\kappa, \lambda \in [n]$ and $i \in [n_\kappa]$, $j \in [n_\lambda]$

$$\begin{array}{l} \text{either } \langle S^{\mu\kappa}_{*,i}, S^{\mu\lambda}_{*,j} \rangle = 0 \text{ for every } \mu \in [m] \\ \text{or there is an } s \in \{-1, +1\} \text{ such that } S^{\mu\kappa}_{*,i} = s S^{\mu\lambda}_{*,j} \text{ for every } \mu \in [m]. \end{array} \tag{8.11}$$

Proof. Let $p \in \mathbb{N}$ be odd. By p-thickening and subsequent 2-stretching we obtain a reduction

$$\mathrm{EVAL}(A') \leq \mathrm{EVAL}(\widetilde{A})$$

for a matrix $A' = (\widetilde{A}^{(p)})^2$ which contains submatrices $\widetilde{B}^{(p)}(\widetilde{B}^{(p)})^T$ and $(\widetilde{B}^{(p)})^T\widetilde{B}^{(p)}$. The same reduction gives $\mathrm{EVAL}((\widetilde{B}^{(p)})^2) \leq \mathrm{EVAL}(\widetilde{B})$ if $\widetilde{B}$ is symmetric. We will give the proof of (8.10) by focusing on $\widetilde{B}^{(p)}(\widetilde{B}^{(p)})^T$. The analogous argument on $(\widetilde{B}^{(p)})^T\widetilde{B}^{(p)}$ yields (8.11).

Let $\widetilde{C} = \widetilde{B}^{(p)}(\widetilde{B}^{(p)})^T$. For $\kappa, \lambda \in [m]$ and $i \in [m_\kappa]$, $j \in [m_\lambda]$ we have

$$\widetilde{C}_{(\kappa,i),(\lambda,j)} = \sum_{(\nu,k)} \widetilde{B}^{(p)}_{(\kappa,i),(\nu,k)}\widetilde{B}^{(p)}_{(\lambda,j),(\nu,k)} = v_\kappa^p v_\lambda^p \sum_{\nu=1}^{n} w_\nu^{2p}\langle S^{\kappa\nu}_{i,*}, S^{\lambda\nu}_{j,*}\rangle. \tag{8.12}$$

Note that by 2-thickening we have a reduction $\mathrm{EVAL}(A'') \leq \mathrm{EVAL}(\widetilde{A})$ for a matrix $A'' = (A')^{(2)}$. This also gives a reduction $\mathrm{EVAL}(\widetilde{C}^{(2)}) \leq \mathrm{EVAL}(\widetilde{B})$ if $\widetilde{B}$ is symmetric. The matrix A'' has only nonnegative entries and contains the submatrix $\widetilde{C}^{(2)}$. Theorem 1.3 (due to Bulatov and Grohe) implies that $\mathrm{EVAL}(\widetilde{C}^{(2)})$ and $\mathrm{EVAL}(A'')$ are #P-hard, in which case Outcome 1 occurs, if $\widetilde{C}^{(2)}$ contains a block of row-rank at least 2. We shall determine the conditions under which this is not the case.

A 2×2 principal submatrix of $\widetilde{C}^{(2)}$, defined by $(\kappa, i), (\lambda, j)$, has determinant

$$\det_{(\kappa,i),(\lambda,j)} := \begin{vmatrix} \widetilde{C}^{(2)}_{(\kappa,i),(\kappa,i)} & \widetilde{C}^{(2)}_{(\kappa,i),(\lambda,j)} \\ \widetilde{C}^{(2)}_{(\lambda,j),(\kappa,i)} & \widetilde{C}^{(2)}_{(\lambda,j),(\lambda,j)} \end{vmatrix} = (\widetilde{C}_{(\kappa,i),(\kappa,i)}\widetilde{C}_{(\lambda,j),(\lambda,j)})^2 - (\widetilde{C}_{(\kappa,i),(\lambda,j)})^4.$$

We have

$$\widetilde{C}^{(2)}_{(\kappa,i),(\kappa,i)} = v_\kappa^{4p}\left(\sum_{\nu=1}^{n} w_\nu^{2p}\langle S^{\kappa\nu}_{i,*}, S^{\kappa\nu}_{i,*}\rangle\right)^2 = v_\kappa^{4p}\left(\sum_{\nu=1}^{n} w_\nu^{2p} n_\nu\right)^2,$$

and therefore

$$\det_{(\kappa,i),(\lambda,j)} = v_\kappa^{4p}v_\lambda^{4p}\left(\left(\sum_{\nu=1}^{n} w_\nu^{2p} n_\nu\right)^4 - \left(\sum_{\nu=1}^{n} w_\nu^{2p}\langle S^{\kappa\nu}_{i,*}, S^{\lambda\nu}_{j,*}\rangle\right)^4\right).$$

This determinant is zero if and only if there is an $s \in \{-1, 1\}$ such that $\langle S^{\kappa\nu}_{i,*}, S^{\lambda\nu}_{j,*}\rangle = sn_\nu$ for all $\nu \in [n]$, which implies $S^{\kappa\nu}_{i,*} = sS^{\lambda\nu}_{j,*}$ for all $\nu \in [n]$. If the determinant is nonzero, then the row-rank is two, so $\mathrm{EVAL}(\widetilde{C}^{(2)})$ is #P-hard if all of the entries of this principal submatrix are nonzero (in which case they are contained in a block). By (8.12) and Lemma 6.5 we further have $\widetilde{C}^{(2)}_{(\kappa,i),(\lambda,j)} = 0$ for arbitrarily large p if and only if $\langle S^{\kappa\nu}_{i,*}, S^{\lambda\nu}_{j,*}\rangle = 0$ for all $\nu \in [n]$.

Assume from now on that (8.10) and (8.11) hold. The next claim states that the rank of each tile of S equals the rank of S itself (which is equal to r, the rank of $\widetilde{B}$, which is the rank of B_A).

Claim 6. $\operatorname{rank} S = \operatorname{rank} S^{\kappa\lambda}$ *for all* $(\kappa, \lambda) \in [m] \times [n]$.

Proof. Equation (8.10) implies that $\operatorname{rank} S^{\kappa\mu} = \operatorname{rank} S^{\kappa\nu}$ for all $\kappa \in [m]$ and $\mu, \nu \in [n]$. Combining this with (8.11), we obtain $\operatorname{rank} S^{\kappa\mu} = \operatorname{rank} S^{\lambda\nu}$ for all $\kappa, \lambda \in [m]$ and $\mu, \nu \in [n]$.

Therefore, it suffices to show that $r = \operatorname{rank} S = \operatorname{rank} S^{11}$ holds. Let S^{*1} denote the matrix

$$S^{*1} = \begin{pmatrix} S^{11} \\ \vdots \\ S^{m1} \end{pmatrix}.$$

Let I be a set of row indices with $|I| = \operatorname{rank} S = r$ such that the set $\{S_{i,*} \mid i \in I\}$ is linearly independent. By (8.10) we have $\langle S_{i,*}, S_{j,*} \rangle = 0$ and $\langle S^{*1}_{i,*}, S^{*1}_{j,*} \rangle = 0$ for all $i \neq j \in I$. Hence, S^{*1} has rank r. As S^{11} is an $m_1 \times n_1$ matrix, there is a set $J \subseteq [n_1]$ such that the columns of S^{*1} with indices in J form a rank r set. Equation (8.11) implies $\langle S^{11}_{*,i}, S^{11}_{*,j} \rangle = 0$ for all $i \neq j \in J$. This proves the claim. ∎

Claim 6 has strong implications on S (and $\widetilde{B}$). It implies that for all $(\kappa, \lambda) \in [m] \times [n]$ there are sets $K_{(\kappa,\lambda)}, L_{(\kappa,\lambda)}$ of cardinality r such that $S^{\kappa\lambda}_{K_{(\kappa,\lambda)} L_{(\kappa,\lambda)}}$ is nonsingular. By (8.10) we take, without loss of generality, $K_{(\kappa,\lambda)} = K_{(\kappa,\lambda')}$ for all $\kappa \in [m]$ and $\lambda, \lambda' \in [n]$. Analogously, (8.11) implies $L_{(\kappa,\lambda)} = L_{(\kappa',\lambda)}$ for all $\kappa, \kappa' \in [m]$ and $\lambda \in [n]$. Therefore, there are sets of indices $K_1, \ldots, K_m$ and $L_1, \ldots, L_n$ each of cardinality r, such that the matrix

$$S^{\kappa\lambda}_{K_\kappa L_\lambda} \text{ is nonsingular for all } (\kappa, \lambda) \in [m] \times [n]. \tag{8.13}$$

If B_A is symmetric, then $\widetilde{B}$ is symmetric and we may assume, by Lemma 8.14, that $K_\kappa = L_\kappa$ for all $\kappa \in [m]$. But there is more we can infer from Claim 5, namely, the above nonsingular subtiles of each tile are (up to row-column negations and permutations) equal.

