DICHOTOMY THEOREMS FOR HOLANT PROBLEMS
(DRAFT V0.7)

by

Michael R. Kowalczyk

A dissertation submitted in partial fulfillment of
the requirements for the degree of

Doctor of Philosophy

(Computer Sciences)

at the

UNIVERSITY OF WISCONSIN–MADISON

2010

To my wife Dea — married eight years and going on two.

ABSTRACT

We present dichotomy theorems within a class of problems known as *holant problems*. The holant framework deals with certain counting problems on graphs, and subsumes a wide variety of problems such as COUNTING WEIGHTED H-HOMOMORPHISMS, WEIGHTED #CSP, and also classical problems such as COUNTING VERTEX COVERS. In the absence of any direct knowledge about long-standing open questions such as "$\mathrm{P} = \mathrm{P}^{\#\mathrm{P}}$?", dichotomy theorems establish classes of problems for which every problem is in one of two complexity classes widely believed not to overlap. In the present work, we show that for a substantial subclass of holant problems, each problem is either in FP or $\#\mathrm{P}\text{-hard}$. Due to holographic algorithms, some of these $\#\mathrm{P}\text{-hard}$ problems can be solved in polynomial time when the input is restricted to planar graphs, and we derive our dichotomy theorems under this restriction as well.

ACKNOWLEDGMENTS

I would like to express my deep gratitude to my advisor, Jin-Yi Cai: the inspiring professor who taught the introductory complexity theory course my first semester of graduate school, who later helped me to get my first teaching assistantship, and who had confidence in my research ability at a time when I did not. I would later recognize that when we started actively working together in a research capacity two years ago, it was a turning point in my graduate career; I never would have expected it was possible to achieve what I did since then, particularly while holding a full-time teaching position at another university. I greatly appreciate his flexibility in advising my research from such a long distance, including the countless emails, the long periods of autonomy, and the full-day marathons to discuss and scrutinize my work when I could make it back to Madison. It is amazing how just a few bits of good advice such as "maybe take a look at this problem" or "don't waste your time reading that" are so valuable. I believe there are very few advisors on par with Jin-Yi. It has been a privilege and my only regret is not asking to work under his direction sooner.

Also many thanks to the other members of my PhD committee: Eric Bach, Shuchi Chawla, Arnold Miller, and Andrew Poe. Each one of you has had a positive impact on my development as a professional, whether through instruction, research advisement, serving as your teaching assistant, being a role model, or simply being an encouraging voice.

I would also like to acknowledge Pinyan Lu and Mingji Xia for their helpful research guidance and suggestions, and to thank Rebecca Hasti for supervising my first two semesters teaching a class as a teaching assistant. Finally, I am very grateful to my wife Dea and to all of the faculty and staff in the Department of Mathematics and Computer Science at Northern Michigan University, where I have been teaching for the last two years. Their confidence and encouragement in completing my doctoral degree was an essential part of what made it possible.

DISCARD THIS PAGE

TABLE OF CONTENTS

Page

Page

DISCARD THIS PAGE

LIST OF SYMBOLS

$\mathbb{Z}$	the set of integers
$\mathbb{Z}^+$	the set of positive integers
$\mathbb{Q}$	the set of rational numbers
$\mathbb{R}$	the set of real numbers
$\mathbb{C}$	the set of complex numbers
$\Re$	the real part of a complex number
$\Im$	the imaginary part of a complex number
Arg	the principal value of the complex argument; i.e., $\mathrm{Arg}(c) \in (-\pi, \pi]$ for all $c \in \mathbb{C} - \{0\}$
$\mathrm{GL}_2(\mathbb{C})$	the general linear group of 2 by 2 invertible matrices over $\mathbb{C}$
$a \otimes b$	the tensor product of a and b
$a^{\otimes j}$	the tensor power $\underbrace{a \otimes a \otimes \cdots \otimes a}_{j \text{ times}}$
$a \times b$	the cartesian product of a and b
$a^{\times j}$	the cartesian power $\underbrace{a \times a \times \cdots \times a}_{j \text{ times}}$
$A \le_{\mathrm{T}}^{\mathrm{P}} B$	A is polynomial-time Turing reducible to B
$\deg$	the degree of a vertex
$\gcd$	the greatest common divisor

Chapter 1

Introduction

In this work we study the complexity of a class of problems known as holant problems. Holant problems encompass a rich and expressive class of counting problems. Some special cases include COUNTING WEIGHTED H-HOMOMORPHISMS and WEIGHTED #CSP, both of which are of significant independent research interest. The holant problem framework can also encode counting versions of classical problems such as k-COLORING, VERTEX COVER, INDEPENDENT SET, MATCHINGS, and PERFECT MATCHINGS.

A line of recent work has shown that for progressively larger subclasses of holant problems, a dichotomy exists where each individual problem is either efficiently computable or belongs to a class of problems widely believed to have no efficient algorithm [4, 5, 6, 9, 10, 11, 25, 26]. As we will see, most of these problems fall in the later class, but there are some notable and surprising exceptions where holant problems are efficiently computable. Specifically, a recently introduced algorithm design technique known as *holographic algorithms* has accounted for efficient solutions to some problems that would at first appear to be intractable. Since holant problems express such a diverse assortment of computational problems, providing a complete and explicit characterization of their complexity would be a worthy achievement. This dissertation makes a step towards this goal, both by expanding the boundary of what is currently known, and by introducing new techniques that may be useful for continuing this progress.

Our focus will be on a subclass of holant problems that have a close connection with COUNTING WEIGHTED H-HOMOMORPHISMS. We prove several dichotomies within this subclass, culminating in a single dichotomy theorem that explicitly characterizes every constituent problem.

1.1 The holant framework

We now introduce the general framework for holant problems. Fix an integer $q \geq 2$, let $\mathcal{D} = \{0, 1, \ldots, q-1\}$, and fix a field $\mathbb{F}$. A *signature grid* $\Omega = (G, \mathcal{F}, \pi)$ consists of a labeled graph $G = (V, E)$ for which π labels each vertex $v \in V$ with a function $f_v \in \mathcal{F}$ such that $f_v : \mathcal{D}^{\deg(v)} \to \mathbb{F}$. We allow G to have multiple edges and self loops. The functions in $\mathcal{F}$ are called *signatures*. Any edge assignment $\sigma : E \to \mathcal{D}$ induces an evaluation at each vertex $v \in V$ of the signature f_v, based on the assignments to the edges incident with v. Specifically, for every $v \in V$ let $\sigma|_{E(v)}$ denote the list of assignments $\sigma(e)$ for every edge $e \in E$ incident with v (in some fixed order), where assignments to self-loops appear twice. Then the computational problem on input instance Ω is to compute the following quantity[1,2]

$$\mathrm{Holant}_\Omega \quad = \sum_{\sigma : E \to \mathcal{D}} \prod_{v \in V} f_v(\sigma|_{E(v)}).$$

For example, suppose $\mathcal{D} = \{0, 1\}$ and consider the EXACT-ONE function, which has output 1 when exactly one of the inputs is 1, and has output 0 otherwise. Then if $\mathcal{F}$ is the set of EXACT-ONE functions of all arities, the resulting holant problem is precisely COUNTING PERFECT MATCHINGS.

In the study of holant problems, we can often, without loss of generality, transform a given problem so that it can be stated as a holant problem where the underlying graph G is bipartite. If $\mathcal{G}$ and $\mathcal{R}$ are both sets of signatures, then the notation $\#\mathcal{G} \mid \mathcal{R}$ is used to denote the problem of computing the holant on bipartite signature grids where every vertex on the left hand side of the graph is labeled with a signature from $\mathcal{G}$ and every signature on the right hand side is labeled with a signature from $\mathcal{R}$. In the case of singleton signature sets this is often written with the signature in place of the containing set, e.g. if $\mathcal{G} = \{g\}$ and $\mathcal{R} = \{r\}$ then we write $\#g \mid r$. The assumption that the input is limited to bipartite signature grids is not restrictive, as we momentarily demonstrate.

[1] The term Holant was first introduced by Valiant in [34] to denote a related exponential sum.

[2] Technically, we must also specify how the arguments of f_v match up with the edges incident to v, i.e. each $v \in V$ is labeled with a permutation ρ_v on the list of assignments $\sigma|_{E(v)}$, and the evaluation at v is $f_v(\rho_v(\sigma|_{E(v)}))$. However, in this thesis f_v will almost always be a symmetric function for which this does not matter. In the few instances where we allow signatures which are not necessarily symmetric, we clearly state this fact, but this permutation will be irrelevant for other reasons.

Suppose, for instance, that we want to study signature grids on general (not necessarily bipartite) graphs, with signatures assigned from a set $\mathcal{G}$. Given such a signature grid Ω with underlying graph $G = (V, E)$, we can construct a signature grid Ω' with underlying bipartite graph G', for which $\text{Holant}_\Omega = \text{Holant}_{\Omega'}$. This is done by introducing EQUALITY signatures (denoted $=_k$, where k is the arity of the signature), which take on the value 1 if all inputs are identical and 0 otherwise. Simply construct G' by replacing every edge $e \in E$ with a length-2 path, where the newly introduced vertex is assigned the signature $=_2$. Then every nonzero term in $\text{Holant}_{\Omega'}$ corresponds with a $\mathcal{D}$-assignment to the original signature grid Ω, and the two signature grids are equivalent. Conversely, any instance of $\#\mathcal{G} \mid =_2$ is equivalent to some signature grid labeled exclusively with signatures from $\mathcal{G}$ by reversing this argument. Hence the two notions are equivalent.

Now suppose we are still considering general graphs $G = (V, E)$ as input, but instead of making $\mathcal{D}$-assignments to the edges and assigning signatures to the vertices, $\mathcal{D}$-assignments are now made to the *vertices* and every *edge* $e \in E$ is assigned an arity-2 signature $g_e \in \mathcal{G}$. The natural adaptation of the holant to signature grids Ω of this type is

$$\text{Holant}_\Omega = \sum_{\sigma: V \to \mathcal{D}} \prod_{(u,v)=e \in E} g_e(\sigma(u), \sigma(v)).$$

One example over $\mathcal{D} = \{0, 1\}$ is where $\mathcal{G}$ consists of the arity-2 OR function. Then the holant problem is precisely counting the number of vertex covers on the input graph. The vertex-assignment and edge-signature setting is also expressible in the standard bipartite setting with edge assignments and vertex signatures. Starting with the original graph G, we again replace every edge $e \in E$ with a length 2 path, except now the newly introduced vertex is assigned the signature g_e. Every original vertex $v \in V$ is assigned the signature $=_{\deg(v)}$. All edges incident to such a vertex must be assigned the same value (lest the evaluation under that assignment be zero), so even though we are making edge assignments this is equivalent to making $\mathcal{D}$-assignments to the vertices. The holant of our newly constructed signature grid precisely mirrors the evaluation of the original. In this way, the vertex-assignment and edge-function setting on general graphs can be articulated as $\#\mathcal{G} \mid \{=_1, =_2, \ldots\}$, where $\mathcal{G}$ is any set of arity-2 signatures. We note that if $\mathcal{G}$ contains only a single signature, then this is precisely the class of problems known as COUNTING WEIGHTED

H-HOMOMORPHISMS, where one fixes a q by q matrix H with entries in $\mathbb{F}$, and given a graph $G = (V, E)$ as input, the problem is to compute the following quantity.

$$Z_H(G) = \sum_{\sigma:V\to\{1,2,\ldots,q\}} \prod_{(u,v)\in E} H_{\sigma(u),\sigma(v)}$$

One well-known example is a counting version of 3-COLORING, where $q = 3$ and $H = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$. When H is a Boolean matrix such as this, it is called unweighted. Dichotomy theorems for unweighted H-homomorphisms with undirected graphs H and directed acyclic graphs H are given in [17] and [16] respectively. A dichotomy theorem for any symmetric matrix H with nonnegative real entries is proved in [3]. Goldberg et al. [19] proved a dichotomy theorem for all real symmetric matrices H. Finally, Cai, Chen, and Lu [4] have proved a dichotomy theorem for all complex symmetric matrices H.

A related and more general setting is counting constraint satisfaction problems (#CSP). A problem instance consists of a set of variables, a finite set of values $\mathcal{D}$ they can take on, a set of constraints on the variables, and the goal of computing how many settings of the variables satisfy all of the constraints. As with H-Homomorphisms, this can be generalized to WEIGHTED #CSP which allows for different weight assignments to the constraints. In terms of the holant framework, WEIGHTED #CSP problems are equivalent to $\#\mathcal{G} \mid \{=_1, =_2, \ldots\}$ where $\mathcal{G}$ can be any fixed set of signatures. Each vertex with an EQUALITY signature corresponds to a variable and each vertex labeled with a generator corresponds to a constraint. For example, we can model #EXACT-ONE-3-SAT by $\#\mathcal{G} \mid \{=_1, =_2, \ldots\}$ over $\mathcal{D} = \{0, 1\}$, where $\mathcal{G}$ contains only the EXACT-ONE function of arity 3. The generator set $\mathcal{G}$ describes the constraint language. Note that the only difference between WEIGHTED #CSP and COUNTING WEIGHTED H-HOMOMORPHISMS is that in WEIGHTED #CSP, $\mathcal{G}$ is allowed to be an arbitrary signature set whereas in COUNTING WEIGHTED H-HOMOMORPHISMS only a single arity-2 signature is contained in $\mathcal{G}$. Much work has been done on constraint satisfaction problems, with dichotomy results known for different variants [2, 3, 13, 12, 15, 16, 17, 30].

1.2 Overview of results

Our study of holant problems can be understood primarily as COUNTING WEIGHTED H-HOMOMORPHISMS, where H is any symmetric 2 by 2 complex matrix and the input is restricted to k-regular graphs, but multiple edges and self-loops are allowed. In terms of holant problems, this equates to the study of *symmetric* signatures over the Boolean domain, where the output value of a signature depends only on the Hamming weight of its inputs. More precisely, this is $\#g \mid =_k$ over domain $\mathcal{D} = \{0, 1\}$, where k is any positive integer and g is any complex-valued symmetric arity-2 signature. When working over the Boolean domain, the notation $[x_0, x_1, \ldots, x_k]$ is used to denote a symmetric signature $g : \{0, 1\}^k \to \mathbb{C}$, where x_i is the value of g on inputs of Hamming weight i.

The remaining chapters are organized chronologically by order of discovery and also by increasing degree of sophistication. In Chapter 2, we introduce the basic technique of interpolation and derive a dichotomy for $\#[x_0, x_1, x_2] \mid [y_0, y_1, y_2, y_3]$ where each $x_i, y_j \in \{0, 1, -1\}$. We also give a new characterization for a polynomial time computable primitive known as *Fibonacci gates*. In Chapter 3, we introduce three new techniques: interpolation using finisher gadgets, algebraic symmetrization of the holant, and the notion of an Eigenvalue Shifted Pair (ESP). We go on to use these tools to derive a dichotomy for $\#[x_0, x_1, x_2] \mid =_3$, where each x_i is an arbitrary complex number. In Chapter 4, we show how to prove a dichotomy for $\#[x_0, x_1, x_2] \mid =_k$ where k is any positive integer and each x_i is an arbitrary real number (actually, the result is slightly more general than this). The approach involves adapting the finisher gadget concept to even-valued k and exploiting a remarkable algebraic relationship that occurs between two particular families of gadgets in order to generalize to all k. In Chapter 5, we carry out a slightly different take on interpolation and subsequently introduce ESP-chains and the notion of a syzygy. These are used to extend the dichotomy to $\#[x_0, x_1, x_2] \mid =_k$ where k is any positive integer and each x_i is an arbitrary complex number. Finally, in Chapter 6, we broaden this characterization to allow for any combination of EQUALITY signatures, attaining the following theorem.

Theorem 1. *Let $S \subseteq \mathbb{Z}^+$ be nonempty, let $\mathcal{R} = \{=_k \,:\, k \in S\}$, and let $d = \gcd(S)$. Then $\#[x_0, x_1, x_2] \mid \mathcal{R}$ is $\#\mathrm{P}$-hard for all $x_0, x_1, x_2 \in \mathbb{C}$, both for unrestricted input and for input restricted to planar graphs, except in the following cases, for which the problem is in* FP*:*

1. $S \subseteq \{=_1, =_2\}$
2. $x_0 x_2 = x_1^2$
3. $x_0 = x_2 = 0$
4. $x_1 = 0$
5. $x_0 x_2 = -x_1^2$ *and* $x_0^{4d} = x_1^{4d}$
6. *the input is restricted to planar graphs and* $x_0^d = x_2^d$

1.3 Definitions and background

We have already seen a general treatment of the holant framework, but for the remainder of this thesis, we will be working with complex-valued symmetric signatures over domain $\mathcal{D} = \{0, 1\}$. That is, any signature grid $\Omega = (G, \mathcal{F}, \pi)$ consists of a labeled graph $G = (V, E)$ (possibly with multiple edges and self-loops) for which π labels each vertex $v \in V$ with a symmetric signature $f_v \in \mathcal{F}$ such that $f_v : \{0, 1\}^{\deg(v)} \to \mathbb{C}$. In this setting, we have

$$\mathrm{Holant}_\Omega \quad = \sum_{\sigma: E \to \{0,1\}} \prod_{v \in V} f_v(\sigma|_{E(v)}),$$

where $\sigma|_{E(v)}$ is a list of assignments $\sigma(e)$ for every edge $e \in E$ incident with v, with each self-loop appearing twice (since f_v is symmetric, the order of this list does not matter). We will usually work in terms of bipartite graphs and use the notation $\#\mathcal{G} \mid \mathcal{R}$ throughout, although we occasionally take the equivalent viewpoint of vertex-assignments and edge-functions as discussed earlier. Signatures in $\mathcal{G}$ are called *generators* and signatures in $\mathcal{R}$ are called *recognizers*. For consistency, all $(2, k)$-regular bipartite graphs are arranged with generators on the degree-2 side and recognizers on the degree-k side. We also refer to the vertices as *recognizer vertices* and *generator vertices* according to which bipartition of the graph they belong to.

1.3.1 $\mathcal{F}$-gates

Signatures from $\mathcal{F} = \mathcal{G} \cup \mathcal{R}$ are assigned to each vertex as part of an input graph. Instead of a single vertex, we can use graph fragments to generalize this notion. In the setting of Boolean domain $\mathcal{D} = \{0, 1\}$ and complex-valued signatures, an $\mathcal{F}$-gate Γ is a triple $(H, \mathcal{F}, \pi)$, where $H = (V, E, D)$ is a graph with internal edge set E and dangling edge set D (see Figure 1.1 for example). As before, π labels each vertex $v \in V$ with a signature $f_v \in \mathcal{F}$ such that $f_v : \{0,1\}^{\deg(v)} \to \mathbb{C}$. Other than the dangling edges, an $\mathcal{F}$-gate is the same as a signature grid. The role of dangling edges is similar to that of external nodes in Valiant's notion [33], however we allow more than one dangling edge for a node. Then we can define a function for this $\mathcal{F}$-gate:

$$\Gamma(b_1, b_2, \ldots, b_\ell) = \sum_{(a_1, a_2, \ldots, a_p) \in \{0,1\}^p} H(a_1, a_2, \ldots, a_p, b_1, b_2, \ldots, b_\ell),$$

where $p = |E|$, $\ell = |D|$, $(b_1, b_2, \ldots, b_\ell) \in \{0,1\}^\ell$ denotes an assignment on the dangling edges, and $H(a_1, a_2, \ldots, a_p, b_1, b_2, \ldots, b_\ell)$ denotes the value of the $\mathcal{F}$-gate on an assignment of all edges, i.e., the product of evaluations at every $v \in V$, for $(a_1, a_2, \ldots, a_p, b_1, b_2, \ldots, b_\ell) \in \{0,1\}^{p+\ell}$. We will also call this function the *signature* of the $\mathcal{F}$-gate Γ. An $\mathcal{F}$-gate can be used in a signature grid as if it is just a single vertex with the same signature. We note that even for a very simple signature set $\mathcal{F}$, the signatures for all $\mathcal{F}$-gates can be quite complicated and expressive. Matchgate signatures are an example, where $\mathcal{F}$ consists of just the EXACT-ONE function [33].

There are three types of $\mathcal{F}$-gates that we use ubiquitously throughout this thesis, known as starter gadgets, recursive gadgets, and finisher gadgets. Each of these $\mathcal{F}$-gates has its dangling edges partitioned into two designations: *leading* edges and *trailing* edges (when depicted pictorially, leading edges are indicated as edges protruding from the top of the $\mathcal{F}$-gate and trailing edges

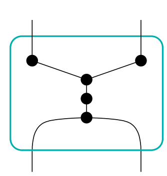


Figure 1.1 An $\mathcal{F}$-gate

from the bottom). Suppose an $\mathcal{F}$-gate has m leading edges and n trailing edges. Then the signature of the $\mathcal{F}$-gate can be organized as a 2^m by 2^n matrix M, where the row is indexed by the $\{0, 1\}$-assignment to the leading edges and the column is indexed by the $\{0, 1\}$-assignment to the trailing edges. If the number of trailing edges in one $\mathcal{F}$-gate matches the number of leading edges in another, then a new $\mathcal{F}$-gate can be formed by merging these edges, and the associated matrix is obtained by multiplying the two original matrices together. In particular, an $\mathcal{F}$-gate with only leading edges would be viewed as a column vector, and then merging with an $\mathcal{F}$-gate with a matching number of trailing edges corresponds to premultiplication by the associated matrix. In this way we can view an $\mathcal{F}$-gate with m leading edges and n trailing edges as transforming $\mathcal{F}$-gates with arity-n signatures into $\mathcal{F}$-gates with arity-m signatures, and we refer to M as the *general transition matrix* for that $\mathcal{F}$-gate. In all cases unless clearly stated otherwise, our $\mathcal{F}$-gates will transform symmetric signatures to symmetric signatures. This implies that there exists an equivalent $m + 1$ by $n + 1$ matrix $\widetilde{M}$ which operates directly on column vectors written in symmetric signature notation. We will henceforth identify this *(symmetric) transition matrix* $\widetilde{M}$ with the $\mathcal{F}$-gate itself.

Now we introduce starter gadgets, recursive gadgets, and finisher gadgets; all of which are defined as bipartite $\mathcal{F}$-gates labeled with generators on one side of the bipartition and recognizers on the other. An *arity-r starter gadget* is an $\mathcal{F}$-gate with r leading edges, all internally incident with generator vertices, and no trailing edges. An *arity-r recursive gadget* is an $\mathcal{F}$-gate with r leading edges and r trailing edges. Internally, we also require that all leading edges of a recursive gadget are incident with generator vertices, while all trailing edges are incident with recognizer vertices. Finally, an $\mathcal{F}$-gate is an *arity-r finisher gadget* if it has r trailing edges, some positive number of leading edges, and a transition matrix where the only nonzero entries are in the top and bottom rows. The trailing edges of a finisher gadget must be internally incident with recognizer vertices. If there are multiple leading edges then they must also be internally incident with recognizer vertices, but if there is only one leading edge it must be internally incident with a generator vertex. The reason why these three gadget types are defined in such a way has to do with maintaining the bipartite structure of signature grids containing them. This will follow because the trailing edges of each recursive gadget and finisher gadget will be merged with the leading edges of some recursive gadget or starter gadget. In the same way, we also need to ensure that the leading edges of finisher gadgets connect externally with the correct kind of vertices in order to preserve the bipartite structure of the containing signature grid. When we speak of a starter gadget, recursive gadget, or finisher gadget *in the context of* $\#\mathcal{G} \mid \mathcal{R}$, we mean that the vertices of that gadget are labeled exclusively with generators from $\mathcal{G}$ and recognizers from $\mathcal{R}$.

To eliminate a potential point of notational confusion, we point out that the term "arity" in the definitions of starter gadgets, recursive gadgets, and finisher gadgets has to do with the type of signatures that they operate on, and doesn't necessarily match up with the arity of that gadget as an $\mathcal{F}$-gate. For example, a "binary recursive gadget" is an arity-4 $\mathcal{F}$-gate.

1.3.2 Degenerate signatures

We call a symmetric signature $[x_0, x_1, x_2, \ldots, x_n]$ *nondegenerate* if the $2 \times n$ matrix given by $\begin{bmatrix} x_0 & x_1 & x_2 & \ldots & x_{n-1} \\ x_1 & x_2 & x_3 & \ldots & x_n \end{bmatrix}$ has rank 2, and *degenerate* otherwise. The following lemma shows that we can conceptualize a degenerate signature of arity n as being functionally equivalent to n unary signatures acting together.

Lemma 1. *Let n be a positive integer and let $\mathcal{U}$ be the set of all unary signatures over $\mathbb{C}$. Then a complex-valued signature $[x_0, x_1, \ldots, x_n]$ is degenerate if and only if there is an $\mathcal{U}$-gate with signature $[x_0, x_1, \ldots, x_n]$.*

Proof. Suppose $[x_0, x_1, \ldots, x_n]$ is degenerate. Then $\begin{bmatrix} x_0 & x_1 & x_2 & \ldots & x_{n-1} \\ x_1 & x_2 & x_3 & \ldots & x_n \end{bmatrix}$ has rank at most 1 and there exists $c \in \mathbb{C}$ such that either $x_{i+1} = cx_i$ for all $0 \le i < n$ or $cx_{i+1} = x_i$ for all $0 \le i < n$. In either case we construct an $\mathcal{U}$-gate Γ having n vertices and one dangling edge per vertex. If $x_{i+1} = cx_i$ for all $0 \le i < n$, we have $[x_0, x_1, \ldots, x_n] = [x_0, cx_0, \ldots, c^n x_0]$ so we label one vertex of Γ with $[x_0, cx_0]$ and the other $n-1$ vertices with $[1, c]$. If $cx_{i+1} = x_i$ for all $0 \le i < n$, then $[x_0, x_1, \ldots, x_n] = [c^n x_n, c^{n-1} x_n, \ldots, x_n]$ so we label one vertex of Γ with $[cx_n, x_n]$ and the remaining $n-1$ vertices with $[c, 1]$. In either case Γ has signature $[x_0, x_1, \ldots, x_n]$.

Conversely, suppose Γ is an $\mathcal{U}$-gate with signature $[x_0, x_1, \ldots, x_n]$. We may assume without loss of generality that the vertices internal to Γ are precisely those incident with its dangling edges. Otherwise there exists a connected component of 2 vertices within Γ, say with signatures $[w_0, w_1]$ and $[z_0, z_1]$, and we can maintain the signature of Γ by removing this component and multiplying some signature incident with a dangling edge by $w_0 z_0 + w_1 z_1$. If $x_0 \neq 0$ then switching from the all-0 assignment on the dangling edges to any assignment with a single 1 multiplies the output by some $c \in \mathbb{C}$. This implies that the vertices of Γ are labeled with signatures of the form $[y_i, cy_i]$ for $1 \leq i \leq n$, where $y_i \in \mathbb{C}$ such that $x_0 = \prod_{0 \leq i \leq n} y_i$. Therefore $[x_0, x_1, \ldots, x_n] = [x_0, cx_0, \ldots, c^n x_0]$ and $[x_0, x_1, \ldots, x_n]$ is a degenerate signature. If $x_n \neq 0$ then switching from the all-1 assignment on the dangling edges to any assignment with a single 0 multiplies the output by some $c \in \mathbb{C}$. This implies that the vertices of Γ are labeled with signatures of the form $[cy_i, y_i]$ for $1 \leq i \leq n$, where $y_i \in \mathbb{C}$ such that $x_n = \prod_{0 \leq i \leq n} y_i$. Thus $[x_0, x_1, \ldots, x_n] = [c^n x_n, c^{n-1} x_n, \ldots, x_n]$ and $[x_0, x_1, \ldots, x_n]$ is still a degenerate signature. Finally, if $x_0 = x_n = 0$ then there is a vertex labeled $[c_1, 0]$ and a vertex labeled $[0, c_2]$ for some $c_1, c_2 \in \mathbb{C}$ (possibly the same vertex). Then we have both $x_i = 0$ for $0 < i \leq n$ and $x_i = 0$ for $0 \leq i < n$, so Γ has an all-zero signature, which is degenerate. $\square$

1.3.3 The Holant Theorem

A general (not necessarily symmetric) signature over domain $\mathcal{D} = \{0, 1\}$ is denoted by its truth table in parentheses; e.g. the symmetric signature $[3, 5, -7]$ is written in *general signature notation* as $(3, 5, 5, -7)$. Although we will be using symmetric signatures exclusively, this general signature notation is adopted when performing holographic reductions, with generators represented as column vectors and recognizers as row vectors. We say that $\#\mathcal{G} \mid \mathcal{R}$ has a *holographic reduction* to $\#\mathcal{G}' \mid \mathcal{R}'$ if there is a *basis* $T \in \mathrm{GL}_2(\mathbb{C})$ such that for all $G \in \mathcal{G}$ and $R \in \mathcal{R}$ there exist $G' \in \mathcal{G}'$ and $R' \in \mathcal{R}'$ such that $G' = T^{\otimes g} G$ and $R' T^{\otimes r} = R$ where g and r are the arity of G and R respectively. Note that this particular definition of a holographic reduction is invertible (other variants exist). This leads us to the Holant Theorem, first discovered by Valiant [34], which closely ties together problems that would otherwise appear unrelated.

Theorem 2 (Holant Theorem)**.** *Suppose there is a holographic reduction from* $\#\mathcal{G} \mid \mathcal{R}$ *to* $\#\mathcal{G}' \mid \mathcal{R}'$ *which induces a mapping of signature grid* Ω *to* Ω'*. Then* $\mathrm{Holant}_\Omega = \mathrm{Holant}_{\Omega'}$.

The Holant Theorem can be extended to $\mathcal{F}$-gates, with the signatures of $\mathcal{F}$-gates taking the place of generators and recognizers. We will have occasion to use this variant of the Holant Theorem, so we will offer a proof of it. Given a basis $T \in \mathrm{GL}_2(\mathbb{C})$, the idea is to introduce the signature T to the dangling edges of generators and T^{-1} to the dangling edges of recognizers. This is done in such a way that the newly introduced signatures match up and cancel, having no effect on the internal edges of the $\mathcal{F}$-gate. The remaining T and T^{-1} signatures on the dangling edges change the signature of the $\mathcal{F}$-gate in a way that mimics a holographic reduction.

Theorem 3 (Holant Theorem for $\mathcal{F}$-gates)**.** *Suppose there is a holographic reduction from* $\#\mathcal{G} \mid \mathcal{R}$ *to* $\#\mathcal{G}' \mid \mathcal{R}'$ *under basis* $T \in \mathrm{GL}_2(\mathbb{C})$ *which induces a mapping from* $\mathcal{F}$*-gate* Γ *to* Γ'*. Identify* Γ *and* Γ' *with their general transition matrices, where dangling edges incident with generator vertices of* Γ *and* Γ' *are leading edges and dangling edges incident with recognizer vertices of* Γ *and* Γ' *are trailing edges. Then* $\Gamma' = T^{\otimes g}\Gamma(T^{-1})^{\otimes r}$.

Proof. In this proof we continue to use general signature notation, with generators written as column vectors and recognizers written as row vectors. Let Γ and Γ' be $\mathcal{F}$-gates in the context of $\#\mathcal{G} \mid \mathcal{R}$ and $\#\mathcal{G}' \mid \mathcal{R}'$ as stated, and let $T \in \mathrm{GL}_2(\mathbb{C})$ be the basis for a holographic reduction mapping Γ to Γ'. Let $\mathcal{F}' = \mathcal{F} \cup \{T, T^{-1}\}$. Let t be aDefine two unary recursive gadgets with transition matrices T and T^{-1}, and Then for every $G \in \mathcal{G}$, we define an $\mathcal{F}'$-gate Γ_G with signature $T^{\otimes g}G$ by adjoining g copies of T, where g is the arity of G. For any $R \in \mathcal{R}$, we define an $\mathcal{F}'$-gate Γ_R with signature $R(T^{-1})^{\otimes r}$ by adjoining r copies of T^{-1}, where r is the arity of R. Then replacing every signature $f \in \{\mathcal{G}\} \cup \{\mathcal{R}\}$ in Γ with Γ_f, we have a signature grid Γ'' which simulates the signature grid Γ'. Since Γ is bipartite, all vertices with signatures T and T^{-1} in Γ'' cancel except on the dangling edges of Γ''. This means Γ'' has the signature $T^{\otimes g}\Gamma(T^{-1})^{\otimes r}$, which as noted, is identical to the signature of Γ'. □

Theorem 2 can be viewed as a corollary of Theorem 3, where the $\mathcal{F}$-gate has no dangling edges. Theorem 2 remains true when the matrix T is singular. This can be proved in a similar way, by defining a signature grid with signatures from $\mathcal{R}'$ on the recognizer side, signatures from $\mathcal{G}$ on the generator side, and introducing unary recursive gadgets with signature T on the edges in between. Then grouping T with either the recognizer side or generator side gives $\mathcal{F}$ gates which mirror $\mathcal{G} \mid \mathcal{R}$ or $\mathcal{G}' \mid \mathcal{R}'$. The holant theorem can also be extended to nonsquare basis matrices which transform between different domain sizes.

Chapter 2

Obtaining a dichotomy the hard way: case-by-case analysis

In this chapter we prove a dichotomy for problems of the form $\#[x_0, x_1, x_2] \mid [y_0, y_1, y_2, y_3]$, for any $x_i, y_i \in \{0, 1, -1\}$. This is proved for both arbitrary signature grids as input, as well as input restricted to planar signature grids. The result is achieved through the use of interpolation and holographic reductions. The techniques are based heavily on [9], where the same result was proved for Boolean-valued signatures. We also use holographic reductions to establish a close connection between Fibonacci gates and the class of problems which can be solved using a particular kind of counting argument.

2.1 Background

Interpolation, as a method to prove hardness of counting problems, was first given by Valiant [31]. This technique was later expanded upon by Dyer, Greenhill, and Vadhan [17, 30]. We will employ a version of this technique as proposed in [9].

Suppose we want to show that $\#[a, b, c] \mid [y_0, y_1, y_2, y_3]$ is $\#\mathrm{P}$-hard, and suppose we have constructed some binary starter gadget S in this context, which has signature $[w, x, z]$. Then we have effectively *simulated* the generator signature $[w, x, z]$. If $\#[w, x, z] \mid [y_0, y_1, y_2, y_3]$ happens to be $\#\mathrm{P}$-hard, then this already constitutes a mapping reduction showing that $\#[a, b, c] \mid [y_0, y_1, y_2, y_3]$ is $\#\mathrm{P}$-hard; given any problem instance Ω of $\#[w, x, z] \mid [y_0, y_1, y_2, y_3]$, we can remove each vertex with signature $[w, x, z]$ and substitute it with a copy of the $\mathcal{F}$-gate S, which has the same signature. This direct gadget approach is simple, but it has limited utility in proving general results.

Now suppose we have some binary starter gadget S and binary recursive gadget M, both in the context of $\#[a,b,c] \mid [y_0,y_1,y_2,y_3]$. Let $N_0 = S$. Now for every integer $i > 0$, recursively define N_i to be the $\mathcal{F}$-gate constructed by merging the leading edges of N_{i-1} with the trailing edges of M. Then for all $i \geq 0$, N_i is a bipartite $\mathcal{F}$-gate which simulates some binary generator signature, using only generator $[a,b,c]$ and recognizer $[y_0,y_1,y_2,y_3]$. The signature of N_i is given in symmetric notation as a column vector by $M^i S$. Depending on M and S, we now potentially have an infinite set of distinct signatures, and while it is true that we can attempt a direct simulation argument as above, such a route is not the aim of this construction. Instead, we will argue that if the set of signatures produced by this construction is sufficiently diverse (in a sense that will be made precise shortly), then *any* binary symmetric signature can be efficiently simulated; not just those that appear as the signature of some N_i. Then the existence of just a single signature $[w,x,z]$ for which the problem $\#[w,x,z] \mid [y_0,y_1,y_2,y_3]$ is #P-hard would imply that the original problem $\#[a,b,c] \mid [y_0,y_1,y_2,y_3]$ is also #P-hard.

Suppose, then, that $w,x,z,y_0,y_1,y_2,y_3 \in \mathbb{Q}$ and $\#[w,x,z] \mid [y_0,y_1,y_2,y_3]$ is #P-hard. Given a signature grid instance Ω of $\#[w,x,z] \mid [y_0,y_1,y_2,y_3]$, we will show that under certain conditions, an oracle for $\#[a,b,c] \mid [y_0,y_1,y_2,y_3]$ can be used to compute Holant_Ω in polynomial time. Let $[w_s,x_s,z_s]$ denote the signature of N_s, and we define signature grid Ω_s to be identical to Ω, except that every vertex with signature $[w,x,z]$ is replaced by a copy of N_s (which is labeled exclusively with $[a,b,c]$ and $[y_0,y_1,y_2,y_3]$). Note that there is a fixed polynomial p with integer coefficients such that $\text{Holant}_{\Omega_s} = p(w_s,x_s,z_s,y_0,y_1,y_2,y_3)$. Furthermore, although p is a sum of exponentially many terms, in every term the sum of the exponents of w_s, x_s, and z_s is n, where n is the number of degree 2 vertices in the graph underlying Ω. This leads to the crucial observation that

$$\text{Holant}_{\Omega_s} = \sum_{i+j+k=n} c_{i,j,k} w_s^i x_s^j z_s^k \ , \tag{2.1}$$

for some $c_{i,j,k}$ which depend only on y_0, y_1, y_2, and y_3. There are two important points here. The first is that (2.1) is a sum in polynomially many terms, and the second is that the $c_{i,j,k}$ are the only unknowns, appearing in (2.1) for every $s \geq 0$ (note that Holant_{Ω_s} is given by the oracle for

$\#[a,b,c] \mid [y_0,y_1,y_2,y_3]$). Thus we can frame this as a linear system for $0 \le s < \binom{n+2}{2}$ and solve for all of the $c_{i,j,k}$ (provided that the system is nonsingular). Then we can directly calculate

$$\text{Holant}_\Omega = \sum_{i+j+k=n} c_{i,j,k} w^i x^j z^k \ ,$$

completing the reduction.