Claim 7. *For all $\kappa \in [m]$ and $\lambda \in [n]$ the sets K_κ and L_λ have orderings*

$$K_\kappa = \{k_{\kappa,1}, \ldots, k_{\kappa,r}\} \text{ and } L_\lambda = \{\ell_{\lambda,1}, \ldots, \ell_{\lambda,r}\}$$

and there are families $\{\tau^R_\kappa : [r] \to \{-1, 1\}\}_{\kappa \in [m]}$ and $\{\tau^C_\lambda : [r] \to \{-1, 1\}\}_{\lambda \in [n]}$ of mappings such that

$$S^{11}_{k_{1,a}\ell_{1,b}} = \tau^R_\kappa(a)\tau^C_\lambda(b) S^{\kappa\lambda}_{k_{\kappa,a},\ell_{\lambda,b}} \text{ for all } (\kappa, \lambda) \in [m] \times [n],\ a, b \in [r].$$

If $\widetilde{B}$ is symmetric, then S is symmetric, and $K_\kappa = L_\kappa$ and $\tau^R_\kappa = \tau^C_\kappa$ for all $\kappa \in [m]$.

Proof. As $S^{11}_{K_1 L_1} = S_{K_1 L_1}$ and $\operatorname{rank} S^{11} = \operatorname{rank} S$, (8.10) implies that every row in S is either a copy or a negated copy of a row in $S_{K_1 *}$. Fix an arbitrary ordering $K_1 = \{k_{1,1}, \ldots, k_{1,r}\}$. As $S^{\kappa 1}_{K_\kappa,*}$ has rank r for all $\kappa \in [m]$, there are an ordering $\{k_{\kappa,1}, \ldots, k_{\kappa,r}\}$ and, for every $a \in [r]$, an $s_a \in \{-1, +1\}$ such that $S^{11}_{k_{1,a},*} = s_a S^{\kappa 1}_{k_{\kappa,a},*}$. Let $\tau^R_\kappa(a) = s_a$. Then $S^{11}_{k_{1,a},*} = \tau^R_\kappa(a) S^{\kappa 1}_{k_{\kappa,a},*}$ for all $a \in [r]$. Equation (8.10) implies that this extends to

$$S^{1\lambda}_{k_{1,a},*} = \tau^R_\kappa(a) S^{\kappa\lambda}_{k_{\kappa,a},*} \text{ for all } a \in [r], \kappa \in [m], \lambda \in [n].$$

An analogous argument on the columns of S using (8.11) yields orderings of the sets L_λ and mappings τ_λ such that

$$S^{\kappa 1}_{*,\ell_{1,b}} = \tau^C_\lambda(b) S^{\kappa\lambda}_{*,\ell_{\lambda,b}} \text{ for all } b \in [r], \kappa \in [m], \lambda \in [n].$$

Combining both finishes the proof of Claim 7.

For $\kappa \in [m]$, let π^R_κ be a permutation of $[m_\kappa]$ which satisfies $\pi^R_\kappa(a) = k_{\kappa,a}$ for $a \in [r]$. For $\lambda \in [n]$, let π^C_λ be a permutation of $[n_\lambda]$ which satisfies $\pi^C_\lambda(a) = \ell_{\lambda,a}$ for all $a \in [r]$.

Let $\hat{S}^{\kappa\lambda}$ be the result of the permutations π^R_κ and π^C_λ when applied to $S^{\kappa\lambda}$; that is, $\hat{S}^{\kappa\lambda} := (S^{\kappa\lambda})_{\pi^R_\kappa,\pi^C_\lambda}$. Let $\hat{B}$ be the matrix defined by $\hat{B}_{(\kappa,i),(\lambda,j)} = v_\kappa w_\lambda \hat{S}^{\kappa\lambda}_{i,j}$ and let $\hat{S}$ be the matrix defined by $\hat{S}_{(\kappa,i),(\lambda,j)} = \hat{S}^{\kappa\lambda}_{i,j}$. Let $\hat{A}$ be the bipartite matrix with underlying block $\hat{B}$. Note that $\mathrm{EVAL}(\hat{A}) \equiv \mathrm{EVAL}(\widetilde{A}) \equiv \mathrm{EVAL}(A)$. The definition of these permutations implies that $\hat{B}$ is symmetric if $\widetilde{B}$ is symmetric (which is true if B_A is symmetric). In this case, $\mathrm{EVAL}(\hat{B}) \equiv \mathrm{EVAL}(\widetilde{B}) \equiv \mathrm{EVAL}(B_A)$. Equation (8.13) simplifies to

$$\hat{S}^{\kappa\lambda}_{[r][r]} \text{ is nonsingular for all } (\kappa,\lambda) \in [m] \times [n], \tag{8.14}$$

and Claim 7 implies furthermore that

$$\hat{S}^{11}_{a,b} = \tau^R_\kappa(a)\tau^C_\lambda(b)\hat{S}^{\kappa\lambda}_{a,b} \text{ for all } (\kappa,\lambda) \in [m] \times [n],\ a,b \in [r]. \tag{8.15}$$

We consider the twin-relation on $\hat{A}$ now. As $\hat{A}$ is bipartite, the equivalence classes of this relation induce collections of equivalence classes separately for the rows and columns of $\hat{B}$. Furthermore, as $\hat{B}_{(\kappa,i),(\lambda,j)} = v_\kappa w_\lambda \hat{S}^{\kappa\lambda}_{i,j}$ and the values v_i are pairwise distinct and positive, two rows corresponding to different v_i values are not twins. This is similarly true for the columns of $\hat{B}$. Hence, the equivalence classes of rows can be grouped into collections $\mathcal{I}_1, \ldots, \mathcal{I}_m$ and the equivalence classes of columns can be grouped into collections $\mathcal{J}_1, \ldots, \mathcal{J}_n$ such that, for every $\kappa \in [m]$, the collection $\mathcal{I}_\kappa$ contains the equivalence classes of rows in the submatrix

$$T^{\kappa *} := \begin{pmatrix} v_\kappa w_1 \hat{S}^{\kappa 1} & \cdots & v_\kappa w_n \hat{S}^{\kappa n} \end{pmatrix}$$

of $\hat{B}$. By (8.10) and (8.14) every row in $T^{\kappa *}$ is either a copy or a negated copy of a row in $(T^{\kappa *})_{[r]*}$. Moreover, every two $i \neq j \in [r]$ belong to different equivalence classes by (8.14).

We may therefore assume, without loss of generality, that the collection $\mathcal{I}_\kappa$ consists of classes $P^{\kappa *}_1, \ldots, P^{\kappa *}_r$ and $N^{\kappa *}_1, \ldots, N^{\kappa *}_r$ such that $i \in P^{\kappa *}_i$ for all $i \in [r]$. Furthermore, the sets $N^{\kappa *}_i$ account for the possible negated copies of rows in $(T^{\kappa *})_{[r]*}$, and therefore some of these sets may be empty. But for all $i \in [r]$ if $N^{\kappa *}_i$ is nonempty, then all $a \in N^{\kappa *}_i$ are indices of negated copies of rows from $P^{\kappa *}_i$.

Similarly, the collection J_λ of equivalence classes of columns corresponds to the submatrix

$$T^{*\lambda} := \begin{pmatrix} v_1 w_\lambda \hat{S}^{1\lambda} \\ \vdots \\ v_m w_\lambda \hat{S}^{m\lambda} \end{pmatrix}$$

of $\hat{B}$. By (8.11) every column in $T^{*\lambda}$ is either a copy or a negated copy of a column in $(T^{*\lambda})_{*[r]}$. Moreover, by (8.14) every two $i \neq j \in [r]$ belong to different equivalence classes of the twin-relation.

We may assume that the collection $\mathcal{J}_\lambda$ consists of classes $P^{*\lambda}_1, \ldots, P^{*\lambda}_r$ and $N^{*\lambda}_1, \ldots, N^{*\lambda}_r$ such that $i \in P^{*\lambda}_i$ for all $i \in [r]$. The sets $N^{*\lambda}_i$ account for the possible negated copies of columns in $(T^{*\lambda})_{*[r]}$, and therefore some of these sets may be empty.

But for all $i \in [r]$ if $N_i^{*\lambda}$ is nonempty, then all $a \in N_i^{*\lambda}$ are indices of negated copies of columns from $P_i^{*\lambda}$.

Note that if $\hat{B}$ is symmetric, the above definitions directly imply that $m = n$ and, for all $\mu \in [m]$, $\mathcal{I}_\mu = \mathcal{J}_\mu$. Also, we can take $P_i^{\mu *} = P_i^{*\mu}$ and $N_i^{\mu *} = N_i^{*\mu}$ for all $i \in [r]$.

Application of the Extended Twin Reduction Lemma, Lemma 8.3, according to these equivalency classes, therefore yields an evaluation problem $\mathrm{EVAL}(\hat{C}, D, \hat{O}) \equiv \mathrm{EVAL}(\hat{A})$ $(\equiv \mathrm{EVAL}(A))$ such that the block $\hat{B}'$ underlying $\hat{C}$ satisfies

$$\hat{B}' = \begin{pmatrix} v_1 w_1 \hat{S}^{11}_{[r][r]} & \dots & v_1 w_n \hat{S}^{1n}_{[r][r]} \\ \vdots & \ddots & \vdots \\ v_m w_1 \hat{S}^{m1}_{[r][r]} & \dots & v_m w_n \hat{S}^{mn}_{[r][r]} \end{pmatrix}.$$

That is, $\hat{B}'$ is an $mr \times nr$ matrix and D and $\hat{O}$ are diagonal matrices of vertex weights of order $mr + nr$. Grouping these vertex weights according to the rows and columns of $\hat{B}'$ to which they correspond, we obtain

$$D = \begin{pmatrix} D^R & 0 \\ 0 & D^C \end{pmatrix} \text{and } \hat{O} = \begin{pmatrix} \hat{O}^R & 0 \\ 0 & \hat{O}^C \end{pmatrix}$$

for $mr \times mr$ diagonal matrices $D^R, \hat{O}^R$ and $nr \times nr$ diagonal matrices $D^C, \hat{O}^C$. Their structure corresponding to the tiles of $\hat{B}'$ in turn is

$$D^R = \begin{pmatrix} D^{R,1} & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & D^{R,m} \end{pmatrix} \text{and } D^C = \begin{pmatrix} D^{C,1} & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & D^{C,n} \end{pmatrix},$$

which holds analogously for $\hat{O}$ such that the $D^{R,\mu}, \hat{O}^{R,\mu}, D^{C,\nu}, \hat{O}^{C,\nu}$ for all $\mu \in [m]$, $\nu \in [n]$ are $r \times r$ diagonal matrices. The definition of these matrices according to the Extended Twin Reduction Lemma, Lemma 8.3, is then, for all $\mu \in [m]$, $\nu \in [n]$, $i, j \in [r]$, given by

$$\begin{aligned} D^{R,\mu}_{i,i} &= |P_i^{\mu *}| + |N_i^{\mu *}| \quad \text{and} \quad D^{C,\nu}_{j,j} = |P_j^{*\nu}| + |N_j^{*\nu}|, \\ \hat{O}^{R,\mu}_{i,i} &= |P_i^{\mu *}| - |N_i^{\mu *}| \quad \text{and} \quad \hat{O}^{C,\nu}_{j,j} = |P_j^{*\nu}| - |N_j^{*\nu}|. \end{aligned} \tag{8.16}$$

If B_A is symmetric then $\hat{B}$ is symmetric, and $D^R = D^C$. Also, $\hat{B}'$ is also symmetric and $\mathrm{EVAL}(\hat{B}', D^R, \hat{O}^R) \equiv \mathrm{EVAL}(\hat{B})$.

Clearly, the matrix D is a diagonal matrix of vertex weights whose diagonal is positive as the sets $P_i^{\kappa *}$ and $P_i^{*\lambda}$ are nonempty by definition for all $\kappa \in [m]$, $\lambda \in [n]$, and $i \in [r]$.

By (8.15), for all $(\kappa, \lambda) \in [m] \times [n]$, the matrix $\hat{S}^{\kappa\lambda}_{[r][r]}$ is—up to negations of rows and columns—just a copy of the matrix $\hat{S}^{11}_{[r][r]}$. However, the diagonal entries of $\hat{O}$ given by (8.16) may be negative in some cases. To satisfy condition (C2), we therefore define mappings $\rho : [r] \to \{-1, 1\}$ and $\gamma : [r] \to \{-1, 1\}$ by

$$\rho(i) = \begin{cases} -1 & \text{if } \hat{O}^{R,1}_{i,i} < 0, \\ 1 & \text{otherwise} \end{cases} \qquad \text{and} \qquad \gamma(j) = \begin{cases} -1 & \text{if } \hat{O}^{C,1}_{j,j} < 0, \\ 1 & \text{otherwise.} \end{cases}$$

We will use these mappings below to "transfer" the signs of diagonal entries of $\hat{O}^{R,1}$ and $\hat{O}^{C,1}$ to $\hat{B}'$. Note that $\rho = \gamma$ if B_A is symmetric since $\hat{O}^R = \hat{O}^C$ in this case. Define

matrices $\check{S}^{\kappa\lambda}_{[r][r]}$ by applying row and column negations according to these mappings; that is,

$$\check{S}^{\kappa\lambda}_{a,b} = \rho(a)\gamma(b)\tau^R_\kappa(a)\tau^C_\lambda(b)\hat{S}^{\kappa\lambda}_{a,b} \text{ for all } (\kappa,\lambda) \in [m]\times[n],\ a,b\in[r]. \tag{8.17}$$

By (8.15), we have the following for all $(\kappa,\lambda)\in[m]\times[n]$ and $a,b\in[r]$:

$$\rho(a)\gamma(b)\hat{S}^{11}_{a,b} = \rho(a)\gamma(b)\tau^R_\kappa(a)\tau^C_\lambda(b)\hat{S}^{\kappa\lambda}_{a,b} = \check{S}^{\kappa\lambda}_{a,b}.$$

Thus

$$\tau^R_1(a)\tau^C_1(b)\check{S}^{11}_{a,b} = \rho(a)\gamma(b)\tau^R_1(a)\tau^C_1(b)\tau^R_1(a)\tau^C_1(b)\hat{S}^{11}_{a,b} = \check{S}^{\kappa\lambda}_{a,b}.$$

But, by their definition in Claim 7, the mappings τ^R_1 and τ^C_1 satisfy $\tau^R_1(i) = \tau^C(i) = 1$ for all $i\in[r]$. So the above equation gives $\check{S}^{11}_{a,b} = \check{S}^{\kappa\lambda}_{a,b}$ for all $(\kappa,\lambda)\in[m]\times[n]$ and $a,b\in[r]$, and so $\check{S}^{11}_{[r][r]} = \check{S}^{\kappa\lambda}_{[r][r]}$ for all $(\kappa,\lambda)\in[m]\times[n]$. Define $H := \check{S}^{11}_{[r][r]}$. Let B be the matrix defined by $B_{(\kappa,i),(\lambda,j)} = v_\kappa w_\lambda H_{i,j}$ so that

$$\begin{aligned} B_{(\kappa,i),(\lambda,j)} &= v_\kappa w_\lambda \check{S}^{11}_{i,j} \\ &= v_\kappa w_\lambda \check{S}^{\kappa\lambda}_{i,j} \\ &= v_\kappa w_\lambda \rho(i)\gamma(j)\tau^R_\kappa(i)\tau^C_\lambda(j)\hat{S}^{\kappa\lambda}_{i,j} \\ &= \rho(i)\gamma(j)\tau^R_\kappa(i)\tau^C_\lambda(j)\hat{B}_{(\kappa,i),(\lambda,j)}. \end{aligned}$$

Let C be the symmetric bipartite matrix with underlying block B. For $\kappa\in[m]$, $\lambda\in[n]$, and $i,j\in[r]$, let

$$O^{R,\kappa}_{i,i} = \rho(i)\tau^R_\kappa(i)\hat{O}^{R,\kappa}_{i,i} \quad \text{and} \quad O^{C,\lambda}_{j,j} = \gamma(j)\tau^C_\lambda(j)\hat{O}^{C,\lambda}_{j,j}.$$

Let O^R be the diagonal matrix with tiles $O^{R,\kappa}$ for $\kappa\in[m]$ and O^C be the diagonal matrix with tiles $O^{C,\lambda}$ for $\lambda\in[n]$. Let O be the matrix

$$O = \begin{pmatrix} O^R & 0 \\ 0 & O^C \end{pmatrix}.$$

Since (as noted above) $\tau^R_1(i) = \tau^C(i) = 1$ for all $i\in[r]$, the matrices $O^{R,1}$ and $O^{C,1}$ are nonnegative.