At this point there are two details that still need to be worked out: 1) under what conditions is the linear system (2.1) nonsingular for $0 \le s < \binom{n+2}{2}$, and 2) when can we be assured that there exists a symmetric binary signature g for which $\#g \mid [y_0,y_1,y_2,y_3]$ is $\#\text{P-hard}$? These are addressed by the following lemmas, which follow from [9].

Lemma 2. *Suppose* $\det(M) \neq 0$*,* S *is not orthogonal to any row eigenvector of* M*, and the characteristic polynomial of* M *is irreducible over* $\mathbb{Q}$ *and not of the form* $x^3 + c$*. Then the system* 2*.1 is nonsingular for* $0 \le s < \binom{n+2}{2}$*.*

Lemma 3. *For any nondegenerate signature* $[y_0,y_1,y_2,y_3]$ *where* $y_i \in \mathbb{Q}$*, there exists a signature* $[x_0,x_1,x_2]$ *with* $x_i \in \mathbb{Q}$ *such that* $\#[x_0,x_1,x_2] \mid [y_0,y_1,y_2,y_3]$ *is* $\#\text{P-hard}$*. Furthermore this remains true even for planar graphs.*

This leads to the following theorem, which is the flavor of interpolation we apply in this chapter. The starter gadget is fixed to be the $\mathcal{F}$-gate consisting of a single vertex incident with two leading edges.

Theorem 4. *Let* $\#[x_0,x_1,x_2] \mid [y_0,y_1,y_2,y_3]$ *be a counting problem where* $x_i, y_j \in \mathbb{Q}$ *and* $[y_0,y_1,y_2,y_3]$ *is nondegenerate. Let* M *be a binary recursive gadget. Suppose that* $\det(M) \neq 0$*,* $[x_0,x_1,x_2]$ *is not orthogonal to any row eigenvector of* M*, and the characteristic polynomial of* M *is irreducible over* $\mathbb{Q}$ *and not of the form* $x^3 + c$*. Then* $\#[x_0,x_1,x_2] \mid [y_0,y_1,y_2,y_3]$ *is* $\#\text{P-hard}$*. Furthermore, if* M *is planar, then* $\#[x_0,x_1,x_2] \mid [y_0,y_1,y_2,y_3]$ *is* $\#\text{P-hard}$ *when restricted to planar graphs.*

2.2 The search for a dichotomy

We start with some discussion regarding [9], where the case of Boolean signatures is considered. Whenever a problem was shown to be polynomial time computable in that paper, it was due to either a counting argument, a connectivity argument, the presence of a degenerate signature, Fibonacci gates, or (for some problems restricted to planar graphs) holographic algorithms. We will presently examine the first three of these.

First we discuss the counting argument. If the generator has the form $[1, 1, 0]$, then it effectively requires that at most half of the edges in the signature grid are assigned to 1 (otherwise that assignment does not contribute anything to the holant). Similarly recognizers of the form $[0, 0, 1, 1]$ require that at least two-thirds of the edges in the signature grid are assigned to 1. Clearly, these cannot both happen simultaneously, so for any signature grid instance Ω of $\#[1, 1, 0] \mid [0, 0, 1, 1]$ we have $\mathrm{Holant}_\Omega = 0$. This argument also applies for any signatures of the form $[x_0, x_1, 0]$ and $[0, 0, y_2, y_3]$, for arbitrary x_i and y_i, i.e. $\mathrm{Holant}_\Omega = 0$ for any instance Ω of $\#[x_0, x_1, 0] \mid [0, 0, y_2, y_3]$.

Any problem where the recognizer has the form $[y_0, 0, 0, y_3]$ and the generator has the form $[x_0, 0, x_2]$ or $[0, x_1, 0]$ can be solved in polynomial time with a connectivity argument. A signature of the form $[z, 0, 0, \ldots, 0, z']$ can be viewed as a WEIGHTED-EQUALITY signature, which might take on a nonzero value if all incident edges have the same assignment, but is zero otherwise. On the other hand, the signature $[0, x_1, 0]$ can only be nonzero when one incident edge is assigned a 1 and the other is assigned a 0. Thus, taking the edge-function and vertex-assignment perspective, we can view signature grids of the form $\#\{[x_0, 0, x_2], [0, x_1, 0]\} \mid [y_0, 0, 0, y_3]$ (which is slightly more general than we need) as a type of 2-coloring problem where $\{0, 1\}$-assignments are made to the vertices and each edge either requires the incident vertices to be the same color or the opposite color. Thus, once a color has been assigned to a single vertex, all adjacent vertices immediately have their colors determined as well. Continuing this for all vertices in a connected component either results in an inconsistency where no coloring satisfies all of the edges, or an assignment where all edges are satisfied. In the later case, reversing the coloring results in the only other consistent $\{0,1\}$-assignment. Thus, it is an easy matter to calculate the holant for each connected component and then take the product of these to find the holant of the whole signature grid. So we have a polynomial time algorithm for $\#\{[x_0,0,x_2],[0,x_1,0]\} \mid [y_0,0,0,y_3]$ where all x_i and y_i are arbitrary.

In the Boolean version of $\#[x_0,x_1,x_2] \mid [y_0,y_1,y_2,y_3]$, the degenerate signatures are limited to $[0,0,0]$, $[0,0,1]$, $[1,0,0]$, $[1,1,1]$, $[0,0,0,0]$, $[0,0,0,1]$, $[1,0,0,0]$, and $[1,1,1,1]$. Any problem of the form $\#[x_0,x_1,x_2] \mid [y_0,y_1,y_2,y_3]$ having one of these signatures is efficiently solvable for trivial reasons. When we allow signatures to take on values from $\{0,1,-1\}$ this is still true. First, the degenerate generators consist of $[0,0,0]$, $[0,0,x]$, $[x,0,0]$, $[x,x,x]$, and $[x,-x,x]$, and the degenerate recognizers are $[0,0,0,0]$, $[0,0,0,y]$, $[y,0,0,0]$, $[y,y,y,y]$, and $[y,-y,y,-y]$, for $x,y \in \{1,-1\}$. Later on we will explicitly give the holant for any problem involving one of these signatures, but for now we will look at the big picture. In light of Lemma 1, if either $[x_0,x_1,x_2]$ or $[y_0,y_1,y_2,y_3]$ is degenerate then the signature grid can be replaced with an equivalent one which is composed of connected components with at most 4 vertices in each component. The holant of every connected component is easily computable and the holant of the entire signature grid is just the product of these.

To completely characterize $\#[x_0,x_1,x_2] \mid [y_0,y_1,y_2,y_3]$ over $\{0,1,-1\}$, we have a total of 3^7, or 2187 problems. Of course, there is significant redundancy and many of these problems are equivalent. Starting in a simple way, we apply Fibonacci gates and the other algorithms discussed above, using a computer program to identify any problem which can be solved using these techniques, which is then eliminated from further consideration. Of the remaining problems, a reasonable next step would be to attempt to apply interpolation using the gadgets introduced in [9] (gadgets 1 and 2 in Figure 2.1). However, since the transition matrices and other calculations required for Lemma 4 are quite laborious to carry out by hand, we have the same computer program check to see if Theorem 4 applies (it computes the transition matrix, calculates the characteristic polynomial, checks irreducibility of the characteristic polynomial, and so on). The result is a classification of all but roughly 50 problems.

One natural choice at this point is to try adding in different gadgets, but the computation becomes unacceptably slow for larger gadgets (there are 32 edges in gadget 3, hence 2^{32} terms to compute). To assist with the calculations, a simple divide-and-conquer approach was implemented. First, the $\mathcal{F}$-gate is divided into two smaller $\mathcal{F}$-gates by splitting along a min-cut of the edges (actually, an approximate randomized min-cut was used since it was more expedient to program). Then the signatures of both smaller $\mathcal{F}$-gates are computed recursively and combined to determine the signature of the entire $\mathcal{F}$-gate. Note that this approach has a poor worst-case complexity, since the runtime is tied to the size of the min-cut, and number of edges crossing the cut can be guaranteed to be large (for example, if the $\mathcal{F}$-gate is an expander graph). Nevertheless, this was enough speedup to enable the efficient investigation of all gadgets contained in this thesis.

The introduction of gadget 3 proved that a few of the remaining problems are $\#\mathrm{P}\text{-hard}$. Note that since gadgets 1, 2, and 3 (and the resulting construction of Theorem 4) are planar, we would not expect this approach to prove #P-hardness for problems that are in FP when the input is restricted to planar graphs. Since we know that some problems will be $\#\mathrm{P}\text{-hard}$ in general but in FP when restricted to planar graphs (this is the case in [9]), a sensible attempt is to use gadgets that are nonplanar. However, this did not help to classify any of the remaining problems. Finally, a program was written to exhaustively enumerate gadgets of a limited size, and this too was a dead end.

Applying a holographic reduction to a degenerate signature results in another degenerate signature, but not all of the polynomial time algorithms discused above apply invariantly under holographic reductions. For example, a connectivity argument may not apply to a given problem, but it might pertain after a suitable holographic reduction has been applied to transform the problem into a more apt form. Additionally, one can multiply each entry of a signature by any nonzero $c \in \mathbb{C}$ without changing the complexity of the problem; for a signature grid Ω, this has the effect of multiplying Holant_Ω by c^s, where s is the number of times that signature appears in Ω.

To take advantage of this, we start over with every problem defining an equivalence class of size 1, and then repeatedly merge equivalence classes for which constituent problems are equivalent (either under a holographic reduction or by multiplying generator or recognizer signatures by -1).

Then we attempt to apply the algorithms and gadgets as before — if a representative of some equivalence class is shown to be in FP or $\#\mathrm{P}$-hard, then we immediately know the complexity of every problem in that equivalence class and we remove those problems from consideration. After all of this, there were only four equivalence classes remaining; three of them contained problems that were already known to be in FP for planar graphs and $\#\mathrm{P}$-hard in general, and the fourth is solvable in polynomial time by an entirely different technique. Although a dichotomy was already proved at this point, the method described above doesn't lend itself well to a human-readable proof. In particular it involves far too many holographic reductions. Through a process of trial-and-error, the program was modified to get the same result while making the most of a few simple operations and keeping the more technical steps to a minimum.

In the course of all of this, it was noticed that once holographic reductions are taken into account, the connectivity argument described above could be used to solve any problem that was also computable with Fibonacci gates. This lead to the discovery of a characterization of Fibonacci gates that we discuss in the next section. This connection is not a special property of $\#[x_0, x_1, x_2] \mid [y_0, y_1, y_2, y_3]$ over $\{0, 1, -1\}$, but rather it applies to a much wider setting of holant problems.

2.3 A characterization of Fibonacci gates

Fibonacci gates are a new tool in the theory of holographic algorithms, introduced in [9]. A symmetric signature $[f_0, f_1, \ldots, f_n]$ is called a *Fibonacci signature* if it satisfies the relation $f_{k+2} = f_{k+1} + f_k$ for all $k \in \{0, 1, \ldots, n-2\}$. If an $\mathcal{F}$-gate happens to have a signature which is a Fibonacci signature, then we will call it a *Fibonacci gate*. Fibonacci gates have the interesting property that if one or more dangling edges of two existing Fibonacci gates are merged together, then the result is another Fibonacci gate. This implies an efficient algorithm for computing the holant of signature grids where every signature is a Fibonacci signature [9]. By the theory of holographic reductions, Fibonacci gates also apply to a more general class of problems. Given a signature grid Ω, if there is a holographic reduction that transforms every signature in Ω to a Fibonacci signature, then the combination of holographic reductions and Fibonacci gates produces a polynomial time algorithm for computing Holant_Ω. Once holographic reductions are taken into account in this way, the following characterization can be made.

Theorem 5. *A set of symmetric generators* $\mathcal{G} = \{G_1, G_2, \ldots, G_s\}$ *and symmetric recognizers* $\mathcal{R} = \{R_1, R_2, \ldots, R_t\}$ *are all simultaneously realizable as Fibonacci signatures after a holographic reduction under some basis* $T \in \mathrm{GL}_2(\mathbb{C})$ *if and only if there exist three constants* $a, b,$ *and* c *such that* $b^2 - 4ac \neq 0$ *and the following two conditions are satisfied:*

1. *For any* $[x_0, x_2, \ldots, x_g] \in \mathcal{G}$ *and any* $k \in \{0, 1, \ldots, g-2\}$*,* $cx_k - bx_{k+1} + ax_{k+2} = 0$*.*
2. *For any* $[y_0, y_2, \ldots, y_r] \in \mathcal{R}$ *and any* $k \in \{0, 1, \ldots, r-2\}$*,* $ay_k + by_{k+1} + cy_{k+2} = 0$*.*

Proof. See [9]. □

Now we show that, under holographic transformations, any bipartite signature grid is realizable as a signature grid of WEIGHTED-EQUALITY signatures precisely if the same two conditions of Theorem 5 hold.

Lemma 4. *A set of symmetric generators* $\mathcal{G} = \{G_1, G_2, \ldots, G_s\}$ *and symmetric recognizers* $\mathcal{R} = \{R_1, R_2, \ldots, R_t\}$ *are all simultaneously realizable as* WEIGHTED-EQUALITY *signatures after a holographic reduction under some basis* $T \in \mathrm{GL}_2(\mathbb{C})$ *if and only if there exist three constants* a*,* b*, and* c *such that* $b^2 - 4ac \neq 0$ *and the following two conditions are satisfied:*

1. *For any* $[x_0, x_2, \ldots, x_g] \in \mathcal{G}$ *and any* $k \in \{0, 1, \ldots, g-2\}$*,* $cx_k - bx_{k+1} + ax_{k+2} = 0$*.*
2. *For any* $[y_0, y_2, \ldots, y_r] \in \mathcal{R}$ *and any* $k \in \{0, 1, \ldots, r-2\}$*,* $ay_k + by_{k+1} + cy_{k+2} = 0$*.*

Proof. Let $\mathcal{G}' = \{G'_1, G'_2, \ldots, G'_s\}$ and $\mathcal{R}' = \{R'_1, R'_2, \ldots, R'_t\}$ such that each G'_i is of the form $G'_i = [a_i, 0, 0, \ldots, 0, b_i]$, and each R'_i is of the form $R'_i = [c_i, 0, 0, \ldots, 0, d_i]$. Let $T = \begin{bmatrix} \alpha_1 & \beta_1 \\ \alpha_2 & \beta_2 \end{bmatrix}$ be any invertible matrix, and let g_i and r_i denote the arity of G'_i and R'_i, respectively. Applying a holographic reduction to $\#\mathcal{G}' \mid \mathcal{R}'$ using T, we have $\widetilde{G_i} = T^{\otimes g_i}\widetilde{G'_i}$, so in symmetric notation $G_i = [a_i\alpha_1^{g_i} + b_i\beta_1^{g_i}, a_i\alpha_1^{g_i-1}\alpha_2 + b_i\beta_1^{g_i-1}\beta_2, \ldots, a_i\alpha_2^{g_i} + b_i\beta_2^{g_i}]$, that is, the element at zero-based index j in the symmetric signature of G_i is $a_i\alpha_1^{g_i-j}\alpha_2^j + b_i\beta_1^{g_i-j}\beta_2^j$. Since $T^{-1} = \frac{1}{d}\begin{bmatrix} \beta_2 & -\beta_1 \\ -\alpha_2 & \alpha_1 \end{bmatrix}$ where

$d = \det(T)$, we find $\widetilde{R_i} = \widetilde{R_i'}(T^{-1})^{\otimes r_i}$ to have $c_i(\beta_2/d)^{r_i - j}(-\beta_1/d)^j + d_i(-\alpha_2/d)^{r_i-j}(\alpha_1/d)^j$ as its element at index j. Interpreting the signatures of G_i and R_i as second order linear homogeneous recurrence relations, we see that the roots of the characteristic polynomials of the recurrences are $\gamma_1 := \alpha_2/\alpha_1$ and $\gamma_2 := \beta_2/\beta_1$ for G_i, and for R_i they are $-\beta_1/\beta_2 = -\gamma_2^{-1}$ and $-\alpha_1/\alpha_2 = -\gamma_1^{-1}$, regardless of i in both cases. The associated characteristic polynomials for the generator and recognizer recurrences are then $x^2 - (\gamma_1 + \gamma_2)x + \gamma_1\gamma_2 = 0$ and $\gamma_1\gamma_2 x^2 + (\gamma_1 + \gamma_2)x + 1 = 0$ respectively, thus we have the relation $cx_k - bx_{k+1} + ax_{k+2} = 0$ for each generator and $ax_k + bx_{k+1} + cx_{k+2} = 0$ for each recognizer where $a = 1, b = \gamma_1 + \gamma_2$, and $c = \gamma_1\gamma_2$. Note that $b^2 - 4ac = (\gamma_1 + \gamma_2)^2 - 4\gamma_1\gamma_2 = (\gamma_1 - \gamma_2)^2 \neq 0$ as required, since $\det(T) \neq 0$.

Conversely, let $\mathcal{G} = \{G_1, G_2, \ldots, G_s\}$ and $\mathcal{R} = \{R_1, R_2, \ldots, R_t\}$ be sets of symmetric signatures, and suppose there exist a, b, c with $b^2 - 4ac \neq 0$ such that for any $[x_0, x_1, \ldots, x_g] \in \{G_1, \ldots, G_s\}$, we have $cx_k - bx_{k+1} + ax_{k+2} = 0$ and for any recognizer $[x_0, x_1, \ldots, x_r] \in \{R_1, \ldots, R_t\}$, we have $ax_k + bx_{k+1} + cx_{k+2} = 0$. Since $b^2 - 4ac \neq 0$, the roots of the characteristic polynomials are distinct, and we can write the generator signature of G_i such that the element at index j is $a_i\alpha_1^{g_i-j}\alpha_2^j + b_i\beta_1^{g_i-j}\beta_2^j$, for some fixed a_i and b_i. Similarly, we can have recognizer R_i take the value $c_i d^{-r_i}(\beta_2)^{r_i-j}(-\beta_1)^j + d_i d^{-r_i}(-\alpha_2)^{r_i-j}(\alpha_1)^j$ at index j, where $d = \det(T)$ as before (note that $d \neq 0$ because $b^2 - 4ac \neq 0$). The constants a_i and b_i in the case of generators and c_i and d_i in the case of recognizers are uniquely determined by the first two values of its signature. Now applying the same holographic reduction as before, we get symmetric signatures with the desired form. □

Now it is easy to see that, under holographic transformations, any bipartite signature grid is realizable as a signature grid of Fibonacci signatures if and only if it is realizable as a signature grid of WEIGHTED-EQUALITY signatures. Recall that if a signature grid consists entirely of WEIGHTED-EQUALITY signatures, then the holant is trivial to compute, since the only nonzero terms of the holant have identical edge assignments within every connected component. Hence whenever a signature grid is computable with Fibonacci gates it can also be computed by performing a holographic reduction and using a connectivity argument.

Corollary 1. *A set of symmetric generators* $\mathcal{G} = \{G_1, G_2, \ldots, G_s\}$ *and symmetric recognizers* $\mathcal{R} = \{R_1, R_2, \ldots, R_t\}$ *are all simultaneously realizable as Fibonacci gates after a holographic reduction under some basis* $T \in \mathrm{GL}_2(\mathbb{C})$ *if and only if they are all simultaneously realizable as* WEIGHTED-EQUALITY *signatures after a holographic reduction under some basis* $T' \in \mathrm{GL}_2(\mathbb{C})$.

Proof. Immediate from Theorem 5 and Lemma 4. □

2.4 Classification of problems

In this section we prove a dichotomy theorem, where we show that every problem of the form $\#[x_0, x_1, x_2] \mid [y_0, y_1, y_2, y_3]$ is either in FP or $\#\mathrm{P}$-hard, where $x_i, y_j \in \{0, 1, -1\}$. We do this both for the general bipartite setting and also when the input is restricted to planar bipartite graphs, so there are three possibilities for any problem:

1. The problem is in FP.
2. The problem is $\#\mathrm{P}$-hard in general, but in FP when restricted to planar graphs.
3. The problem is $\#\mathrm{P}$-hard, even when restricted to planar graphs.

We start with a few observations regarding relationships between different problems.

1. Reversing the order of both the generator and recognizer signatures has no effect on the complexity, and is justified by a holographic reduction under the basis $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ (or by switching the roles of the 0s and 1s in the assignments to the edges).
2. Multiplying each entry of a signature by -1 has the effect of multiplying the value of the signature grid by $(-1)^s$ where s is the number of vertices labeled with that signature - hence this operation does not change the complexity of the problem.
3. The problems $\#[x_0, x_1, x_2] \mid [y_0, y_1, y_2, y_3]$ and $\#[x_0, -x_1, x_2] \mid [y_0, -y_1, y_2, -y_3]$ are equivalent by a holographic reduction under the basis $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$.

Now define the equivalence relation $\sim$ so that two problems are considered equivalent under $\sim$ if and only if one can be reduced to the other via some combination of one or more of the above 3 transformations, so that members of each equivalence class of $\sim$ share the same complexity. This equivalence relation will simplify our discussion.

2.4.1 Tractable problems

Here we list which problems are in FP and how they can be solved efficiently. These problems can be solved efficiently using the same techniques used in the case of binary signatures [9]. We first consider the degenerate signatures. These are problems that have the generator signature $[0,0,0]$, $[0,0,x]$, $[x,0,0]$, $[x,x,x]$, or $[x,-x,x]$, as well as any problems with recognizer signature $[0,0,0,0]$, $[0,0,0,y]$, $[y,0,0,0]$, $[y,y,y,y]$, or $[y,-y,y,-y]$, where $x,y \in \{1,-1\}$. In the following, s is the number of generators and t to is the number of recognizers in the signature grid.

- $\#[0,0,0] \mid [y_0,y_1,y_2,y_3]$ and $\#[x_0,x_1,x_2] \mid [0,0,0,0]$ trivially evaluate to zero.
- $\#[0,0,x] \mid [y_0,y_1,y_2,y_3]$ and $\#[x_0,x_1,x_2] \mid [0,0,0,y]$ evaluate to $x^s y_3^t$ and $x_2^s y^t$ respectively.
- $\#[x,x,x] \mid [y_0,y_1,y_2,y_3]$ and $\#[x_0,x_1,x_2] \mid [y,y,y,y]$ evaluate to $x^s(y_0+3y_1+3y_2+y_3)^t$ and $(x_0+2x_1+x_2)^s y^t$ respectively.

All remaining problems involving a degenerate signature can be related to a problem already discussed above:

$$\begin{aligned}
\#[x,0,0] \mid [y_0,y_1,y_2,y_3] &\sim \#[0,0,x] \mid [y_3,y_2,y_1,y_0],\\
\#[x_0,x_1,x_2] \mid [y,0,0,0] &\sim \#[x_2,x_1,x_0] \mid [0,0,0,y],\\
\#[x,-x,x] \mid [y_0,y_1,y_2,y_3] &\sim \#[x,x,x] \mid [y_0,-y_1,y_2,-y_3],\\
\#[x_0,x_1,x_2] \mid [y,-y,y,-y] &\sim \#[x_0,-x_1,x_2] \mid [y,y,y,y].
\end{aligned}$$

Generators of the form $[x_0,x_1,0]$ effectively require that at most half of the edges are assigned to 1, and recognizers of the form $[0,0,y_2,y_3]$ demand that at least two-thirds of the edges are assigned to 1. These requirements are incompatible so for any problem instance Ω of the form $\#[x_0, x_1, 0] \mid [0, 0, y_2, y_3]$, we have $\text{Holant}_\Omega = 0$. This is similarly the case for $\#[0, x_1, x_2] \mid [y_0, y_1, 0, 0]$.

Problems where recognizers have the form $[y_0, 0, 0, y_3]$ and generators have the form $[x_0, 0, x_2]$ or $[0, x_1, 0]$ can be solved in polynomial time with a connectivity argument. That is, once an assignment to an edge has been made, all edge assignments to adjacent edges become determined if that assignment is to result in a nonzero evaluation, and the entire connected component has its edge assignments determined as a result (if a consistent assignment to that connected component even exists). Once the holant has been computed for each connected component, the product of these is the holant of the entire signature grid. Given Corollary 1, this technique becomes widely applicable to the problems we are considering. Furthermore, a connectivity argument can also be carried out for problems of the form $\#[x, 0, -x] \mid [y, 0, y, 0]$, $\#[x, 0, -x] \mid [0, y, 0, y]$, and $\#[x, 0, x] \mid [y, z, -y, -z]$. Using the holographic reduction $R = [c, 0, 0, d] \cdot T^{\otimes 3}$, $G = (T^{-1})^{\otimes 2} \cdot [0, a, 0]^{\mathrm{T}}$, these problems reduce to $\#[0, a, 0] \mid [c, 0, 0, d]$ for some $a, c, d \in \mathbb{C}$ using the bases $T_1 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$, $T_2 = \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}$, and $T_3 = \begin{bmatrix} 1 & \mathfrak{i} \\ 1 & -\mathfrak{i} \end{bmatrix}$ respectively.

One final class of problems remain that are computable in FP over general graphs. These are the problems with generators of the form $[x, x, -x]$ or $[x, -x, -x]$ and recognizers of the form $[y, 0, 0, z]$, $[y, 0, y, 0]$, or $[0, y, 0, y]$ where $x, y, z \in \{1, -1\}$. These are covered by the following lemma, which follows from [11].

Lemma 5. *If* Ω *is a signature grid that consists only of the signatures* $[1, 1, -1]$, $[1, -1, -1]$, $[0, 1, 0, 1]$, $[1, 0, 1, 0]$, $[1, 0, 0, -1]$, *and* $[1, 0, 0, 1]$, *then* Holant_Ω *can be computed in polynomial time.*

2.4.2 Problems that are tractable for planar graphs but #P-hard in general

Some problems are #P-hard in general but are in FP when restricted to planar graphs. For example, it is known that the problems $\#[1, 0, 1] \mid [0, 1, 0, 0]$, $\#[1, 0, 1] \mid [0, 1, 1, 0]$, and $\#[0, 1, 0] \mid$

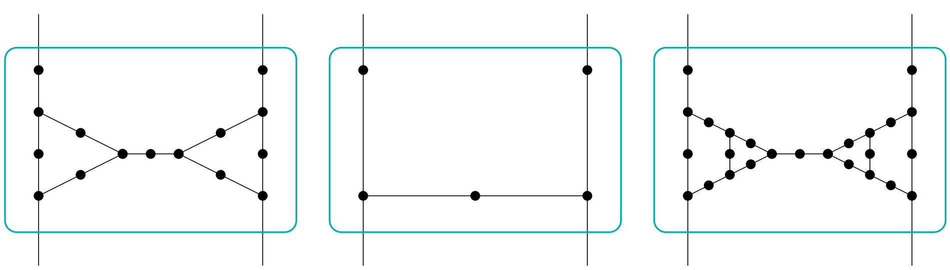
$[0,1,1,0]$ fall in this category [9]. Then we get

$$\begin{aligned}\#[1,0,1] \mid [0,1,0,0] &\sim \#[x,0,x] \mid [0,y,0,0], \\ \#[1,0,1] \mid [0,1,1,0] &\sim \#[x,0,x] \mid [0,y,z,0], \\ \#[0,1,0] \mid [0,1,1,0] &\sim \#[0,x,0] \mid [0,y,z,0]\end{aligned}$$

for all $x, y, z \in \{1, -1\}$. It turns out that these are the only problems under consideration which are $\#\mathrm{P}$-hard in general but are in FP when restricted to planar graphs, as we will verify shortly.

2.4.3 Problems that are $\#\mathrm{P}$-hard even for planar graphs

There are 48 problems which we show to be $\#\mathrm{P}$-hard, even in the planar case, by using the general strategy of interpolation as in Theorem 4. In each case, one of three planar gadgets is applied to the problem, the transition matrix is calculated, and sufficient conditions on the matrix are verified to be met. The list of problems, which gadgets were applied, and the resulting irreducible characteristic polynomials are in Tables 2.3 and 2.4. For most problems, at least one of the two gadgets given in [9] was sufficient for interpolation, but in a few cases a new gadget (see Figure 2.1(c)) was needed. Since the polynomials have integer coefficients, they can be shown to be irreducible over $\mathbb{Q}$ via Gauss's lemma by checking that the roots are not integral.



(a) Gadget 1 (b) Gadget 2 (c) Gadget 3

Figure 2.1 Three binary recursive gadgets

To illustrate the process, we will prove that $\#[-1,-1,1] \mid [-1,1,1,1]$ is $\#\mathrm{P}$-hard. For this particular problem, it turns out that both gadget 1 and gadget 2 do not meet the conditions of Theorem 4, so we will try gadget 3. Using the software, we calculate that the transition matrix is $M = \begin{bmatrix} -9216 & -36864 & -4096 \\ 15360 & -8192 & -12288 \\ 7168 & 20480 & -4096 \end{bmatrix}$, which means that an $\mathcal{F}$-gate built using s iterations of gadget 3 will have a signature given by $M^s \cdot [-1, -1, 1]^{\mathrm{T}}$ (note that symmetry of the final $\mathcal{F}$-gate's signature is immediate from graph symmetry in the construction). Now we verify that the technical conditions hold. The characteristic polynomial of M is $f(x) = x^3 + 21504x^2 + 994050048x + 3229815406592$, so clearly $\det(M) \neq 0$ and $f(x)$ is not of the form $x^3 + c$. There is only one real root of $f(x)$, and it is at $x \approx -3467.28$. Since the polynomial has integer coefficients and no integer roots, we conclude by Gauss's lemma that $f(x)$ is irreducible over the rationals. Finally, we need to verify that $[-1, -1, 1]$ is not orthogonal to any row eigenvector of M. Suppose u is a row eigenvector of M and u is orthogonal to $[-1, -1, 1]$, so that $u = [a, b, a + b]$ for some a and b and $uM = \lambda u$ where $\lambda \neq 0$. Then $\lambda u = uM = -2048[a - 11b, 8a - 6b, 4a + 8b]$, thus $-2048(4a + 8b) = \lambda(a + b) = \lambda a + \lambda b = -2048(a - 11b + 8a - 6b)$, which yields $a = 5b$. Then $\lambda[5b, b, 6b] = \lambda u = [-6b, 34b, 28b]$, from which we conclude that $b = 0$, $a = 0$, and no row eigenvector is orthogonal to $[-1, -1, 1]$. Gadget 3 is planar, so by Theorem 4, $\#[-1, -1, 1] \mid [-1, 1, 1, 1]$ is $\#\mathrm{P}$-hard, even for planar graphs. Meeting the technical conditions of the theorem verifies that we can build a linear system of full rank to solve for the constants $c_{i,j,k}$ in equation (2.1). If the $c_{i,j,k}$ constants are in hand, then one can solve any problem of the form $\#[x_0, x_1, x_2] \mid [-1, 1, 1, 1]$, but since $[-1, 1, 1, 1]$ is nondegenerate, there also exist x_0, x_1, and x_2 such that $\#[x_0, x_1, x_2] \mid [-1, 1, 1, 1]$ is $\#\mathrm{P}$-hard, and this completes the reduction.

2.4.4 Putting it all together

Theorem 6. *All problems of the form* $\#[x_0, x_1, x_2] \mid [y_0, y_1, y_2, y_3]$ *where* $x_i, y_j \in \{0, 1, -1\}$ *are either 1)* $\#\mathrm{P}$-hard *in general but in* FP *when restricted to planar graphs, 2)* $\#\mathrm{P}$-hard *even for planar graphs, or 3) in* FP.

Proof. As we saw earlier, all such problems which contain a degenerate signature are in FP, so we need not consider any setting where the generator or recognizer are degenerate (this handles 9 generators and 9 recognizers). Under $\sim$, the remaining 72 recognizers fall into 12 equivalence classes: 6 of them have 8 members each (we will identify these by the representatives $[0, 1, 1, 1]$, $[-1, 1, 1, 1]$, $[1, 0, 1, 1]$, $[0, 0, 1, 1]$, $[-1, 0, 1, 1]$, and $[0, -1, 1, 1]$), and the other 6 have 4 members each (identified by the representatives $[-1, -1, 1, 1]$, $[0, 1, 0, 1]$, $[1, 0, 0, 1]$, $[0, -1, 0, 1]$, $[0, 1, 1, 0]$, and $[0, 0, 1, 0]$). To classify the complexity of all of these problems, it suffices to classify all 18 nondegenerate generators in combination with each of these recognizer representatives. In the cases where the problem turns out to be in FP, either a counting argument, connectivity argument, or Lemma 5 is applied, as discussed earlier. The problems that are tractable when the input is restricted to planar graphs but $\#\mathrm{P}\text{-hard}$ in general are established by holographic reductions above. Each problem that is $\#\mathrm{P}\text{-hard}$ even when restricted to planar graphs is either proved directly using interpolation or indirectly using a holographic reduction. The problems are categorized in Tables 2.1 and 2.2, and the technical calculations for applying interpolation are summarized in Tables 2.3 and 2.4. Throughout the following, we use x, y, and z to denote ± 1, with no dependence on each other.

1. For $[0, 1, 1, 1]$, connectivity arguments apply with generators $[x, -x, -x]$ and $[x, -x, 0]$. The remaining 14 problems are $\#\mathrm{P}\text{-hard}$. This is shown indirectly for $\#[0, x, -x] \mid [0, 1, 1, 1]$, as $\#[1, 0, -1] \mid [0, -1, -1, -1]$ reduces to $\#[0, -1, -1] \mid [0, -1, 1, -1]$ under basis $\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$.
2. For $[-1, 1, 1, 1]$, generators $[x, -x, -x]$ and $[x, -x, 0]$ admit a connectivity argument. The other 14 posibilities for generators are $\#\mathrm{P}\text{-hard}$.
3. For $[1, 0, 1, 1]$, generators $[x, 0, x]$, $[0, x, x]$, and $[x, -x, 0]$ admit a connectivity argument. The other 12 posibilities are $\#\mathrm{P}\text{-hard}$.
4. For $[0, 0, 1, 1]$, generators $[0, x, 0]$ and $[x, y, 0]$ admit a counting argument. The other 12 cases are $\#\mathrm{P}\text{-hard}$.
5. For $[-1, 0, 1, 1]$, generators $[x, -x, 0]$, $[x, 0, -x]$, and $[0, x, -x]$ admit a connectivity argument. The other 12 cases are $\#\mathrm{P}\text{-hard}$.

6. For $[0,-1,1,1]$, generators $[x,x,0]$ and $[x,-x,-x]$ admit a connectivity argument. The 14 remaining problems are $\#\mathrm{P}$-hard. In the case of $[x,0,-x]$, this follows from the fact that $\#[0,1,-1] \mid [0,1,1,-1]$ reduces to $\#[1,0,-1] \mid [0,1,-1,-1]$ under basis $\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$.

7. For $[-1,-1,1,1]$, generators $[x,-x,-x]$, $[x,x,-x]$, $[0,x,0]$, and $[x,0,y]$ admit a connectivity argument. The other 8 possibilities are $\#\mathrm{P}$-hard (note that this recognizer has an extra degree of self-symmetry, we can apply negative and reversals, so each case in the table counts for 4).

8. For $[0,1,0,1]$, generators $[x,0,y]$ and $[0,x,0]$ admit a connectivity argument. The case where generators are $[x,-x,-x]$ or $[x,x,-x]$ are solvable in polynomial time by Lemma 5. The other 8 cases are $\#\mathrm{P}$-hard.

9. For $[1,0,0,1]$, generators $[x,0,y]$ and $[0,x,0]$ admit a connectivity argument. The case where generators are $[x,-x,-x]$ or $[x,x,-x]$ is solvable in polynomial time by Lemma 5. There are 8 $\#\mathrm{P}$-hard cases. Generators $[x,-x,0]$ and $[0,x,-x]$ are proved to be $\#\mathrm{P}$-hard by the fact that $\#[1,0,-1] \mid [0,-1,1,-1]$ reduces to $\#[0,1,-1] \mid [-1,0,0,-1]$ under basis $\begin{bmatrix} 1 & -1 \\ -1 & 0 \end{bmatrix}$.

10. For $[0,-1,0,1]$, generators $[x,-x,-x]$, $[x,x,-x]$, $[0,x,0]$, and $[x,0,y]$ admit a connectivity argument. The other 8 cases are $\#\mathrm{P}$-hard.

11. For $[0,1,1,0]$, generators $[x,-x,0]$, $[0,x,-x]$, and $[x,0,-x]$ admit a connectivity argument. Generators $[0,x,0]$ and $[x,0,x]$ are in FP when the input is restricted to planar graphs but $\#\mathrm{P}$-hard in general. The 8 cases remaining are $\#\mathrm{P}$-hard.

12. For $[0,0,1,0]$, generators $[x,y,0]$ and $[0,x,0]$ admit a counting argument. Generators of the form $[x,0,y]$ are in FP when the input is restricted to planar graphs but $\#\mathrm{P}$-hard in general. The 8 cases remaining are $\#\mathrm{P}$-hard.

□

Table 2.1 Classification of problems, where x,$y \in \{1, -1\}$

Recognizer	#P-hard, even for planar graphs	#P-hard in general, but in FP when planar	In FP by counting argument	In FP by connectivity argument	In FP by Lemma 5
$[0, 1, 1, 1]$	$[0, x, x]$,$[x, x, 0]$, $[x, 0, y]$,$[x, x, -x]$, $[0, x, 0]$,$[0, x, -x]$ [1]			$[x, -x, -x]$ $[x, -x, 0]$	
$[-1, 1, 1, 1]$	$[0, x, x]$,$[x, x, 0]$, $[x, 0, y]$,$[x, x, -x]$, $[0, x, 0]$,$[0, x, -x]$			$[x, -x, -x]$ $[x, -x, 0]$	
$[1, 0, 1, 1]$	$[-x, x, x]$,$[-x, 0, x]$, $[0, -x, x]$,$[x, x, -x]$, $[x, x, 0]$,$[0, x, 0]$			$[x, 0, x]$ $[0, x, x]$ $[x, -x, 0]$	
$[0, 0, 1, 1]$	$[0, x, x]$,$[-x, x, x]$, $[x, 0, y]$,$[0, x, -x]$, $[x, x, -x]$		$[0, x, 0]$ $[x, y, 0]$		
$[-1, 0, 1, 1]$	$[0, x, x]$,$[-x, x, x]$, $[x, 0, x]$,$[x, x, -x]$, $[x, x, 0]$,$[0, x, 0]$			$[x, -x, 0]$ $[x, 0, -x]$ $[0, x, -x]$	
$[0, -1, 1, 1]$	$[0, x, x]$,$[x, 0, x]$, $[0, x, -x]$,$[x, x, -x]$, $[0, x, 0]$,$[x, -x, 0]$ $[x, 0, -x]$ [2]			$[x, x, 0]$ $[-x, x, x]$	

[1] $\#[-1, 0, 1] \mid [0, 1, 1, 1]$ reduces to $\#[0, -1, 1] \mid [0, 1, 1, 1]$ under basis $\begin{bmatrix} -1 & -1 \\ 0 & 1 \end{bmatrix}$.