The Row-Column Negation Lemma, Lemma 8.4, implies

$$\mathrm{EVAL}(\hat{C}, D, \hat{O}) \equiv \mathrm{EVAL}(C, D, O).$$

The block B satisfies (C1) and the matrices D and O satisfy (C2). The definitions of D and $\hat{O}$ in (8.16) and the definition of O imply that $D+O$ and $D-O$ are nonnegative, as required. If B_A is symmetric, then $\widetilde{B}$ and S are symmetric, so $\tau^R_\kappa = \tau^C_\kappa$ and $\pi^R_\kappa = \pi^C_\kappa$, so $\hat{S}$ and $\hat{B}$ are symmetric. Since $\rho = \gamma$, B is also symmetric. So the Row-Column Negation Lemma, Lemma 8.4, implies

$$\mathrm{EVAL}(\hat{B}', D^R, \hat{O}^R) \equiv \mathrm{EVAL}(B, D^R, O^R).$$

Furthermore, it is easy to see that all operations performed to form C, D, O from the matrix A are polynomial-time computable. This finishes the proof. ∎

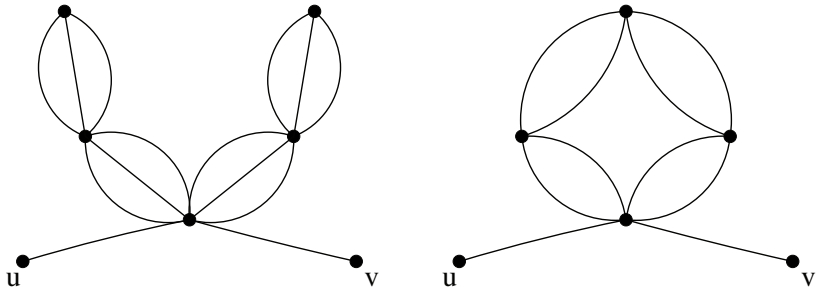

FIG. 8.1. *The gadget templates* $T(1,3,2)$ *and* $T(2,2,1)$.

The remainder of this section relies on a gadget which consists of arrangements of paths of length 2. These paths affect the matrices C, D, O in a way similar to 2-stretching. It is therefore convenient to have a look at the effect this operation has. Clearly 2-stretching yields $\mathrm{EVAL}(CDC, D, O) \leq \mathrm{EVAL}(C, D, O)$. If B is symmetric, then it also yields $\mathrm{EVAL}(BD^RB, D^R, O^R) \leq \mathrm{EVAL}(B, D^R, O^R)$.

Assume that C and D, O satisfy conditions (C1) and (C2). Recall that $B = vw^T \otimes H$ holds for the block B underlying C. Furthermore, the matrix CDC contains the submatrices BD^CB^T and B^TD^RB and

$$BD^CB^T = \begin{pmatrix} v_1v_1H(\sum_{\nu=1}^n w_\nu^2 D^{C,\nu})H^T & \dots & v_1v_mH(\sum_{\nu=1}^n w_\nu^2 D^{C,\nu})H^T \\ \vdots & \ddots & \vdots \\ v_mv_1H(\sum_{\nu=1}^n w_\nu^2 D^{C,\nu})H^T & \dots & v_mv_mH(\sum_{\nu=1}^n w_\nu^2 D^{C,\nu})H^T \end{pmatrix}.$$

With analogous analysis of B^TD^RB, we have

$$BD^CB^T = vv^T \otimes \left(H \left(\sum_{\nu=1}^n w_\nu^2 D^{C,\nu} \right) H^T \right) \quad \text{and} \tag{8.18}$$

$$B^TD^RB = ww^T \otimes \left(H^T \left(\sum_{\mu=1}^m v_\mu^2 D^{R,\mu} \right) H \right).$$

We define a *reduction template* $T(t,p,q)$ which will be used in the proofs of Lemmas 8.17 and 8.19. Let $P(t,p)$ be a graph constructed as follows. Start with an edge with a distinguished endpoint a. Then perform in succession a t-thickening, then a 2-stretch, and finally a p-thickening. (Informally, there is a vertex b connected to a by t many length-2 paths such that all edges in those paths have multiplicity p.)

The reduction $T(t,p,q)$ works as follows. In a given graph $G = (V,E)$, we 2-stretch each edge $e \in E$ and call the middle vertex v_e. We attach q disjoint copies of $P(t,p)$ by identifying their terminal vertices with v_e. Figure 8.1 illustrates the construction.

Recall that $M \circ N$ denotes the Hadamard product of matrices M and N.

LEMMA 8.16. *Suppose* C *and* D, O *satisfy* (C1) *and* (C2). *At least one of the following outcomes occurs.*

Outcome 1. $\mathrm{EVAL}(C, D, O)$ *is* #P*-hard. If* B *is symmetric, then* $\mathrm{EVAL}(B, D^R, O^R)$ *is* #P*-hard.*

Outcome 2. *For $t, p, q \in \mathbb{N}$ and $p' = 2p+1$ and $q' = 2q$ there are $r \times r$ matrices $\Theta = \Theta(t,p')$ and $\Xi = \Xi(t,p')$ defined by*

$$\Theta = (\gamma_{p'}^R)^t \cdot \sum_{\mu=1}^{m} v_\mu^{tp'} \cdot \begin{cases} D^{R,\mu} & \text{if } t \text{ is even,} \\ O^{R,\mu} & \text{if } t \text{ is odd,} \end{cases}$$

$$\Xi = (\gamma_{p'}^C)^t \cdot \sum_{\nu=1}^{n} w_\nu^{tp'} \cdot \begin{cases} D^{C,\nu} & \text{if } t \text{ is even,} \\ O^{C,\nu} & \text{if } t \text{ is odd} \end{cases}$$

for positive constants $\gamma_{p'}^R$ and $\gamma_{p'}^C$ depending on p'.

The reduction $T(t,p',q')$ yields $\mathrm{EVAL}(C\Delta C, D, O) \le \mathrm{EVAL}(C, D, O)$ *for a diagonal matrix*

$$\Delta = \Delta(t,p',q') = \begin{pmatrix} \Delta^R & 0 \\ 0 & \Delta^C \end{pmatrix} \text{ and a matrix } C\Delta C = \begin{pmatrix} B\Delta^C B^T & 0 \\ 0 & B^T\Delta^R B \end{pmatrix}.$$

Δ^R is a diagonal $rm \times rm$ matrix of $r \times r$ tiles $\Delta^{R,\mu} = v_\mu^{tp'q'} D^{R,\mu} \circ \Theta^{(q')}$ for all $\mu \in [m]$. Δ^C is a diagonal $rn \times rn$ matrix of $r \times r$ tiles $\Delta^{C,\nu} = w_\nu^{tp'q'} D^{C,\nu} \circ \Xi^{(q')}$ for all $\nu \in [n]$. If B is symmetric, then the same reduction yields

$$\mathrm{EVAL}(B\Delta^R B, D^R, O^R) \le \mathrm{EVAL}(B, D^R, O^R).$$

Proof. Let p', q' be as above.

Claim 8. *Either Outcome 1 occurs or there are constants $\gamma_{p'}^R$ and $\gamma_{p'}^C$ depending on p' such that*

(8.19)
$$B^{(p')} D^C (B^{(p')})^T = (vv^T)^{(p')} \otimes \gamma_{p'}^R I_r \quad \text{and} \quad (B^{(p')})^T D^R B^{(p')} = (ww^T)^{(p')} \otimes \gamma_{p'}^C I_r.$$

Proof. We have $\mathrm{EVAL}(C^{(p')} D C^{(p')}, D, O) \le \mathrm{EVAL}(C, D, O)$ by p'-thickening followed by 2-stretching. If B is symmetric, this also yields $\mathrm{EVAL}(B^{(p')} D^R B^{(p')}, D^R, O^R) \le \mathrm{EVAL}(B, D^R, O^R)$. Matrix $C^{(p')} D C^{(p')}$ contains submatrices $X := B^{(p')} D^C (B^{(p')})^T$ and $Y := (B^{(p')})^T D^R B^{(p')}$. We show the first part of (8.19) by an argument based on the matrix X. The second part then follows analogously using Y. (Recall from (C1) that $D^R = D^C$ when B is symmetric, in which case $X = Y$.)

Define $\Pi = \sum_{\nu=1}^{n} w_\nu^2 D^{C,\nu}$. By (8.18) we have $X = (vv^T)^{p'} \otimes \big(H\Pi H^T\big)$. Therefore, if $\mathrm{abs}(H\Pi H^T)$ contains a block of row rank at least two, then X does.

As H is a $\{-1,1\}$-matrix, we have $(H\Pi H^T)_{i,i} = \mathrm{tr}(\Pi)$ for all $i \in [r]$ and the trace of Π is positive. Furthermore, $|(H\Pi H^T)_{i,j}| < \mathrm{tr}(\Pi)$ for all $j \ne i$ by the nonsingularity of H. Hence, we obtain a block of rank at least 2 in $\mathrm{abs}(H\Pi H^T)$ if there is a nonzero entry $(H\Pi H^T)_{i,j}$ for some $i \ne j \in [r]$. The proof follows with $\gamma_{p'}^R = \mathrm{tr}(\Pi)$.

For convenience, let $T = T(t)$ denote the matrix D if t is even and O otherwise.

Recall the reduction template; let $(\mu, i), (\kappa, k) \in [m+n] \times [r]$ denote the spins of v_e and b.

The diagonal (μ, i) entries of Δ correspond to the partition function of the reduction template with vertex v_e fixed to (μ, i). Therefore, for $\mu \in [m]$,

$$\begin{aligned}\Delta_{i,i}^{R,\mu} &= D_{i,i}^{R,\mu}\left(\sum_{\kappa=1}^{m}\sum_{k=1}^{r} T_{k,k}^{R,\kappa}(C^{(p')}DC^{(p')})^t_{(\mu,i),(\kappa,k)}\right)^{q'} \\ &= D_{i,i}^{R,\mu}\left(\sum_{\kappa=1}^{m}\sum_{k=1}^{r} T_{k,k}^{R,\kappa}(B^{(p')}D^C(B^{(p')})^T)^t_{(\mu,i),(\kappa,k)}\right)^{q'} \\ &= v_\mu^{tp'q'} D_{i,i}^{R,\mu}\left((\gamma_{p'}^R)^t \cdot \sum_{\kappa=1}^{m} v_\kappa^{tp'} T_{i,i}^{R,\kappa}\right)^{q'},\end{aligned}$$

where the last equation follows from Claim 8. Similarly, for $\nu \in [n]$,

$$\begin{aligned}\Delta_{ii}^{C,\nu} &= D_{i,i}^{C,\nu}\left(\sum_{\kappa=1}^{n}\sum_{k=1}^{r} T_{k,k}^{C,\kappa}(C^{(p')}DC^{(p')})^t_{(\nu,i),(\kappa,k)}\right)^{q'} \\ &= D_{i,i}^{C,\nu}\left(\sum_{\kappa=1}^{n}\sum_{k=1}^{r} T_{k,k}^{C,\kappa}((B^{(p')})^T D^R B^{(p')})^t_{(\nu,i),(\kappa,k)}\right)^{q'} \\ &= w_\nu^{tp'} D_{i,i}^{C,\nu}\left((\gamma_{p'}^C)^t \sum_{\kappa=1}^{n} w_\kappa^{tp'} T_{i,i}^{C,\kappa}\right)^{q'}.\end{aligned}$$

With Θ and Ξ defined as in the statement of the lemma, the proof follows. ∎

LEMMA 8.17. *Let C and D, O satisfy* (C1) *and* (C2)*. At least one of the following outcomes occurs.*

Outcome 1. $\mathrm{EVAL}(C, D, O)$ *is* #P*-hard. If B is symmetric, then* $\mathrm{EVAL}(B, D^R, O^R)$ *is* #P*-hard.*

Outcome 2. *Conditions* (C3) *and* (C4) *are satisfied.*

Proof. The #P-hardness part will be shown using a gadget construction $T(2, p', q')$ with $p' = 2p + 1$ and $q' = 2q$ for $p, q \in \mathbb{N}$. By Lemma 8.16 this yields a reduction $\mathrm{EVAL}(C\Delta C, D, O) \le \mathrm{EVAL}(C, D, O)$ such that $C\Delta C$ contains submatrices $B\Delta^C B^T$ and $B^T\Delta^R B$. If B is symmetric, then $\mathrm{EVAL}(B\Delta^R B, D^R, O^R) \le \mathrm{EVAL}(B, D^R, O^R)$. Focusing on $B^T\Delta^R B$, we will prove (C3) and the part of (C4) which claims that $D^{R,\mu} = \alpha_\mu^R I_r$. The proof for $D^{C,\nu} = \alpha_\nu^C I_r$ then follows by analogous arguments based on $B\Delta^C B^T$.

Recall that by the proof of (8.18) we have $B^T\Delta^R B = (ww^T) \otimes (H^T\Delta' H)$ for an $r \times r$ diagonal matrix Δ' defined by

$$\Delta' = \sum_{\mu=1}^{m} v_\mu^2 \Delta^{R,\mu} = \left(\sum_{\mu=1}^{m} v_\mu^{2p'q'+2} D^{R,\mu}\right) \circ \Theta^{[p]^{(q')}}$$

$$\text{with } \Theta^{[p]} = \Theta(2, p', q') = (\gamma_{p'}^R)^2 \cdot \sum_{\mu=1}^{m} v_\mu^{2p'} \cdot D^{R,\mu}. \tag{8.20}$$

If $\mathrm{abs}(H^T\Delta' H)$ contains a block of rank at least 2, then $\mathrm{abs}(B\Delta^R B)$ does. So, if $\mathrm{abs}(H^T\Delta' H)$ contains a block of rank at least 2, then Outcome 1 occurs by Lemma 6.4.

By the definition of $H^T\Delta' H$, we have $(H^T\Delta' H)_{i,i} = \mathrm{tr}(\Delta')$ for all $i \in [r]$, and this trace is positive by the definition of Δ'. Therefore, every principal 2×2 submatrix of $\mathrm{abs}(H^T\Delta' H)$ has the form

$$\begin{pmatrix} \mathrm{tr}(\Delta') & |(H^T\Delta' H)_{i,j}| \\ |(H^T\Delta' H)_{j,i}| & \mathrm{tr}(\Delta') \end{pmatrix}.$$

As H is nonsingular, $|(H^T\Delta' H)_{i,j}| < \mathrm{tr}(\Delta')$ for all $i \neq j \in [r]$, and, therefore, every such submatrix has a nonzero determinant. Furthermore, such a submatrix is part of a block if $(H^T\Delta' H)_{i,j} \neq 0$. Therefore, we have Outcome 1 if we can show that $(H^T\Delta' H)_{i,j} \neq 0$ for some $i \neq j \in [r]$ and some $p, q \in \mathbb{N}$.

Assume, therefore, that $(H^T\Delta' H)_{i,j} = 0$ for all $i \neq j \in [r]$ and all $p, q \in \mathbb{N}$. The remainder of the proof is to show that in this case conditions (C3) and (C4) are satisfied.

Let $\vartheta_{p,q,i} = \sum_{\mu=1}^{m} v_\mu^{2p'q'+2} D_{i,i}^{R,\mu}$ for all $i \in [r]$. Note that $\Delta'_{i,i} = \vartheta_{p,q,i}{\Theta^{[p]}}^{q'}_{i,i}$. We define an equivalence relation $\sim$ on $[r]$ by letting $i \sim j$ if and only if $D_{i,i}^{R,\mu} = D_{j,j}^{R,\mu}$ for all $\mu \in [m]$. Let $\mathbf{I}$ be the set of equivalence classes. We will use the notation $D_I^{R,\mu}$ to denote the value $D_{i,i}^{R,\mu}$ for $i \in I$. Similarly, we use the notation $\vartheta_{p,q,I}$ and $\Theta_{p,I}$ to denote the values $\vartheta_{p,q,i}$ and $\Theta_{i,i}^{[p]}$ for $i \in I$.

For $i, j \in [r]$ define sets $\mathcal{P}_{ij} = \{k \in [r] \mid H_{k,i}H_{k,j} > 0\}$ and $\mathcal{N}_{ij} = \{k \in [r] \mid H_{k,i}H_{k,j} < 0\}$.

Then we have

$$\begin{aligned}(H^T\Delta' H)_{i,j} = \sum_{k=1}^{r} H_{k,i}H_{k,j}\Delta'_{k,k} &= \sum_{k=1}^{r} H_{k,i}H_{k,j}\vartheta_{p,q,k}\left({\Theta^{[p]}}_{k,k}\right)^{q'} \\ &= \left(\sum_{k\in\mathcal{P}_{ij}} \vartheta_{p,q,k}({\Theta^{[p]}}_{k,k})^{q'} - \sum_{l\in\mathcal{N}_{ij}} \vartheta_{p,q,l}({\Theta^{[p]}}_{l,l})^{q'}\right).\end{aligned}$$

Then

$$\begin{aligned}(H^T\Delta' H)_{i,j} &= \sum_{I\in\mathbf{I}} \left(\sum_{k\in I\cap\mathcal{P}_{ij}} \vartheta_{p,q,k}({\Theta^{[p]}}_{k,k})^{q'} - \sum_{l\in I\cap\mathcal{N}_{ij}} \vartheta_{p,q,l}({\Theta^{[p]}}_{l,l})^{q'}\right) \\ &= \sum_{I\in\mathbf{I}} \Theta_{p,I}^{q'} \left(\sum_{k\in I\cap\mathcal{P}_{ij}} \vartheta_{p,q,I} - \sum_{l\in I\cap\mathcal{N}_{ij}} \vartheta_{p,q,I}\right) \\ &= \sum_{I\in\mathbf{I}} \vartheta_{p,q,I}\Theta_{p,I}^{q'} \left(|I\cap\mathcal{P}_{i,j}| - |I\cap\mathcal{N}_{i,j}|\right).\end{aligned}$$

Claim 9. *Suppose that $(H^T\Delta' H)_{i,j} = 0$ for all $i \neq j \in [r]$ and all $p, q \in \mathbb{N}$. Then there is a $J \in \mathbf{I}$ such that $|J \cap \mathcal{P}_{ij}| = |J \cap \mathcal{N}_{ij}|$ for all $i \neq j \in [r]$.*

Proof. Recall that the values v_μ in the definition of $\vartheta_{p,q,I}$ and ${\Theta^{[p]}}_{i,i}$ are pairwise distinct and nonnegative. Assume without loss of generality that the values v_μ are ordered decreasingly, i.e., $v_1 > v_2 > \cdots > v_m$. For each $I \in \mathbf{I}$ consider the vector $(D_I^{R,1}, D_I^{R,2}, \ldots, D_I^{R,m})$. Let $J \in \mathbf{I}$ such that the corresponding vector is maximal in the lexicographical order of these vectors. The definition of J implies that it is

unique. Further, we claim that, for every $I \neq J$,

$$\text{there is an } r_I \text{ such that, for all } r \geq r_I,\ \sum_{\mu=1}^{m} v_\mu^r D_I^{R,\mu} < \sum_{\mu=1}^{m} v_\mu^r D_J^{R,\mu}. \tag{8.21}$$

To see this fix some $I \in \mathbf{I}$ and let $\kappa \in [m]$ be the smallest index such that $D_J^{R,\kappa} > D_I^{R,\kappa}$. Then the inequality of (8.21) holds if

$$v_\kappa^r (D_J^{R,\kappa} - D_I^{R,\kappa}) > \sum_{\mu=\kappa+1}^{m} v_\mu^r (D_J^{R,\mu} - D_I^{R,\mu}),$$

which holds for large enough r since $v_\kappa > v_\mu$ for all $\mu > \kappa$.