[2] $\#[0, 1, 1] \mid [0, -1, 1, 1]$ reduces to $\#[-1, 0, 1] \mid [0, -1, 1, 1]$ under basis $\begin{bmatrix} -1 & 1 \\ 0 & 1 \end{bmatrix}$, so the generators $[x, 0, -x]$ are also hard.

Table 2.2 Classification of problems, where x,$y \in \{1, -1\}$, continued

Recognizer	#P-hard, even for planar graphs	#P-hard in general, but in FP when planar	In FP by counting argument	In FP by connectivity argument	In FP by Lemma 5
$[-1,-1,1,1]$	$[0,x,y]$,$[x,y,0]$			$[x,-x,-x]$ $[x,x,-x]$ $[0,x,0]$ $[x,0,y]$	
$[0,1,0,1]$	$[0,x,y]$,$[x,y,0]$			$[x,0,y]$ $[0,x,0]$	$[-x,x,x]$ $[x,x,-x]$
$[1,0,0,1]$	$[0,x,x]$,$[x,x,0]$ $[x,-x,0]$,$[0,x,-x]$ [3]			$[x,0,y]$ $[0,x,0]$	$[-x,x,x]$ $[x,x,-x]$
$[0,-1,0,1]$	$[0,x,y]$,$[x,y,0]$			$[-x,x,x]$ $[x,x,-x]$ $[0,x,0]$ $[x,0,y]$	
$[0,1,1,0]$	$[0,x,x]$,$[x,x,0]$, $[-x,x,x]$,$[x,x,-x]$	$[0,x,0]$ $[x,0,x]$		$[x,-x,0]$ $[0,x,-x]$ $[x,0,-x]$	
$[0,0,1,0]$	$[0,x,y]$,$[x,x,-x]$, $[-x,x,x]$	$[x,0,y]$	$[x,y,0]$ $[0,x,0]$		

[3] Cases $[x,-x,0]$ and $[0,x,-x]$ are handled by the fact that $\#[-1,0,1] \mid [0,1,1,1]$ reduces to $\#[0,1,-1] \mid [1,0,0,1]$ under basis $\begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix}$ and thus are hard.

Table 2.3 Problems which are shown to be $\#\mathrm{P}\text{-hard}$ by Theorem 4

Problem	Gadget	Irreducible characteristic polynomial
$\#[0,1,1] \mid [0,1,1,1]$	1	$X^3 - 15498X^2 + 419904X - 19683$
$\#[1,0,1] \mid [0,1,1,1]$	2	$X^3 - 6X^2 - 3X + 2$
$\#[-1,0,1] \mid [0,1,1,1]$	1	$X^3 + 2X^2 + 4X + 1$
$\#[-1,-1,1] \mid [0,1,1,1]$	2	$X^3 - 3X^2 + 12X + 32$
$\#[1,1,0] \mid [0,1,1,1]$	1	$X^3 - 1370X^2 + 105835X - 352450$
$\#[0,1,0] \mid [0,1,1,1]$	1	$X^3 - 184X^2 + 1600X - 512$
$\#[0,1,1] \mid [-1,1,1,1]$	1	$X^3 - 11691X^2 + 1285956X - 1259712$
$\#[1,0,1] \mid [-1,1,1,1]$	3	$X^3 - 4800X^2 + 1683456X - 69468160$
$\#[-1,0,1] \mid [-1,1,1,1]$	1	$X^3 - 16X^2 + 256X + 4096$
$\#[0,-1,1] \mid [-1,1,1,1]$	1	$X^3 + 17X^2 + 100X + 64$
$\#[-1,-1,1] \mid [-1,1,1,1]$	3	$X^3 + 21504X^2 +$ $994050048X + 3229815406592$
$\#[1,1,0] \mid [-1,1,1,1]$	2	$X^3 - 3X^2 + 40X - 48$
$\#[0,1,0] \mid [-1,1,1,1]$	1	$X^3 + 32X^2 + 1024X - 32768$
$\#[-1,1,1] \mid [1,0,1,1]$	2	$X^3 - 7X^2 - 18X + 72$
$\#[-1,0,1] \mid [1,0,1,1]$	2	$X^3 + X^2 + X + 2$
$\#[0,-1,1] \mid [1,0,1,1]$	2	$X^3 - X^2 + 5X + 2$
$\#[-1,-1,1] \mid [1,0,1,1]$	2	$X^3 + 5X^2 + 2X + 24$
$\#[1,1,0] \mid [1,0,1,1]$	2	$X^3 - 7X^2 - 11X - 2$
$\#[0,1,0] \mid [1,0,1,1]$	2	$X^3 - X^2 - 4X - 4$
$\#[0,1,1] \mid [0,0,1,1]$	2	$X^3 - 14X^2 + 16X - 1$
$\#[-1,1,1] \mid [0,0,1,1]$	2	$X^3 - 12X^2 + 32X - 8$
$\#[1,0,1] \mid [0,0,1,1]$	2	$X^3 - 3X^2 - X + 1$
$\#[-1,0,1] \mid [0,0,1,1]$	2	$X^3 + X^2 + X - 1$
$\#[0,-1,1] \mid [0,0,1,1]$	2	$X^3 - 2X^2 + 4X - 1$

Table 2.4 Problems which are shown to be #P-hard by Theorem 4, continued

Problem	Gadget	Irreducible characteristic polynomial
$\#[-1,-1,1] \mid [0,0,1,1]$	2	X^3+8X-8
$\#[0,1,1] \mid [-1,0,1,1]$	2	$X^3-13X^2+37X-14$
$\#[-1,1,1] \mid [-1,0,1,1]$	2	$X^3-15X^2+62X-56$
$\#[1,0,1] \mid [-1,0,1,1]$	2	X^3-3X^2-X+2
$\#[-1,-1,1] \mid [-1,0,1,1]$	2	$X^3-3X^2+26X+56$
$\#[1,1,0] \mid [-1,0,1,1]$	2	X^3+5X^2+X-14
$\#[0,1,0] \mid [-1,0,1,1]$	2	X^3+X^2+4X-4
$\#[0,1,1] \mid [0,-1,1,1]$	2	$X^3-2X^2+11X-8$
$\#[1,0,1] \mid [0,-1,1,1]$	2	X^3-4X^2-X+6
$\#[0,-1,1] \mid [0,-1,1,1]$	2	$X^3-4X^2+37X-48$
$\#[-1,-1,1] \mid [0,-1,1,1]$	2	$X^3+13X^2+36X-288$
$\#[0,1,0] \mid [0,-1,1,1]$	2	$X^3+7X^2+16X+8$
$\#[-1,1,0] \mid [0,-1,1,1]$	2	$X^3+14X^2+43X+22$
$\#[0,1,1] \mid [-1,-1,1,1]$	2	$X^3-1X^2+26X-40$
$\#[0,-1,1] \mid [-1,-1,1,1]$	2	$X^3-5X^2+34X-40$
$\#[0,1,1] \mid [0,1,0,1]$	2	X^3-6X^2-8X-3
$\#[1,1,0] \mid [0,1,0,1]$	2	X^3-7X^2+5X+3
$\#[0,1,1] \mid [1,0,0,1]$	1	$X^3-14X^2+16X-1$
$\#[0,1,1] \mid [0,-1,0,1]$	2	X^3+4X^2+2X-5
$\#[1,1,0] \mid [0,-1,0,1]$	2	$X^3-7X^2+13X-5$
$\#[0,1,1] \mid [0,1,1,0]$	2	$X^3-14X^2+39X-14$
$\#[-1,1,1] \mid [0,1,1,0]$	2	$X^3+4X^2+24X-56$
$\#[0,1,1] \mid [0,0,1,0]$	2	X^3-7X^2+9X-1
$\#[-1,1,1] \mid [0,0,1,0]$	2	$X^3-5X^2+18X-8$

Chapter 3

Obtaining a dichotomy the easy way: finisher gadgets and Eigenvalue Shifted Pairs

In this chapter we prove a complexity dichotomy theorem for $\#[x_0, x_1, x_2] \mid [1, 0, 0, 1]$, where each $x_i \in \mathbb{C}$. This can be equivalently understood as holant problems on 3-regular graphs where $\{0, 1\}$-assignments are made to the vertices and a single arbitrary complex-valued symmetric signature is assigned to the edges. Three new techniques are introduced. (1) We introduce a method to construct gadgets that carry out iterations at a higher dimension, and then collapse to a lower dimension for the purpose of constructing unary signatures. This involves a binary starter gadget, a binary recursive gadget, and a binary finisher gadget. We prove a lemma that guarantees that among polynomially many iterations, some subset of the $\mathcal{F}$-gates produced by the construction satisfies properties sufficient for interpolation to succeed (it may not be known *a priori* which subset worked, but that does not matter). (2) Eigenvalue Shifted Pairs are coupled pairs of gadgets whose transition matrices differ by δI where $\delta \neq 0$. They have shifted eigenvalues, and by analyzing their failure conditions, we can show that except on very rare points, one or the other gadget succeeds. (3) Algebraic symmetrization: we derive a new expression of the holant polynomial over 3-regular graphs, with a crucially reduced degree. This simplification of the holant and related polynomials condenses the problem of proving $\#\mathrm{P}$-hardness to the point where all remaining cases can be handled by symbolic computation. We also use the same expression to prove tractability, as it ties together problems that at first seem unrelated.

3.1 Background and discussion of techniques

The class of problems $\#[x_0, x_1, x_2] \mid [1, 0, 0, 1]$ has been studied previously for Boolean-valued x_i in [9] and for real-valued x_i in [10]. This subclass of holant problems can equivalently be considered as COUNTING WEIGHTED H-HOMOMORPHISMS (or H-COLORING) problems [3, 4, 16, 17, 19, 21] with an arbitrary 2×2 symmetric complex matrix H, however *restricted to* 3-regular graphs G as input.

The crucial difference between holant problems and WEIGHTED #CSP is that in the later, EQUALITY functions of arbitrary arity are *presumed* to be present. In terms of H-homomorphism problems, this means that the input graph is allowed to have vertices of arbitrarily high degrees. This may appear to be a minor distinction; in fact it has a major impact on complexity. It turns out that if EQUALITY signatures of arbitrary arity are freely available in possible inputs then it is technically easier to prove $\#\mathrm{P}$-hardness. Proofs of previous dichotomy theorems make extensive use of constructions called thickening and stretching. These constructions require the availability of EQUALITY signatures of arbitrary arity (equivalently, vertices of arbitrarily high degrees) to carry out. Proving $\#\mathrm{P}$-hardness becomes more challenging in the degree restricted case. Furthermore there are indeed cases within this class of counting problems where the problem is $\#\mathrm{P}$-hard for general graphs, but solvable in FP when restricted to 3-regular graphs.

With some modifications and additional insights, the results of this chapter can be extended to k-regular graphs; this is accomplished in Chapters 4 and 5. We remark that one can also use holographic reductions [34] to extend the following main result of this chapter to more general holant problems (i.e. to recognizers other than just $[1, 0, 0, 1]$).

Theorem 7. *The holant problem* $\#[x_0, x_1, x_2] \mid [1, 0, 0, 1]$ *is* $\#\mathrm{P}$-hard *for all* $x_0, x_1, x_2 \in \mathbb{C}$*, both for unrestricted input and for input restricted to planar graphs, except in the following cases, for which the problem is in* FP.[1]

1. $x_1 = 0$

[1]Technically, computational complexity involving complex or real numbers should, in the Turing model, be restricted to computable numbers. In other models such as the Blum-Shub-Smale model [1] no such restrictions are needed. Our results are not sensitive to the exact model of computation.

2. $x_0x_2 = x_1^2$
3. $x_0 = x_2 = 0$
4. $x_0x_2 = -x_1^2$ *and* $x_0^{12} = x_1^{12}$
5. *The input is restricted to planar graphs and* $x_0^3 = x_2^3$

First, if $x_1 = 0$, this holant problem is easily solvable in FP using a connectivity argument. Also, multiplying every term of the signature $[x_0, x_1, x_2]$ by a some nonzero $c \in \mathbb{C}$ has the effect of multiplying Holant_Ω by c^s where s is the number of vertices assigned that signature in the signature grid Ω. Hence if $x_1 \neq 0$ we may normalize the signature and assume $x_1 = 1$ without changing the complexity of the holant problem. This allows us to simplify notation a little, and our aim is now to prove the following.

Theorem 8. *The holant problem* $\#[a, 1, b] \mid [1, 0, 0, 1]$ *is* $\#\mathrm{P}\text{-hard}$ *for all* $a, b \in \mathbb{C}$*, both for unrestricted input and for input restricted to planar graphs, except in the following cases, for which the problem is in* FP*:*

1. $ab = 1$
2. $a = b = 0$
3. $ab = -1$ *and* $a^{12} = 1$
4. *The input is restricted to planar graphs and* $a^3 = b^3$

We also use the notation $\mathrm{Hol}(a, b)$ as a shorthand for $\#[a, 1, b] \mid [1, 0, 0, 1]$.

3.1.1 Finisher gadgets

Some new proof techniques were devised in order to discover the main result of this chapter. We discuss these in the context of some previous results. In Chapter 2 the main technique (from [9]) was to provide certain algebraic criteria which ensure that interpolation succeeds, and then apply these criteria to prove that (a large number yet) finitely many individual problems are $\#\mathrm{P}\text{-hard}$. This involved (a small number of) *binary* recursive gadgets, and the algebraic criteria were powerful enough to show that they succeeded in each case. Nonetheless this approach involves a case-by-case verification and the signatures are restricted to the rational numbers. In [10] this theorem was extended to all real-valued a and b, where there are infinitely many problems to consider. So instead of focusing on one problem, the authors devised (a large number of) *unary* recursive gadgets and analyzed their *failure sets* - regions of $(a, b) \in \mathbb{R}^2$ where they fail to prove $\#\mathrm{P}$-hardness. The algebraic criteria from [9] are Galois theoretic, and are not suitable for general a and b, which is why they formulated weaker but simpler criteria using gadgets of smaller arity:

Lemma 6. *If M is a real 2 by 2 matrix and S is a real 2 by 1 vector, then $\{M^i S\}_{i \geq 0}$ is a series of pairwise linearly independent vectors if all of the following conditions hold.*

1. $\det(M) \neq 0$,
2. $\mathrm{tr}(M) \neq 0$,
3. $(\mathrm{tr}(M))^2 - 4\det(M) > 0$,
4. $\det[MS, S] \neq 0$.

Furthermore, suppose $a, b \in \mathbb{R}$ such that $ab \neq 1$, $a \neq b$, $(a, b) \notin \{(1, -1), (-1, 1), (0, 0)\}$, and there is a unary starter gadget S and a unary recursive gadget M in the context of $\#[a, 1, b] \mid [1, 0, 0, 1]$ for which the conditions above are true. Then $\#[a, 1, b] \mid [1, 0, 0, 1]$ is $\#\mathrm{P}$-hard.

Using these criteria, the analysis of the failure set becomes expressible as containment of semi-algebraic sets. As semi-algebraic sets are decidable, this offered the ultimate possibility that if enough gadgets were collected to prove $\#\mathrm{P}$-hardness in all cases, then there would be a *computational* proof (of computational intractability) in a finite number of steps. However this turned out to be a tremendous undertaking in symbolic computation, and many additional ideas were needed to finally carry out this plan. The complexity of the final symbolic proof courted the limit of what can be accomplished on current hardware. In the absence of any clever new insights, extending this directly to the complex numbers would cause a tremendous increase in computational overhead, so it would seem hopeless to use this approach for all complex a and b. The core difficulty is that the failure set for each gadget is a large region, defined in such a way that proving several of these regions have an empty intersection over the complex numbers is far too daunting, even for a computer.

Going back to [9], the main difficulty in adapting Lemma 4 in Chapter 2 (besides the fact that we are restricted to the rational numbers) is that we need to verify that the characteristic polynomial of the transition matrix for the recursive gadget is irreducible. This amounts to trivial calculations when each entry of the transition matrix is some fixed rational number, but attempting to apply this to $\#[a, 1, b] \mid [1, 0, 0, 1]$ where a and b vary over $\mathbb{Q}$, we run into the problem of finding (and proving the existence of) a large set of points $(a, b) \in \mathbb{Q}^2$ for which some given cubic polynomial, which has rational polynomials in a and b as coefficients, is irreducible. At the same time, fixing a binary recursive gadget and using computer search on a lattice of points $(a, b) \in \mathbb{Q}^2$, most points (a, b) correspond to irreducible polynomials, and it appears as though the failure set of a typical gadget is a union of points and curves; not regions as in the unary gadget construction of [10] (actually, this can be argued analytically as well).

So on one hand, we have a construction which gives rise to very small failure sets, but it isn't clear how to turn this into a general *proof* of $\#\mathrm{P}$-hardness (the binary construction of [9]). On the other hand, we have a construction which is capable of obtaining results over large classes of problems, but the implicit representation of the large failure sets produced causes the symbolic complexity of the proof to become impractical for use over the complex numbers (the unary construction of [10]). In this chapter a hybrid construction is presented that uses a higher dimensional (binary) recursive structure, but then collapses down to lower dimensional (unary) signatures by concatenating one of several possible *binary finisher gadgets*, each having a single leading edge. This means we will be interpolating unary signatures, but the failure sets will be small thanks to the higher dimensional recursive gadget. In essence, this construction retains the best properties of both previous constructions: the failure sets are small and the conditions for interpolation to succeed are simple, thus more suitable for proving general results. The interpolation construction starts with a single binary starter gadget, some number of iterations with a binary recursive gadget, and ends with one application of a binary finisher gadget with a single leading edge. See Figure 3.1.

(a) A starter gadget (b) A recursive gadget (c) A finisher gadget (d) A planar embedding of a single iteration

Figure 3.1 The main construction

3.1.2 Eigenvalue Shifted Pairs

Once the interpolation result with finisher gadgets has been proved, the most significant remaining hurdle is to actually find a set of binary recursive gadgets that works in all cases (and to prove that it works). The main requirement for a binary recursive gadget to succeed in our new construction is that the eigenvalues of the transition matrix do not all have the same norm. Again, this is easy to verify on a case-by-case and gadget-by-gadget basis, but it is less clear how this can be argued for large sets of a and b over the complex numbers. For this, we introduce a second main ingredient called an *Eigenvalue Shifted Pair* (ESP). The idea is that if we can find two binary recursive gadgets whose transition matrices differ by δI, where δ is some nonzero complex number, then we know that the eigenvalues of both matrices differ only by a shift of δ in the complex plane. Such ESPs exist, and the shift in eigenvalues makes it easy to argue that both gadgets fail only in rare cases.

3.1.3 Algebraic symmetrization

In [10], in order to reduce the complexity of the symbolic computation needed to obtain a proof of computational hardness, a coordinate change was made from (a, b) to (x, y), where $a = -\sqrt{x} + y - 1$ and $b = \sqrt{x} + y - 1$. Taking advantage of certain symmetries in the holant, this change mapped certain polynomials in a and b to polynomials in x and y. When combined with other ideas, this reduced the complexity of proving hardness to the point where the remaining symbolic proof could be completed by a computer.

We introduce a similar coordinate change $X = ab$ and $Y = a^3 + b^3$. This results in a significant reduction in the degree of the polynomials involved, but this is not an ad hoc transformation. We give a direct proof that the holant of any signature grid of the form $\#[a, 1, b] \mid [1, 0, 0, 1]$ is an integer polynomial in X and Y (where the precise polynomial depends on the signature grid). This implies that the computational complexity of $\#[a, 1, b] \mid [1, 0, 0, 1]$ is captured entirely in terms of X and Y. Theorem 8 can then be rewritten as the following.

Theorem 9. *The holant problem $\#[a, 1, b] \mid [1, 0, 0, 1]$ is $\#\mathrm{P}\text{-hard}$ for all $a, b \in \mathbb{C}$, both for unrestricted input and for input restricted to planar graphs, except in the following cases, for which the problem is in* FP*:*

1. $X = 1$.
2. $X = Y = 0$.
3. $X = -1$ *and* $Y = 0$.
4. $X = -1$ *and* $Y^2 = -4$.
5. *The input is restricted to planar graphs and* $Y^2 = 4X^3$.

3.1.4 The development of interpolation with finisher gadgets

In this section we give a detailed technical account of how finisher gadgets were first discovered and how the proof techniques evolved. The main purpose of this is to provide additional motivation and insight for the interested reader, and it may be skipped without loss of continuity.

We start by illustrating the proof details of Lemma 2, since this was the starting point for developing the new proof technique. As a preliminary, we will derive one additional lemma that will be needed in the proof. Suppose M is a 2^m by 2^n matrix. Then M can be viewed as a general transition matrix which transforms arity-n signatures written in general signature notation as column vectors into arity-m signatures, also written in general signature notation as column vectors. If M is closed as a linear transformation over symmetric signatures, then M has a symmetric equivalent $\widetilde{M}$, which is an $m + 1$ by $n + 1$ matrix. Given the redundancies present in a symmetric arity-n signature g written in general signature notation, it follows that we can form $\widetilde{M}$ from M in two steps. First, adding together the columns in M that correspond with the repeated entries in g and then arranging the resulting columns in an order that matches symmetric signature notation, we now have a 2^m by $n+1$ matrix $\widehat{M}$ which transforms arity-n signatures in symmetric notation into symmetric arity-m signatures written in general signature notation. Since $\widehat{M}$ is still closed with respect to symmetric signatures as a linear transformation, we may selectively strike out redundant rows of $\widehat{M}$ and arrange the remaining rows in the proper order to get the $m+1$ by $n+1$ matrix $\widetilde{M}$. The following lemma shows that for any nonsingular matrix M and positive integer j, the matrix $M^{\otimes j}$ has a nonsingular symmetric equivalent $\widetilde{M^{\otimes j}}$. Note that a symmetric signature written in general signature notation as a vector x is a special case where $\widehat{x}$ is the same signature in symmetric notation.

Lemma 7. *Let M be an invertible ℓ by ℓ matrix. Then for any positive integer n, $M^{\otimes n}$ has a symmetric equivalent $\widetilde{M^{\otimes n}}$, which is a $\binom{n+\ell-1}{\ell-1}$ by $\binom{n+\ell-1}{\ell-1}$ invertible matrix.*

Proof. Let the rows and columns of $M^{\otimes n}$ be indexed by $t_1 t_2 \cdots t_n \in \{0,1,2,\cdots,\ell-1\}^{\times n}$ (i.e. n digits in base ℓ). Define equivalence relation $\sim$ on $\{0,1,2,\cdots,\ell-1\}^{\times n}$ so that $t_1 t_2 \cdots t_n \sim t'_1 t'_2 \cdots t'_n$ if there exists some permutation σ such that $t_{\sigma(1)} t_{\sigma(2)} \cdots t_{\sigma(n)} = t'_1 t'_2 \cdots t'_n$. Let $\widehat{M^{\otimes n}}$ be the ℓ^n by $\binom{n+\ell-1}{\ell-1}$ matrix where column j is defined to be the sum of all columns in $M^{\otimes n}$ from the j^{th} equivalence class of $\sim$. Since $M^{\otimes n}$ has full rank, so does $\widehat{M^{\otimes n}}$ (any nontrivial linear combination of columns from $\widehat{M^{\otimes n}}$ can also be obtained as a nontrivial linear combination of columns from $M^{\otimes n}$). Suppose $t \sim t'$. Then there is some permutation σ such that for any $c \in \{0,1,2,\cdots,\ell-1\}^{\times n}$ we have

$$\begin{aligned}
(M^{\otimes n})_{t_1 t_2 \cdots t_n, c_1 c_2 \cdots c_n} &= M_{t_1,c_1} M_{t_2,c_2} \cdots M_{t_n,c_n} \\
&= M_{t_{\sigma(1)},c_{\sigma(1)}} M_{t_{\sigma(2)},c_{\sigma(2)}} \cdots M_{t_{\sigma(n)},c_{\sigma(n)}} \\
&= (M^{\otimes n})_{t_{\sigma(1)} t_{\sigma(2)} \cdots t_{\sigma(n)}, c_{\sigma(1)} c_{\sigma(2)} \cdots c_{\sigma(n)}} \\
&= (M^{\otimes n})_{t'_1 t'_2 \cdots t'_n, c_{\sigma(1)} c_{\sigma(2)} \cdots c_{\sigma(n)}}.
\end{aligned}$$

Let a_j denote the j^{th} equivalence class of $\sim$ and note σ induces a permutation on each a_j. Then

$$\begin{aligned}
\widehat{M^{\otimes n}}_{t,j} &= \sum_{c\in a_j}(M^{\otimes n})_{t_1t_2\cdots t_n,c_1c_2\cdots c_n} \\
&= \sum_{c\in a_j}(M^{\otimes n})_{t'_1t'_2\cdots t'_n,c_{\sigma(1)}c_{\sigma(2)}\cdots c_{\sigma(n)}} \\
&= \sum_{c\in a_j}(M^{\otimes n})_{t'_1t'_2\cdots t'_n,c_1c_2\cdots c_n} \\
&= \widehat{M^{\otimes n}}_{t',j}
\end{aligned}$$

thus the rows in $\widehat{M^{\otimes n}}$ indexed by any particular equivalence class of $\sim$ are all equal, and removing repeated rows maintains full rank, giving us a $\binom{n+\ell-1}{\ell-1}$ by $\binom{n+\ell-1}{\ell-1}$ nonsingular matrix. Note that if x and y are symmetric signatures written in general signature notation, then $y = M^{\otimes n}x$ implies $\widetilde{y} = \widetilde{M^{\otimes n}}\widetilde{x}$, so $\widetilde{M^{\otimes n}}$ is in fact the symmetric equivalent of $M^{\otimes n}$. □

The following theorem from [9] is our starting point, and we provide a copy of the proof here for convenience.

Theorem 10. *Suppose a there is a binary recursive gadget M built in the context of $\#\mathcal{G} \mid \mathcal{R}$ such that*

1. $\det(M) \neq 0$,
2. *some signature $[x_0, y_0, z_0] \in \mathcal{G}$ is not orthogonal to any row eigenvector of M,*
3. *for all $(i, j, k) \in \mathbb{Z}^3 - \{(0, 0, 0)\}$ with $i + j + k = 0$, $\alpha^i\beta^j\gamma^k \neq 1$.*

Then for any $x, y, z \in \mathbb{C}$, $\#\mathcal{G} \cup \{[x, y, z]\} \mid \mathcal{R} \leq^{\mathrm{P}}_{\mathrm{T}} \#\mathcal{G} \mid \mathcal{R}$.

Proof. Let $\Omega = (G, \mathcal{G} \cup \mathcal{R}, \pi)$ be a signature grid instance of $\#\mathcal{G} \mid \mathcal{R}$. Suppose $g \in \mathcal{G}$ is a symmetric signature of arity 2, and write $g = [x, y, z]$. Let V_g be the subset of vertices assigned g in Ω, and let $n = |V_g|$. Then we can rewrite Holant_Ω as

$$\mathrm{Holant}_\Omega = \sum_{i+j+k=n} c_{i,j,k}x^iy^jz^k,$$

where $c_{i,j,k}$ is the sum over all edge assignments σ, of products of evaluations at all $v \in V(G) - V_g$, where σ satisfies the property that the number of vertices in V_g having exactly 0, 1, or 2 incident edges assigned 1 is i, j or k, respectively. If we can evaluate these $c_{i,j,k}$, we can evaluate Holant_Ω.

Now suppose $\{f_s\}_{s\geq 0}$ is a sequence of symmetric functions of arity 2, with signatures $[x_s, y_s, z_s]$ for all nonnegative integers s. If we replace each occurence of g by f_s in Ω we get a new signature grid Ω_s with

$$\text{Holant}_\Omega = \sum_{i+j+k=n} c_{i,j,k} x_s^i y_s^j z_s^k, \tag{3.1}$$

Note that the same set of values $c_{i,j,k}$ occur. We can treat $c_{i,j,k}$ in (3.1) as a set of unknowns in a linear system. The idea of interpolation is to find a suitable sequence $\{f_s\}_{s\geq 0}$ such that we can evaluate Holant_{Ω_s}, and then to find all $c_{i,j,k}$ by solving a linear system (3.1). We will set $\{f_s\}_{s\geq 0} = \{M^s S\}_{s\geq 0}$, where S is a single vertex starter gadget labeled with signature $[x_0, y_0, z_0]$. We write $M = T^{-1}\text{diag}(\alpha, \beta, \gamma)T$ where α, β, and γ are the eigenvalues of M and the rows of T are the row eigenvectors of M. Let $(u, v, w)^{\text{T}} = T(x_0, y_0, z_0)^{\text{T}}$ be the inner products of the row eigenvectors with the initial values. Then

$$\begin{bmatrix} x_s \\ y_s \\ z_s \end{bmatrix} = T^{-1} \begin{bmatrix} \alpha^s & 0 & 0 \\ 0 & \beta^s & 0 \\ 0 & 0 & \gamma^s \end{bmatrix} T \begin{bmatrix} x_0 \\ y_0 \\ z_0 \end{bmatrix} = T^{-1} \begin{bmatrix} u & 0 & 0 \\ 0 & v & 0 \\ 0 & 0 & w \end{bmatrix} \begin{bmatrix} \alpha^s \\ \beta^s \\ \gamma^s \end{bmatrix}.$$

Let $B = T^{-1}\text{diag}(u, v, w)$, and B is nonsingular since $uvw \neq 0$. It follows that

$$\begin{bmatrix} x_s \\ y_s \\ z_s \end{bmatrix}^{\otimes n} = B^{\otimes n} \begin{bmatrix} \alpha^s \\ \beta^s \\ \gamma^s \end{bmatrix}^{\otimes n}.$$

By Lemma 7, $\widetilde{B^{\otimes n}}$ is an invertible $\binom{n+2}{2}$ by $\binom{n+2}{2}$ matrix. Now consider the linear system (3.1), for $0 \leq s < \binom{n+2}{2}$. If we consider this as a linear equation system with unknowns $c_{i,j,k}$, it has a coefficient matrix $(\widetilde{B^{\otimes n}}\mathbf{V})^{\text{T}}$, where $\mathbf{V}$ is a Vandermonde matrix. The rows of $\mathbf{V}$ are indexed by $\{(i, j, k) \in \mathbb{Z}^3 : i \geq 0, j \geq 0, k \geq 0, i + j + k = n\}$, the columns are indexed by $0 \leq s < \binom{n+2}{2}$, and the entry of $\mathbf{V}$ at $((i, j, k), s)$ is $(\alpha^i\beta^j\gamma^k)^s$. This Vandermonde matrix is of full rank since all entries $\alpha^i\beta^j\gamma^k$ are distinct, therefore the linear system (3.1) is nonsingular for $0 \leq s < \binom{n+2}{2}$. $\square$

Condition 3 of Theorem 10 can be translated into more concretely testable conditions using the following lemma, also from [9].

Lemma 8. *Let* $f(x) = x^3 + c_2x^2 + c_1x + c_0 \in \mathbb{Q}[x]$ *be a given polynomial with rational coefficients and roots* α*,* β *and* γ*. It is decidable in polynomial time whether any nontrivial solution to* $\alpha^i\beta^j\gamma^j = 1$ *exists, and if so, to find all solutions (in terms of a short basis of the lattice). If* f *is irreducible, except of the form* $x^3 + c$ *for some* $c \in \mathbb{Q}$*, then there are no nontrivial solutions to* $\alpha^i\beta^j\gamma^j = 1$*.*

We would like to prove dichotomy theorems for larger classes of problems, such as $\#[a, 1, b] \mid [1, 0, 0, 1]$, where each $a, b \in \mathbb{C}$. Given a binary recursive gadget M, let $A \subseteq \mathbb{C}^2$ be the set of pairs (a, b) for which Theorem 10 implies that $\#[a, 1, b] \mid [1, 0, 0, 1]$ is $\#\mathrm{P}$-hard. Using Lemma 8, there is a straightforward (automated) process by which membership in A can be decided for individual points $(a, b) \in \mathbb{Q}$. For arbitrary a and b, conditions 1 and 2 of Theorem 10 can be stated as (a, b) not being in the zero set of two polynomials with integer coefficients: the determinant of M and the polynomial given in Lemma 27. These conditions are more apt for making general statements regarding the set A than condition 3 of Theorem 10, which is difficult to deal with, even with the aid of Lemma 8. Therefore, our main aim will be to eliminate this condition or replace it with something more suitable for making more general statements. Ideally, this condition would be another zero-test of an integer polynomial in a and b. Then the problem of proving $\#\mathrm{P}$-hardness simplifies to the zero set of a single polynomial (the product of the three polynomials), where the polynomial depends on which recursive gadget we apply.

The finisher gadget approach is crucially motivated by the lattice condition of Theorem 10. The condition comes from the fact that there are three eigenvalues, which is due to M being a *binary* recursive gadget. A unary recursive gadget would only have two eigenvalues (which is much easier to deal with), but this comes at the cost of failing to prove $\#\mathrm{P}$-hardness over a larger set of points (a, b). This is why we introduce a binary finisher gadget at the end of the construction of [9]. Making the transition to a lower dimension causes this lattice condition to become more manageable. We will start gradually, first seeing how the introduction of a single finisher gadget effects the result.

Lemma 9. *Suppose that the following gadgets can be built using complex-valued signatures from a finite generator set $\mathcal{G}$ and a finite recognizer set $\mathcal{R}$.*

1. *A binary recursive gadget with nonsingular transition matrix M, for which the eigenvalues are all distinct.*
2. *A binary starter gadget with signature $[x_0, y_0, z_0]$ which is not orthogonal to any row eigenvector of M.*
3. *A binary finisher gadget with a rank 2 transition matrix $F \in \mathbb{C}^{2\times 3}$.*

Additionally assume that for all positive integers n, at least $n+1$ of the first $O(\mathrm{poly}(n))$ terms of the series $\{\frac{\widehat{\beta}^s\widehat{\gamma}^{-s}+c}{\widehat{\alpha}^s\widehat{\gamma}^{-s}+d}\}_{s\geq 0}$ are well-defined and distinct, for 3 by 3 permutation matrices P such that $\begin{bmatrix} \widehat{\alpha} \\ \widehat{\beta} \\ \widehat{\gamma} \end{bmatrix} = P \begin{bmatrix} \alpha \\ \beta \\ \gamma \end{bmatrix}$. *Then for any $x, y \in \mathbb{C}$, $\#\mathcal{G} \cup \{[x,y]\} \mid \mathcal{R} \leq_{\mathrm{T}}^{\mathrm{P}} \#\mathcal{G} \mid \mathcal{R}$.*

Proof. The construction begins with a binary starter gadget N_0 with signature $[x_0, y_0, z_0]$. Recursively, $\mathcal{F}$-gate N_i is defined to be N_{i-1} connected to the binary recursive gadget M in such a way that the trailing edges of M are merged with the leading edges of N_{i-1}. Then gadget G_i is defined to be N_i connected to the finisher gadget, such that the trailing edges of the finisher gadget are merged with the leading edges of N_i (see Figure 3.1). Note that the signatures of G_i and N_i are symmetric for all $i \geq 0$, which we denote by $[X_i, Y_i]$ and $[x_i, y_i, z_i]$ respectively. Thus $\{[x_i, y_i, z_i]^{\mathrm{T}}\}_{i\geq 0} = \{M^i N_0\}_{i\geq 0}$ and $\{[X_i, Y_i]^{\mathrm{T}}\}_{i\geq 0} = \{FM^i N_0\}_{i\geq 0}$.

We are given a bipartite signature grid $\Omega = (G, \mathcal{F}, \pi)$ as input, which is an instance of $\#\mathcal{G} \cup \{[x,y]\} \mid \mathcal{R}$ and we are given oracle access to $\#\mathcal{G} \mid \mathcal{R}$. Let $Q \subseteq G$ be the set of vertices labeled with $[x,y]$, and let $n = |Q|$. If we replace every element of Q with a copy of G_s, we get a signature grid Ω_s which is an instance of $\#\mathcal{G} \mid \mathcal{R}$ (note that the correct bipartite signature structure is preserved). Moreover, although $\mathrm{Holant}_{\Omega_s}$ is a sum of exponentially many terms, each nonzero term has the form $c_i X_s^i Y_s^{n-i}$ for some i, and for some $c_i \in \mathbb{C}$ which does not depend on X_s or Y_s. Then $\mathrm{Holant}_{\Omega_s}$ can be rewritten as

$$\mathrm{Holant}_{\Omega_s} = \sum_{0\leq i\leq n} c_i X_s^i Y_s^{n-i}.$$

The important point is that the c_i values do not depend on X_s or Y_s. Since each signature grid Ω_s is an instance of $\#\mathcal{G} \mid \mathcal{R}$, $\operatorname{Holant}_{\Omega_s}$ can be solved exactly using the oracle. Using many different settings of s, we arrive at a linear system where the c_i values are the unknowns. If this linear system has rank $n+1$ then we can solve for all of the c_i. With the c_i values in hand, we can calculate $\operatorname{Holant}_\Omega = \sum_{0 \le i \le n} c_i x^i y^{n-i}$ directly, which completes the reduction. Our only remaining task, then, is to verify that there is a a polynomial-sized linear system with rank $n+1$.