By (8.21) we can thus fix a p which satisfies $p \geq r_I$ for all $I \in \mathbf{I}$. The definition of the values $\vartheta_{p,q,I}$ and $\Theta_{p,I}$ therefore implies that for any $q \in \mathbb{N}$ and $I \in \mathbf{I}$, we have $0 < \vartheta_{p,q,I} < \vartheta_{p,q,J}$ and $0 < \Theta_{p,I} < \Theta_{p,J}$.

Now consider $i \neq j \in [r]$. For all $I \in \mathbf{I}$, let $c_I = |I \cap \mathcal{P}_{ij}| - |I \cap \mathcal{N}_{ij}|$.

Since $(H^T \Delta' H)_{i,j} = 0$, for all $q \in \mathbb{N}$,

$$\begin{aligned} 0 &= \sum_{I \in \mathbf{I}} c_I \vartheta_{p,q,I} \Theta_{p,I}^{2q} \\ &= c_J \vartheta_{p,q,J} \Theta_{p,J}^{2q} + \sum_{I \in \mathbf{I} \setminus \{J\}} c_I \vartheta_{p,q,I} \Theta_{p,I}^{2q} \\ &= c_J + \sum_{I \in \mathbf{I} \setminus \{J\}} c_I \frac{\vartheta_{p,q,I}}{\vartheta_{p,q,J}} \left(\frac{\Theta_{p,I}}{\Theta_{p,J}} \right)^{2q}. \end{aligned} \tag{8.22}$$

As q tends to infinity, the sum tends to 0, so $c_J = 0$.

Assume now that $(H^T \Delta' H)_{i,j} = 0$ for all $i \neq j \in [r]$ and $p, q \in \mathbb{N}$. Fix $J \in \mathbf{I}$ such that $|J \cap \mathcal{P}_{ij}| = |J \cap \mathcal{N}_{ij}|$ for all $i \neq j \in [r]$. Recall that $H_{J,*}$ denotes the submatrix of H consisting of the rows of H with indices in J. For each pair $i \neq j \in [r]$, the fact that $|J \cap \mathcal{P}_{ij}| = |J \cap \mathcal{N}_{ij}|$ implies $\langle (H_{J,*})_{*,i}, (H_{J,*})_{*,j} \rangle = 0$. Hence, the columns in $H_{J,*}$ are pairwise orthogonal. Since the rank of H is r, this implies that $|J| = r$. Now since the rows of H^T are pairwise orthogonal, we have $H^T H = r I_r$, so the inverse of H^T is $r^{-1} H$. As right inverses of matrices are also left inverses, we have $r^{-1} H H^T = I_r$, and therefore H is a Hadamard matrix, and we have proved condition (C3).

Finally, $J = [r]$ implies that $D_{i,i}^{R,\mu} = D_{j,j}^{R,\mu}$ for all $i, j \in [r]$. Equivalently, $D^{R,\mu} = \alpha_\mu^R I_r$ for some appropriate α_μ^R. This proves (C4). ∎

We call a diagonal matrix D *preuniform* if there is a nonnegative d such that all diagonal entries $D_{i,i}$ of D satisfy $D_{i,i} \in \{0, d\}$. An important technical tool in the last step of our proof of conditions (C1)–(C5) will be the following lemma.

LEMMA 8.18 (Preuniform Diagonal Lemma). *Let H be a nonsingular $r \times r$ $\{-1, 1\}$-matrix and D be an $r \times r$ diagonal matrix with nonnegative entries in $\mathbb{R}$. If D is not preuniform, then there is a $p \in \mathbb{N}$ such that* $\operatorname{abs}(H D^{(p)} H^T)$ *contains a block of row-rank at least* 2.

Proof. Note that, if the diagonal of D is constantly zero, then D is preuniform. Assume therefore that there is some positive diagonal entry in D. Define $B := H D^{(p)} H^T$, $K := \{k \in [r] \mid D_{k,k} > 0\}$, and $s := |K|$. Hence, for $i, j \in [r]$,

$$\begin{aligned} B_{ij} &= \textstyle\sum_{k=1}^{r} H_{i,k} H_{j,k} (D_{k,k})^p = \sum_{k \in K} H_{i,k} H_{j,k} (D_{k,k})^p \\ &= (H_{*,K} D^{(p)} (H_{*,K})^T)_{i,j}. \end{aligned} \tag{8.23}$$

That is, for every $I \subseteq [r]$, we have $B_{I,I} = H_{I,K} D^{(p)}_{K,K} (H_{I,K})^T$. Fix a set $I \subseteq [r]$ such that $|I| = s$ and the matrix $H_{I,K}$ has rank s. Since $H_{I,K}$ is nonsingular, every 2×2 principal submatrix of $B_{I,I}$ has a nonzero determinant. To see this, note that by (8.23) we have $B_{i,i} = \mathrm{tr}(D^{(p)}_{K,K})$ for all $i \in I$ and this trace is positive. Then every such principal 2×2 submatrix has determinant

$$\begin{vmatrix} \mathrm{tr}(D^{(p)}_{K,K}) & |(H_{I,K} D^{(p)}_{KK} (H_{I,K})^T)_{i,j}| \\ |(H_{I,K} D^{(p)}_{K,K} (H_{I,K})^T)_{j,i}| & \mathrm{tr}(D^{(p)}_{K,K}) \end{vmatrix},$$

and by the nonsingularity of $H_{I,K}$ we have $|(H_{I,K} D^{(p)}_{K,K} (H_{I,K})^T)_{i,j}| < \mathrm{tr}(D^{(p)}_{K,K})$ (compare with (8.23)). Hence the above determinant is nonzero.

Assume that, for all $p \in \mathbb{N}$, there are no nontrivial blocks in $B_{I,I}$, i.e., $B_{i,j} = 0$ for all $i \neq j \in I$. We will show that this implies that D is preuniform.

For $i, j \in I$ define the sets $\mathcal{P}_{i,j} := \{k \in K \mid H_{i,k} H_{j,k} = 1\}$ and $\mathcal{N}_{i,j} := \{k \in K \mid H_{i,k} H_{j,k} = -1\}$. That is, $\mathcal{P}_{i,j}$ and $\mathcal{N}_{i,j}$ form a partition of K. Therefore, for $i, j \in I$ we have

$$B_{i,j} = \sum_{k=1}^{n} H_{i,k} H_{j,k} D^p_{k,k} = \sum_{k \in \mathcal{P}_{i,j}} D^p_{k,k} - \sum_{k \in \mathcal{N}_{i,j}} D^p_{k,k}.$$

Partition K into equivalence classes J such that $i, j \in K$ are in the same equivalence class if and only if $D_{i,i} = D_{j,j}$. Let $\mathcal{J}$ be the set of these equivalence classes, and for each $J \in \mathcal{J}$ define $D_J := D_{j,j}$ for some $j \in J$. We have

$$B_{i,j} = \sum_{J \in \mathcal{J}} \sum_{k \in J \cap \mathcal{P}_{i,j}} (D_{k,k})^p - \sum_{k \in J \cap \mathcal{N}_{i,j}} (D_{k,k})^p = \sum_{J \in \mathcal{J}} (|J \cap \mathcal{P}_{i,j}| - |J \cap \mathcal{N}_{i,j}|)(D_J)^p.$$

As the D_J are positive and pairwise distinct, Lemma 6.5 implies that for all p we have $B_{i,j} = 0$ if and only if $|J \cap \mathcal{P}_{i,j}| = |J \cap \mathcal{N}_{i,j}|$ for all J. By our assumption that this is true for all $i \neq j \in I$, we see that the $s \times |J|$ matrix $H_{I,J}$ is orthogonal, which implies $|J| = s$. In particular, $J = K$, and $D_{K,K}$ is linearly dependent on I_s, which implies the preuniformity of D. ∎