Let α, β, and γ be the eigenvalues of M, and since these are all distinct, we can write $M = T^{-1}\operatorname{diag}(\alpha,\beta,\gamma)T$ where the rows of T are the row eigenvectors of M. Let $[u,v,w]^{\mathrm{T}} = T[x_0,y_0,z_0]^{\mathrm{T}}$ be the inner products of the row eigenvectors with the initial values. Then

$$\begin{bmatrix} x_s \\ y_s \\ z_s \end{bmatrix} = T^{-1} \begin{bmatrix} \alpha^s & 0 & 0 \\ 0 & \beta^s & 0 \\ 0 & 0 & \gamma^s \end{bmatrix} T \begin{bmatrix} x_0 \\ y_0 \\ z_0 \end{bmatrix} = T^{-1} \begin{bmatrix} u & 0 & 0 \\ 0 & v & 0 \\ 0 & 0 & w \end{bmatrix} \begin{bmatrix} \alpha^s \\ \beta^s \\ \gamma^s \end{bmatrix} = B \begin{bmatrix} \alpha^s \\ \beta^s \\ \gamma^s \end{bmatrix}$$

where $B = T^{-1}\operatorname{diag}(u,v,w)$ is nonsingular. Applying a finisher gadget (represented by its 2 by 3 rank 2 transition matrix F), we get

$$\begin{bmatrix} X_s \\ Y_s \end{bmatrix} = F \begin{bmatrix} x_s \\ y_s \\ z_s \end{bmatrix} = FB \begin{bmatrix} \alpha^s \\ \beta^s \\ \gamma^s \end{bmatrix}. \tag{3.2}$$

Then for some 3 by 3 permutation matrix P, 2 by 2 invertible matrix A, and $c, d \in \mathbb{C}$,

$$\begin{bmatrix} X_s \\ Y_s \end{bmatrix} = A(A^{-1}FBP^{-1})P \begin{bmatrix} \alpha^s \\ \beta^s \\ \gamma^s \end{bmatrix} = A \begin{bmatrix} 1 & 0 & d \\ 0 & 1 & c \end{bmatrix} P \begin{bmatrix} \alpha^s \\ \beta^s \\ \gamma^s \end{bmatrix} = A \begin{bmatrix} \widehat{\alpha}^s + d\widehat{\gamma}^s \\ \widehat{\beta}^s + c\widehat{\gamma}^s \end{bmatrix} \tag{3.3}$$

where we let $\begin{bmatrix} \widehat{\alpha} \\ \widehat{\beta} \\ \widehat{\gamma} \end{bmatrix} = P \begin{bmatrix} \alpha \\ \beta \\ \gamma \end{bmatrix}$. Now taking the tensor power, we have

$$\begin{bmatrix} X_s \\ Y_s \end{bmatrix}^{\otimes n} = A^{\otimes n} \begin{bmatrix} \widehat{\alpha}^s + d\widehat{\gamma}^s \\ \widehat{\beta}^s + c\widehat{\gamma}^s \end{bmatrix}^{\otimes n}.$$

By lemma 7, there exists an $n+1$ by $n+1$ invertible matrix $\widetilde{A^{\otimes n}}$ such that

$$\begin{bmatrix} X_s^n Y_s^0 \\ X_s^{n-1} Y_s^1 \\ \vdots \\ X_s^0 Y_s^n \end{bmatrix} = \widetilde{\begin{bmatrix} X_s \\ Y_s \end{bmatrix}^{\otimes n}} = \widetilde{A^{\otimes n}} \widetilde{\begin{bmatrix} \widehat{\alpha}^s + d\widehat{\gamma}^s \\ \widehat{\beta}^s + c\widehat{\gamma}^s \end{bmatrix}^{\otimes n}} = (\widehat{\alpha}^s + d\widehat{\gamma}^s)^n \widetilde{A^{\otimes n}} \begin{bmatrix} (\frac{\widetilde{\beta}^s+c}{\widetilde{\alpha}^s+d})^0 \\ (\frac{\widetilde{\beta}^s+c}{\widetilde{\alpha}^s+d})^1 \\ \vdots \\ (\frac{\widetilde{\beta}^s+c}{\widetilde{\alpha}^s+d})^n \end{bmatrix}$$

where $\widetilde{\beta} = \frac{\widehat{\beta}}{\widehat{\gamma}}$, $\widetilde{\alpha} = \frac{\widehat{\alpha}}{\widehat{\gamma}}$, and for $s \geq 1$ such that $\widetilde{\alpha}_s \neq -d$. Then for any such s,

$$\begin{aligned} \text{Holant}_{\Omega_s} &= \sum_{0 \leq i \leq n} c_i X_s^i Y_s^{n-i} \\ &= [X_s^n Y_s^0 \;\; X_s^{n-1} Y_s^1 \;\; \cdots \;\; X_s^0 Y_s^n] \begin{bmatrix} c_n \\ c_{n-1} \\ \vdots \\ c_0 \end{bmatrix} \\ &= \left[\left(\frac{\widetilde{\beta}^s + c}{\widetilde{\alpha}^s + d} \right)^0 \; \left(\frac{\widetilde{\beta}^s + c}{\widetilde{\alpha}^s + d} \right)^1 \; \cdots \; \left(\frac{\widetilde{\beta}^s + c}{\widetilde{\alpha}^s + d} \right)^n \right] (\widehat{\alpha}^s + d\widehat{\gamma}^s)^n \widetilde{A^{\otimes n}}^{\mathrm{T}} \begin{bmatrix} c_n \\ c_{n-1} \\ \vdots \\ c_0 \end{bmatrix} \end{aligned}$$

It follows that

$$\begin{bmatrix} \text{Holant}_{\Omega_1} \\ \text{Holant}_{\Omega_2} \\ \vdots \\ \text{Holant}_{\Omega_{g(n)}} \end{bmatrix} = \begin{bmatrix} (\widehat{\alpha}^1 + d\widehat{\gamma}^1)^n & & & \\ & (\widehat{\alpha}^2 + d\widehat{\gamma}^2)^n & & \\ & & \ddots & \\ & & & (\widehat{\alpha}^{g(n)} + d\widehat{\gamma}^{g(n)})^n \end{bmatrix} V^{\mathrm{T}} \widetilde{A^{\otimes n}}^{\mathrm{T}} \begin{bmatrix} c_n \\ c_{n-1} \\ \vdots \\ c_0 \end{bmatrix}$$

where V is the Vandermonde matrix where the entry at index (i, s) is $(\frac{\widetilde{\beta}^s+c}{\widetilde{\alpha}^s+d})^{i-1}$, and $g(n) = O(\text{poly}(n))$. Since at least $n+1$ of the first $O(\text{poly}(n))$ terms of the series $\frac{\widetilde{\beta}^s+c}{\widetilde{\alpha}^s+d}$ are well-defined and distinct, then the $n+1$ corresponding columns of V are linearly independent, and the respective entries of the diagonal matrix are nonzero (since $\widetilde{\alpha}^s + d \neq 0$), thus we can solve the linear system.

□

Now we need to contend with proving that enough terms of the series $\{\frac{\widehat{\beta}^s\widehat{\gamma}^{-s}+c}{\widehat{\alpha}^s\widehat{\gamma}^{-s}+d}\}_{s\geq 0}$ are well-defined and distinct. This work would be simplified if we could choose the permutation matrix P such that $\begin{bmatrix} \widehat{\alpha} \\ \widehat{\beta} \\ \widehat{\gamma} \end{bmatrix} = P \begin{bmatrix} \alpha \\ \beta \\ \gamma \end{bmatrix}$ instead of working with arbitrary P. Examining the above proof more carefully, this comes down to the product FB in equation (3.2). It would suffice to guarantee that any 2 by 2 submatrix of FB is nonsingular. However, this simply is not true for a single finisher gadget F in general. Therefore, we will use a set of finisher gadgets instead. The essential property is that given any 2 by 2 matrix W (i.e. a submatrix of B), there is a finisher gadget F in this set for which FW is nonsingular. Then any two columns of FB can be choosen to be a nonsingular submatrix, and the row operations performed by A in equation 3.3 can be choosen in such a way to convert this submatrix into either of the two possible 2 by 2 permutation matrices. The choice of three possible submatrices and two possible 2 by 2 permutation matrices gives a total of 6 six possibilities, each of which corresponds with a different permutation matrix P. Three finisher gadgets will suffice to prove the crucial property, and we give a way to test for this in terms of an algebraic property that occurs between the three finisher gadgets.

Lemma 10. *Let $F, F', F'' \in \mathbb{C}^{2\times 3}$ and $N \in \mathbb{C}^{3\times 2}$ all be rank 2 matrices, and suppose that the intersection of the row spaces of F, F', and F'' is the zero vector. Then UN is nonsingular for some $U \in \{F, F', F''\}$.*

Proof. Note that $\ker(N^{\mathrm{T}})$ is a 1-dimensional linear subspace of $\mathbb{C}^3$, so by assumption let $U \in \{F, F', F''\}$ such that the column space of U^{T} intersected with $\ker(N^{\mathrm{T}})$ is $\{0\}$. Then $U^{\mathrm{T}} \begin{bmatrix} m \\ n \end{bmatrix} \in \ker(N^{\mathrm{T}})$ if and only if $m = n = 0$. In other words, $\ker(N^{\mathrm{T}}U^{\mathrm{T}}) = \{0\}$, so UN is an invertible 2 by 2 matrix. □

Now we move on to proving that the series $\{\frac{\widehat{\beta}^s\widehat{\gamma}^{-s}+c}{\widehat{\alpha}^s\widehat{\gamma}^{-s}+d}\}_{s\geq 0}$ has enough terms that are well-defined and distinct. Even with the ability to choose the permutation matrix P, this still requires a bit of technical work. We divide up the work into several lemmas.

Lemma 11. *If n is a positive integer and γ is a nonzero complex number, then there exists an integer k such that $1 \le k \le n$ and $|\mathrm{Arg}(\gamma^k)| < 2\pi/n$.*

Proof. Let σ be a permutation on the set $\{0, 1, \cdots, n\}$ such that $-\pi < \mathrm{Arg}(\gamma^{\sigma(0)}) \le \mathrm{Arg}(\gamma^{\sigma(1)}) \le \cdots \le \mathrm{Arg}(\gamma^{\sigma(n)}) \le \pi$. Since $0 \le \mathrm{Arg}(\gamma^{\sigma(n)}) - \mathrm{Arg}(\gamma^{\sigma(0)}) < 2\pi$, there must exist i with $0 \le i < n$ such that $0 \le \mathrm{Arg}(\gamma^{\sigma(i+1)}) - \mathrm{Arg}(\gamma^{\sigma(i)}) < 2\pi/n$ and moreover $0 \le \mathrm{Arg}(\gamma^{\sigma(i+1)-\sigma(i)}) < 2\pi/n$, so let $k = |\sigma(i+1) - \sigma(i)|$ so that $|\mathrm{Arg}(\gamma^k)| = |\mathrm{Arg}(\gamma^{\sigma(i+1)-\sigma(i)})| < 2\pi/n$ and $1 \le k \le n$. □

Lemma 12. *Let α and β be nonzero complex numbers where α and β are not roots of unity and $|\alpha| \ne |\beta|$. Assume that either $|\alpha|, |\beta| \ge 1$ or $|\alpha|, |\beta| \le 1$, and let f_s denote $\frac{\beta^s-1}{\alpha^s-1}$. Then there exists a constant q such that for any positive integer n there exists a positive integer $\ell \le qn$ such that all terms of the series $\{f_{\ell s}\}_{1\le s\le n}$ are distinct.*

Proof. First note that all terms of the series $\{f_s\}_{s\ge1}$ are well-defined and nonzero since α and β are not roots of unity. Assume without loss of generality that either $|\beta| > |\alpha| \ge 1$ or $|\beta| < |\alpha| \le 1$. If $|\alpha| > 1$, then let $h = |\frac{\beta}{\alpha}| > 1$ and since $\lim_{s\to\infty} |\frac{1-\beta^{-s}}{1-\alpha^{-s}}| = 1$ we can choose $\ell \ge 1$ such that for all $s \ge \ell$, $h^{-1/2} < |\frac{1-\beta^{-s}}{1-\alpha^{-s}}| < h^{1/2}$. Then for any $s \ge \ell$, $|\frac{\beta^s-1}{\alpha^s-1}| = |\frac{\beta^s}{\alpha^s}| \cdot |\frac{1-\beta^{-s}}{1-\alpha^{-s}}| = h^s|\frac{1-\beta^{-s}}{1-\alpha^{-s}}| < h^{s+1/2} < h^{s+1}|\frac{1-\beta^{-(s+1)}}{1-\alpha^{-(s+1)}}| = |\frac{\beta^{s+1}}{\alpha^{s+1}}| \cdot |\frac{1-\beta^{-(s+1)}}{1-\alpha^{-(s+1)}}| = |\frac{\beta^{s+1}-1}{\alpha^{s+1}-1}|$, hence all terms of the series $\{f_s\}_{s\ge\ell}$ are distinct, and in particular, so are all terms of the series $\{f_{\ell s}\}_{1\le s\le n}$.

Now suppose $|\alpha| = 1$ and $|\beta| > 1$. Let $p = \lceil \log_{|\beta|} 5 \rceil$, and by applying Lemma 11 to α^p, we let integer m such that $1 \le m \le 2n$ and $|\mathrm{Arg}(\alpha^{pm})| < \pi/n$, and note $|\beta|^{pm} \ge 5$. Let $\widehat{\beta} = \beta^{pm}$ and $\widehat{\alpha} = \alpha^{pm}$. Then for any $s \ge 1$, $|\widehat{\beta}^{1+s} - 1| \ge |\widehat{\beta}^{1+s}| - 1 \ge 5|\widehat{\beta}^s| - 1 > 2|\widehat{\beta}^s| + 2 \ge 2|\widehat{\beta}^s - 1|$. Also $|\widehat{\alpha}^s - 1| = \sqrt{\sin^2(s\theta) + (\cos(s\theta) - 1)^2} = \sqrt{\sin^2(s\theta) + \cos^2(s\theta) + 1 - 2\cos(s\theta)} = \sqrt{2 - 2\cos(s\theta)} = |\sin(s\theta/2)|$ where $\theta = \mathrm{Arg}(\widehat{\alpha})$, so for $1 \le s \le n$, $|s\theta/2| < \pi/2$ and $|\widehat{\alpha}^s - 1| = |\sin(s\theta/2)| \ge |\sin(\theta/2)| = |\widehat{\alpha} - 1|$. Then, for any such s, we have $|\widehat{\alpha}^{s+1} - 1| = |\widehat{\alpha}^s - \widehat{\alpha}^{-1}| = |\widehat{\alpha}^s - 1 + 1 - \widehat{\alpha}^{-1}| \le |\widehat{\alpha}^s - 1| + |1 - \widehat{\alpha}^{-1}| = |\widehat{\alpha}^s - 1| + |\widehat{\alpha} - 1| \le 2|\widehat{\alpha}^s - 1|$ so $|\frac{\widehat{\beta}^{s+1}-1}{\widehat{\alpha}^{s+1}-1}| > |\frac{\widehat{\beta}^s-1}{\widehat{\alpha}^s-1}|$. Therefore, all terms of the series $\{f_{\ell s}\}_{1\le s\le n}$ are distinct, where $\ell = pm$.

Suppose now that $|\beta| < |\alpha| \le 1$. We have already established that for any n, there exists a bounded integer ℓ such that all terms of the series $\{\frac{(\beta^{-1})^{\ell s}-1}{(\alpha^{-1})^{\ell s}-1}\}_{1\le s\le n}$ are distinct. In other words, if i and j are integers with $1 \le i < j \le n$, we know $\frac{\beta^{-j\ell}-1}{\alpha^{-j\ell}-1} \ne \frac{\beta^{-i\ell}-1}{\alpha^{-i\ell}-1}$ but then $\frac{\beta^{-j\ell}-1}{\alpha^{-j\ell}-1} \ne$

$\frac{\beta^{-j\ell}-\beta^{-i\ell}}{\alpha^{-j\ell}-\alpha^{-i\ell}}$ hence multiplying by $\frac{\beta^{j\ell}}{\alpha^{j\ell}}$, $\frac{\beta^{j\ell}-1}{\alpha^{j\ell}-1} \neq \frac{\beta^{(j-i)\ell}-1}{\alpha^{(j-i)\ell}-1}$, and we conclude that all terms of the series $\{\frac{\beta^{\ell s}-1}{\alpha^{\ell s}-1}\}_{1\leq s\leq n}$ are distinct. □

Lemma 13. *Let $\alpha, \beta \in \mathbb{C}$ where α, β, and α/β are not roots of unity, and $|\beta| = |\alpha| = 1$. Let f_s denote $\frac{\beta^s-1}{\alpha^s-1}$. Then all terms of the series $\{f_{ms}\}_{1\leq s\leq n}$ are distinct, for some integer m with $1 \leq m \leq 8n^3$.*

Proof. Note that f_s is nonzero and well-defined for all $s \geq 1$. By Lemma 11, let k such that $1 \leq k \leq 4n^2$ and $|\mathrm{Arg}(\alpha^k)| < \pi/(2n^2)$. Apply Lemma 11 a second time, so that we have h with $1 \leq h \leq 2n$ and $|\mathrm{Arg}((\beta^k)^h)| < \pi/n$, and then $|\mathrm{Arg}(\alpha^{kh})| < \pi/n$. Let $m = kh$, $\widehat{\beta} = \beta^m$, and $\widehat{\alpha} = \alpha^m$, and note that $\widehat{\alpha} \neq \widehat{\beta}$ since α/β is not a root of unity. Then since $\arg(\gamma - 1) = (\arg(\gamma) + \pi)/2$ for any $\gamma \in \mathbb{C}$ with $|\gamma| = 1$ and $\gamma \neq 1$, it follows that $\arg(\frac{\widehat{\alpha}^s-1}{\widehat{\beta}^s-1}) = \arg(\widehat{\alpha}^s - 1) - \arg(\widehat{\beta}^s - 1) = (\arg(\widehat{\alpha}^s) + \pi)/2 - (\arg(\widehat{\beta}^s) + \pi)/2 = s\arg(\widehat{\alpha}) - s\arg(\widehat{\beta}) = s(\arg(\widehat{\alpha}) - \arg(\widehat{\beta}))$. Since $0 < |\mathrm{Arg}(\widehat{\alpha}) - \mathrm{Arg}(\widehat{\beta})| < 2\pi/n$, we have for any $1 \leq s < t \leq n$ that $\arg(\frac{\widehat{\alpha}^s-1}{\widehat{\beta}^s-1}) = s(\arg(\widehat{\alpha}) - \arg(\widehat{\beta})) \neq t(\arg(\widehat{\alpha}) - \arg(\widehat{\beta})) = \arg(\frac{\widehat{\alpha}^t-1}{\widehat{\beta}^t-1})$. □

Lemma 14. *Let $\alpha, \beta, c, d \in \mathbb{C}$ where α and β nonzero and are not roots of unity, and either $|\beta|, |\alpha| \geq 1$ or $|\beta|, |\alpha| \leq 1$. Then at least n of the first $O(n^3)$ terms of the series $f_s = \{\frac{\beta^s+c}{\alpha^s+d}\}_{s\geq 0}$ are well-defined, nonzero, and distinct (where the asymptotic constant depends on α, β, c, and d).*

Proof. Note that since α and β are not roots of unity, there is at most one setting of s for which $\beta^s = -c$ and similarly for $\alpha^s = -d$, so by lemma 12, let $m = O(n^2)$ such that all terms of the series $\{\frac{\beta^{ms}-1}{\alpha^{ms}-1}\}_{1\leq s\leq n^2}$ are distinct, and both $\beta^{ms} + c \neq 0$ and $\alpha^{ms} + d \neq 0$ for all $s \geq 1$. Let $\widehat{\beta} = \beta^m$, $\widehat{\alpha} = \alpha^m$, and $\widehat{f_s} = \frac{\beta^{ms}+c}{\alpha^{ms}+d}$. Now that $\widehat{f_s}$ is well-defined and nonzero for all $s \geq 1$, we will choose a set $S \subseteq \{1, 2, \cdots, n^2\}$ with $|S| = n$ such that for all distinct $s, t \in S$, $\widehat{f_s} \neq \widehat{f_t}$. We start out with $S = \{1\}$. Now suppose $|S| = k < n$ and we will show how to adjoin a new element to S while maintaining $S \subseteq \{1, 2, \cdots, (k+1)^2\}$ and $\widehat{f_s} \neq \widehat{f_t}$ for all distinct $s, t \in S$. Suppose $i \in S$ and if for some $j > i$ we have $\frac{\widehat{\beta}^i+c}{\widehat{\alpha}^i+d} = \frac{\widehat{\beta}^j+c}{\widehat{\alpha}^j+d}$, then this can be written as $\frac{\widehat{\beta}^j-\widehat{\beta}^i}{\widehat{\alpha}^j-\widehat{\alpha}^i} = \frac{\widehat{\beta}^j+c}{\widehat{\alpha}^j+d}$ or equivalently $\frac{\widehat{\beta}^{j-i}-1}{\widehat{\alpha}^{j-i}-1} = \frac{\widehat{\alpha}^i(\widehat{\beta}^i+c)}{\widehat{\beta}^i(\widehat{\alpha}^i+d)}$. The right hand side depends only on i, and since every term $\frac{\widehat{\beta}^{j-i}-1}{\widehat{\alpha}^{j-i}-1}$ is distinct for different settings of $j - i$ with $1 \leq j - i \leq n^2$, $\widehat{f_i}$ excludes at most one term j in the range $[i + 1, n + i]$. That is, there is at most one j with $i + 1 \leq j \leq n^2 + i$ such that $\widehat{f_j} = \widehat{f_i}$, and furthermore at most k different settings of j for which $k^2 < j \leq (k+1)^2$ and $\widehat{f_j} = \widehat{f_r}$ for some $r \in S$ (using $k+1 \leq n$). Since $(k+1)^2 - k^2 > k$, there is at least one j such that $k^2 < j \leq (k+1)^2$ and $\widehat{f_j} \neq \widehat{f_i}$ for all $i \in S$. We conclude that we can construct our set S, so at least n of the first n^2 terms of the series $\widehat{f_s}$ are distinct, and at least n of the first $O(n^3)$ terms of the series f_s are distinct. □

There is still a condition in Lemma 9 that requires the eigenvalues are all distinct. By analyzing the Jordan Normal Form of the recurrence matirx more carefully, we can refine this requirement.

Lemma 15. *Suppose A is a 3 by 3 invertible complex matrix and let $[x, y, z]^{\mathrm{T}}$ be a complex vector. If A is diagonalizable, then there exists a matrix B such that $A^s[x, y, z]^{\mathrm{T}} = B[\alpha^s, \beta^s, \gamma^s]^{\mathrm{T}}$, where α, β, and γ are the eigenvalues of A. If the Jordan normal form of A has two Jordan blocks, then there exists a matrix B such that $A^s[x, y, z]^{\mathrm{T}} = B[\alpha^s, \beta^s, s\beta^{s-1}]^{\mathrm{T}}$, where α and β are the eigenvalues of A. In either case, B is singular if and only if $[x, y, z]$ is orthogonal to some row eigenvector of A.*

Proof. Let $A = T^{-1}DT$ be the Jordan normal form for A, and let u, v, w such that $[u, v, w]^{\mathrm{T}} = T[x, y, z]^{\mathrm{T}}$. If D is diagonal then T denotes the row eigenvectors of A organized as a 3 by 3 matrix, and we let $B = T^{-1}\mathrm{diag}(u, v, w)$, where

$$A^s \begin{bmatrix} x \\ y \\ z \end{bmatrix} = T^{-1} \begin{bmatrix} \alpha^s & 0 & 0 \\ 0 & \beta^s & 0 \\ 0 & 0 & \gamma^s \end{bmatrix} T \begin{bmatrix} x \\ y \\ z \end{bmatrix} = T^{-1} \begin{bmatrix} u\alpha^s \\ v\beta^s \\ w\gamma^s \end{bmatrix} = T^{-1} \begin{bmatrix} u & 0 & 0 \\ 0 & v & 0 \\ 0 & 0 & w \end{bmatrix} \begin{bmatrix} \alpha^s \\ \beta^s \\ \gamma^s \end{bmatrix} = B \begin{bmatrix} \alpha^s \\ \beta^s \\ \gamma^s \end{bmatrix}.$$

Since T is nonsingular we know B is singular if and only if $uvw = 0$, which is true precisely if there is a row eigenvector of A which is orthogonal to $[x, y, z]$.

If the Jordan normal form of A has two Jordan blocks, then we get the following, where $B = T^{-1}\begin{bmatrix} u & 0 & 0 \\ 0 & v & 0 \\ 0 & w & v \end{bmatrix}$.

$$A^s \begin{bmatrix} x \\ y \\ z \end{bmatrix} = T^{-1}\begin{bmatrix} \alpha^s & 0 & 0 \\ 0 & \beta^s & 0 \\ 0 & s\beta^{s-1} & \beta^s \end{bmatrix} T \begin{bmatrix} x \\ y \\ z \end{bmatrix} = T^{-1}\begin{bmatrix} \alpha^s & 0 & 0 \\ 0 & \beta^s & 0 \\ 0 & s\beta^{s-1} & \beta^s \end{bmatrix}\begin{bmatrix} u \\ v \\ w \end{bmatrix}$$

$$= T^{-1}\begin{bmatrix} u\alpha^s \\ v\beta^s \\ w\beta^s + vs\beta^{s-1} \end{bmatrix} = T^{-1}\begin{bmatrix} u & 0 & 0 \\ 0 & v & 0 \\ 0 & w & v \end{bmatrix}\begin{bmatrix} \alpha^s \\ \beta^s \\ s\beta^{s-1} \end{bmatrix} = B\begin{bmatrix} \alpha^s \\ \beta^s \\ s\beta^{s-1} \end{bmatrix}$$

Note B is singular if and only if $uv = 0$, or equivalently $[x, y, z]$ is orthogonal to a row eigenvector of A (the first two rows of T are row eigenvectors, and the last row is a generalized eigenvector).

□

We will also need a corresponding result for Lemma 15 with the series $\frac{\alpha^s+d\beta^s}{s\beta^{s-1}+c\beta^s}$. We assume $\alpha \neq 0$ and $\beta \neq 0$. Then we want to show that there are n polynomially bounded settings of s such that $\frac{\alpha^s+d\beta^s}{s\beta^{s-1}+c\beta^s}$ is distinct (we will use a choice of finisher gadget to get this particular form), which for convenience we rewrite as $\frac{\theta^s+d}{s/\beta+c}$.

Lemma 16. *Suppose $\alpha, \beta, c, d \in \mathbb{C}$ where α and β are nonzero, and $|\beta| \neq |\alpha|$. Then there is a positive integer m such that all terms of the series $\{f_{ms}\}_{s\geq 1}$ are nonzero and distinct, where $f_s = \frac{\alpha^s+d\beta^s}{s\beta^{s-1}+c\beta^s}$.*

Proof. Let $\theta = \alpha/\beta$ and we will argue in terms of $\frac{\theta^s+d}{s/\beta+c}$. If $|\theta| > 1$, then let $m \in \mathbb{Z}^+$ such that $|\theta^m| \geq 8$ and $1/2 < |\frac{1+d\theta^{-s}}{1+c\beta/s}| < 2$ for all $s \geq m$. Then for $s \geq 1$, $|\frac{\theta^{ms}+d}{ms/\beta+c}| = |\frac{\theta^{ms}\beta}{ms}| \cdot |\frac{1+d\theta^{-ms}}{1+c\beta/(ms)}| < 2|\frac{\theta^{ms}\beta}{ms}| \leq 4|\frac{\theta^{ms}\beta}{ms+m}| < 8|\frac{\theta^{ms}\beta}{ms+m}| \cdot |\frac{1+d\theta^{-(ms+m)}}{1+c\beta/(ms+m)}| \leq |\frac{\theta^{ms+m}\beta}{ms+m}| \cdot |\frac{1+d\theta^{-(ms+m)}}{1+c\beta/(ms+m)}| = |\frac{\theta^{ms+m}+d}{(ms+m)/\beta+c}|$. We conclude that all terms of the series $\{f_{ms}\}_{s\geq 1}$ are distinct.

Now suppose $|\theta| < 1$. If $d = 0$ then let m such that $m \geq 2|\beta c|$ and then for all $s \in \mathbb{Z}^+$ we have $|ms/\beta + c| \leq ms|1/\beta| + |c| \leq ms|1/\beta| + m|1/\beta| - |c| = m(s+1)|1/\beta| - |c| \leq |m(s+1)/\beta + c|$

hence $|\frac{\theta^{ms}}{ms/\beta+c}| > |\frac{\theta^{m(s+1)}}{m(s+1)/\beta+c}|$. Otherwise, let $m \in \mathbb{Z}^+$ such that $|\theta^m| \leq \min(1,|d|)/6$ and $m \geq 3|\beta c|$. Then for any $s,t \in \mathbb{Z}^+$, $|\theta^{mt}+d| \leq |d|+|\theta^{mt}| \leq |d|+6^{-t}|d| = |d|(1+6^{-t})$ and also $|\theta^{ms}+d| \geq |d|-|\theta^{ms}| \geq |d|-6^{-s}|d| = |d|(1-6^{-s})$, so $|\frac{\theta^{mt}+d}{\theta^{ms}+d}| \leq \frac{1+6^{-t}}{1-6^{-s}}$. Then for $s \geq 1$, $|\frac{\theta^{m(s+1)}+d}{\theta^{ms}+d}| \leq \frac{1+6^{-(s+1)}}{1-6^{-s}} = \frac{6^s+6^{-1}}{6^s-1} < \frac{s+1-1/3}{s+1/3} \leq \frac{s+1-|\beta c/m|}{s+|\beta c/m|} = \frac{|m(s+1)/\beta|-|c|}{|ms/\beta|+|c|} \leq |\frac{m(s+1)/\beta+c}{ms/\beta+c}|$, where $\frac{6^s+6^{-1}}{6^s-1} < \frac{s+1-1/3}{s+1/3}$ holds if and only if $(6^s+1/6)(s+1/3) < (6^s-1)(s+2/3)$, or equivalently $\frac{1}{18}+\frac{2}{3} < \frac{6^s}{3}-\frac{7s}{6}$, i.e. $13 < 6^{s+1}-21s$, which holds for $s \geq 1$. Now, $|\frac{\theta^{m(s+1)}+d}{m(s+1)/\beta+c}| < |\frac{\theta^{ms}+d}{ms/\beta+c}|$, and we conclude that all terms of the series $\{f_{ms}\}_{s\geq 1}$ are distinct. □

Now we are finally ready to give our new version of interpolation.

Lemma 17. *Suppose that the following gadgets can be built using complex-valued signatures from a finite generator set $\mathcal{G}$ and a finite recognizer set $\mathcal{R}$.*

1. *A binary recursive gadget with nonsingular transition matrix M, for which some eigenvalues α and β have the property that $\frac{\alpha}{\beta}$ is not a root of unity.*
2. *A binary starter gadget with signature $[x_0, y_0, z_0]$ which is not orthogonal to any row eigenvector of M.*
3. *Three binary finisher gadgets with rank 2 matrices $F_1, F_2, F_3 \in \mathbb{C}^{2\times 3}$, where the intersection of the row spaces of F_1, F_2, and F_3 is trivial.*

Then for any $x, y \in \mathbb{C}$, $\#\mathcal{G} \cup \{[x,y]\} \mid \mathcal{R} \leq_{\mathrm{T}}^{\mathrm{P}} \#\mathcal{G} \mid \mathcal{R}$.

Proof. The construction begins with a binary starter gadget N_0 with signature $[x_0, y_0, z_0]$. Recursively, $\mathcal{F}$-gate N_i is defined to be N_{i-1} connected to the binary recursive gadget M in such a way that the trailing edges of M are merged with the leading edges of N_{i-1}. Then gadget G_i is defined to be N_i connected to one of the finisher gadgets, such that the trailing edges of the finisher gadget are merged with the leading edges of N_i (see Figure 3.1). The precise choice of finisher gadget will depend only on the matrix M. Note that the signatures of G_i and N_i are symmetric for all $i \geq 0$, which we denote by $[X_i, Y_i]$ and $[x_i, y_i, z_i]$ respectively. Thus $\{[x_i, y_i, z_i]^{\mathrm{T}}\}_{i\geq 0} = \{M^i N_0\}_{i\geq 0}$ and $\{[X_i, Y_i]^{\mathrm{T}}\}_{i\geq 0} = \{F_j M^i N_0\}_{i\geq 0}$ for some integer j where $1 \leq j \leq 3$.

We are given a bipartite signature grid $\Omega = (G, \mathcal{F}, \pi)$ as input, which is an instance of $\#\mathcal{G} \cup \{[x, y]\} \mid \mathcal{R}$ and we are given oracle access to $\#\mathcal{G} \mid \mathcal{R}$. Let $Q \subseteq G$ be the set of vertices labeled with $[x, y]$, and let $n = |Q|$. If we replace every element of Q with a copy of G_s, we get a signature grid Ω_s which is an instance of $\#\mathcal{G} \mid \mathcal{R}$ (note that the correct bipartite signature structure is preserved). Moreover, although $\mathrm{Holant}_{\Omega_s}$ is a sum of exponentially many terms, each nonzero term has the form $c_i X_s^i Y_s^{n-i}$ for some i, and for some $c_i \in \mathbb{C}$ which does not depend on X_s or Y_s. Then $\mathrm{Holant}_{\Omega_s}$ can be rewritten as

$$\mathrm{Holant}_{\Omega_s} = \sum_{0 \leq i \leq n} c_i X_s^i Y_s^{n-i}.$$

The important point is that the c_i values do not depend on X_s or Y_s. Since each signature grid Ω_s is an instance of $\#\mathcal{G} \mid \mathcal{R}$, $\mathrm{Holant}_{\Omega_s}$ can be solved exactly using the oracle. Using many different settings of s, we arrive at a linear system where the c_i values are the unknowns. If this linear system has rank $n + 1$ then we can solve for all of the c_i. With the c_i values in hand, we can calculate $\mathrm{Holant}_{\Omega} = \sum_{0 \leq i \leq n} c_i x^i y^{n-i}$ directly, which completes the reduction. Our only remaining task, then, is to verify that there is a a polynomial-sized linear system with rank $n + 1$.

Let α, β, and γ be the eigenvalues of M, and since at least two of these are distinct, Lemma 15 applies and we can write the following for some nonsingular 3 by 3 matrix B (where $\delta_s = \gamma^s$ or $\delta_s = s\beta^{s-1}$, depending on whether the Jordan normal form of M has one or two Jordan blocks),

$$\begin{bmatrix} x_s \\ y_s \\ z_s \end{bmatrix} = M^s \begin{bmatrix} x_0 \\ y_0 \\ z_0 \end{bmatrix} = B \begin{bmatrix} \alpha^s \\ \beta^s \\ \delta_s \end{bmatrix}.$$

Applying a finisher gadget (represented by its 2 by 3 rank 2 transition matrix F_j), we get

$$\begin{bmatrix} X_s \\ Y_s \end{bmatrix} = F_j B \begin{bmatrix} \alpha^s \\ \beta^s \\ \delta_s \end{bmatrix}.$$

If $\delta_s = \gamma^s$, let $\begin{bmatrix} \widehat{\alpha}_s \\ \widehat{\beta}_s \\ \widehat{\gamma}_s \end{bmatrix} = P \begin{bmatrix} \alpha^s \\ \beta^s \\ \delta_s \end{bmatrix}$ where P is a permutation matrix choosen such that $|\widehat{\beta}_s| > |\widehat{\alpha}_s| \geq |\widehat{\gamma}_s|$ or $|\widehat{\beta}_s| < |\widehat{\alpha}_s| \leq |\widehat{\gamma}_s|$ for $s \geq 1$. If $\delta_s = s\beta^{s-1}$, then choose P such that $\widehat{\alpha}_s = \alpha^s$, $\widehat{\gamma}_s = \beta^s$, and $\widehat{\beta}_s = s\beta^{s-1}$. By applying Lemma 10 to any 3 by 2 submatrix of B we can choose any 2 columns of the product F_jB to be linearly independent (by choice of finisher gadget). Then choose $1 \leq j \leq 3$, so that for some invertible matrix A and $c, d \in \mathbb{C}$,

$$\begin{bmatrix} X_s \\ Y_s \end{bmatrix} = A(A^{-1}UBP^{-1})P \begin{bmatrix} \alpha^s \\ \beta^s \\ \delta_s \end{bmatrix} = A \begin{bmatrix} 1 & 0 & d \\ 0 & 1 & c \end{bmatrix} P \begin{bmatrix} \alpha^s \\ \beta^s \\ \delta_s \end{bmatrix} = A \begin{bmatrix} \widehat{\alpha}_s + d\widehat{\gamma}_s \\ \widehat{\beta}_s + c\widehat{\gamma}_s \end{bmatrix}.$$

Now taking the tensor power, we have

$$\begin{bmatrix} X_s \\ Y_s \end{bmatrix}^{\otimes n} = A^{\otimes n} \begin{bmatrix} \widehat{\alpha}_s + d\widehat{\gamma}_s \\ \widehat{\beta}_s + c\widehat{\gamma}_s \end{bmatrix}^{\otimes n}.$$

By lemma 7, there exists an $n+1$ by $n+1$ invertible matrix $\widetilde{A^{\otimes n}}$ such that

$$\begin{bmatrix} X_s^n Y_s^0 \\ X_s^{n-1} Y_s^1 \\ \vdots \\ X_s^0 Y_s^n \end{bmatrix} = \widetilde{\begin{bmatrix} X_s \\ Y_s \end{bmatrix}^{\otimes n}} = \widetilde{A^{\otimes n}} \widetilde{\begin{bmatrix} \widehat{\alpha}_s + d\widehat{\gamma}_s \\ \widehat{\beta}_s + c\widehat{\gamma}_s \end{bmatrix}^{\otimes n}} = (\widehat{\alpha}_s + d\widehat{\gamma}_s)^n \widetilde{A^{\otimes n}} \begin{bmatrix} (\frac{\widetilde{\beta}_s + c}{\widetilde{\alpha}_s + d})^0 \\ (\frac{\widetilde{\beta}_s + c}{\widetilde{\alpha}_s + d})^1 \\ \vdots \\ (\frac{\widetilde{\beta}_s + c}{\widetilde{\alpha}_s + d})^n \end{bmatrix}$$

where $\widetilde{\beta}_s = \frac{\widehat{\beta}_s}{\widehat{\gamma}_s}$, $\widetilde{\alpha}_s = \frac{\widehat{\alpha}_s}{\widehat{\gamma}_s}$, and for $s \geq 1$ is such that $\widetilde{\alpha}_s \neq -d$. Then for any such s,

$$\begin{aligned}
\mathrm{Holant}_{\Omega_s} &= \sum_{0 \leq i \leq n} c_i X_s^i Y_s^{n-i} \\
&= [X_s^n Y_s^0 \;\; X_s^{n-1} Y_s^1 \;\; \cdots \;\; X_s^0 Y_s^n] \begin{bmatrix} c_n \\ c_{n-1} \\ \vdots \\ c_0 \end{bmatrix} \\
&= \left[\left(\frac{\widetilde{\beta}_s + c}{\widetilde{\alpha}_s + d} \right)^0 \; \left(\frac{\widetilde{\beta}_s + c}{\widetilde{\alpha}_s + d} \right)^1 \; \cdots \; \left(\frac{\widetilde{\beta}_s + c}{\widetilde{\alpha}_s + d} \right)^n \right] (\widehat{\alpha}_s + d\widehat{\gamma}_s)^n \widetilde{A^{\otimes n}}^{\mathrm{T}} \begin{bmatrix} c_n \\ c_{n-1} \\ \vdots \\ c_0 \end{bmatrix}
\end{aligned}$$

It follows that

$$\begin{bmatrix} \mathrm{Holant}_{\Omega_1} \\ \mathrm{Holant}_{\Omega_2} \\ \vdots \\ \mathrm{Holant}_{\Omega_{g(n)}} \end{bmatrix} = \begin{bmatrix} (\widehat{\alpha}_1 + d\widehat{\gamma}_1)^n & & & \\ & (\widehat{\alpha}_2 + d\widehat{\gamma}_2)^n & & \\ & & \ddots & \\ & & & (\widehat{\alpha}_{g(n)} + d\widehat{\gamma}_{g(n)})^n \end{bmatrix} V^{\mathrm{T}} \widetilde{A^{\otimes n}}^{\mathrm{T}} \begin{bmatrix} c_n \\ c_{n-1} \\ \vdots \\ c_0 \end{bmatrix}$$

where V is the Vandermonde matrix where the entry at index (i, s) is $(\frac{\widetilde{\beta}_s + c}{\widetilde{\alpha}_s + d})^{i-1}$, and $g(n) = O(\mathrm{poly}(n))$. If at least $n+1$ of the first $O(\mathrm{poly}(n))$ terms of the series $\frac{\widetilde{\beta}_s + c}{\widetilde{\alpha}_s + d}$ are well-defined and distinct, then the $n+1$ corresponding columns of V are linearly independent, and the respective entries of the diagonal matrix are nonzero (since $\widetilde{\alpha}_s + d \neq 0$), thus we can solve the linear system. If $\delta_s = s\beta^{s-1}$ then we are done by Lemma 16. If $\delta_s = \gamma^s$, then we already have $|\widetilde{\beta}| > |\widetilde{\alpha}| \geq 1$ or $|\widetilde{\beta}| < |\widetilde{\alpha}| \leq 1$, so we are done by Lemma 14 unless $\widetilde{\beta}$ or $\widetilde{\alpha}$ is a root of unity, which is to say either $\frac{\beta}{\gamma}$, $\frac{\alpha}{\gamma}$, or $\frac{\beta}{\alpha}$ is a root of unity. Suppose $\frac{\beta}{\gamma}$ is a k^{th} root of unity for some $k \geq 1$. Then

$$\begin{bmatrix} X_{ks} \\ Y_{ks} \end{bmatrix} = UB \begin{bmatrix} \alpha^{ks} \\ \beta^{ks} \\ \gamma^{ks} \end{bmatrix} = UB \begin{bmatrix} \alpha^{ks} \\ \beta^{ks} \\ \beta^{ks} \end{bmatrix} = UB \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \alpha^{ks} \\ \beta^{ks} \end{bmatrix} = UC \begin{bmatrix} \alpha^{ks} \\ \beta^{ks} \end{bmatrix} = L \begin{bmatrix} \alpha^{ks} \\ \beta^{ks} \end{bmatrix}.$$

By Lemma 10, at least one of the three finisher gadgets available results in L being invertible. Then this reduces to the same Vandermonde matrix as above, where $c = d = 0$. Furthermore $\frac{\alpha}{\beta}$ must not be a root of unity hence the Vandermonde matrix is nonsingular and interpolation holds (otherwise $\frac{\alpha}{\gamma} = \frac{\alpha}{\beta} \cdot \frac{\beta}{\gamma}$ is also a root of unity, and this contradicts the fact that the norms of the eigenvalues are not all identical). By applying a similar argument to the cases where $\frac{\alpha}{\beta}$ or $\frac{\alpha}{\gamma}$ is a root of unity, we conclude that the linear system has full rank. We remark that computation of the eigenvalues is not necessary in the reduction; one can simply evaluate all three finisher gadgets for polynomially many iterations of the binary recursive gadget to derive a full rank matrix to invert and solve for the c_i values. □

When all of the lemmas are tallied up, the interpolation proof outlined above is about eight pages of work, much of it rather technical. But while the proof is rather drawn out, the final result is cleanly stated. In fact, the condition on the eigenvalues in Lemma 17 is equivalent to the requirement that the recurrence matrix $\frac{M}{\det(M)}$ is acyclic. This begged the question of whether there was an easier way to prove all of this without eigenvalues, but instead based on the fact that the normalized transition matrix was acylic. It turns out that this is true, and the resulting proof is remarkably simpler (Lemmas 18 and 19 in the next section). We presently describe how this simpler proof was discovered.

Recall that multiplying a signature by a nonzero scalar has no effect on the complexity of determining the holant of a signature grid containing that signature. Similarly, our interpolation technique is "unaware" of nonzero constant factor differences in the signatures produced by the construction — all that really matters is that they are pairwise linearly independent. In order for our strategy of interpolation to succeed, we need to show that the our construction results in an infinite set of pairwise linearly independent unary signatures. Otherwise, up to a normalization factor, we have a finite set of signatures for which interpolation will fail on sufficiently large signature grids.

Since a finisher gadget simply acts as a projection from $\mathbb{C}^3$ to $\mathbb{C}^2$, this implies the *necessary* condition that the construction must produce an infinite set of pairwise linearly independent *binary* signatures before a finisher gadget is applied. Up to nonzero scalar factors, it is clear that any recursive gadget for which $\frac{M}{\det(M)}$ is cyclic is doomed to simulate only a finite set of signatures.

But even if $\frac{M}{\det(M)}$ is acyclic, this does not immediately guarantee success. It is possible that $\frac{M}{\det(M)}$ is acyclic but nevertheless the series $\{(\frac{M}{\det(M)})^i S\}_{i \geq 0}$ is cyclic for some starter gadget S. Even a single linear dependence in this series would imply a cycle, up to constant factors. Ultimately, the purpose of condition 2 of Lemma 17 is to ensure that this doesn't happen.

Now having understood why these conditions are necessary, let's reason why they are sufficient for interpolation to succeed. Suppose we have a starter gadget S and recursive gadget M for which all signatures produced by the recursive construction $\{M^i S\}_{i \geq 0}$ are pairwise linearly independent. The projection of a finisher gadget F might map this series to a finite set of pairwise linearly independent signatures. Hence we revert back to our earlier trick of adding more finisher gadgets. Suppose we have three finisher gadgets F_1, F_2, and F_3, with the same row space intersection property as before. In the current setting, this property implies that for any pair of symmetric binary signatures s_1 and s_2, there is a finisher gadget F_j for which $F_j s_1$ and $F_j s_2$ are linearly independent. That is, for any two linearly independent input vectors, some finisher gadget "picks up on" the difference between them. Each input vector s has a unique "fingerprint" described by the images under F_1, F_2, and F_3, and in particular, any linearly independent vectors s and t will be mapped to different one-dimensional linear subspaces under at least one of the three finisher gadgets. This implies that, given roughly n^3 pairwise linearly independent input vectors, at least one of the finisher gadgets maintains that at least n of them are still pairwise linearly independent after the finisher gadget is applied; otherwise we would have run out of fingerprints!

3.2 Interpolation techniques

3.2.1 Binary recursive construction with finisher gadgets

In this section, we develop the new technique of higher dimensional iterations for interpolation of unary signatures, using finisher gadgets. The following Lemma formalizes the "fingerprint" concept discussed in Section 3.1.4.

Lemma 18. *Suppose $M \in \mathbb{C}^{3 \times 3}$ is a nonsingular matrix, $s \in \mathbb{C}^3$ is a nonzero vector, and for all integers $k \geq 1$, s is not a column eigenvector of M^k. Let $F_i \in \mathbb{C}^{2 \times 3}$ be three matrices, where*

$\mathrm{rank}(F_i) = 2$ *for* $1 \le i \le 3$*, and the intersection of the row spaces of* F_i *is trivial* $\{0\}$*. Then for every* n*, there exists some* $F \in \{F_i : 1 \le i \le 3\}$*, and some* $S \subseteq \{FM^k s : 0 \le k \le n^3\}$*, such that* $|S| \ge n$ *and vectors in* S *are* pairwise *linearly independent.*

Proof. Let $k > j \ge 0$ be integers. Then $M^k s$ and $M^j s$ are nonzero and also linearly independent, since otherwise s is an eigenvector of M^{k-j}. Let $N = [M^j s, M^k s] \in \mathbb{C}^{3\times 2}$, then $\mathrm{rank}(N) = 2$, and $\ker(N^{\mathrm{T}})$ is a 1-dimensional linear subspace. It follows that there exists an $F \in \{F_i : 1 \le i \le 3\}$ such that the row space of F does not contain $\ker(N^{\mathrm{T}})$, and hence has trivial intersection with $\ker(N^{\mathrm{T}})$. In other words, $\ker(N^{\mathrm{T}}F^{\mathrm{T}}) = \{0\}$. We conclude that $FN \in \mathbb{C}^{2\times 2}$ has rank 2, and $FM^j s$ and $FM^k s$ are linearly independent.

Each F_i, where $1 \le i \le 3$, defines a coloring of the set $K = \{0, 1, \ldots, n^3\}$ as follows: color $k \in K$ with the linear subspace spanned by $F_i M^k s$. Thus, F_i defines an equivalence relation $\approx_i$ where $k \approx_i k'$ iff they receive the same color. Assume for a contradiction that for each F_i, where $1 \le i \le 3$, there are not n pairwise linearly independent vectors among $\{F_i M^k s : k \in K\}$. Then, including possibly the 0-dimensional space $\{0\}$, there can be at most n distinct colors assigned by F_i. By the pigeonhole principle, some k and k' with $0 \le k < k' \le n^3$ must receive the same color for all F_i, where $1 \le i \le 3$. This is a contradiction and we are done. □

The next lemma says that under suitable conditions we can construct all unary signatures $[x, y]$. The method will be interpolation at a higher dimensional iteration, and finishing up with a suitable *finisher* gadget, which projects to a lower dimension. A crucial new idea here is that when iterating at a higher dimension, we can guarantee the existence of *one* finisher gadget that succeeds on polynomially many steps, which results in overall success. Different finisher gadgets may work for different initial signatures and different input size n, but these need not be known in advance and have no impact on the final success of the reduction. Note that the finisher gadgets in the following lemma all have a single leading edge, which is implicit from the dimensions of their transition matrices.

Lemma 19. *Suppose that the following gadgets can be built using complex-valued signatures from a finite generator set* $\mathcal{G}$ *and a finite recognizer set* $\mathcal{R}$*.*

1. *A binary starter gadget with nonzero signature* $[z_0, z_1, z_2]$.

2. *A binary recursive gadget with nonsingular transition matrix* M*, for which* $[z_0, z_1, z_2]^{\mathrm{T}}$ *is not a column eigenvector of* M^k *for any positive integer* k.

3. *Three binary finisher gadgets with rank 2 transition matrices* $F_1, F_2, F_3 \in \mathbb{C}^{2\times 3}$*, where the intersection of the row spaces of* F_1*,* F_2*, and* F_3 *is trivial.*

Then for any $x, y \in \mathbb{C}$*,* $\#\mathcal{G} \cup \{[x, y]\} \mid \mathcal{R} \leq_{\mathrm{T}}^{\mathrm{P}} \#\mathcal{G} \mid \mathcal{R}$.

Proof. Assume we have oracle access to queries of the from $\#\mathcal{G} \mid \mathcal{R}$. Let $\mathcal{F} = \mathcal{G} \cup \mathcal{R}$. The construction begins with the binary starter gadget with signature $[z_0, z_1, z_2]$, which we call N_0. Recursively, $\mathcal{F}$-gate N_k is defined to be N_{k-1} connected to the binary recursive gadget in such a way that the trailing edges of the binary recursive gadget are merged with the leading edges of N_{k-1}. Then $\mathcal{F}$-gate G_k is defined to be N_k connected to one of the finisher gadgets, with the trailing edges of the finisher gadget merged with the leading edges of N_k (see Figure 3.1(d)). Herein we analyze the construction with respect to a given bipartite signature grid Ω for the holant problem $\#\mathcal{G} \cup \{[x, y]\} \mid \mathcal{R}$, with underlying graph $G = (V, E)$. Let $Q \subseteq V$ be the set of vertices with $[x, y]$ signatures, and let $n = |Q|$. By Lemma 18 fix j so that at least $n + 2$ of the first $(n + 2)^3 + 1$ vectors of the form $F_j M^k [z_0, z_1, z_2]^{\mathrm{T}}$ are pairwise linearly independent. We use finisher gadget F_j in the recursive construction, so that the signature of G_k is $F_j M^k [z_0, z_1, z_2]^{\mathrm{T}}$, which we denote by $[X_k, Y_k]$. We note that there exists a subset S of these signatures for which each Y_k is nonzero and $|S| = n + 1$. We will argue using only the existence of S, so there is no need to algorithmically "find" such a set, and for that matter, one can try out all three finisher gadgets without any need to determine which finisher gadget is "the correct one" beforehand. If we replace every element of Q with a copy of G_k, we obtain an instance of $\#\mathcal{G} \mid \mathcal{R}$ (note that the correct bipartite signature structure is preserved), and we denote this new signature grid by Ω_k. Then

$$\mathrm{Holant}_{\Omega_k} = \sum_{0 \leq i \leq n} c_i X_k^i Y_k^{n-i}$$

where $c_i = \sum_{\sigma \in J_i} \prod_{v \in V \setminus Q} f_v(\sigma|_{E(v)})$, J_i is the set of $\{0, 1\}$ edge assignments where the number of 0s assigned to the edges incident to the copies of G_k is i, f_v is the signature at v, and $E(v)$ is the set of edges incident to v. The important point is that the c_i values do not depend on X_k or Y_k. Since each signature grid Ω_k is an instance of $\#\mathcal{G} \mid \mathcal{R}$, Holant_{Ω_k} can be solved exactly using the oracle. Carrying out this process for every $k \in \{0, 1, \ldots, (n+2)^3\}$, we arrive at a linear system where the c_i values are the unknowns.

$$\begin{bmatrix} \text{Holant}_{\Omega_0} \\ \text{Holant}_{\Omega_1} \\ \vdots \\ \text{Holant}_{\Omega_{(n+2)^3}} \end{bmatrix} = \begin{bmatrix} X_0^0 Y_0^n & X_0^1 Y_0^{n-1} & \cdots & X_0^n Y_0^0 \\ X_1^0 Y_1^n & X_1^1 Y_1^{n-1} & \cdots & X_1^n Y_1^0 \\ \vdots & \vdots & \ddots & \vdots \\ X_{(n+2)^3}^0 Y_{(n+2)^3}^n & X_{(n+2)^3}^1 Y_{(n+2)^3}^{n-1} & \cdots & X_{(n+2)^3}^n Y_{(n+2)^3}^0 \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_n \end{bmatrix}.$$

$$\begin{bmatrix} y_0^{-n} \cdot \text{Holant}_{\Omega_0} \\ y_1^{-n} \cdot \text{Holant}_{\Omega_1} \\ \vdots \\ y_n^{-n} \cdot \text{Holant}_{\Omega_n} \end{bmatrix} = \begin{bmatrix} x_0^0 y_0^0 & x_0^1 y_0^{-1} & \cdots & x_0^n y_0^{-n} \\ x_1^0 y_1^0 & x_1^1 y_1^{-1} & \cdots & x_1^n y_1^{-n} \\ \vdots & \vdots & \ddots & \vdots \\ x_n^0 y_n^0 & x_n^1 y_n^{-1} & \cdots & x_n^n y_n^{-n} \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_n \end{bmatrix}.$$

The matrix above has entry $(x_r/y_r)^c$ at index (r, c). Due to pairwise linear independence of $[x_r, y_r]$, x_r/y_r is pairwise distinct for $0 \le r \le n$. Hence this is a Vandermonde system of full rank. Therefore the initial feasible linear system has full rank and we can solve it for the c_i values. With these values in hand, we calculate $\text{Holant}_\Omega = \sum_{0 \le i \le n} c_i x^i y^{n-i}$ directly, completing the reduction. □

The ability to simulate all unary signatures will allow us to prove #P-hardness. The next lemma says that, if $\mathcal{R}$ contains the EQUALITY gate $=_3$, then other than on a 1-dimensional curve $ab = 1$ and an isolated point $(a, b) = (0, 0)$, the ability to simulate unary signatures gives a reduction from COUNTING VERTEX COVERS. Note that COUNTING VERTEX COVERS on 3-regular graphs is just $\#[0, 1, 1] \mid [1, 0, 0, 1]$. Xia et al. showed that this is #P-hard even when the input is restricted to planar graphs [36]. We will see shortly that on the curve $ab = 1$ and at $(a, b) = (0, 0)$, the problem $\text{Hol}(a, b)$ is tractable.

Lemma 20. *Suppose that* $(a, b) \in \mathbb{C}^2 - \{(a, b) : ab = 1\} - \{(0, 0)\}$ *and let* $\mathcal{G}$ *and* $\mathcal{R}$ *be finite signature sets where* $[a, 1, b] \in \mathcal{G}$ *and* $[1, 0, 0, 1] \in \mathcal{R}$. *Further assume that* $\#\mathcal{G} \cup \{[x_i, y_i] : 0 \le$

$i < m\} \mid \mathcal{R} \leq_{\mathrm{T}}^{\mathrm{P}} \#\mathcal{G} \mid \mathcal{R}$ for any $x_i, y_i \in \mathbb{C}$ and $m \in \mathbb{Z}^+$. Then $\#\mathcal{G} \cup \{[0,1,1]\} \mid \mathcal{R} \leq_{\mathrm{T}}^{\mathrm{P}} \#\mathcal{G} \mid \mathcal{R}$, and $\#\mathcal{G} \mid \mathcal{R}$ is $\#\mathrm{P}$-hard.

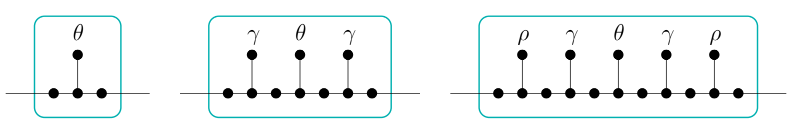
Proof. Assume $ab \neq 1$ and $(a, b) \neq (0, 0)$. Since $\mathrm{Hol}(0, 1)$ (which is the same as $\#[0, 1, 1] \mid [1, 0, 0, 1]$, or counting vertex covers on 3-regular graphs) is $\#\mathrm{P}$-hard, we only need to show how to simulate the generator signature $[0, 1, 1]$. We split this into three cases, and use a chain of three reductions, each involving a gadget in Figure 3.2 (each gadget has $[1, 0, 0, 1]$ assigned to the degree 3 vertices and $[a, 1, b]$ assigned to the degree 2 vertices).

1. $ab \neq 0$ and $ab \neq -1$
2. $ab = 0$
3. $ab = -1$

If $ab \neq 0$ and $ab \neq -1$, then we use gadget 3, and we set its unary signatures to be $\theta = [(ab + 1)/(1-ab), -a^2(ab+1)/(1-ab)]$, $\gamma = [-a^{-2}, b^{-1}(1+ab)^{-1}]$, and $\rho = [-b/(ab-1), a/(ab-1)]$. Calculating the resulting signature of gadget 3, we find that it is $[0, 1, 1]$ as desired.

If $ab = 0$ then assume without loss of generality that $a = 0$ and $b \neq 0$. This time we use gadget 1, setting $\theta = [b, b^{-1}]$. Then gadget 1 simulates a $[b^{-1}, 1, 2b]$ generator signature, but since this signature fits the criteria of case 1 above, we are done by reduction from that case.

Similarly, if $ab = -1$, then gadget 2 exhibits a generator signature of the form $[0, 1, 5/(2a)]$ under the signatures $\theta = [1/(6a), -a/24]$ and $\gamma = [-3/a, a]$. Since $5/(2a)$ is nonzero, we are done by reduction from case 2. □



(a) Gadget 1 (b) Gadget 2 (c) Gadget 3

Figure 3.2 Gadgets used to simulate the [0,1,1] signature

The gadgets of Lemma 20 were found by a manual search with the assistance of computer algebra to eliminate tedious computations. Each of the gadgets in Figure 3.2 has a signature that can be calculated as a string of matrix multiplications. An arity-2 vertex corresponds to the matrix $\begin{bmatrix} a & 1 \\ 1 & b \end{bmatrix}$, and each arity-3 vertex corresponds to the matrix $\begin{bmatrix} x & 0 \\ 0 & y \end{bmatrix}$, where $[x, y]$ is the signature assigned to the adjacent degree-1 vertex. Calculating the signature of gadget 1 with respect to an arbitrary signature $\theta = [s, t]$, we find that it has the signature $[a^2 s + t, as + bt, s + b^2 t]$. Setting $t = -a^2 s$, we get the signature $[0, a, ab{+}1]$ (up to a constant factor), hence it is possible to simulate a weighted version of VERTEX COVER with gadget 1, but in general not the signature $[0, 1, 1]$. The next step was to try a slightly more expressive gadget (gadget 2 in Figure 3.2). The signature γ is applied once on either side of the gadget so as to guarantee that the signature of gadget 2 would be symmetric for all settings of the unary signatures θ and γ. However, no such universal setting of θ and γ was found in this setting either. Finally, the same process was attempted with gadget 3, and after some reasonable judgments on how to simplify the resulting polynomials without sacrificing too much generality, a setting of the unary signatures was found that simulated $[0, 1, 1]$ in all but a few exceptional settings of a and b, which were subsequently addressed as special cases by gadgets 1 and 2. One way to understand this successful setting of the unary signatures in gadget 3 is as follows. We already know how to simulate the signature $[0, a, ab + 1]$ using gadget 1, so we will simulate this signature in the center of gadget 3 using the same setting for θ. This signature differs from $[0, 1, 1]$ only by a factor of a diagonal matrix, so we will try to get the remaining left and right side vertices to each simulate a diagonal matrix. Setting ρ to the correct signature forces the said matrix to be diagonal, and γ provides the extra degree of freedom to select exactly what diagonal matrix we want. Along these lines it can be noted that small modifications to the signatures given in Lemma 20 permits the simulation of any signature of the form $[0, x, y]$ for any $x, y \in \mathbb{C}$.

It will be helpful to have conditions that are easier to check than those in Lemma 19. To this end, we establish condition 2 in terms of eigenvalues, and we build general-purpose finisher gadgets to eliminate condition 3. Let M_4, M_5, and F be the transition matrices for gadget 4, gadget 5, and the simplest possible binary finisher gadget (each built using generator signature $[a, 1, b]$ and recognizer signature $[1, 0, 0, 1]$; see Figures 3.3(a), 3.3(b), and 3.1(c)). Provided that $ab \neq 1$ and $a^3 \neq b^3$, it turns out that the finisher gadget sets $\{F, FM_4, FM_4^2\}$ and $\{F, FM_4, FM_5\}$ satisfy condition 3 of Lemma 19 when $ab \neq 0$ and $ab = 0$, respectively. Together with Lemma 20, these observations yield the following.

Theorem 11. *If the following gadgets can be built using generator* $[a, 1, b]$ *and recognizer* $[1, 0, 0, 1]$ *where* $a, b \in \mathbb{C}$*,* $ab \neq 1$*, and* $a^3 \neq b^3$*, then the problem* $\mathrm{Hol}(a, b)$ *is* $\#\mathrm{P}\text{-hard}$.

1. *A binary recursive gadget with nonsingular transition matrix* M *which has eigenvalues* α *and* β *such that* $\frac{\alpha}{\beta}$ *is not a root of unity.*
2. *A binary starter gadget with signature* s *which is not orthogonal to any row eigenvector of* M.

Proof. First we show how to build general-purpose binary finisher gadgets for the main construction using the assumed generator and recognizer, starting first with the case where $ab \neq 0$. Using the simplest possible choice for a finisher gadget F (Figure 3.1(c)), we get $F = \begin{bmatrix} a & 0 & 1 \\ 1 & 0 & b \end{bmatrix}$. Let M_4 be the transition matrix for binary recursive gadget 4 (Figure 3.3(a)), and we calculate that

$$M_4 = \begin{bmatrix} a^3 & 2a & b \\ a^2 & ab+1 & b^2 \\ a & 2b & b^3 \end{bmatrix}.$$

We build two more finisher gadgets F' and F'' using gadget 4 so that $F' = FM_4$ and $F'' = FM_4^2$. Since F and M_4 both have full rank (note $\det(M_4) = ab(ab-1)^3$), it follows that F' and F'' also have full rank. Now we will show that the row spaces of F, F' and F'' have trivial intersection, and it suffices to verify that the cross products of the row vectors of F, F', and F'' (denoted respectively by v, v', and v'') are linearly independent. (To see this, suppose u is a complex vector in the intersection of the row spaces of F, F', and F''. Then v, v', and v'' are all orthogonal to u, but since v, v', and v'' are linearly independent, they span the conjugate vector $\overline{u}$ which is then also orthogonal to u. This means $|u|^2 = u\overline{u} = 0$, and that $u = 0$.) The cross products of the row vectors of F, F', and F'' are $[0, 1-ab, 0]$, $(ab-1)^2[2b^2, -ab(ab+1), 2a^2]$, and $(ab-1)^3[2b(a^2b^3+a^2+ab^2+b^4), -ab(a^3b^3+2a^3+2a^2b^2+ab+2b^3), 2a(a^4+a^3b^2+a^2b+b^2)]$ respectively. Then to see that these 3 vectors are linearly independent, it suffices to verify that the matrix $\begin{bmatrix} 2b^2 & 2a^2 \\ 2b(a^2b^3 + a^2 + ab^2 + b^4) & 2a(a^4 + a^3b^2 + a^2b + b^2) \end{bmatrix}$ is nonsingular. Since $a \neq 0$, $b \neq 0$, and $ab \neq 1$, we just check $\det \begin{bmatrix} b & a \\ a^2b^3 + a^2 + ab^2 + b^4 & a^4 + a^3b^2 + a^2b + b^2 \end{bmatrix} = (ab - 1)(a^3 - b^3) \neq 0$, so the row spaces of F, F', and F'' have trivial intersection when $ab \neq 0$.

Now suppose $ab = 0$. Since $a^3 \neq b^3$, by symmetry, if $ab = 0$ we may assume without loss of generality that $a \neq 0$ and $b = 0$. Let M_5 be the transition matrix for binary recursive gadget 5 (Figure 3.3(b)).

$$M_5 = \begin{bmatrix} a^6 + 2a^3 + 1 & 2a^4 + 2a & a^2 \\ a^5 + a^2 & 2a^3 + 1 & a \\ a^4 & 2a^2 & 1 \end{bmatrix}.$$

Composing F with M_5, we get a finisher gadget with matrix FM_5, which has full rank since F has full rank and $\det(M_5) = 1$. It is also straightforward to see that F' has full rank, as $F' = \begin{bmatrix} a^4 + a & 2a^2 & 0 \\ a^3 & 2a & 0 \end{bmatrix}$. The cross products of the rows of F, F', and FM_5 are $[0, 1, 0]$, $[0, 0, 2a^2]$, and $[-2a, 2a^3 + 1, -2a^2(1 + a)(a^2 - a + 1)]$ respectively. Then the matrix of cross products is clearly nonsingular, and we conclude that for any $a, b \in \mathbb{C}$, we have 3 finisher gadgets satisfying item 3 of Lemma 19 unless $ab = 1$ or $a^3 = b^3$.

Now we want to show that s is not a column eigenvector of M^k for any positive integer k (note that s is nonzero by assumption). Writing out the Jordan Normal Form for M, we have $M^k s = T^{-1}D^kTs$, where D^k has the form $\begin{bmatrix} \alpha^k & 0 & 0 \\ 0 & \beta^k & 0 \\ 0 & * & * \end{bmatrix}$, and where α and β are eigenvalues of M for which $\frac{\alpha}{\beta}$ is not a root of unity. Let $t = Ts$ and write $t = [c, d, e]^{\mathrm{T}}$. By hypothesis, s is not orthogonal to the first two rows of T, thus $c, d \neq 0$. If s were an eigenvector of M^k for some positive integer k, then $T^{-1}D^kTs = M^k s = \lambda s$ for some nonzero complex value λ, and $D^k t = T(\lambda s) = \lambda t$. But then $c\alpha^k = \lambda c$ and $d\beta^k = \lambda d$, which means $\frac{\alpha^k}{\beta^k} = 1$, contradicting the fact that $\frac{\alpha}{\beta}$ is not a root of unity.

We have now met all the criteria for Lemma 19, so the reduction $\#\mathcal{S} \cup \{[a,1,b],[x,y]\} \mid [1,0,0,1] \leq_{\mathrm{T}}^{\mathrm{P}} \#\mathcal{S} \cup \{[a,1,b]\} \mid [1,0,0,1]$ holds for any $x, y \in \mathbb{C}$ and any finite signature set $\mathcal{S}$. By Lemma 20 the problem $\mathrm{Hol}(a,b)$ is $\#\mathrm{P}\text{-hard}$. □

The discovery of finisher gadgets is somewhat of a trial-and-error process. One useful heuristics in this search is that gadgets with less vertices tend to be more effective than larger ones. This is because the degree of the polynomials involved is lower. Also, a convenient and productive way to form finisher gadget sets is by fixing a single finisher gadget and then composing it with one or more recursive gadgets to form new finisher gadgets (as we did above). In any case, using a computational algebra package to compute and factor the determinant of the resulting matrix of cross products is a big time saver in making such a search.

3.2.2 Unary recursive construction

Now we consider a construction based on unary starter and recursive gadgets. The following lemma arrives from [30] and is stated explicitly in [10]. It can be viewed as a unary version of Lemma 19 without finisher gadgets.

Lemma 21. *Suppose there is a unary recursive gadget with nonsingular matrix M and a unary starter gadget with nonzero signature s. If the ratio of the eigenvalues of M is not a root of unity and s is not a column eigenvector of M, then $\{M^i s\}_{s \geq 0}$ can be used to interpolate all unary signatures.*

Surprisingly, a set of general-purpose starter gadgets can be made for this construction as long as $ab \neq 1$ and $a^3 \neq b^3$, so we refine this lemma by eliminating the starter gadget requirement. The starter gadgets are Fs, $FM_4 s$, and $FM_6 s$ where M_6 is gadget 6 and s is the single-vertex starter gadget (see Figures 3.3(c) and 3.1(a)).

Theorem 12. *Suppose there is a unary recursive gadget with nonsingular matrix M, and the ratio of the eigenvalues of M is not a root of unity. Then for any $a, b \in \mathbb{C}$ where $ab \neq 1$ and $a^3 \neq b^3$, there is a starter gadget built using generator $[a,1,b]$ and recognizer $[1,0,0,1]$ for which the resulting construction can be used to interpolate all unary signatures.*

Proof. Let M_4, M_6, F, and s be gadget 4, gadget 6, the binary finisher gadget in Figure 3.1(c), and single-vertex binary starter gadget (Figure 3.1(a)), respectively. Note $s = [a, 1, b]^{\mathrm{T}}$ and

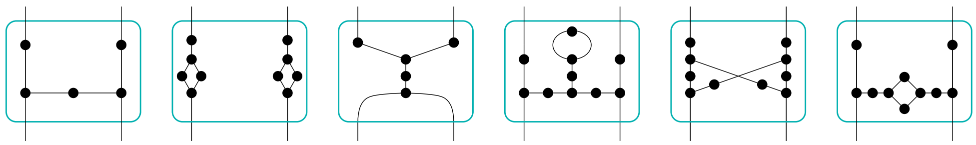
$$M_6 = \begin{bmatrix} a^3+1 & 0 & a^2+b \\ a^2+b & 0 & a+b^2 \\ a+b^2 & 0 & b^3+1 \end{bmatrix}.$$

Calculating the determinants of the matrices $[FM_4s, Fs]$, $[FM_6s, Fs]$, and $[FM_4s, FM_6s]$, we have

$$\begin{aligned} \det[FM_4s, Fs] &= (a^3-b^3)(ab-1)^2 \\ \det[FM_6s, Fs] &= (a^3-b^3)(ab-1)^2 \\ \det[FM_4s, FM_6s] &= (a^3-b^3)(ab-1)^3, \end{aligned}$$

and all nonsingular since $ab \neq 1$ and $a^3 \neq b^3$. Therefore the vectors Fs, FM_4s, and FM_6s are pairwise linearly independent. Since the ratio of the eigenvalues of M is not a root of unity, then the eigenvalues of M are distinct, each eigenvalue corresponds to an eigenspace of dimension 1, and at least one element of $\{FM_4s, FM_6s, Fs\}$ is not a column eigenvector of M. The corresponding starter gadget can be used with M in a recursive construction and the result follows from Lemma 21. □

One might hope to further refine the binary recursive construction of Lemma 11 by constructing a similar set of general-purpose starter gadgets, but this turns out to be more challenging. The condition that the starter gadget be non-orthogonal to any row eigenvector of a binary recursive gadget M establishes (at most) 3 forbidden two-dimensional linear subspaces, and we would need to argue that we can find a starter gadget with a signature that is not contained in any of these. For example, if we can find 7 binary starter gadgets such that any 3 of them form a linearly independent set, then each row eigenvector of M is orthogonal to at most 2 of them, hence one of these has a signature which is not orthogonal to any row eigenvector of M. Finding 7 such starter gadgets seems rather unwieldly, but this condition could be refined somewhat. Another possibility is to adapt the circular construction of Chapter 5 to binary recursive gadgets to ease the search for starter gadgets. We leave the question of general-purpose binary starter gadgets as an open question.



(a) Gadget 4 (b) Gadget 5 (c) Gadget 6 (d) Gadget 7 (e) Gadget 8 (f) Gadget 9

Figure 3.3 Binary recursive gadgets

3.3 Classification of problems

3.3.1 Tractable problems and algebraic symmetrization

Now we aim to characterize $\mathrm{Hol}(a, b)$ where $a, b \in \mathbb{C}$. The next lemma introduces the technique of algebraic symmetrization. We show that over 3-regular graphs, the holant value is expressible as an integer polynomial $P(X, Y)$, where $X = ab$ and $Y = a^3 + b^3$. This change of variable, from (a, b) to (X, Y), is crucial in two ways. First, it allows us to derive tractability results easily, drawing connections between problems that may appear unrelated, and the tractability of one implies the other. Second, it facilitates the proof of hardness for those (a, b) where the problem is indeed $\#\mathrm{P}\text{-hard}$ by reducing the degree of the polynomials involved. Once this transformation is made, four binary recursive gadgets easily cover all of the $\#\mathrm{P}\text{-hard}$ problems where X and Y are real-valued, with a straightforward symbolic computation using CylindricalDecomposition in Mathematica™. All gadget constructions in this section use $[a, 1, b]$ and $[1, 0, 0, 1]$ signatures exclusively, and we henceforth denote $X = ab$ and $Y = a^3 + b^3$ for the remainder of this chapter.

Lemma 22. *Let G be a 3-regular graph. Then there exists a polynomial $P(\cdot, \cdot)$ with two variables and integer coefficients such that for any signature grid Ω having underlying graph G and every edge labeled $[a, 1, b]$, the holant value is $\mathrm{Holant}_\Omega = P(ab, a^3 + b^3)$.*

Proof. Consider any $\{0, 1\}$ vertex assignment σ with a nonzero valuation. If σ' is the complement assignment switching all 0's and 1's in σ, then for σ and σ', we have the sum of valuations $a^i b^j + a^j b^i$ for some i and j. Here i (resp. j) is the number of edges connecting two degree 3 vertices both assigned 0 (resp. 1) by σ. We note that $a^i b^j + a^j b^i = (ab)^{\min(i,j)}(a^{|i-j|} + b^{|i-j|})$.

We prove $i \equiv j \pmod 3$ inductively. For the all-0 assignment, this is clear since every edge contributes a factor a and the number of edges is divisible by 3 for a 3-regular graph. Now starting from any assignment σ, if we switch the assignment on one vertex from 0 to 1, it is easy to verify that it changes the valuation from $a^i b^j$ to $a^{i'} b^{j'}$, where $i - j = i' - j' + 3$. As every $\{0, 1\}$ assignment is obtainable from the all-0 assignment by a sequence of switches, the conclusion $i \equiv j \pmod 3$ follows.