LEMMA 8.19. *Let C and D, O satisfy conditions* (C1)–(C4)*. At least one of the following outcomes occurs.*

Outcome 1. $\mathrm{EVAL}(C, D, O)$ *is* #P*-hard. If B is symmetric, then* $\mathrm{EVAL}(B, D^R, O^R)$ *is* #P*-hard.*

Outcome 2. *Condition* (C5) *is satisfied.*

Proof. We will use reduction template $T(1, p', q')$ with $p' = 2p + 1$ and $q' = 2q$ for $p, q \in \mathbb{N}$. By Lemma 8.16 this yields a reduction $\mathrm{EVAL}(C\Delta C, D, O) \leq \mathrm{EVAL}(C, D, O)$ such that $C\Delta C$ contains submatrices $B\Delta^C B^T$ and $B^T \Delta^R B$. If B is symmetric, then it yields the reduction $\mathrm{EVAL}(B\Delta^R B, D^R, O^R) \leq \mathrm{EVAL}(B, D^R, O^R)$. We base our argument on $B^T \Delta^R B$ to prove that $O^{R,\mu} = \beta^R_\mu I_{r;\Lambda^R}$ for all $\mu \in [m]$ and some β^R_μ and $\Lambda^R \subseteq [r]$. The analogous argument on $B\Delta^C B^T$ then yields the result for the submatrices of O^C.

Recall that by (8.18) we have $B^T \Delta^R B = (ww^T) \otimes (H^T \Delta' H)$ for an $r \times r$ diagonal matrix Δ'. With

$$\Theta^{[p]} = \Theta(1, p') = \gamma^R_{p'} \cdot \sum_{\mu=1}^{m} v^{p'}_\mu \cdot O^{R,\mu}, \tag{8.24}$$

the $r \times r$ diagonal matrix Δ' is defined by

$$\Delta' = \sum_{\mu=1}^{m} v_\mu^2 \Delta^{R,\mu} = \left(\sum_{\mu=1}^{m} v_\mu^{p'q'+2} D^{R,\mu} \right) \circ \Theta^{[p]^{(q')}} = \left(\sum_{\mu=1}^{m} v_\mu^{p'q'+2} \alpha_\mu I_r \right) \circ \Theta^{[p]^{(q')}}.$$

The last equality holds by condition (C4). Taking

$$\vartheta := \sum_{\mu=1}^{m} v_\mu^{p'q'+2} \alpha_\mu, \text{ we have } \Delta' = \vartheta \Theta^{[p]^{(q')}}. \tag{8.25}$$

If $\mathrm{abs}(H^T \Delta' H)$ contains a block of rank at least 2, then $\mathrm{abs}(B^T \Delta^R B)$ does. So, if $\mathrm{abs}(H^T \Delta' H)$ contains a block of rank at least 2, then Outcome 1 occurs by Lemma 6.4.

By the definition of $H^T \Delta' H$, we have $(H^T \Delta' H)_{i,i} = \mathrm{tr}(\Delta')$ for all $i \in [r]$, and this trace is nonnegative by the definition of Δ'. Therefore, every principal 2×2 submatrix of $\mathrm{abs}(H^T \Delta' H)$ has the form

$$\begin{pmatrix} \mathrm{tr}(\Delta') & |(H^T \Delta' H)_{i,j}| \\ |(H^T \Delta' H)_{j,i}| & \mathrm{tr}(\Delta') \end{pmatrix}.$$

As H is nonsingular, $|(H^T \Delta' H)_{i,j}| < \mathrm{tr}(\Delta')$ for all $i \neq j \in [r]$, and, therefore, every such submatrix has a nonzero determinant if $\mathrm{tr}(\Delta')$ is positive. Furthermore, such a submatrix is part of a block if $(H^T \Delta' H)_{i,j} \neq 0$ and $\mathrm{tr}(\Delta') \neq 0$. Therefore, we have Outcome 1 if we can show that $(H^T \Delta' H)_{i,j} \neq 0$ and $\mathrm{tr}(\Delta') \neq 0$ for some $i \neq j \in [r]$ and some $p, q \in \mathbb{N}$.

Assume therefore that either $(H^T \Delta' H)_{i,j} = 0$ or $\mathrm{tr}(\Delta') = 0$ for all $i \neq j \in [r]$ and all $p, q \in \mathbb{N}$. The remainder of the proof is to show that in this case condition (C5) is satisfied.

Recall that by (8.25) the value ϑ is positive for all $p, q \in \mathbb{N}$. Therefore, $\Delta'_{i,i} = 0$ if and only if $\Theta^{[p]}{}_{i,i} = 0$.

Claim 10. *There is a $p_0 \in \mathbb{N}$ such that for all $p \geq p_0$ and all $i \in [r]$ we have*

$$\Theta^{[p]}{}_{i,i} = 0 \text{ if and only if } (O_{i,i}^{R,\mu} = 0 \text{ for all } \mu \in [m]).$$

Proof. For each $i \in [r]$, application of Lemma 6.6 to (8.24) yields that there is a p_i such that for all $p \geq p_i$ we have

$$\Theta^{[p]}{}_{i,i} = 0 \text{ if and only if } (O_{i,i}^{R,\mu} = 0 \text{ for all } \mu \in [m]).$$

The claim follows with $p_0 := \max\{p_1, \ldots, p_r\}$.

Claim 11. *Let $p \in \mathbb{N}$. If $(H^T \Delta' H)_{i,j} = 0$ for all $i \neq j \in [r]$ and all $q \in \mathbb{N}$, then $\Theta^{[p]^{(2)}}$ is preuniform.*

Proof. Define $\Pi = (\Theta^{[p]})^{(2)}$. Then all entries of Π are nonnegative and $\Pi^{(q)} = (\Theta^{[p]})^{(q')}$. With $H^T \Delta' H = \vartheta(H^T \Theta^{[p]^{(q')}} H) = \vartheta(H^T \Pi^{(q)} H)$ the claim follows by the preuniform Diagonal Lemma, Lemma 8.18.

Claim 12. *There is a $p_= \in \mathbb{N}$ such that for all $p \geq p_=$ and all $i, j \in [r]$ we have*

$$\Theta^{[p]}{}_{i,i}^2 = \Theta^{[p]}{}_{j,j}^2 \text{ if and only if } (O_{i,i}^{R,\mu} = O_{j,j}^{R,\mu} \text{ for all } \mu \in [m]).$$

Proof. The backward direction holds for all $p \in \mathbb{N}$. Fix $i, j \in [r]$. By (8.24) the equality ${\Theta^{[p]}}^2_{i,i} = {\Theta^{[p]}}^2_{j,j}$ implies

$$\left| \sum_{\mu=1}^{m} v_\mu^{p'} O^{R,\mu}_{i,i} \right| = \left| \sum_{\mu=1}^{m} v_\mu^{p'} O^{R,\mu}_{j,j} \right|.$$

By Lemma 6.6 either we have a $p_{i,j}$ such that for all $p \geq p_{i,j}$

$${\Theta^{[p]}}^2_{i,i} = {\Theta^{[p]}}^2_{j,j} \text{ if and only if } O^{R,\mu}_{i,i} = O^{R,\mu}_{j,j} \text{ for all } \mu \in [m]$$

or there is a $p^-_{i,j}$ such that for all $p \geq p^-_{i,j}$

$${\Theta^{[p]}}^2_{i,i} = {\Theta^{[p]}}^2_{j,j} \text{ if and only if } O^{R,\mu}_{i,i} = -O^{R,\mu}_{j,j} \text{ for all } \mu \in [m].$$

However, the second possibility would particularly imply that $O^{R,1}_{i,i} < 0$ for some $i \in [r]$, which was precluded by condition (C2). Therefore, the first possibility holds with $p_{i,j}$. The claim now follows with $p_= = \max\{p_{i,j} \mid i, j \in [r]\}$. ∎

These claims now enable us to finish the proof. Note first that condition (C5) is satisfied with $\Lambda^R = \emptyset$ if $O^{R,\mu}_{i,i} = 0$ for all $\mu \in [m]$ and $i \in [r]$.

Assume therefore that O^R has nonzero diagonal entries. Fix values $p_0, p_= \in \mathbb{N}$ according to Claims 10 and 12 and define $p = \max\{p_0, p_=\}$. This implies $\operatorname{tr}(\Delta') \neq 0$. To see this note that there is some $i \in [r]$ and some $\mu \in [m]$ such that $O^{R,\mu}_{i,i} \neq 0$ which by our choice of p implies ${\Theta^{[p]}}_{i,i} \neq 0$.

By our assumption, $\operatorname{tr}(\Delta') \neq 0$ implies $(H^T \Delta' H)_{i,j} = 0$ for all $i \neq j \in [r]$ and all $q \in \mathbb{N}$ which by Claim 11 yields the preuniformity of ${\Theta^{[p]}}^{(2)}$.