Now $a^i b^j + a^j b^i = (ab)^{\min(i,j)}(a^{3k} + b^{3k})$, for some $k \geq 0$ and a simple induction $a^{3(k+1)} + b^{3(k+1)} = (a^{3k} + b^{3k})(a^3 + b^3) - (ab)^3(a^{3(k-1)} + b^{3(k-1)})$ shows that the holant is a polynomial $P(ab, a^3 + b^3)$ with integer coefficients. □

Corollary 2. *If $X = -1$ and $Y \in \{0, \pm 2\mathfrak{i}\}$, then $\mathrm{Hol}(a, b)$ is in FP.*

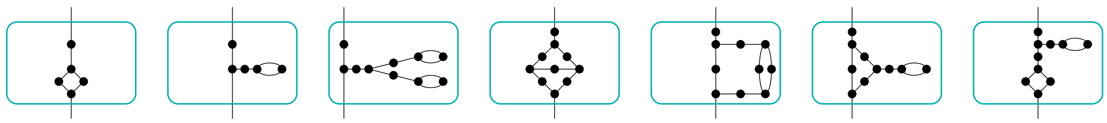
Proof. The problems $\mathrm{Hol}(1, -1)$, $\mathrm{Hol}(-\mathfrak{i}, -\mathfrak{i})$, and $\mathrm{Hol}(\mathfrak{i}, \mathfrak{i})$ are all solvable in FP (these fall within the families $\mathcal{F}_1$, $\mathcal{F}_2$, and $\mathcal{F}_3$ in [4]); $X = -1$ for each, whereas the value of Y for these problems is 0, $2\mathfrak{i}$, and $-2\mathfrak{i}$ respectively. Since the value of any 3-regular signature grid is completely determined by X, Y, and the polynomial $P(\cdot, \cdot)$ (which in turn depends only on the underlying graph G), any a and b such that $ab = -1$ and $a^3 + b^3 \in \{0, \pm 2\mathfrak{i}\}$ (i.e. $ab = -1$ and $a^{12} = 1$) is computable in polynomial time. □

We now list all of the cases where $\mathrm{Hol}(a, b)$ is computable in polynomial time.

Theorem 13. *If any of the following four conditions is true, then $\mathrm{Hol}(a, b)$ is solvable in FP:*

1. $X = 1$,
2. $X = Y = 0$,
3. $X = -1$ *and* $Y \in \{0, \pm 2\mathfrak{i}\}$
4. $4X^3 = Y^2$ *and the input is restricted to planar graphs.*

Proof. If $X = 1$ then the signature $[a, 1, b]$ is degenerate and the holant can be computed in polynomial time. If $X = Y = 0$ then $a = b = 0$, and a 2-coloring algorithm can be employed on the edges. If $X = -1$ and $Y \in \{0, \pm 2\mathfrak{i}\}$ then we are done by Corollary 2. If we restrict the input to planar graphs and $4X^3 = Y^2$ (equivalently, $a^3 = b^3$), holographic algorithms can be applied [7]. □



(a) Gadget 10 (b) Gadget 11 (c) Gadget 12 (d) Gadget 13 (e) Gadget 14 (f) Gadget 15 (g) Gadget 16

Figure 3.4 Unary recursive gadgets

3.3.2 Eigenvalue Shifted Pairs

Our main task in this chapter is to prove that all remaining problems are #P-hard. The following two lemmas provide sufficient conditions to satisfy the eigenvalue requirement of the recursive constructions. They are motivated by the desire for concrete algebraic conditions which are easy to check over large classes of problems.

Lemma 23. *If both roots of the complex polynomial $x^2 + Bx + C$ have the same norm, then $B|C| = \overline{B}C$ and $B^2\overline{C} = \overline{B}^2 C$. If further $B \neq 0$ and $C \neq 0$, then $\operatorname{Arg}(B^2) = \operatorname{Arg}(C)$.*

Proof. If the roots have equal norm, then for some $a, b \in \mathbb{C}$ and nonnegative $r \in \mathbb{R}$ and we can write $x^2 + Bx + C = (x - ra)(x - rb)$, where $|a| = |b| = 1$, so $B|C| = -r(a + b)r^2 = -r(a^{-1} + b^{-1})r^2 ab = \overline{B}C$. Squaring both sides and dividing by C, we have $B^2\overline{C} = \overline{B}^2 C$ (note this is justified since this equality still holds when $C = 0$). Multiplying $B|C| = \overline{B}C$ by B we get $B^2|C| = |B^2|C$, and if B and C are both nonzero then $\frac{B^2}{|B^2|} = \frac{C}{|C|}$, that is, $\operatorname{Arg}(B^2) = \operatorname{Arg}(C)$. □

Lemma 24. *If all roots of the complex polynomial $x^3 + Bx^2 + Cx + D$ have the same norm, then $C|C|^2 = \overline{B}|B|^2 D$.*

Proof. If the roots have equal norm, then for some $a, b, c \in \mathbb{C}$ and nonnegative $r \in \mathbb{R}$ we can write $x^3 + Bx^2 + Cx + D = (x - ra)(x - rb)(x - rc)$, where $|a| = |b| = |c| = 1$, so $B = -r(a + b + c)$, $C = r^2(ab + bc + ca)$, and $D = -r^3 abc$. Then

$$C|C|^2 = r^2(ab + bc + ca)r^4|ab + bc + ca|^2 = r(\overline{a + b + c})r^2|a + b + c|^2 r^3 abc = \overline{B}|B|^2 D,$$

where we used the fact that $|ab + bc + ca| = |ab + bc + ca| \cdot |a^{-1}b^{-1}c^{-1}| = |a^{-1} + b^{-1} + c^{-1}| = |\overline{a + b + c}| = |a + b + c|$. $\square$

Lemmas 23 and 24 are used in the contrapositive. That is, we try to show that $C|C|^2 \neq \overline{B}|B|^2 D$ in the case of a binary recursive gadget, and conclude that the roots of the polynomial do not all have the same norm. As one might expect, Lemmas 23 and 24 can be generalized to higher degree polynomials. With each increase of 2 in the arity of the recursive gadget, another equation is added, making the gadget more powerful. Thus, most of the theory of recursive gadgets presented here can be readily generalized to higher arity, with the most important remaining question being how to certify that a given finisher gadget set is always capable of projecting higher dimensional signatures down to a lower dimension without losing too much in the way of pairwise linear independence. As we will see in later chapters, it isn't the *arity* of the $\mathcal{F}$-gate given by the construction that matters, so much as the *dimension* of the subspace of signatures to be interpolated. The question of finisher gadgets of higher arity and the exploration of higher arity recursive gadgets are an interesting topic, but beyond the scope of this thesis. Having laid the basic groundwork, we leave these as open questions.

In Chapter 2, we discussed the implementation of an algorithm for computing the transition matrices of recursive gadgets. This algorithm can be easily adapted for computing these matrices in general terms, i.e. for $\#[a, 1, b] \mid [1, 0, 0, 1]$ where each entry of the transition matrix is an integer polynomial in a and b. Using this in conjunction with an exhaustive search of recursive gadgets, we can automatically generate a complete list of unary and binary recursive gadgets with a limited number of vertices, complete with transition matrices and characteristic polynomials. As a further step, it is often useful to input the coefficients of these characteristic polynomials (which integer polynomials in a and b) into a computer algebra system like Mathematica$^{\text{TM}}$, so they can be factored and further manipulated ad hoc. We remark that the automated factorization of these polynomials alone is a huge boost in understanding when and how to apply these gadgets.

If we were to attempt to apply Lemmas 12 and 23 as is, we would end up with a large list of failure conditions of the form $\text{Arg}(B^2) = \text{Arg}(C)$, each pertaining to unary gadget, where B and C are integer polynomials in a and b. For the most part, these polynomials are too large to be manipulated by hand in any sensible way. So one is reduced to staring at this list of (factored) polynomials wondering how to begin to derive theorems using data of this sort. One observation is that if two gadgets share the same polynomial as a B coefficient, then we can derive a failure condition of the form $\mathrm{Arg}(C_1) = \mathrm{Arg}(C_2)$ using both of these gadgets. This does happen, in fact, because there are "coincidences" where gadgets share the exact same trace as polynomials in a and b. If the resulting polynomials C_1 and C_2 could be further simplified as a result of common polynomial factors, this could result in a condition simple enough to be of use. We will make use of this idea later on, but it turns out not to be of much help at the moment. A new idea is needed.

Studying the transition matrices of two of the simplest possible unary recursive gadgets (gadgets 10 and 11), we notice that they differ by $ab-1$ along the diagonal and are identical elsewhere. This implies that their eigenvalues are closely related, only shifted by $ab-1$ in the complex plane. To see why this is important, suppose that gadget 10 fails with respect to some a and b, meaning that both eigenvalues have the same norm. Then almost *any* shift in the complex plane will cause the eigenvalues to have different norms, meaning that gadget 11 probably has eigenvalues with distinct norms. A necessary condition for both of these gadgets to fail is that the shift $ab-1$ must align perfectly with the sum of the two eigenvalues for both gadgets, that is, the trace of both gadgets and the eigenvalue shift must all be colinear in the complex plane. A similar statement can also be made about the determinant of either gadget and the square of the eigenvalue shift. This *Eigenvalue Shifted Pair (ESP)* is the key ingredient that makes it possible for us to progress towards a general result.

Definition 1. *A pair of nonsingular square matrices M and M' is called an* Eigenvalue Shifted Pair (ESP) *if $M' = M + \delta I$ for some nonzero $\delta \in \mathbb{C}$, and M has distinct eigenvalues.*

Clearly for such a pair, M' also has distinct eigenvalues. Gadgets 10 and 11 form an Eigenvalue Shifted Pair for nearly all $a, b \in \mathbb{C}$. Before we make significant use of such Eigenvalue Shifted Pairs, we will first try to nail down precisely what power they hold. The following lemma relates the trace $\alpha + \beta$ and the determinant $\alpha\beta$ of a 2 by 2 matrix to the eigenvalue shift δ.

Lemma 25. *Suppose $\alpha, \beta, \delta \in \mathbb{C}$, $|\alpha| = |\beta|$, $\alpha \neq \beta$, $\delta \neq 0$, and $|\alpha + \delta| = |\beta + \delta|$. Then there exists $r, s \in \mathbb{R}$ such that $r\delta = \alpha + \beta$ and $s\delta^2 = \alpha\beta$.*

Proof. After a rotation in the complex plane, we can assume $\alpha = \overline{\beta}$, and then since $\alpha+\beta, \alpha\beta \in \mathbb{R}$ we just need to prove $\delta \in \mathbb{R}$. Then $(\alpha + \delta)\overline{(\alpha + \delta)} = |\alpha + \delta|^2 = |\beta + \delta|^2 = (\beta + \delta)\overline{(\beta + \delta)} = (\overline{\alpha} + \delta)(\alpha + \overline{\delta})$ and we distribute to get $\alpha\overline{\alpha} + \delta\overline{\delta} + \alpha\overline{\delta} + \overline{\alpha}\delta = \alpha\overline{\alpha} + \delta\overline{\delta} + \overline{\alpha}\overline{\delta} + \alpha\delta$. Canceling repeated terms and factoring, we have $(\overline{\alpha} - \alpha)(\overline{\delta} - \delta) = 0$, and since $\alpha \neq \beta = \overline{\alpha}$ we know $\overline{\delta} = \delta$ therefore $\delta \in \mathbb{R}$. □

Corollary 3. *Let M and M' be an Eigenvalue Shifted Pair of 2 by 2 matrices. If both M and M' have eigenvalues of equal norm, then there exists $r, s \in \mathbb{R}$ such that $\operatorname{tr}(M) = r\delta$ (possibly 0) and $\det(M) = s\delta^2$.*

Proof. Let α and β be the eigenvalues of M, so $\alpha + \delta$ and $\beta + \delta$ are the eigenvalues of M'. Suppose that $|\alpha| = |\beta|$ and $|\alpha + \delta| = |\beta + \delta|$. Then by Lemma 25, there exists $r, s \in \mathbb{R}$ such that $\operatorname{tr}(M) = \alpha + \beta = r\delta$ and $\det(M) = \alpha\beta = s\delta^2$. □

We now apply an ESP to prove that most settings of $\operatorname{Hol}(a, b)$ are $\#\mathrm{P}$-hard.

Lemma 26. *Suppose $X \neq \pm 1$, $X^2 + X + Y \neq 0$, and $4(X - 1)^2(X + 1) \neq (Y + 2)^2$. Then either unary gadget 10 or unary gadget 11 has nonzero eigenvalues with distinct norm, unless X and Y are both real numbers.*

Proof. Gadgets 10 and 11 have $M_{10} = \begin{bmatrix} a^3+1 & a+b^2 \\ a^2+b & b^3+1 \end{bmatrix}$ and $M_{11} = \begin{bmatrix} a^3+ab & a+b^2 \\ a^2+b & ab+b^3 \end{bmatrix}$ as their transition matrices, so $M_{11} = M_{10} + (X - 1)I$, and the eigenvalue shift is nonzero. Checking the determinants, $\det(M_{10}) = (X - 1)^2(X + 1) \neq 0$ and $\det(M_{11}) = (X - 1)(X^2 + X + Y) \neq 0$. Also, $\operatorname{tr}(M_{10})^2 - 4\det(M_{10}) = (Y + 2)^2 - 4(X - 1)^2(X + 1) \neq 0$, so the eigenvalues of M_{10} are distinct. Therefore by Corollary 3, either M_{10} or M_{11} has nonzero eigenvalues of distinct norm unless $\operatorname{tr}(M_{10}) = r(X - 1)$ and $\det(M_{10}) = s(X - 1)^2$ for some $r, s \in \mathbb{R}$. Then we would have $(X-1)^2(X+1) = s(X-1)^2$ so $X = s-1 \in \mathbb{R}$ and $Y+2 = r(X-1)$ so $Y = r(X-1)-2 \in \mathbb{R}$. □

Computer search can be used to automate the process of finding ESPs, but the process of deciding which ESP is the most useful for a given situation has been done by manual inspection. This is one reason why the trace and determinant of unary recursive gadgets (not to mention eigenvalue shifts) are always studied in factored form: the ideal situation is one where the trace and the eigenvalue shift (or determinant and squared eigenvalue shift) only differ by a small polynomial factor. This is certainly true for gadgets 10 and 11, where the eigenvalue shift is $X - 1$, the determinant of gadget 10 is $(X - 1)^2(X + 1)$. The fact that the trace is $Y + 2$ is also important, since this allows us to conclude that Y is real when X is real. Also, it is not an accident that an ESP of such simple gadgets contains so much power in proving a general result; the polynomials involved are all simple, due to the size of the gadget, and simple polynomials give way to stronger statements, as testified by Lemma 26. We also comment that although many ESPs of unary recursive gadgets exist, no binary recursive gadgets were found that form an ESP, except in very special cases for a and b.

3.3.3 Problems that are $\#\mathrm{P}$-hard even for planar graphs

Now we will deal with the following exceptional cases from Lemma 26 ($X = 1$ is tractable by Theorem 13).

0. $X \in \mathbb{R}$ and $Y \in \mathbb{R}$
1. $X^2 + X + Y = 0$
2. $X = -1$
3. $4(X - 1)^2(X + 1) = (Y + 2)^2$

Note that unary gadgets are much less useful for making progress on condition 0 than conditions 1 through 3. This is because when the trace and determinant of a unary gadget are real-valued, the power of Lemma 23 is significantly reduced. The case where X and Y are both real is dealt with using the tools developed in Section 3.2, and some symbolic computation. This includes the case where a and b are both real as a subcase. As noted earlier, a dichotomy theorem for the complexity of $\mathrm{Hol}(a, b)$ when a and b are both real has already been proved in [10] with a significant effort. With the new tools developed we offer a simpler proof, which also covers some cases where a or b are complex. Working with real-valued X and Y is a significant advantage, since the failure condition given by Lemma 24 is simplified by the disappearance of norms and conjugates. Working with X and Y instead of a and b causes a major speedup in symbolic computation (due to the reduced degree of polynomials involved), and brings the problem of proving $\#\mathrm{P}$-hardness within reach of symbolic computation via cylindrical decomposition. We note that the trace and determinant always turn out to be polynomials in X and Y, and this can be proved along similar lines of Lemma 22 (though it isn't necessary to do so). This observation actually fails for certain gadgets in higher degree signature grids. We apply Theorem 11 to gadgets 4, 7, 8, and 9 (Figure 3.3) together with a starter gadget (Figure 3.1(a)) to prove that problems over real-valued X and Y are $\#\mathrm{P}\text{-hard}$. Conditions 1 and 2 of Theorem 11 are encoded directly into a query for CYLINDRICALDECOMPOSITION in Mathematica$^{\mathrm{TM}}$, but first we give a lemma to show how to encode condition 2 of Lemma 11.

Lemma 27. *Suppose $M \in \mathbb{C}^{n\times n}$ and $s \in \mathbb{C}^{n\times 1}$. If $\det([s, Ms, M^2s, \ldots, M^{n-1}s]) \neq 0$ then s is not orthogonal to any row eigenvector of M.*

Proof. Suppose s is orthogonal to a row eigenvector v of M with eigenvalue λ. Then $v[s, Ms, ..., M^{n-1}s] = 0$, since $vM^is = \lambda^i vs = 0$. Since $v \neq 0$ this is a contradiction. □

There is no fundamental reason why the gadgets for the following lemma were selected. There were several other combinations of gadgets that gave the same result, and the simplest gadgets among these were used in the version proved here.

Theorem 14. *Suppose $a, b \in \mathbb{C}$, $X, Y \in \mathbb{R}$, $X \neq 1$, $4X^3 \neq Y^2$, and it is not the case that both $X = -1$ and $Y = 0$. Then the problem $\mathrm{Hol}(a, b)$ is $\#\mathrm{P}\text{-hard}$.*

Proof. We will use binary recursive gadgets 4, 7, 8, and 9 together with the single-vertex starter gadget given in Figure 3.1(a) (denote the respective matrices by M_4, M_7, M_8, M_9, and s). Calculating the transition matrices of these gadgets, we get

$$\begin{aligned}
M_7 &= \begin{bmatrix} a^6+a^4b+a^3+a^2b^2 & 2a^4+4a^2b+2ab^3 & a^2+ab^2+b^4+b \\ a^5+a^3b+a^2+ab^2 & a^4b+a^3+2a^2b^2+ab^4+2ab+b^3 & a^2b+ab^3+b^5+b^2 \\ a^4+a^2b+a+b^2 & 2a^3b+4ab^2+2b^4 & a^2b^2+ab^4+b^6+b^3 \end{bmatrix}, \\
M_8 &= \begin{bmatrix} a^6+2a^3+1 & 2a^4+4a^2b+2b^2 & a^2+2ab^2+b^4 \\ a^5+a^3b+a^2+b & 2a^3+2a^2b^2+2ab+2b^3 & ab^3+a+b^5+b^2 \\ a^4+2a^2b+b^2 & 2a^2+4ab^2+2b^4 & b^6+2b^3+1 \end{bmatrix}, \\
M_9 &= \begin{bmatrix} a^6+2a^3+a^2b^2 & 2a^4+2a^2b+2ab^3+2a & a^2+b^4+2b \\ a^5+2a^2+ab^2 & a^4b+a^3+a^2b^2+ab^4+2ab+b^3+1 & a^2b+b^5+2b^2 \\ a^4+2a+b^2 & 2a^3b+2ab^2+2b^4+2b & a^2b^2+b^6+2b^3 \end{bmatrix}.
\end{aligned}$$

Calculating the characteristic polynomials x^3+Bx^2+Cx+D of gadgets 4, 7, 8, and 9, we get

$$\begin{aligned}
B_4 &= -(X+Y+1) \\
C_4 &= (X^2+X+Y)(X-1) \\
D_4 &= -X(X-1)^3 \\
B_7 &= -(-2X^3+4X^2+2XY+2X+Y^2+2Y) \\
C_7 &= (X-1)(X^5-4X^4-X^3Y+6X^3+7X^2Y+4X^2+4XY^2+5XY+X+Y^3+2Y^2+Y) \\
D_7 &= -(X-1)^3(2X+Y)(X^4-X^3+X^2Y+3X^2+2XY+X+Y^2+Y) \\
B_8 &= -(-2X^3+2X^2+2X+Y^2+4Y+2) \\
C_8 &= (X-1)^2(X^4-2X^3+2X^2+4XY+6X+2Y^2+4Y+1) \\
D_8 &= -2(X-1)^6X(X+1) \\
B_9 &= -(3X^2+XY+2X+Y^2+3Y+1) \\
C_9 &= (X-1)(X^5-3X^4-2X^3Y-X^3+4X^2Y+7X^2+2XY^2+6XY+4X+Y^3+4Y^2+4Y) \\
D_9 &= -(X-1)^3(X+Y+1)(X^4-2X^3+X^2+2XY+4X+Y^2+2Y)
\end{aligned}$$

Suppose $X \neq 1$, $4X^3 \neq Y^2$ (equivalently, $a^3 \neq b^3$), and it is not the case that both $X = -1$ and $Y = 0$. For any real-valued setting of X and Y compatible with these constraints, we will see that at least one of these four binary recursive gadgets satisfies the requirements of Theorem 11 (the only exception is $(X, Y) = (0, -1)$, but by Lemma 22 any such problem is equivalent to $\mathrm{Hol}(0, -1)$ which is known to be #P-hard - see Chapter 2 or [10, 25]). To verify that gadget j satisfies condition 1 of Theorem 11, we apply Lemma 24 and check that $D_j(B_j^3 D_j - C_j^3) \neq 0$ (note that the norm and conjugate disappear from the test since we are only considering real valued X and Y). By Lemma 27, gadget 4 satisfies condition 2 because $\det[s, M_4 s, M_4^2 s] = (X - 1)^4(b^3 - a^3) \neq 0$. However, $\det[s, M_7 s, M_7^2 s] = (X - 1)^5(b^3 - a^3)(X^2 + X + Y)(X + Y + 1)$, $\det[s, M_8 s, M_8^2 s] = (X - 1)^5(b^3 - a^3)(X^2Y + 4X^2 + 2XY + Y^2 + Y)$, and $\det[s, M_9 s, M_9^2 s] = (X - 1)^6(b^3 - a^3)(X + 1)(Y + 2)$, so these are zero for some settings of X and Y. We summarize the essential observations in terms of (X, Y) coordinates as follows.

$$
\begin{aligned}
X = 1 &\iff ab = 1 \\
4X^3 = Y^2 &\iff a^3 = b^3 \\
X = 0 \wedge Y = -1 &\iff (a = 0 \wedge b^3 = -1) \vee (a^3 = -1 \wedge b = 0) \\
X = -1 \wedge Y = 0 &\iff a^6 = 1 \wedge ab = -1 \\
D_4(B_4^3 D_4 - C_4^3) \neq 0 &\implies \text{Gadget 4 satisfies Theorem 11} \\
D_7(B_7^3 D_7 - C_7^3)(X^2 + X + Y)(X + Y + 1) \neq 0 &\implies \text{Gadget 7 satisfies Theorem 11} \\
D_8(B_8^3 D_8 - C_8^3)(X^2Y + 4X^2 + 2XY + Y^2 + Y) \neq 0 &\implies \text{Gadget 8 satisfies Theorem 11} \\
D_9(B_9^3 D_9 - C_9^3)(X + 1)(Y + 2) \neq 0 &\implies \text{Gadget 9 satisfies Theorem 11}
\end{aligned}
$$

If we can verify that at least one of the 8 conditions on the left hand side holds for any real-valued setting of X and Y then we are done. Note that a disjunction of the left hand sides is a semi-algebraic set, and as such, is decidable by Tarski's Theorem [28]. Using symbolic computation via the CYLINDRICALDECOMPOSITION function from Mathematica™, we verify that for any $X, Y \in \mathbb{R}$, at least one of the eight conditions above is true. □

Now we can assume that $X \notin \mathbb{R}$ or $Y \notin \mathbb{R}$, and we deal with the remaining three conditions. In general, the presence of restrictions such as these three conditions make the process of finding a suitable recursive gadget much easier. For example, gadget 12 was found for the condition $X^2 + X + Y = 0$ by making the symbolic substitution $Y = -X - X^2$ and examining the resulting (factored) ratio between the determinant and squared trace for all gadgets of a limited size. In the presence of this substitution, the determinant and trace line up *just right* for proving $\#\mathrm{P}$-hardness. This is only one of many instances where such an algebraic coincidence occured, and a fundamental explanation for why this happens is unknown at this point in time. Note that if $X^2 + X + Y = 0$ then $X \in \mathbb{R}$ implies $Y \in \mathbb{R}$. So in the following lemma, the assumption that X and Y are not both real numbers amounts to $X \notin \mathbb{R}$.

Lemma 28. *If $X^2 + X + Y = 0$ and $X \notin \mathbb{R}$ then the transition matrix of unary gadget 12 has nonzero eigenvalues with distinct norm.*

Proof. Let M_{12} be the transition matrix for unary gadget 12.

$$M_{12} = \begin{bmatrix} a^6 + 2a^4b + a^3 + 3a^2b^2 + ab^4 & a^4 + 3a^2b + 2ab^3 + b^5 + b^2 \\ a^5 + 2a^3b + a^2 + 3ab^2 + b^4 & a^4b + 3a^2b^2 + 2ab^4 + b^6 + b^3 \end{bmatrix}$$

Then the determinant is the polynomial $X^6 - 6X^5 - X^4Y + 16X^4 + 11X^3Y - 10X^3 + 5X^2Y^2 - 7X^2Y - X^2 + XY^3 - 4XY^2 - 3XY - Y^3 - Y^2$. *Amazingly*, with the condition $X^2 + X + Y = 0$, this polynomial factors into $-X^2(X-1)^5$. Similarly, the trace, which is $-2X^3 + 6X^2 + 3XY + Y^2 + Y$, also factors into $X(X-1)^3$. Since $\det(M_{12}) \neq 0$, $\operatorname{tr}(M_{12}) \neq 0$, and $(1-X)\det(M_{12}) = \operatorname{tr}(M_{12})^2$, we know $\operatorname{Arg}(\det(M_{12})) \neq \operatorname{Arg}(\operatorname{tr}(M_{12})^2)$ and conclude by Lemma 23 that the eigenvalues of M_{12} (which are nonzero) have distinct norm. □

Similarly, gadgets 11 and 13 can be used to deal with the $X = -1$ condition. Again, we make the substitution $X = -1$ and examine the resulting quantity $\frac{\det(M)}{\operatorname{tr}^2(M)}$ for different gadgets M in order to select these for the proof. Recall that any setting of a and b such that $X = -1$ and $Y = \pm 2\mathfrak{i}$ is tractable by Theorem 13.

Lemma 29. *If $X = -1$, $Y \neq \pm 2\mathfrak{i}$, and $Y \notin \mathbb{R}$, then either gadget 11 or gadget 13 has a transition matrix with nonzero eigenvalues with distinct norm.*

Proof. Suppose $|Y| \neq 2$, $Y \notin \mathbb{R}$, and let M_{11} be the transition matrix for unary gadget 11. Well, $\det(M_{11}) = -2Y \neq 0$ and $\operatorname{tr}(M_{11}) = Y - 2$, so $\overline{\operatorname{tr}(M_{11})} \cdot \det(M_{11}) - \operatorname{tr}(M_{11}) \cdot |\det(M_{11})| = -(\overline{Y} - 2)(2Y) - (Y - 2) \cdot |-2Y| = 4Y - 2|Y|^2 - 2Y \cdot |Y| + 4|Y| = -2(|Y| - 2)(|Y| + Y) \neq 0$. Thus $\overline{\operatorname{tr}(M_{11})} \cdot \det(M_{11}) \neq \operatorname{tr}(M_{11}) \cdot |\det(M_{11})|$ and by Lemma 23, M_{11} has (nonzero) eigenvalues with distinct norm.

Now suppose $|Y| = 2$, but $Y \neq \pm 2\mathrm{i}$ and $Y \notin \mathbb{R}$. Let M_{13} be the transition matrix for unary gadget 13.

$$M_{13} = \begin{bmatrix} a^6 + 3a^3 + 3ab + b^3 & a^4 + 2a^2b + ab^3 + a + b^5 + 2b^2 \\ a^5 + a^3b + 2a^2 + 2ab^2 + b^4 + b & a^3 + 3ab + b^6 + 3b^3 \end{bmatrix}.$$

Then $\det(M_{13}) = -16Y \neq 0$. Using the substitution $\overline{Y} = 4/Y$,

$$\begin{aligned} \operatorname{tr}(M_{13})^2\overline{\det(M_{13})} - \overline{\operatorname{tr}(M_{13})}^2 \det(M_{13}) &= -16(Y - \overline{Y}) \cdot \\ &\quad (-16 + 8Y\overline{Y} + 8Y^2\overline{Y} + Y^3\overline{Y} + 8Y\overline{Y}^2 + Y^2\overline{Y}^2 + Y\overline{Y}^3) \\ &= \frac{-64(Y - \overline{Y})(4 + Y^2)(4 + 8Y + Y^2)}{Y^2} \\ &\neq 0. \end{aligned}$$

Hence $\operatorname{tr}(M_{13})^2\overline{\det(M_{13})} \neq \overline{\operatorname{tr}(M_{13})}^2 \det(M_{13})$ and the eigenvalues of M_{13} (which are nonzero) have distinct norm by Lemma 23. $\square$

The condition $4(X - 1)^2(X + 1) = (Y + 2)^2$ seemed somewhat resilient to individual unary recursive gadgets; no single gadget seemed to single-handedly prove #P-hardness in this setting. Nevertheless, by using a second Eigenvalue Shifted Pair, at least we can reduce it to simpler conditions. This particular ESP was selected so that the remaining conditions would have Y appear only as a linear term.

Lemma 30. *Suppose* $4(X - 1)^2(X + 1) = (Y + 2)^2$*. Then either unary gadget 13 or unary gadget 14 has nonzero eigenvalues with distinct norm, unless either* $X^3 + 2X^2 + X + 2Y = 0$*, or* $X^3 + 4X^2 + 2Y - 1 = 0$*, or both* $X, Y \in \mathbb{R}$.

Proof. Assume that $X^3+2X^2+X+2Y \neq 0$, $X^3+4X^2+2Y-1 \neq 0$, and it is not the case that both $X, Y \in \mathbb{R}$. Note that $X \notin \{0,1\}$ since otherwise $Y \in \mathbb{R}$ and we know that X and Y are not both real. The transition matrix for gadget 14 is

$$M_{14} = \begin{bmatrix} a^6+3a^3+a^2b^2+ab+b^3+1 & a^4+2a^2b+ab^3+a+b^5+2b^2 \\ a^5+a^3b+2a^2+2ab^2+b^4+b & a^3+a^2b^2+ab+b^6+3b^3+1 \end{bmatrix}$$

so $M_{14} = M_{13}+(X-1)^2 I$, and the eigenvalue shift is nonzero. Now, $\det(M_{13}) = (X-1)^3(X^3+2X^2+X+2Y) \neq 0$ and note that $\operatorname{tr}(M_{13}) = -2X^3+6X+Y^2+4Y$ simplifies to $\operatorname{tr}(M_{13}) = -2X^3+6X+Y^2+4Y-(Y+2)^2+4(X-1)^2(X+1) = 2X(X-1)^2$ using the fact that $4(X-1)^2(X+1) = (Y+2)^2$.

Similarly, $\det(M_{14}) = \det(M_{14})+(X-1)^2(4(X-1)^2(X+1)-(Y+2)^2) = (X-1)^3(X^3+4X^2+2Y-1) \neq 0$. Furthermore $\operatorname{tr}[M_{13}]^2-4\det(M_{13}) = 4X^2(X-1)^4-4(X-1)^3(X^3+2X^2+X+2Y) = -4(X-1)^3(3X^2+X+2Y)$. If this is zero, then substituting $Y = (-3X^2-X)/2$ into $(Y+2)^2-4(X-1)^2(X+1) = 0$ we get $X(X-1)^2(9X+8) = 0$ and $X \in \mathbb{R}$, with $Y \in \mathbb{R}$ as a direct consequence. Corollary 3 implies that either gadget 13 or gadget 14 has nonzero eigenvalues of distinct norm, unless $\operatorname{tr}(M_{13}) = r(X-1)^2$ and $\det(M_{13}) = s(X-1)^4$ for some $r, s \in \mathbb{R}$. But then $2X(X-1)^2 = r(X-1)^2$ hence $X = r/2 \in \mathbb{R}$, and $(X-1)^3(X^3+2X^2+X+2Y) = s(X-1)^4$ hence $Y = (-X^3-2X^2-X+s(X-1))/2 \in \mathbb{R}$. A contradiction. ☐

Now we take advantage of another interesting coincidence mentioned earlier; two gadgets with transition matrices that have identical trace. By this point, a computer program had been written to more thoroughly investigate ESPs and *trace coincidences*, both by listing all such pairs and by displaying them as a "coincidence graph": a graph drawing where every gadget is represented as a vertex and every ESP and trace coincidence is represented as an edge.

Lemma 31. *If $X^2+X+Y \neq 0$, $4(X-1)^2(X+1) = (Y+2)^2$, and either $X^3+2X^2+X+2Y = 0$ or $X^3+4X^2+2Y-1 = 0$, then the transition matrix of unary gadget 15 or unary gadget 16 has nonzero eigenvalues with distinct norm, unless both $X, Y \in \mathbb{R}$.*

Proof. The transition matrices for gadget 15 and gadget 16 are

$$M_{15} = \begin{bmatrix} a^6 + a^4 b + 2a^3 + a^2 b^2 + 2ab + b^3 & a^4 + 3a^2 b + 2ab^3 + b^5 + b^2 \\ a^5 + 2a^3 b + a^2 + 3ab^2 + b^4 & a^3 + a^2 b^2 + ab^4 + 2ab + b^6 + 2b^3 \end{bmatrix},$$

$$M_{16} = \begin{bmatrix} a^6 + a^4 b + 2a^3 + a^2 b^2 + 2ab + b^3 & a^4 + a^3 b^2 + a^2 b + 2ab^3 + a + b^5 + b^2 \\ a^5 + 2a^3 b + a^2 b^3 + a^2 + ab^2 + b^4 + b & a^3 + a^2 b^2 + ab^4 + 2ab + b^6 + 2b^3 \end{bmatrix}.$$

Let $T = X^3+2X^2+X+2Y$, $U = X^3+4X^2+2Y-1$, and let R denote $(Y+2)^2-4(X-1)^2(X+1)$. Note that regardless of whether $T = 0$ or $U = 0$, $X \in \mathbb{R}$ implies $Y \in \mathbb{R}$, so we will assume $X \notin \mathbb{R}$. The main diagonals of M_{15} and M_{16} are identical, so $\mathrm{tr}(M_{15}) = \mathrm{tr}(M_{16})$. Furthermore, if $T = 0$ then $\mathrm{tr}(M_{15}) = \mathrm{tr}(M_{15}) - R - (X-1)T/2 = -X(X-1)^3/2 \neq 0$. If $U = 0$ then $\mathrm{tr}(M_{15}) = \mathrm{tr}(M_{15}) - R - (X-1)U/2 = -(X-1)(X^3-1)/2$, and we claim this is nonzero as well. Otherwise, $X^3 = 1$ then since $U = 0$, $Y = -2X^2$ and using $(Y+2)^2 = 4(X-1)^2(X+1)$ we get $(X^2-1)^2 = (X-1)^2(X+1)$ i.e. $(X-1)^2(X+1)^2 = (X-1)^2(X+1)$ together with $X \notin \mathbb{R}$ we get a contradiction. Next, $\det(M_{16}) = (X-1)^3(X+1)(X^2+X+Y)$ and $\det(M_{15}) = \det(M_{15}) - R(X-1)^2 = (X-1)^3(X+4)(X^2+X+Y)$, so these are both nonzero. If both M_{15} and M_{16} have eigenvalues with equal norm, then applying Lemma 23 twice, $\mathrm{Arg}(\det(M_{15})) = \mathrm{Arg}(\mathrm{tr}(M_{15})^2) = \mathrm{Arg}(\mathrm{tr}(M_{16})^2) = \mathrm{Arg}(\det(M_{16}))$. However, this would imply $\mathrm{Arg}(X+4) = \mathrm{Arg}(X+1)$ and $X \in \mathbb{R}$, so we conclude that either M_{15} or M_{16} has nonzero eigenvalues with distinct norm. □

Now we sum up the result of these lemmas.

Theorem 15. *Suppose $a, b \in \mathbb{C}$ such that $X \neq 1$, $4X^3 \neq Y^2$, and $(X,Y) \neq (-1,0)$. Then the problem $\mathrm{Hol}(a,b)$ is #P-hard.*

Proof. Under these assumptions, if X and Y are both real then $\mathrm{Hol}(a,b)$ is #P-hard by Lemma 14, so assume either X or Y is not real. For any such a and b, we know by Lemma 26 that either gadget 10 or 11 has a transition matrix with nonzero eigenvalues of distinct norm, except in the following cases, where we will use other gadgets to fill this requirement.

1. $X^2 + X + Y = 0$.

2. $X = -1$.

3. $4(X-1)^2(X+1) = (Y+2)^2$.

If $X^2 + X + Y = 0$ then $X \notin \mathbb{R}$, lest X and Y be real, so Lemma 28 implies that unary gadget 12 has a transition matrix of the required form. If $X = -1$, then Lemma 29 indicates that either gadget 11 or gadget 13 satisfies the requirement, unless $Y = \pm 2\mathrm{i}$. Now we may assume $X^2 + X + Y \neq 0$, so by Lemmas 30 and 31 if $4(X-1)^2(X+1) = (Y+2)^2$ then either unary gadget 13, 14, 15, or 16 has a suitable transition matrix. In any case, we have a unary recursive gadget whose transition matrix has nonzero eigenvalues of distinct norm. Hence we are done by Theorem 12 and Lemma 20. □

3.3.4 Problems that are tractable for planar graphs but $\#\mathrm{P}$-hard in general

Recall COUNTING VERTEX COVERS is $\#\mathrm{P}$-hard on 3-regular planar graphs, and note that all gadgets discussed are planar (in the case of gadget 8, each iteration can be redrawn in a planar way by "going around" the previous iterations; see Figure 3.1(d)). Thus, all of the hardness results proved so far still apply even when the input graphs are restricted to planar graphs. There are, however, some problems that are $\#\mathrm{P}$-hard in general, yet polynomial time computable when the input is restricted to planar graphs. This class of problems corresponds exactly with the problems we still need to resolve at this point, i.e. when $4X^3 = Y^2$ but $X \notin \{0, \pm 1\}$. As observed in [9], sometimes a smaller transition matrix can be used when extra symmetry occurs in the signatures of a holant problem. In terms of matrices, there is no difference between interpolation techniques for lower dimensional iterations and for higher dimensional iterations with such extra symmetries. The next Lemma works along these lines, and also abstracts how the signatures are initially produced (any polynomial time algorithm suffices).