Define $\Lambda^R := \left\{ i \in [r] \mid {\Theta^{[p]}}_{i,i} \neq 0 \right\}$. By the preuniformity of ${\Theta^{[p]}}^{(2)}$ Claim 12 implies that, for each $\mu \in [m]$ and every $i \in \Lambda^R$, there is a β^R_μ such that $O^{R,\mu}_{i,i} = \beta^R_\mu$. Furthermore, Claim 10 implies that for each $\mu \in [m]$ and every $i \in [r] \setminus \Lambda^R$ we have $O^{R,\mu}_{i,i} = 0$. This finishes the proof. ∎

8.3.1. Putting everything together. We are now able to prove Lemma 3.2.

Proof of Lemma 3.2. *Bipartite A.* Consider first the case in which A is bipartite. By Lemmas 8.15, 8.17, and 8.19, the evaluation problem EVAL(A) is #P-hard unless EVAL(A) $\equiv$ EVAL(C, D, O) for matrices C, D, O satisfying conditions (C1)–(C5).

C is a symmetric bipartite matrix with underlying block B. Conditions (C1)–(C5) imply that $B = vw^T \otimes H$, $D^R = D^{R''} \otimes I_r$, $D^C = D^{C''} \otimes I_r$, $O^R = O^{R''} \otimes I_{r;\Lambda^R}$, and $O^C = O^{C''} \otimes I_{r;\Lambda^C}$ for diagonal $m \times m$ matrices $D^{R''}$ and $O^{R''}$ defined by $D^{R''}_{\mu,\mu} = \alpha^R_\mu$ and $O^{R''}_{\mu,\mu} = \beta^R_\mu$ for all $\mu \in [m]$. The $n \times n$ diagonal matrices $D^{C''}$ and $O^{C''}$ are defined analogously in terms of α^C_ν and β^C_ν. Then we have

$$D'' = \begin{pmatrix} D^{R''} & 0 \\ 0 & D^{C''} \end{pmatrix}, O'' = \begin{pmatrix} O^{R''} & 0 \\ 0 & O^{C''} \end{pmatrix}, \text{ and } C'' = \begin{pmatrix} 0 & vw^T \\ wv^T & 0 \end{pmatrix}.$$

Note that $D+O$ and $D-O$ are nonnegative by condition (C2). Hence with M, Λ being the bipartization of H, Λ^R, and Λ^C, we have EVAL(C, D, O) $\equiv$ EVAL($M, I_{2r}, I_{2r;\Lambda}$) by Lemma 8.12.

Nonbipartite A. Now suppose that A is not bipartite. Let M be the bipartization of A. Recall that this is a matrix of the form

$$M = \begin{pmatrix} 0 & A \\ A & 0 \end{pmatrix}.$$

By Lemmas 8.15, 8.17, and 8.19, the evaluation problem EVAL(A) is #P-hard unless there are matrices C, D, O with block B underlying C satisfying conditions (C1)–(C5) such that EVAL(A) $\equiv$ EVAL(B, D^R, O^R).

Conditions (C1)–(C5) imply that $B = vv^T \otimes H$, $D^R = D^{R''} \otimes I_r$, and $O^R = O^{R''} \otimes I_{r;\Lambda^R}$ for diagonal $m \times m$ matrices $D^{R''}$ and $O^{R''}$ defined by $D^{R''}_{\mu,\mu} = \alpha^R_\mu$ and $O^{R''}_{\mu,\mu} = \beta^R_\mu$ for all $\mu \in [m]$. Hence we have EVAL(B, D^R, O^R) $\equiv$ EVAL($A, I_r, I_{r;\Lambda^R}$) by Corollary 8.11.

Finishing the proof. It remains to state the polynomial time computability. Note that conditions (C2)–(C5) are straightforwardly checkable in polynomial time and for (C1) this follows from Lemma 8.15. ∎

Acknowledgment. We thank the referees for many helpful comments and for suggesting the current proof of Lemma 7.12, which is much simpler than our original version.

REFERENCES

[1] L. Barto, M. Kozik, and T. Niven, *Graphs, polymorphisms and the complexity of homomorphism problems*, in STOC '08: Proceedings of the 40th Annual ACM Symposium on Theory of Computing, ACM, New York, 2008, pp. 789–796.

[2] M. Bläser and H. Dell, *Complexity of the cover polynomial*, in Proceedings of the 34th International Colloquium on Automata, Languages and Programming, Lecture Notes in Comput. Sci. 4596, L. Arge, Ch. Cachin, T. Jurdzinski, and A. Tarlecki, eds., Springer-Verlag, New York, 2007, pp. 801–812.

[3] A. Bulatov, *A dichotomy theorem for constraint satisfaction problems on a 3-element set*, J. ACM, 53 (2006), pp. 66–120.

[4] A. Bulatov, *The complexity of the counting constraint satisfaction problem*, in Proceedings of the 35th International Colloquium on Automata, Languages and Programming, Lecture Notes in Comput. Sci. 5125, Springer-Verlag, New York, 2008, pp. 646–661.

[5] A. Bulatov and V. Dalmau, *Towards a dichotomy theorem for the counting constraint satisfaction problem*, in Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science, IEEE Computer Society, Washington, DC, 2003, pp. 562–571.

[6] A. Bulatov and M. Grohe, *The complexity of partition functions*, Theoret. Comput. Sci., 348 (2005), pp. 148–186.

[7] J.-Y. Cai, X. Chen, and P. Lu, *Graph homomorphisms with complex values: A dichotomy theorem*, in Proceedings of the 37th International Colloquium on Automata, Languages and Programming (ICALP '10), Lecture Notes in Comput. Sci. 6198, Springer-Verlag, New York, 2010, pp. 275–286.

[8] M. Dyer and C. Greenhill, *The complexity of counting graph homomorphisms*, Random Structures Algorithms, 17 (2000), pp. 260–289.

[9] M. Dyer, L. A. Goldberg, and M. Jerrum, *A complexity dichotomy for hypergraph partition functions*, J. Computational Complexity, to appear.

[10] M. Dyer, L. A. Goldberg, and M. Paterson, *On counting homomorphisms to directed acyclic graphs*, J. ACM, 54 (2007), p. 27.

[11] A. Ehrenfeucht and M. Karpinski, *The Computational Complexity of (xor, and)-Counting Problems*, Tech. Report 8543-CS, available at http://citeseer.ist.psu.edu/ehrenfeucht90computational.html, 1990.

[12] M. Freedman, L. Lovász, and A. Schrijver, *Reflection positivity, rank connectivity, and homomorphism of graphs*, J. Amer. Math. Soc., 20 (2007), pp. 37–51.

[13] L. A. Goldberg, S. Kelk, and M. Paterson, *The complexity of choosing an H-colouring (nearly) uniformly at random*, in Proceedings of the 34th ACM Symposium on Theory of Computing, ACM, New York, 2002, pp. 53–62.

[14] L. A. Goldberg and M. Jerrum, *Inapproximability of the Tutte polynomial*, in Proceedings of the 39th Annual ACM Symposium on Theory of Computing, ACM, New York, 2007, pp. 459–468.

[15] P. Hell and J. Nešetřil, *On the complexity of H-coloring*, J. Combin. Theory Ser. B, 48 (1990), pp. 92–110.

[16] F. Jaeger, D. L. Vertigan, and D. J. A. Welsh, *On the computational complexity of the Jones and Tutte polynomials*, Mathematical Proceedings of the Cambridge Philosophical Society, 108 (1990), pp. 35–53.
[17] R. E. Ladner, *On the structure of polynomial time reducibility*, J. ACM, 22 (1975), pp. 155–171.
[18] R. Lidl and H. Niederreiter, *Finite Fields*, 2nd ed., Encyclopedia Math. Appl. 20, Cambridge University Press, Cambridge, UK, 1997.
[19] M. Lotz and J. A. Makowsky, *On the algebraic complexity of some families of coloured Tutte polynomials*, Adv. in Appl. Math., 32 (2004), pp. 327–349.
[20] L. Lovász, *The rank of connection matrices and the dimension of graph algebras*, European J. Combin., 27 (2006), pp. 962–970.
[21] L. Lovász and A. Schrijver, *Graph parameters and semigroup functions*, European J. Combin., 29 (2008), pp. 987–1002.
[22] A. Sokal, *The multivariate Tutte polynomial*, in Surveys in Combinatorics, Cambridge University Press, Cambridge, UK, 2005, pp. 173–226.
[23] M. Thurley, *The Complexity of Partition Functions*, Ph.D. thesis, Humboldt-Universität zu Berlin, Berlin, 2009.
[24] D. J. A. Welsh, *Complexity: Knots, Colourings and Counting*, London Math. Soc. Lecture Note Ser. 186, Cambridge University Press, Cambridge, UK, 1993.