Lemma 32. *Fix a finite generator set $\mathcal{G}$ and a finite recognizer set $\mathcal{R}$, and suppose that there is an algorithm $\mathcal{A}$ that, on input $n \in \mathbb{Z}^+$, has a runtime polynomial in n and outputs a set of n binary starter gadgets in the context of $\#\mathcal{G} \mid \mathcal{R}$. Further assume that these starter gadgets have pairwise* *linearly independent signatures of the form* $[c, d, c]$ *for various* $c, d \in \mathbb{C}$*. Then for any* $x, y \in \mathbb{C}$*,* $\#\mathcal{G} \cup \{[x, y, x]\} \mid \mathcal{R} \leq_{\mathrm{T}}^{\mathrm{P}} \#\mathcal{G} \mid \mathcal{R}$*.*

Proof. Assume we have oracle access to querries of the form $\#\mathcal{G} \mid \mathcal{R}$, and we are given a bipartite signature grid Ω for the holant problem $\#\mathcal{G} \cup \{[x, y, x]\} \mid \mathcal{R}$, with underlying graph $G = (V, E)$. Let $Q \subseteq V$ be the set of vertices labeled with generator $[x, y, x]$, and let $n = |Q|$. Let $\{N_0, N_1, \ldots, N_{n+1}\}$ be the set of starter gadgets given by $\mathcal{A}$ on input $n + 2$, and denote the signature of N_k by $[X_k, Y_k, X_k]$. At most one such Y_k can be zero, so we may assume that $Y_k \neq 0$ for all $0 \leq k \leq n$. If we replace every vertex $v \in Q$ with a copy of N_k, we obtain an instance of $\#\mathcal{G} \mid \mathcal{R}$ (note that the correct bipartite signature structure is preserved), and we denote this new signature grid by Ω_k. Although $\mathrm{Holant}_{\Omega_k}$ is a sum of exponentially many terms, each nonzero term has the form $c_i X_k^i Y_k^{n-i}$ for some i, and for some $c_i \in \mathbb{C}$ which does not depend on X_k or Y_k. Then the sum can be rewritten as

$$\mathrm{Holant}_{\Omega_k} = \sum_{0 \leq i \leq n} c_i X_k^i Y_k^{n-i}.$$

Since each signature grid Ω_k is an instance of $\#\mathcal{G} \mid \mathcal{R}$, $\mathrm{Holant}_{\Omega_k}$ can be solved exactly using the oracle. Carrying out this process for every $k \in \{0, 1, \ldots, n\}$, we arrive at a linear system where the c_i values are the unknowns.

$$\begin{bmatrix} \mathrm{Holant}_{\Omega_0} \\ \mathrm{Holant}_{\Omega_1} \\ \vdots \\ \mathrm{Holant}_{\Omega_n} \end{bmatrix} = \begin{bmatrix} X_0^0 Y_0^n & X_0^1 Y_0^{n-1} & \cdots & X_0^n Y_0^0 \\ X_1^0 Y_1^n & X_1^1 Y_1^{n-1} & \cdots & X_1^n Y_1^0 \\ \vdots & \vdots & \ddots & \vdots \\ X_n^0 Y_n^n & X_n^1 Y_n^{n-1} & \cdots & X_n^n Y_n^0 \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_n \end{bmatrix}.$$

This is easily rewritten as

$$\begin{bmatrix} Y_0^{-n} \cdot \mathrm{Holant}_{\Omega_0} \\ Y_1^{-n} \cdot \mathrm{Holant}_{\Omega_1} \\ \vdots \\ Y_n^{-n} \cdot \mathrm{Holant}_{\Omega_n} \end{bmatrix} = \begin{bmatrix} X_0^0 Y_0^0 & X_0^1 Y_0^{-1} & \cdots & X_0^n Y_0^{-n} \\ X_1^0 Y_1^0 & X_1^1 Y_1^{-1} & \cdots & X_1^n Y_1^{-n} \\ \vdots & \vdots & \ddots & \vdots \\ X_n^0 Y_n^0 & X_n^1 Y_n^{-1} & \cdots & X_n^n Y_n^{-n} \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_n \end{bmatrix}.$$

The matrix above has entry $(X_r/Y_r)^c$ at row r and column c. Due to pairwise linear independence of $[X_r, Y_r, X_r]$, X_r/Y_r is distinct for $0 \leq r \leq n$. Hence this is a Vandermonde system of full rank, and we can solve it for the c_i values. With these values in hand, we calculate $\mathrm{Holant}_\Omega = \sum_{0 \leq i \leq n} c_i X^i Y^{n-i}$ directly, completing the reduction. $\square$

The construction consists of a single-vertex binary starter gadget S (Figure 3.1(a)) concatentated with zero or more iterations of a binary recursive gadget M (no finisher gadget is used here). We will use this to focus on problems where $a = b$ (which is a subset of $4X^3 = Y^2$). More precisely, $\mathcal{F}$-gate N_0 is defined to be S, and for all integers $i > 0$, $\mathcal{F}$-gate N_i is defined by merging the trailing edges of M with the leading edges of N_{i-1}. The assumption $a = b$ causes an extra degree of symmetry, so let's first understand how this effects the signatures of $\mathcal{F}$-gates produced.

Let A be any $\mathcal{F}$-gate where $\mathcal{F} = \{[a, 1, b], =_k\}$, and consider some $\{0, 1\}$-assignment σ to its dangling edges. Then the value of A under σ is some polynomial in a and b with integer coefficients: call it $p(a, b)$. Now, the value of A under the complement assignment σ' to the dangling edges is $p(b, a)$. This reason is that for every assignment ρ to the internal edges of A under σ, there is a corresponding complement assignment ρ' to the internal edges of A under σ', and the evaluation A under σ' and ρ' is the same as σ and ρ, only with the roles of a and b reversed. If $a = b$, this implies that $\mathcal{F}$-gate signatures are invariant under complementation of $\{0, 1\}$-assignments to the dangling edges.

In particular, if $a = b$ then all N_i have signatures of the form $[a_0, a_1, a_0]$, and the transition matrix of M is of the form $\begin{bmatrix} b_0 & b_1 & b_2 \\ b_3 & b_4 & b_3 \\ b_2 & b_1 & b_0 \end{bmatrix}$. The extra symmetry causes redundancy, so we denote the signature of N_i with just the first two entries as a column vector. The signature of N_i is then given by $(M')^i[a, 1]^{\mathrm{T}}$, where $M' = \begin{bmatrix} b_0 + b_2 & b_1 \\ 2b_3 & b_4 \end{bmatrix}$. The fact that this is represented by a 2 by 2 transition matrix M' implies a result analagous to Lemma 21.

Corollary 4. *Let* $S = \begin{bmatrix} s_0 \\ s_1 \\ s_0 \end{bmatrix}$ *be a binary starter gadget and* $M = \begin{bmatrix} m_0 & m_1 & m_2 \\ m_3 & m_4 & m_3 \\ m_2 & m_1 & m_0 \end{bmatrix}$ *be a nonsingular binary recursive gadget, both in the context of* $\#[a,1,a] \mid \{=_1, =_2, \ldots\}$. *Let* $M' = \begin{bmatrix} m_0 + m_2 & m_1 \\ 2m_3 & m_4 \end{bmatrix}$ *and* $S' = \begin{bmatrix} s_0 \\ s_1 \end{bmatrix}$. *Assume* $\frac{M'}{\det(M')}$ *is acyclic (equivalently, the ratio of the eigenvalues of* M' *is not a root of unity), and* S' *is not a column eigenvector of* M'. *Then* $\{M^i S\}_{i \geq 0}$ *is a series of pairwise linearly independent signatures of the form* $[c, d, c]$ *for various* $c, d \in \mathbb{C}$. *In particular, for any* $x, y \in \mathbb{C}$, $\#\mathcal{G} \cup \{[x, y, x]\} \mid \mathcal{R} \leq_T^P \#\mathcal{G} \mid \mathcal{R}$.

Proof. The value of $[a, 1, a]$ and any EQUALITY signature remains unchanged by taking the complement of a given assignment to the inputs, so it follows that any $\mathcal{F}$-gate in the context of $\#[a,1,a] \mid \{=_1, =_2, \ldots\}$ also has a signature which is not effected by complementation of the assignment to the dangling edges. In particular, any binary $\mathcal{F}$-gate has a signature of the form $[c, d, c]$ for some $c, d \in \mathbb{C}$. Furthermore, $M^i S = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \end{bmatrix} (M')^i S'$ for all $i \geq 0$, so it suffices to show that all signatures in the series $\{(M')^i S'\}_{i \geq 0}$ are pairwise linearly independent. Diagonalizing M', we have $(M')^i = T^{-1} D^i T$ for some diagonal matrix D, where the rows of T are the row eigenvectors of M'. By assumption S' is not a column eigenvector of M', so by Lemma 27, S' is not orthogonal to any row eigenvector of M'. Also, TS is a vector for which both entries are nonzero. Since the diagonal entries of D are nonzero and have a ratio which is not a root of unity, we know that pairwise linear independence holds for $\{D^i TS\}_{i \geq 0}$, and also for $\{(M')^i S'\}_{i \geq 0}$. Since both gadgets are labeled with a finite number of signatures, they exist in the context of a problem $\#[a, 1, a] \mid \mathcal{R}'$, where $\mathcal{R}' \subset \{=_1, =_2, \ldots\}$ is finite, and we are done by Lemma 32. □

Now we use gadget 4 and a single-vertex starter gadget to get the interpolation result.

Lemma 33. *Let* M *be gadget 4 and* S *be the single vertex starter gadget in the context of* $\#[a, 1, a] \mid [1, 0, 0, 1]$. *If* $a \in \{0, \pm 1, \pm \mathrm{i}\}$ *then* $\#[a, 1, a] \mid [1, 0, 0, 1]$ *is in* FP. *Otherwise,*

$\{M^iS\}_{i\geq 0}$ *is a series of pairwise linearly independent signatures of the form* $[x, y, x]$*, and* $\#[a, 1, a] \mid [1, 0, 0, 1]$ *is* #P-hard.

Proof. If $a \in \{0, \pm 1, \pm \mathrm{i}\}$ then this is in FP by Theorem 13. First assume $a \notin \mathbb{R}$ and $a \neq \pm\mathrm{i}$. We will use binary recursive gadget 4 together with Corollary 4, and we calculate $M' = \begin{bmatrix} a(a^2+1) & 2a \\ 2a^2 & a^2+1 \end{bmatrix}$. Now, $\det(M') = a(a-1)^2(a+1)^2$ and $\mathrm{tr}(M') = (a+1)(a^2+1)$ are both nonzero under our assumptions. It can be verified (using the RESOLVE function of Mathematica™) that $\mathrm{tr}(M')|\det(M')| \neq \overline{\mathrm{tr}(M')}\det(M')$ provided that $a \notin \mathbb{R}$, so by Lemma 23, the eigenvalues of M' have distinct norm. Also, $M' \begin{bmatrix} a \\ 1 \end{bmatrix} = (a+1) \begin{bmatrix} a(a^2-a+2) \\ (2a^2-a+1) \end{bmatrix}$, so $[a, 1]^{\mathrm{T}}$ is not an eigenvector of M'. We conclude by Corollary 4 that we can efficiently produce the required set of signatures, and interpolate all signatures of the form $[x, y, x]$. Since $\#[0, 1, 0] \mid [0, 1, 1, 0]$ is known to be #P-hard [9] and equivalent to $\#[-\omega(\omega^2-2)/3, 1, -\omega(\omega^2-2)/3] \mid [1, 0, 0, 1]$ by a holographic reduction (where ω is the principal 12^{th} root of unity), we conclude that $\#[a, 1, a] \mid [1, 0, 0, 1]$ is #P-hard.

Now assume $a \in \mathbb{R} - \{0, \pm 1\}$, and a querry to the CYLINDRICALDECOMPOSITION function of Mathematica™ verifies that all of the conditions of Lemma 6 hold for binary recursive gadget 4 together with the single vertex starter gadget. Again, we can efficiently produce the required set of signatures, interpolate all signatures of the form $[x, y, x]$, and $\#[a, 1, a] \mid [1, 0, 0, 1]$ is #P-hard for the same reasons as above. □

Finally, we perform some holographic reductions to generalize Lemma 33.

Lemma 34. *Suppose that* $4X^3 = Y^2$*. If further* $X \in \{0, \pm 1\}$*, then* $\mathrm{Hol}(a, b)$ *is in* FP*; otherwise we can efficiently simulate a set of pairwise linearly independent signatures of the form* $[x, y, x]$*, and* $\mathrm{Hol}(a, b)$ *is* #P-hard.

Proof. If $X = 0$ then $X = Y = 0$ and the problem is in P by Theorem 13. Otherwise, $X \neq 0$, let $\omega = ba^{-1}$, and applying a holographic reduction to $\#[a, 1, b] \mid [1, 0, 0, 1]$ under the basis $\begin{bmatrix} \omega & 0 \\ 0 & \omega^2 \end{bmatrix}$ we see that the problem $\#[a, 1, b] \mid [1, 0, 0, 1]$ is equivalent to $\#[\omega^2 a, 1, \omega b] \mid$

$[1, 0, 0, 1]$, because $\omega^3 = b^3 a^{-3} = 1$. Since $\omega^2 a = \omega b$, we can apply Lemma 33 and the problem $\#[a, 1, b] \mid [1, 0, 0, 1]$ is in FP if $ab = \omega^2 a \cdot \omega b = \pm 1$ and #P-hard otherwise. $\square$

Given this, we have proved Theorem 9.

Chapter 4

A dichotomy for k-regular graphs with a symmetric real-valued edge function

In this chapter we adapt algebraic symmetrization to the class of holant problems $\#[x_0, x_1, x_2] \mid =_k$, proving a complexity dichotomy theorem for all $k \geq 1$ and for a particular subset of $x_0, x_1, x_2 \in \mathbb{C}$ which contains all $x_0, x_1, x_2 \in \mathbb{R}$. These problems can be viewed as COUNTING WEIGHTED H-HOMOMORPHISMS from an arbitrary k-regular input graph G to the weighted two vertex graph defined by $H = \begin{bmatrix} x_0 & x_1 \\ x_1 & x_2 \end{bmatrix}$. In Chapter 5, we extend this to all $x_0, x_1, x_2 \in \mathbb{C}$.

4.1 Background and notation

In Chapter 3 we managed to find a way to drastically reduce the dependence of symbolic computation and extend the theorem of [10] to all complex valued functions h. This was accomplished by a new method of higher dimensional iterations combined with finisher gadgets for gadget construction, Eigenvalue Shifted Pairs, and by finding a new polynomial expression for Holant_Ω for 3-regular signature grids Ω.

In this chapter we find a corresponding polynomial expression for Holant_Ω on k-regular signature grids, where $X = ab$ and $Y = a^k + b^k$. The dichotomy will be for problems of the form $\#[a, 1, b] \mid =_k$, for any $k \geq 1$ and any $a, b \in \mathbb{C}$ such that $X, Y \in \mathbb{R}$. Note this includes are real-valued a and b as a subcase.

The situation with an arbitrary degree k requirement creates at least two additional difficulties. The first is that with infinitely many k, it seems likely that we will need an infinite number of collections of gadgets, one for each k. The statement involving a variable k cannot be stated for a semi-algebraic set. If we follow this strategy, we can hope to prove at best a small number of concretely given constants k; the symbolic computation from the decidability of semi-algebraic sets will soon overwhelm this attempt, as k increases.

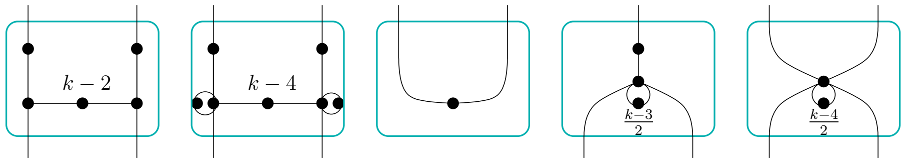
The second difficulty is presented by the parity of k. It turns out that for even degree k, the proof from the previous chapter cannot be directly extended. The technical reason is that it is not possible to construct an $\mathcal{F}$-gate with an odd number of dangling edges in a regular graph of even degree. It is not possible to construct starter and finisher gadgets as described in Chapter 3.

We overcome the first difficulty by fortuitously choosing a universal set of gadget families for all k, and showing that collectively they always work. Here the substitution $X = ab$ and $Y = a^k + b^k$ is shown to essentially eliminate all symbolic dependence on k. We overcome the second difficulty by changing the strategy of constructing all unary signatures to constructing all binary signatures of a certain kind. This set of binary signatures plays the virtual role of all unary signatures for our purposes, and this is enabled by the introduction of finisher gadgets with multiple leading edges. Our main theorem is as follows:

Theorem 16. *The holant problem* $\#[a, 1, b] \mid [1, 0, 0, 1]$ *is* $\#\mathrm{P}$-hard, *whether or not the input is restricted to planar graphs, for all* $a, b \in \mathbb{C}$ *such that* $X, Y \in \mathbb{R}$ *except in the following cases, for which the problem is in* FP.

1. $X = 1$.
2. $X = Y = 0$.
3. $X = -1$ *and* $Y = 0$.
4. $X = -1$, *k is even, and* $Y = \pm 2$
5. *The input is restricted to planar graphs and* $Y^2 = 4X^k$.

Throughout this chapter, we denote $X = ab$ and $Y = a^k + b^k$, and we assume that $X, Y \in \mathbb{R}$ and $a, b \in \mathbb{C}$. In all cases our gadgets have signature $[a, 1, b]$ assigned to the degree 2 vertices and signature $=_k$ assigned to the degree k vertices. We use S_i, M_i, and F_i to denote the (transition matrices



(a) Gadget M_1 (b) Gadget M_2 (c) Gadget S_1 (d) Gadget F_1 (e) Gadget F_2

Figure 4.1 Labels indicate the number of pairs of edges in parallel.

of the) gadgets displayed in Figures 4.1 and 4.3. We will also denote $\mathrm{Hol}_k(a, b) = \#[a, 1, b] \mid =_k$, and Pl-$\mathrm{Hol}_k(a, b)$ to denote $\#[a, 1, b] \mid =_k$ when restricted to planar graphs as input.

4.2 Interpolation technique

In this section we introduce the interpolation technique we will use in this chapter. We start with Lemma 19 from Chapter 3. Note that implicitly, the finisher gadgets are the 1-leading-edge variety.

Lemma 35. *Suppose that the following gadgets can be built using complex-valued signatures from a finite generator set $\mathcal{G}$ and a finite recognizer set $\mathcal{R}$.*

1. *A binary starter gadget with nonzero signature $s = [z_0, z_1, z_2]$.*
2. *A binary recursive gadget with nonsingular transition matrix M, for which $[z_0, z_1, z_2]^{\mathrm{T}}$ is not a column eigenvector of M^ℓ for any positive integer ℓ.*
3. *Three binary finisher gadgets with rank 2 matrices $F_1, F_2, F_3 \in \mathbb{C}^{2\times 3}$, where the intersection of the row spaces of F_1, F_2, and F_3 is trivial.*

Then for any $x, y \in \mathbb{C}$, $\#\mathcal{G} \cup \{[x, y]\} \mid \mathcal{R} \leq_{\mathrm{T}}^{\mathrm{P}} \#\mathcal{G} \mid \mathcal{R}$.

It will be more convenient to reframe condition 2 in terms of the eigenvalues of M. The proof of this is the same as before. Assume that we are using a nonsingular recursive gadget M and a starter gadget whose signature s is not orthogonal to any row eigenvector of M. Additionally assume that there exist eigenvalues α and β of M for which $\frac{\alpha}{\beta}$ is not a root of unity. Then we want to show that s is not a column eigenvector of M^ℓ for any positive integer ℓ (note that s is nonzero).

Writing out the Jordan Normal Form for M, we have $M^\ell s = T^{-1} D^\ell T s$, where (without loss of generality) D^ℓ has the form $\begin{bmatrix} \alpha^\ell & 0 & 0 \\ 0 & \beta^\ell & 0 \\ 0 & * & * \end{bmatrix}$. Let $t = Ts$ and write $t = \begin{bmatrix} c \\ d \\ e \end{bmatrix}$. The first two rows of T are row eigenvectors of M. Then s is not orthogonal to the first two rows of T, hence $c, d \neq 0$. If s were an eigenvector of M^ℓ for some positive integer ℓ, then $T^{-1} D^\ell T s = M^\ell s = \lambda s$ for some nonzero complex value λ ($\lambda \neq 0$ since M^ℓ is nonsingular), and $D^\ell t = T(\lambda s) = \lambda t$. But then $c\alpha^\ell = \lambda c$ and $d\beta^\ell = \lambda d$, which means $\frac{\alpha^\ell}{\beta^\ell} = 1$, contradicting the fact that $\frac{\alpha}{\beta}$ is not a root of unity.

We satisfy condition 3 by explicitly building finisher gadgets for all $k \geq 3$. Since in regular graphs with even degree it is impossible to build an $\mathcal{F}$-gate with an odd number of dangling edges, we will use 1-leading-edge finisher gadgets when k is odd and the 2-leading-edges variant when k is even. In all cases, the later type will be built in such a way that both leading edges are incident with the same vertex with signature $[1, 0, 0, 1]$. The fact that each of these finisher gadgets has a matrix where the middle row is all zeros follows from this, satisfying the definition of a multiple-leading-edge finisher gadget. The finisher gadgets were discovered by a process similar to the last chapter, but while attempting different generalizations of the gadget family to higher k. This required a by-hand computation of the transition matrices.

Lemma 36. *Suppose $k \geq 3$ is odd, $X \notin \{0, 1\}$, and $a^k \neq b^k$. Then F_1, $F_1 M_1$, and $F_1 M_1^2$ (see Figures 4.1(d) and 4.1(a)) are all rank 2 matrices and their row spaces have trivial intersection.*

Proof. Finisher gadget F_1 is given, and we build two more finisher gadgets F_1' and F_1'' using M_1 so that $F_1' = F_1 M_1$ and $F_1'' = F_1 M_1^2$. Since F_1 and M_1 both have full rank (note $\det(M_1) = X^{k-2}(X-1)^3$ and F_1 has a submatrix with determinant $X^{(k-3)/2}(X-1)$), it follows that F_1' and F_1'' also have full rank. To show that the row spaces of F_1, F_1' and F_1'' have trivial intersection, it suffices to show that the cross products of the row vectors of F_1, F_1', and F_1'' (which we denote by v, v', and v'' respectively) are linearly independent. (To see this, suppose u is a complex vector in the intersection of the row spaces of F_1, F_1', and F_1''. Then v, v', and v'' are all orthogonal to u, but since v, v', and v'' are linearly independent, they span the conjugate vector $\overline{u}$ which is then also orthogonal to u. This means $|u|^2 = u\overline{u} = 0$, and that $u = 0$.) Let N be the matrix which has as its rows, v', v', and v'' respectively. Then $\det(N) = 4X^{(5k-13)/2}(X-1)^7(a^k - b^k) \neq 0$. □

Now consider even $k \geq 4$. The construction is similar to the odd case, with two important differences: we now have 2 leading edges per finisher gadget and a recognizer vertex is internally incident to the leading edges instead of a generator vertex. Because of this, we will be interpolating recognizer signatures for even k. It may appear as though this causes a problem with the main construction, but for any such finisher gadget F_i that we construct, there will be a unique matrix $F \in \mathbb{C}^{2\times 3}$ such that $F_i = \begin{bmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 1 \end{bmatrix} F$. Thus, the interpolation technique still applies, but in the case of even k we end up with the reduction $\#\mathcal{G} \mid \mathcal{R} \cup \{[x,0,y]\} \leq_T^P \#\mathcal{G} \mid \mathcal{R}$ for any $x, y \in \mathbb{C}$.

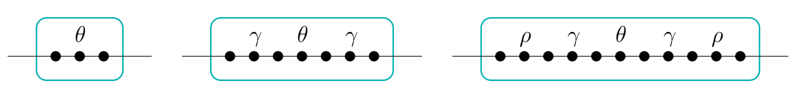
Lemma 37. *Suppose $k \geq 4$ is even and let F be the unique $\mathbb{C}^{2\times 3}$ matrix such that $F_2 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 1 \end{bmatrix} F$ (see Figure 4.1(e)). If $X \notin \{0,1\}$ and $a^k \neq b^k$ then F, FM_1, and FM_1^2 are all rank 2 matrices and their row spaces have trivial intersection.*

Proof. We get $F = \begin{bmatrix} a^{(k-4)/2} & 0 & 0 \\ 0 & 0 & b^{(k-4)/2} \end{bmatrix}$. Let $F' = FM_1$ and $F'' = FM_1^2$. Since F and M_1 both have full rank (as $X \notin \{0,1\}$), it follows that F' and F'' also have full rank. To show that the row spaces of F, F' and F'' have trivial intersection, we show that the cross products of the row vectors of F, F', and F'' are linearly independent. Let N be the matrix which has as its rows, the cross products of the rows of F, F', and F'' respectively. Then $\det(N) = 4X^{(5k-16)/2}(X-1)^4(a^k - b^k) \neq 0$. □

We will interpolate generator signatures of the form $[x,y]$ for odd k and recognizer signatures of the form $[x,0,y]$ for even k. In the case of odd k, connecting a vertex with signature $=_k$ to a vertex with signature $[x,y]$ and $k-3$ vertices with signature $[1,1]$ results in an $\mathcal{F}$-gate with signature $[x,0,y]$. This means that regardless of which variant of finisher gadget we apply, we can simulate any recognizer signature of the form $[x,0,y]$. With $[x,0,y]$ signatures in hand, we will simulate the generator signature $[0,1,1]$ directly. Thus we can reduce from COUNTING VERTEX COVERS on k-regular graphs, which is $\#\mathrm{P}$-hard by Lemma 48 in the Appendix of this chapter. The next Lemma can be viewed as a modification of Lemma 20 from Chapter 3 to accomodate binary signatures of the form $[x,0,y]$. The gadgets and the proof are conceptually identical. The only difference is the assumption that all arity-2 recognizers of the form $[x,0,y]$ are directly available, instead of having to simulate them by connecting a $[1,0,0,1]$ recognizer to a $[x,y]$ generator.

Lemma 38. *Suppose that* $(a,b) \in \mathbb{C}^2 - \{(a,b) : ab = 1\} - \{(0,0)\}$ *and let* $\mathcal{G}$ *and* $\mathcal{R}$ *be finite signature sets where* $[a,1,b] \in \mathcal{G}$, $=_k \in \mathcal{R}$, *and* $k \geq 3$. *Further assume that* $\#\mathcal{G} \mid \mathcal{R} \cup \{[x_i,0,y_i] : 0 \leq i < m\} \leq_{\mathrm{T}}^{\mathrm{P}} \#\mathcal{G} \mid \mathcal{R}$ *for any* $x_i, y_i \in \mathbb{C}$ *and* $m \in \mathbb{Z}^+$. *Then* $\#\mathcal{G} \cup \{[0,1,1]\} \mid \mathcal{R} \leq_{\mathrm{T}}^{\mathrm{P}} \#\mathcal{G} \mid \mathcal{R}$, *and* $\#\mathcal{G} \mid \mathcal{R}$ *is* $\#\mathrm{P}$-hard.

Proof. Since $\#[0,1,1] \mid =_k$ is $\#\mathrm{P}$-hard for $k \geq 3$, we only need to show how to simulate the generator signature $[0,1,1]$. Respectively, gadgets 1, 2, and 3 (Figure 4.2) can be used to simulate generator signatures $[b^{-1},1,2b]$, $[0,1,5/(2a)]$, and $[0,1,1]$ in the cases where $ab = 0$, $ab = -1$, and both $ab \neq 0$ and $ab \neq -1$ (when $ab = 0$, we assume without loss of generality that $a = 0$ and $b \neq 0$). To carry this out, we set $\theta = [b,0,b^{-1}]$ in gadget 1; $\theta = [1/(6a),0,-a/24]$ and $\gamma = [-3/a,0,a]$ in gadget 2; and $\theta = (ab+1)(1-ab)^{-1}[1,0,-a^2]$, $\gamma = [-a^{-2},0,b^{-1}(1+ab)^{-1}]$, and $\rho = (ab-1)^{-1}[-b,0,a]$ in gadget 3 - all unlabeled vertices are assigned the generator signature $[a,1,b]$. This results in a chain of reductions to simulate $[0,1,1]$ in all cases (i.e. gadget 2 simulates a signature to be used as a generator signature in gadget 1, which in turn simulates a generator signature to be used in gadget 3, and gadget 3 simulates $[0,1,1]$). ∎



(a) Gadget 1 (b) Gadget 2 (c) Gadget 3

Figure 4.2 Gadgets used to simulate the [0,1,1] signature

This gives us the following result.

Theorem 17. *If the following can be built using generator* $[a,1,b]$ *and recognizer* $=_k$ *where* $X \notin \{0,1\}$, $k \geq 3$, *and* $a^k \neq b^k$, *then* $\text{Pl-Hol}_k(a,b)$ *is* $\#\mathrm{P}$-hard*:*

1. A planar binary recursive gadget with nonsingular transition matrix M which has eigenvalues α and β such that $\frac{\alpha}{\beta}$ is not a root of unity.

2. A planar binary starter gadget with signature s which is not orthogonal to any row eigenvector of M.

4.3 Classification of problems

4.3.1 Tractable problems and algebraic symmetrization

Once we show that X and Y capture the complexity of the holant problems we are studying, the problem of proving tractability (or #P-hardness) becomes easier. To extend this idea from Chapter 3 to k-regular graphs for all $k \geq 3$, we need to consider a parity issue that arises when k is even and the number of vertices in the graph is odd. It is impossible to have an odd number of vertices when k is odd, and when the number of vertices in the graph is even the holant is a polynomial in X and Y. However, when the number of vertices is odd (which can only happen for even k), the holant is no longer a polynomial in X and Y; there is an extra factor $(a^{k/2} + b^{k/2})$. Nevertheless, we will still show directly that the complexity of $\mathrm{Hol}_k(a, b)$ and Pl-$\mathrm{Hol}_k(a, b)$ depend only on X and Y. The following lemma is proved using an argument similar to Lemma 22 in Chapter 3.

Lemma 39. *Let G be a k-regular graph with n vertices. If n is even, then there exists a polynomial $P(\cdot, \cdot)$ with two variables and integer coefficients such that for any signature grid Ω having underlying graph G and every edge labeled $[a, 1, b]$, the holant value is $\mathrm{Holant}_\Omega = P(ab, a^k + b^k)$. If n is odd, then there exists a polynomial $P(\cdot, \cdot)$ as before such that $\mathrm{Holant}_\Omega = (a^{k/2} + b^{k/2})P(ab, a^k + b^k)$.*

Proof. First note if k and n are both odd then no k-regular graph exists on n vertices, so k must be even whenever n is odd.

Consider any $\{0, 1\}$ vertex assignment σ. If σ' is the complement assignment switching all 0's and 1's in σ, then the sum of valuations for σ and σ' in Holant_Ω is $a^i b^j + a^j b^i$ where i (resp. j) is the number of edges connecting two degree k vertices both assigned 0 (resp. 1) by σ. We note that $a^i b^j + a^j b^i = (ab)^{\min(i,j)}(a^{|i-j|} + b^{|i-j|})$.

For the all-0 assignment, $i - j = kn/2$. Now starting from any assignment σ, if we switch the assignment on one vertex v from 0 to 1, it is easy to verify that it changes the valuation from $a^i b^j$ to $a^{i'} b^{j'}$, where $i - j = i' - j' + k$. This takes into account the changes among all edges incident to v, including self loops at v, if any. Every $\{0, 1\}$ assignment σ is obtainable from the all-0 assignment by a sequence of switches, hence $i - j \equiv kn/2 \pmod{k}$.

If n is even, then $kn/2 \equiv 0 \pmod{k}$. Thus, for every assignment σ, we have $i - j \equiv 0 \pmod{k}$. Now $a^i b^j + a^j b^i = (ab)^{\min(i,j)}(a^{k\ell} + b^{k\ell})$, for some integer $\ell \geq 0$, and a simple induction

$$a^{k(\ell+1)} + b^{k(\ell+1)} = (a^{k\ell} + b^{k\ell})(a^k + b^k) - (ab)^k(a^{k(\ell-1)} + b^{k(\ell-1)})$$

shows that Holant_Ω is a polynomial $P(ab, a^k + b^k)$ with integer coefficients.

If n is odd, then in particular k is even. For every assignment σ, we have $i - j \equiv k/2 \pmod{k}$. Now $a^i b^j + a^j b^i = (ab)^{\min(i,j)}(a^{k/2+k\ell} + b^{k/2+k\ell})$, for some integer $\ell \geq 0$. We verify that at $\ell = 0$ and $\ell = 1$, $a^{k/2+k\ell} + b^{k/2+k\ell}$ becomes $a^{k/2} + b^{k/2}$ and $a^{3k/2} + b^{3k/2} = (a^{k/2} + b^{k/2})(a^k + b^k - (ab)^{k/2})$ respectively, both of which are of the form: a product of $a^{k/2} + b^{k/2}$ with an integer polynomial in $(ab, a^k + b^k)$. Then an easy induction

$$\begin{aligned} a^{k/2+k(\ell+1)} + b^{k/2+k(\ell+1)} &= (a^{k/2+k\ell} + b^{k/2+k\ell})(a^k + b^k) - \\ &\quad (ab)^k(a^{k/2+k(\ell-1)} + b^{k/2+k(\ell-1)}) \end{aligned}$$

shows that $a^{k/2+k\ell} + b^{k/2+k\ell}$ is of this form for all $\ell \geq 0$. □

Corollary 5. *Let G be any k-regular graph with n vertices, where k is even and n is odd, and let Ω be any signature grid having underlying graph G and every edge labeled $[a, 1, b]$. If $a^{k/2} + b^{k/2} = 0$, then $\mathrm{Holant}_\Omega = 0$.*

If the number of vertices n is odd then k must be even, and we may assume $a^{k/2} + b^{k/2} \neq 0$. Then we can change Ω to Ω' by adding an extra vertex with $k/2$ simple loops. Then Ω' has an even number of vertices. The holant value of Ω' is $\mathrm{Holant}_{\Omega'} = (a^{k/2} + b^{k/2})\mathrm{Holant}_\Omega$, hence we can compute Holant_Ω from $\mathrm{Holant}_{\Omega'}$. Therefore we will always assume the number of vertices is even from now on, and Lemma 39 says that X and Y capture the essence of (in)tractability for the holant problems under consideration (when k is even and $a^{k/2} + b^{k/2} = 0$, Corollary 5 simply says that a subset of the problem instances are trivially computable; the complexity of the holant problem depends on instances where there are an even number of vertices, hence the complexity is still captured by X and Y). If we find the complexity for any one setting of a and b such that $X = ab$ and $Y = a^k + b^k$, then we have already characterized all settings of a and b that result in the same X and Y. Specifically, given a signature $[a, 1, b]$ as input, one can compute the holant in terms of any a' and b' for which $a'b' = X$ and $(a')^k + (b')^k = Y$.

The standard bag of tricks covers all of the tractable problems.

Theorem 18. *If any of the following four conditions is true, then* $\mathrm{Hol}_k(a, b)$ *is solvable in* P*:*

1. $X = 1$
2. $X = 0$ *and* $Y = 0$
3. $X = -1$ *and* $Y = 0$
4. $X = -1$ *and* [$Y = \pm 2$ *if* k *is even, and* $Y = \pm 2\mathfrak{i}$ *if* k *is odd*]

If $Y^2 = 4X^k$ *then* $\text{Pl-Hol}_k(a, b)$ *is solvable in* P.

Proof. If $X = 1$ then the signature $[a, 1, b]$ is degenerate and the holant can be computed in polynomial time. If $X = Y = 0$, then $a = b = 0$ and a 2-coloring argument can be applied to calculate the holant. If $X = -1$, then applying a holographic transformation under basis $T = \begin{bmatrix} 1 & 0 \\ 0 & a \end{bmatrix}$, we get $T^{\otimes 2} g = [a, a, -a]^{\mathrm{T}}$ and $r(T^{-1})^{\otimes k} = [1, 0, 0, \ldots, 0, a^{-k}]$, where $r = [1, 0, 0, \ldots, 0, 1]$ is the $=_k$ signature and $g = [a, 1, -a^{-1}]^{\mathrm{T}}$ (note this g corresponds to the assumption $X = -1$). Multiplying the signature $[a, a, -a]$ by a^{-1} does not change the complexity of the problem, so $\#g \mid r$ is equivalent in complexity to $\#[1, 1, -1] \mid [1, 0, 0, \ldots, 0, a^{-k}]$, which is known to be tractable in P if $a^k \in \{1, -1, \mathfrak{i}, -\mathfrak{i}\}$, by families $\mathcal{F}_1$ and $\mathcal{F}_3$ in [11]. If k is even, then $Y = a^k + a^{-k}$, which can be set to -2, 0, or 2 by using any $a \in \mathbb{C}$ such that a^k is -1, $\mathfrak{i}$, or 1 respectively. If k is odd, then $Y = a^k - a^{-k}$, which can be set to $-2\mathfrak{i}$, 0, or $2\mathfrak{i}$ by using any $a \in \mathbb{C}$ such that a^k is $-\mathfrak{i}$, 1, or $\mathfrak{i}$, respectively. Finally, if $Y^2 = 4X^k$, then $a^k = b^k$ and holographic algorithms using matchgates can be applied when the input graph is planar (see [7], Lemmas 4.4 and 4.8). $\square$

4.3.2 Problems that are $\#\mathrm{P}\text{-hard}$ even for planar graphs

In this section we show that the remaining problems are $\#\mathrm{P}\text{-hard}$ (aside from when $Y^2 = 4X^k$). This is carried out primarily by applying binary recursive gadgets to Theorem 17 for different real-valued settings of X and Y (note this includes some cases where a or b are complex). Usually when we speak of a gadget in this section, we really mean a member of a family of gadgets; most of the gadgets in Figures 4.1 and 4.3 actually define families of gadgets, with a different gadget for each k. We will make use of the following lemma, proved in Chapter 3.

Lemma 40. *If all roots of the complex polynomial* $x^3 + Bx^2 + Cx + D$ *have the same norm, then* $C|C|^2 = \overline{B}|B|^2 D$.

This criterion can be used to study the suitability of binary recursive gadgets for interpolation. Every recursive gadget we use has a transition matrix with a characteristic polynomial of the form $x^3 + Bx^2 + Cx + D$ where B, C, and D are polynomials in X and Y with integer coefficients. Since X and Y are real, Lemma 40 says that the eigenvalues have distinct norm if (X, Y) is not in the zero set of the real polynomial $f(X, Y) = C^3 - B^3 D$. This becomes an important tool in proving $\#$P-hardness: we show that for any remaining X and Y, there is a planar binary recursive gadget with a nonsingular transition matrix such that the corresponding polynomial $f(X, Y)$ is nonzero (except when $Y^2 = 4X^k$, which is tractable for planar graphs and needs to be handled using a different technique). This implies that condition 1 of Theorem 17 is satisfied (condition 2 can be shown separately). However, there is some difficulty in applying this lemma; not only is the degree of f high in a and b for all but the smallest of gadgets, but the exponents in the polynomial f are functions of k. It is not obvious how to obtain suitable binary recursive gadgets for all k. Furthermore, for a family of gadgets indexed by k, if we treat k as a variable, the question can no longer be formulated as one about semi-algebraic sets. Nevertheless, there exists a pair of binary recursive gadget families M_1 and M_2 suitable for handling these difficulties (see Figures 4.1(a) and 4.1(b)). It is the *combination* of these two gadget families and the algebraic relationship *between* them, combined with the coordinate change $X = ab$ and $Y = a^k + b^k$, which allows us to eliminate k entirely and to finally derive a general result. When $k \leq 4$ this family of gadget pairs does not work, so we will deal with this case separately, by selecting different binary recursive gadgets for $k = 4$. We also need to find starter gadgets suitable to be used with M_1 and M_2 in the recursive construction, so recall the following easy way of identifying such starter gadgets, proved in Chapter 3.

Lemma 41. *Let $M \in \mathbb{C}^{n\times n}$ and let $s \in \mathbb{C}^{n\times 1}$. If $\det([s, Ms, \dots, M^{n-1}s]) \neq 0$ then s is not orthogonal to any row eigenvector of M.*

Lemma 42. *Suppose $k \geq 5$, $X \notin \{0,1\}$, and $a^k \neq b^k$. If $X = -1$, additionally assume that k is odd and $Y \neq 0$. Then $\text{Pl-Hol}_k(a,b)$ is $\#\text{P-hard}$.*

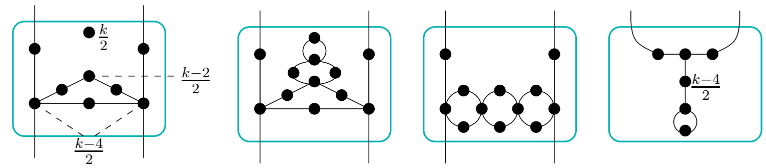
Proof. We show that for every setting of X and Y under consideration, either gadget M_1 or M_2 satisfies Theorem 17 when used with S_1 as a starter gadget. First, $\det([S_1, M_1S_1, M_1^2S_1]) = (X-1)^3(X^{k-2}-1)(b^k-a^k) \neq 0$ and $\det([S_1, M_2S_1, M_2^2S_1]) = X^2(X-1)^3(X^{k-4}-1)(b^k-a^k) \neq 0$, so S_1 is not orthogonal to any row eigenvector of M_1 or M_2. Let the characteristic polynomials of gadgets M_1 and M_2 be $x^3 + B_1x^2 + C_1x + D_1$ and $x^3 + B_2x^2 + C_2x + D_2$ respectively, and let $Z = X^{k-3}$. Then $\det(M_1) = XZ(X-1)^3 \neq 0$ and $\det(M_2) = X^2Z(X-1)^3 \neq 0$. Now suppose $X \neq -1$. If all eigenvalues of M_i have the same norm, then by Lemma 40, $C_i^3 - B_i^3D_i = 0$. We claim that this cannot be the case for both gadgets. Otherwise, we factorize polynomials to get

$$C_1^3 - B_1^3D_1 = (X-1)^3(XZ-1)(XZ(X+1)^2(X^2Z+XZ+X+3Y+1)-Y^3) \quad (4.1)$$
$$C_2^3 - B_2^3D_2 = X^2(X-1)^3(Z-X)(XZ(X+1)^2(X^2+XZ+X+3Y+Z)-Y^3) \quad (4.2)$$

hence $Y^3 = XZ(X+1)^2(X^2Z+XZ+X+3Y+1)$ and $Y^3 = XZ(X+1)^2(X^2+XZ+X+3Y+Z)$. But then, by some fortuitous factorization,

$$\begin{aligned} 0 &= XZ(X+1)^2(X^2Z+XZ+X+3Y+1) \\ &\quad -XZ(X+1)^2(X^2+XZ+X+3Y+Z) = XZ(X+1)^3(X-1)(Z-1) \neq 0. \end{aligned}$$

Now suppose $X = -1$, k is odd, and $Y \neq 0$. We will show that gadget M_1 has a pair of eigenvalues with distinct norm. In this case, the characteristic polynomial of M_1 is $x^3 - Yx^2 - 2Yx - 8$, so by Lemma 40, if all roots of the characteristic polynomial have the same norm, then $-8Y^3 = C^3 = B^3D = 8Y^3$, but this implies $Y = 0$. □



(a) Gadget M_3 (b) Gadget M_4 (c) Gadget M_5 (d) Gadget S_2

Figure 4.3 Labels for gadget M_3 indicate the number of 2-cycles on each recognizer vertex. The label in gadget S_2 indicates the number pairs of edges in parallel

The discovery of these gadgets came from a careful study of the factorized failure conditions of small gadgets that were generalized to all k in a simple way. It was separately noted that these two gadgets had polynomials that simplified quite nicely, and the two were put together to get the result. It is this remarkable alignment of polynomials 4.1 and 4.2 which makes the preceding proof so short and simple. At the same time, the result is quite powerful and proves #P-hardness for nearly all releveant settings of X, Y, *and* k. To fully appreciate how remarkably well this gadget pair works together, recall that in the previous chapter we resorted to symbolic computation to prove the same result for $k = 3$, and the same result was proved using different gadgets and serious manipulation and symbolic computation in [10]. We shed some light on why this pair of gadgets works so well in Chapter 6.

The existing computer software for computing transition matrices of recursive gadgets was not adapted to discover gadget families or compute the transition matrices for them. The following gadget was found by identifying a gadget that worked for a few small k, calculating the recurrence matrix by hand for general k, and finally computing the characteristic polynomial using a computer algebra package. The following Lemma deals with even $k \geq 4$ when both $X = -1$ and $Y \in \mathbb{R} - \{-2, 0, 2\}$. Note that when k is even, $X = -1$, and $Y \in \{-2, 0, 2\}$ the problem $\text{Hol}_k(a, b)$ is tractable.

Lemma 43. *Suppose* $k \geq 4$ *is even,* $X = -1$ *and* $Y \in \mathbb{R} - \{-2, 0, 2\}$. *Then* $\text{Pl-Hol}_k(a, b)$ *is* #P-hard.

Proof. If $X = -1$, then the characteristic polynomial of gadget M_3 is $x^3 + (4 - Y^2)x^2 + 2(4 - Y^2)(2 + (-1)^{k/2}Y)x + 8(4 - Y^2)(2 + (-1)^{k/2}Y)$, so the determinant is nonzero. By Lemma

40, if all roots of the characteristic polynomial have the same norm, then $C^3 = B^3 D$ and this amounts to $(2 + (-1)^{k/2} Y)^2 = 4 - Y^2$, but then $4 \pm 4Y + Y^2 = 4 - Y^2$ and $Y(Y \pm 2) = 0$, which is not true. Finally, applying Lemma 41 to M_3 and S_1, we get $\det([S_1, M_3 S_1, M_3^2 S_1]) = -16Y(Y^2 - 4)^3 (2 + (-1)^{k/2} Y)(2(-1)^{k/2} + Y) \neq 0$. □

The bulk of the work is now done.

Lemma 44. *Suppose* $k \geq 3$, $X \notin \{0, 1\}$, $a^k \neq b^k$, $(X, Y) \neq (-1, 0)$. *Then* $\text{Pl-Hol}_k(a, b)$ *is* $\#\text{P-hard}$.

Proof. This result is already known for $k = 3$ (see Chapter 3). If $k \geq 5$ then this is established by Lemmas 42 and 43 (note that if k is even, then $X = -1$ and $Y = \pm 2$ together imply $a^k = b^k$).

Now suppose $k = 4$, and we will prove that $\text{Pl-Hol}_4(a, b)$ is $\#\text{P-hard}$ by using symbolic computation to show that gadgets M_1, M_4, M_5, and S_1 together satisfy Theorem 17 (see Figures 4.1(a), 4.3(b), 4.3(c), 4.1(c)). Calculating the characteristic polynomials $x^3 + Bx^2 + Cx + D$ of gadgets M_1, M_4, and M_5, we get

$$
\begin{aligned}
B_1 &= -X - Y - 1 \\
C_1 &= (X - 1)(X^3 + X^2 + Y) \\
D_1 &= -X^2 (X - 1)^3 \\
B_4 &= 2X^4 - 2X^3 - 2X^2 - 2XY - 2X - Y^2 - 2Y \\
C_4 &= (X - 1)(X^7 - X^6 - 4X^5 - X^4 Y + 8X^4 + 5X^3 Y + 3X^3 + X^2 Y^2 + 5X^2 Y \\
&\quad + X^2 + 4XY^2 + 3XY + Y^3 + Y^2) \\
D_4 &= -X(X - 1)^3 (2X + Y)(X^5 - 2X^4 + 2X^3 + X^2 Y + 2X^2 + 2XY + X + Y^2 + Y) \\
B_5 &= 2X^4 - X^3 - 3X^2 - XY - X - Y^2 - 3Y - 1 \\
C_5 &= (X - 1)(X^7 - X^6 - 2X^5 - 2X^4 Y - 2X^4 + 2X^3 Y + 5X^3 + X^2 Y^2 + 6X^2 Y \\
&\quad + 7X^2 + XY^2 + 2XY + Y^3 + 4Y^2 + 4Y) \\
D_5 &= -(X - 1)^3 (X^2 + Y + 1)(X^6 - 2X^4 + 2X^2 Y + 5X^2 + Y^2 + 2Y)
\end{aligned}
$$

For any real-valued setting of X and Y compatible with the constraints $X \neq 1$, $a^4 \neq b^4$, and $(X, Y) \neq (-1, 0)$, we will see that at least one of these three binary recursive gadgets satisfies the requirements of Theorem 17. To verify that gadget M_j satisfies condition 1 of Theorem 17, we apply Lemma 40 and check that $D_j(B_j^3 D_j - C_j^3) \neq 0$. With condition 2 of Theorem 17 and Lemma 41 in mind, we calculate $\det[S_1, M_1 S_1, M_1^2 S_1] = -(a^4 - b^4)(X-1)^4(X+1)$, $\det[S_1, M_4 S_1, M_4^2 S_1] = -(a^4 - b^4)(X-1)^4(X+Y+1)(X^5 - X^4 + X^3 + X^2 Y + 3X^2 + 3XY + Y^2)$, and $\det[S_1, M_5 S_1, M_5^2 S_1] = -(a^4 - b^4)(X-1)^6(X+1)^3(Y+2)$. We summarize the essential observations in terms of (X, Y) coordinates as follows.

$$
\begin{aligned}
X = 1 \quad &\Longleftrightarrow \quad ab = 1 \\
Y^2 = 4X^4 \quad &\Longleftrightarrow \quad a^4 = b^4 \\
X = -1 \wedge Y = 0 \quad &\Longleftrightarrow \quad a^8 = -1 \wedge ab = -1 \\
D_1(B_1^3 D_1 - C_1^3)(X-1)^4(X+1) \neq 0 \quad &\Longrightarrow \quad \text{Gadget } M_1 \text{ satisfies Theorem 17} \\
D_4(B_4^3 D_4 - C_4^3)(X-1)^4(X+Y+1)& \\
(X^5 - X^4 + X^3 + X^2 Y + 3X^2 + 3XY + Y^2) \neq 0 \quad &\Longrightarrow \quad \text{Gadget } M_4 \text{ satisfies Theorem 17} \\
D_5(B_5^3 D_5 - C_5^3)(X-1)^6(X+1)^3(Y+2) \neq 0 \quad &\Longrightarrow \quad \text{Gadget } M_5 \text{ satisfies Theorem 17}
\end{aligned}
$$

If we can verify that at least one of the six conditions on the left hand side holds for any real-valued setting of X and Y then we are done. Note that a disjunction of the left hand sides is a semi-algebraic set, and as such, is decidable by Tarski's Theorem [28]. Using symbolic computation via the CylindricalDecomposition function from Mathematica™, we verify that for any $X, Y \in \mathbb{R}$, at least one of the six conditions above is true, and we are done. □

Two cases that remain are $X = 0$ and $a^k = b^k$. Whenever $X = 0$ and $Y \notin \{0, -1\}$, either gadget $M_1 S_1$ or gadget S_2 simulates a signature that is already covered in Lemma 44 so we are done by reduction from that case. Similarly, when $X = 0$ and $Y = -1$ a reduction from the case where $X = 0$ and $Y \notin \{0, -1\}$ can be made using gadget $M_1 S_2$.

Lemma 45. *If* $k \geq 3$*,* $X = 0$*, and* $Y \neq 0$ *then* $\text{Pl-Hol}_k(a, b)$ *is* $\#\text{P-hard}$.

Proof. If $X = 0$ then either $a = 0$ or $b = 0$, so by symmetry and $Y \neq 0$ assume without loss of generality that $b = 0$ and $a \neq 0$. We will break this down into two cases: $Y \neq -1$ and $Y = -1$. We will carry out the proof by reducing from Lemma 44.

First suppose $Y \neq -1$. Then $M_1 S_1$ has signature $[2a + a^{k+1}, 1 + a^k, a^{k-1}]$ and gadget S_2 has signature $[a + a^{k+1}, a^k, a^{k-1}]$ (see Figures 4.1(a), 4.1(c), and 4.3(d)). We claim that either $\#[2a + a^{k+1}, 1 + a^k, a^{k-1}] \mid =_k$ or $\#[a + a^{k+1}, a^k, a^{k-1}] \mid =_k$ is $\#\text{P-hard}$, and if this is true we are done with this case. Let $a' = \frac{a+a^{k+1}}{a^k}$, $b' = a^{-1}$, $a'' = \frac{2a+a^{k+1}}{1+a^k}$, and $b'' = \frac{a^{k-1}}{1+a^k}$ so we want to show that either $\#[a', 1, b'] \mid =_k$ or $\#[a'', 1, b''] \mid =_k$ is $\#\text{P-hard}$. First, $a'b' = \frac{1+a^k}{a^k} = 1 + Y^{-1} \notin \{0, 1\}$. If $a^k = -2$ then $|a'| = |a/2| < |a^{-1}| = |b'|$, otherwise $|a^2| \geq 2$, which would imply that $|a^k| > 2$, a contradiction. Therefore it follows that $|a'|^k \neq |b'|^k$ and furthermore $(a')^k + (b')^k \neq 0$, so $\#[a', 1, b'] \mid =_k$ is $\#\text{P-hard}$ and we can now assume $a^k \neq -2$.

Now we have $a''b'' = \frac{2a^k+a^{2k}}{(1+a^k)^2} \neq 0$ and since $2a^k + a^{2k} - (1 + a^k)^2 = -1$ we also have $a''b'' \neq 1$. Next we verify that $(a'b', (a')^k + (b')^k) \neq (-1, 0)$. Otherwise, $\frac{1+Y}{Y} = a'b' = -1$ so $Y = -\frac{1}{2}$, and furthermore $\frac{Y(1+Y)^k}{Y^k} + Y^{-1} = (a')^k + (b')^k = 0$ hence $(1 + Y)^k = -Y^{k-2}$, but $|1 + Y|^k = |\frac{1}{2}|^k \neq |\frac{1}{2}|^{k-2} = |-Y^{k-2}|$, so this cannot be. Similarly, suppose for a contradiction we have $(a''b'', (a'')^k + (b'')^k) = (-1, 0)$. Then $2Y + Y^2 + (1 + Y)^2 = 0$, meaning $Y = -1 \pm \sqrt{2}/2$, and from $(a'')^k + (b'')^k = 0$ we derive $(2 + Y)^k = Y^{k-2}$. However, $|2 + Y|^k = |1 \pm \sqrt{2}/2|^k \neq |-1 \pm \sqrt{2}/2|^{k-2} = |Y^{k-2}|$ contradicting our assumption. All that remains is to show that we cannot simultaneously have $(a')^k = (b')^k$ and $(a'')^k = (b'')^k$. For this it suffices to refute $(2a + a^{k+1})^k = a^{k(k-1)} = (a + a^{k+1})^k$ or equivalently $Y(2+Y)^k = Y(1+Y)^k$, but this can only hold if $|1+Y| = |2 + Y|$, implying $Y = -3/2$, but then $|(2a + a^{k+1})^k| = |Y(2 + Y)^k| < 1 < |Y^{k-1}| = |a^{k(k-1)}|$, meaning $(2a + a^{k+1})^k \neq a^{k(k-1)}$.

Now suppose $Y = -1$, and we still assume that $b = 0$ and $a \neq 0$. Then gadget $M_1 S_2$ has signature $[-2a, -1, 0]$, and hence we can simulate signature $[2a, 1, 0]$. This means we can simulate a problem where $X = 0$ and $Y = 2^k a^k = -2^k \neq -1$, so we are done by reduction from the $Y \neq -1$ case. □

4.3.3 Problems that are tractable for planar graphs but $\#\mathrm{P}$-hard in general

If $a^k = b^k$ and $X \notin \{-1, 0, 1\}$, then $\mathrm{Hol}_k(a, b)$ is $\#\mathrm{P}$-hard, yet can be solved in polynomial time when the input is restricted to planar graphs. After a suitable holographic reduction, we can use gadget S_1 and either M_1 or M_2 (without a finisher gadget) to interpolate all signatures of the form $[x, y, x]$. Then we can use the $[1, 1, 1]$ signature between pairs of vertices with the $=_k$ signature to simulate $=_3$, completing a reduction from $\mathrm{Hol}_3(a, b)$, which is known to be $\#\mathrm{P}$-hard (see Chapter 3). Note that planarity does not need to be preserved. Also, we can assume that the number of recognizer vertices in the input graph is even since we are reducing from $\mathrm{Hol}_3(a, b)$ and 3-regular graphs always have an even number of vertices.

First we will transform the problem into a more convenient form. Note that in the following lemma, $a\omega^2 \cdot a\omega^2 = ab$, so X is invariant under the transformation given there. Subsequently then, it will suffice to prove that $\#[a, 1, a] \mid [1, 0, 0, e]$ is $\#\mathrm{P}$-hard for all a and e such that $a^2 \in \mathbb{R} - \{0, \pm 1\}$ and $e = \pm 1$.

Lemma 46. *Suppose k is a positive integer and $a^k = b^k$. Then for some $e \in \{1, -1\}$ and for any ω such that $\omega^4 = ba^{-1}$, the problem $\#[a, 1, b] \mid =_k$ is equivalent to $\#[a\omega^2, 1, a\omega^2] \mid [1, 0, 0, e]$.*

Proof. Let ω be any complex number such that $\omega^4 = ba^{-1}$, and note $\omega^{4k} = 1$. Applying a holographic reduction to $\#[a, 1, b] \mid =_k$ under the basis $\begin{bmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{bmatrix}$, we see that the problem $\#[a, 1, b] \mid =_k$ is equivalent to $\#[a\omega^2, 1, a\omega^2] \mid [\omega^{-k}, 0, 0, \ldots, 0, \omega^k]$. Since $\omega^k \in \{\pm 1, \pm \mathrm{i}\}$ and multiplying the recognizer signature by a nonzero constant does not change the complexity of the problem, we have $\#[a\omega^2, 1, a\omega^2] \mid [1, 0, 0, \ldots, 0, \pm 1]$. $\square$

Our gadget construction will be that of Lemma 4 in Chapter 3. In the setting $a = b$, gadgets M_1 and M_2 have 2 by 2 transition matrices $M_1 = \begin{bmatrix} a^{k-2} + a^k & 2a \\ 2a^{k-1} & a^2 + 1 \end{bmatrix}$ and $M_2 = \begin{bmatrix} a^{k-2} + a^k & 2a^3 \\ 2a^{k-1} & a^2(a^2 + 1) \end{bmatrix}$. Following [10], we test for nonzero eigenvalues of distinct norm with the condition $\det(M_j) \neq 0 \wedge \mathrm{tr}(M_j) \neq 0 \wedge (\mathrm{tr}(M_j))^2 - 4\det(M_j) > 0$ and for a non-eigenvector starter gadget with $\det([M_j S_1, S_1]) \neq 0$. Satisfying these two conditions is sufficient to interpolate any signature of the form $[x, y, x]$, by Lemma 4. Recall that $X, Y \in \mathbb{R}$. In the following lemma this translates to $a^2, 2a^k \in \mathbb{R}$.

Lemma 47. *If $a \notin \{0, \pm 1, \pm \mathrm{i}\}$ and $r = [1, 0, 0, \ldots, 0, \pm 1]$ has arity at least 3, then we can efficiently simulate a set of pairwise linearly independent signatures of the form $[x, y, x]$, and $\#[a, 1, a] \mid r$ is* #P-hard.

Proof. Let e such that $r = [1, 0, 0, \ldots, 0, e]$. Supposing $k \geq 5$, we verify that $\det(M_1) = ea^{k-2}(a-1)^2(a+1)^2 \neq 0$, $\det(M_2) = ea^k(a-1)^2(a+1)^2 \neq 0$, $\operatorname{tr}(M_1) = (a^2+1)(a^{k-2}+e) \neq 0$, and $\operatorname{tr}(M_2) = a^2(a^2+1)(a^{k-4}+e) \neq 0$. In the case of $\operatorname{tr}(M_1)$, this is true because if $a^{k-2} + e = 0$ then $|a| = 1$ but since $a^2 = X \in \mathbb{R}$ we would have $a \in \{\pm 1, \pm \mathrm{i}\}$, which is not true (similarly for $\operatorname{tr}(M_2)$). Also, $\det[M_1 S_1, S_1] = -a(a-1)(a+1)(a^{k-2}+e) \neq 0$ and $\det[M_2 S_1, S_1] = -a^3(a-1)(a+1)(a^{k-4}+e) \neq 0$. Hence we only need to verify that for every setting of a, the discriminant of either M_1 or M_2 is positive. We calculate that $\operatorname{tr}(M_1)^2 - 4\det(M_1) = X^2 - eXY + 2X + Y^2/4 + 6eY + 1 + X^{-1}Y^2/2 - eX^{-1}Y + X^{-2}Y^2/4$ and $\operatorname{tr}(M_2)^2 - 4\det(M_2) = X^4 + 2X^3 - eX^2Y + X^2 + 6eXY + Y^2/4 - eY + X^{-1}Y^2/2 + X^{-2}Y^2/4$, and note that the change in variables to X and Y completely eliminates any appearance of k. Thus, with a simple query to CylindricalDecomposition in Mathematica$^{\text{TM}}$, we find that one of these two polynomials is positive for any $X, Y \in \mathbb{R}$ unless $(X, Y) = (-1, 0)$ or $(X, Y) = (1, -2e)$, so we can interpolate any signature of the form $[x, y, x]$ when $k \geq 5$. For $k = 4$, note that $\det(M_1) \neq 0$, $\operatorname{tr}(M_1) \neq 0$, and $\det[M_1 S_1, S_1] \neq 0$. Running a second query using only M_1 with $X = a^2$ and $Y = 2a^4$, and we find that the discriminant is positive for any real-valued setting of a (excluding ± 1). We conclude that we can interpolate any signature of the form $[x, y, x]$ when $k \geq 4$. However, we will only need the signature $[1, 1, 1]$. We reduce from $\operatorname{Hol}_3(ea, ea)$ (equvalently, $\#[ea, 1, ea] \mid =_3$) with the following chain of reductions.

$$\begin{aligned}
\operatorname{Hol}_3(ea, ea) &\leq_{\mathrm{T}}^{\mathrm{P}} \#[a, 1, a] \mid [1, 0, 0, e] \\
&\leq_{\mathrm{T}}^{\mathrm{P}} \#\{[a, 1, a], [1, 1, 1]\} \mid r \\
&\leq_{\mathrm{T}}^{\mathrm{P}} \#[a, 1, a] \mid r
\end{aligned}$$

Any instance of $\text{Hol}_3(ea, ea)$ must have an even number of recognizer vertices. The first step follows from a holographic reduction under basis $\begin{bmatrix} 1 & 0 \\ 0 & e \end{bmatrix}$, so that $\text{Hol}_3(ea, ea)$ is equivalent to $\#[ea, e, ea] \mid [1, 0, 0, e]$, which has the same complexity as $\#[a, 1, a] \mid [1, 0, 0, e]$. Note the number of recognizer vertices is preserved. For the next step of the reduction, any pair of vertices with signature $[1, 0, 0, e]$ can simulated by a pair of vertices with signature r. Simply introduce $k - 3$ generator vertices; each has signature $[1, 1, 1]$ and is adjacent to both recognizer vertices. The last step of the reduction follows by interpolation using gadgets S_1, M_1, and M_2 as described above. Since $ea \notin \{0, \pm 1, \pm \mathrm{i}\}$ we know $\text{Hol}_3(ea, ea)$ is $\#\text{P-hard}$ (Chapter 3) and we are done. □

This completes Theorem 16. We add one last remark: Corollary 5 implies the existence of an interesting subset of holant problems when k is even and $a^{k/2} + b^{k/2} = 0$. Since $Y + 2X^{k/2} = (a^{k/2} + b^{k/2})^2$, this condition is equivalently written in terms of X and Y as $Y = -2X^{k/2}$. Given Theorem 16, these problems are $\#\text{P-hard}$ aside from the tractable subcases $X \in \{0, \pm 1\}$ and when the input is a planar graph. If $X \notin \{0, \pm 1\}$ and the input is over general graphs, then the problem is trivially computable when the number of vertices in the input graph is odd, but $\#\text{P-hard}$ over inputs where the number of vertices is even. There is such a fine line between tractability and intractability.

4.4 Appendix

Lemma 48. COUNTING VERTEX COVERS *on k-regular planar multigraphs (with self-loops and multiple edges) is* $\#\text{P-hard}$ *for* $k \geq 3$.

Proof. We will do a reduction from COUNTING VERTEX COVERS on 3-regular planar graphs, which is known to be $\#\text{P-hard}$ [36]. First, we can easily reduce from the input 3-regular planar graph $G = (V, E)$ to a k-regular planar graph when k is odd by using a gadget with a single vertex, one dangling edge, and $(k-1)/2$ self-loops. Connect $k-3$ of these gadgets to every vertex $v \in V$. Due to the self-loops, every copy of this gadget must have its vertex included in the vertex cover, but the graph induced by removing those vertices and their incident edges is identical to G, so the number of vertex covers is the same.

Now we reduce to a k-regular planar graph when k is even. The gadget is similar, with a single vertex, two dangling edges, and $(k-2)/2$ self-loops. Being 3-regular, every connected component of G has an even number of vertices, so considering the vertices in pairs and applying $k-3$ copies of this gadget to each pair of vertices, we are done by the same reasoning as before. However, the resulting graph is not necessarily planar, so will argue that the vertices V can be paired in such a way that the gadgets can be introduced while preserving planarity. Each vertex will be paired with either an adjacent vertex or a vertex at distance 2. Clearly, adjacent pairs admit a planar drawing of the gadgets, but pairs at distance 2 also admit a planar drawing of the gadgets because the middle vertex has degree 3, allowing the gadget to be drawn in a neighborhood of those two edges on one of the two sides.

Let T be any spanning forest of G. We will argue that as long as T has at least two vertices, we can pair some of the vertices in such a way that the forest induced by removing those vertices and all incident edges still has an even number of vertices in every connected component. Let v be an arbitrary degree 1 vertex in T, and let t be the vertex adjacent to v. We start by pairing v with t and removing v and its incident edges from T. Note the connected component in T containing t has an odd number of vertices, and we now process t in the following manner. Let S be the set of vertices now adjacent to t in T (note $|S| \leq 2$), and then remove t. If every connected component of T containing a vertex in S has an even number of vertices, then we are done. Otherwise, since T has an even number of vertices remaining there must be exactly two vertices in S and both are in connected components with an odd number of vertices. Now recursively process both $s \in S$ in the same manner as t.

The above algorithm identifies at least one pair of vertices, and every identified pair has distance at most 2 in T, hence distance at most 2 in G. Also, there are matching removals of the constituent vertices of every pair. Finally, it terminates with an even number of vertices in every remaining connected component of T. □

Chapter 5

A dichotomy for k-regular graphs with a symmetric complex-valued edge function

In this chapter we complete a complexity dichotomy theorem for the class of holant problems $\#[x_0, x_1, x_2] \mid =_k$, for all $x_0, x_1, x_2 \in \mathbb{C}$ and for all $k \geq 1$.

5.1 Interpolation technique

5.1.1 Circular gadget construction

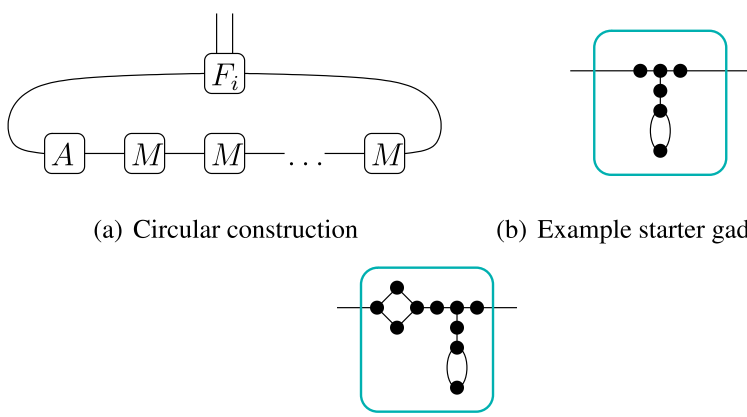
In this section we develop the main interpolation technique we will use in this chapter. The following can be viewed as an improvement on the unary recursive construction from Chapter 3. In this construction, it is easy to find an appropriate starter gadget and prove that the required conditions on the starter gadget hold. Also, this construction addresses a parity issue in the earlier construction; it is not even possible to construct a unary starter gadget on a regular graph with even degree, so we develop a way around this obstacle.

The first lemma is quite similar to Lemma 18, but applies to finisher gadgets with any number of leading edges.

Lemma 49. *Suppose $\{m_k\}_{k\geq 0}$ is a series of pairwise linearly independent column vectors in $\mathbb{C}^3$. Let F', F'', and $F''' \in \mathbb{C}^{\ell\times 3}$ be three matrices, each of rank 2, where $\ell \geq 2$ and the intersection of the row spaces of F', F'', and F''' is trivial $\{0\}$. Then for every n, there exists some $F \in \{F', F'', F'''\}$, and some $S \subseteq \{Fm_k : 0 \leq k \leq n^3\}$, such that $|S| \geq n$ and vectors in S are* pairwise *linearly independent.*

Proof. Let $k > j \geq 0$ be integers, let $N = [m_j, m_k] \in \mathbb{C}^{3\times 2}$, and then $\operatorname{rank}(N) = 2$ and $\ker(N^{\mathrm{T}})$ is a 1-dimensional linear subspace. It follows that there exists an $F \in \{F', F'', F'''\}$ such that the row space of F does not contain $\ker(N^{\mathrm{T}})$, and hence has trivial intersection with $\ker(N^{\mathrm{T}})$. In other words, $\ker(N^{\mathrm{T}} F^{\mathrm{T}}) = \ker(F^{\mathrm{T}})$. In particular, $\dim(\ker(N^{\mathrm{T}} F^{\mathrm{T}})) = \dim(\ker(F^{\mathrm{T}})) = \ell - 2$, so $FN \in \mathbb{C}^{\ell\times 2}$ has rank 2, hence Fm_j and Fm_k are linearly independent.

Each $F \in \{F', F'', F'''\}$ defines a coloring of the set $K = \{0, 1, \ldots, n^3\}$ as follows: color $k \in K$ with the linear subspace spanned by Fm_k. Assume for a contradiction that for each $F \in \{F', F'', F'''\}$ there are not n pairwise linearly independent vectors among $\{Fm_k : k \in K\}$. Then, including possibly the 0-dimensional space $\{0\}$, there can be at most n distinct colors assigned by each $F \in \{F', F'', F'''\}$. By the pigeonhole principle, some k and k' with $0 \leq k < k' \leq n^3$ must receive the same color for all $F \in \{F', F'', F'''\}$. This is a contradiction and we are done. $\square$



(a) Circular construction

(b) Example starter gadget (A)

(c) Example recursive gadget (M)

Figure 5.1 Circular construction

Lemma 50. *Fix a finite generator set $\mathcal{G}$ and a finite recognizer set $\mathcal{R}$, and suppose that there is an algorithm $\mathcal{A}$ that, on input $n \in \mathbb{Z}^+$, has a runtime polynomial in n and outputs a set of n binary starter gadget $\mathcal{F}$-gates having symmetric and pairwise linearly independent signatures, where $\mathcal{F} = \mathcal{G} \cup \mathcal{R}$. Also suppose that there exist three finisher gadget $\mathcal{F}$-gates with rank 2 matrices $F', F'', F''' \in \mathbb{C}^{3\times 3}$, where the intersection of the row spaces of F', F'', and F''' is trivial. Then for any $x, y \in \mathbb{C}$, $\#\mathcal{G} \mid \mathcal{R} \cup \{[x, 0, y]\} \leq_{\mathrm{T}}^{\mathrm{P}} \#\mathcal{G} \mid \mathcal{R}$.*

Proof. Assume we have oracle access to querries of the form $\#\mathcal{G} \mid \mathcal{R}$, and we are given a bipartite signature grid Ω for the holant problem $\#\mathcal{G} \mid \mathcal{R} \cup \{[x, 0, y]\}$, with underlying graph $G = (V, E)$. Let $Q \subseteq V$ be the set of vertices with $[x, 0, y]$ recognizers, and let $n = |Q|$. Let $\{N_0, N_1, \ldots, N_{(n+2)^3}\}$ be the $\mathcal{F}$-gates given by $\mathcal{A}$ on input $(n+2)^3+1$, and let G_k be the resulting $\mathcal{F}$-gate when N_k is connected to one of the finisher gadgets, with the trailing edges of the finisher gadget merged with the leading edges of N_k. For every $k \geq 0$, let m_k denote the (symmetric) signature of N_k written as a column vector in $\mathbb{C}^3$, and we know these signatures are pairwise linearly independent. By Lemma 49 there exists some $F \in \{F', F'', F'''\}$ such that at least $n+2$ of the first $(n+2)^3+1$ vectors of the form Fm_k are pairwise linearly independent. Fix such an F, so that the signature of G_k is Fm_k, which we denote by $[X_k, 0, Y_k]$ (recall that the middle row of a 3 by 3 finisher gadget matrix is all zeros, so the middle term of the signature G_k is also zero). At most one such Y_k can be zero, so there exists a subset S of these signatures for which each Y_k is nonzero and $|S| = n+1$. We will argue using only the existence of S, so there is no need to algorithmically "find" such a set, and for that matter, one can try out all three finisher gadgets without any need to determine which finisher gadget is "the correct one" beforehand. If we replace every element of Q with a copy of G_k, we obtain an instance of $\#\mathcal{G} \mid \mathcal{R}$ (note that the correct bipartite signature structure is preserved), and we denote this new signature grid by Ω_k. Although Holant_{Ω_k} is a sum of exponentially many terms, each nonzero term has the form $c_i X_k^i Y_k^{n-i}$ for some i, and for some $c_i \in \mathbb{C}$ which does not depend on X_k or Y_k. Then the sum can be rewritten as

$$\text{Holant}_{\Omega_k} = \sum_{0 \leq i \leq n} c_i X_k^i Y_k^{n-i}.$$

Since each signature grid Ω_k is an instance of $\#\mathcal{G} \mid \mathcal{R}$, Holant_{Ω_k} can be solved exactly using the oracle. Carrying out this process for every $k \in \{0, 1, \ldots, (n+2)^3\}$, we arrive at a linear system where the c_i values are the unknowns.

$$\begin{bmatrix} \text{Holant}_{\Omega_0} \\ \text{Holant}_{\Omega_1} \\ \vdots \\ \text{Holant}_{\Omega_{(n+2)^3}} \end{bmatrix} = \begin{bmatrix} X_0^0 Y_0^n & X_0^1 Y_0^{n-1} & \cdots & X_0^n Y_0^0 \\ X_1^0 Y_1^n & X_1^1 Y_1^{n-1} & \cdots & X_1^n Y_1^0 \\ \vdots & \vdots & \ddots & \vdots \\ X_{(n+2)^3}^0 Y_{(n+2)^3}^n & X_{(n+2)^3}^1 Y_{(n+2)^3}^{n-1} & \cdots & X_{(n+2)^3}^n Y_{(n+2)^3}^0 \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_n \end{bmatrix}.$$

For $0 \leq i \leq n$, let k_i such that $S = \{[X_{k_0}, 0, Y_{k_0}], [X_{k_1}, 0, Y_{k_1}], \ldots, [X_{k_n}, 0, Y_{k_n}]\}$, and let $[x_i, 0, y_i] = [X_{k_i}, 0, Y_{k_i}]$. Then we have a subsystem

$$\begin{bmatrix} y_0^{-n} \cdot \mathrm{Holant}_{\Omega_0} \\ y_1^{-n} \cdot \mathrm{Holant}_{\Omega_1} \\ \vdots \\ y_n^{-n} \cdot \mathrm{Holant}_{\Omega_n} \end{bmatrix} = \begin{bmatrix} x_0^0 y_0^0 & x_0^1 y_0^{-1} & \cdots & x_0^n y_0^{-n} \\ x_1^0 y_1^0 & x_1^1 y_1^{-1} & \cdots & x_1^n y_1^{-n} \\ \vdots & \vdots & \ddots & \vdots \\ x_n^0 y_n^0 & x_n^1 y_n^{-1} & \cdots & x_n^n y_n^{-n} \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_n \end{bmatrix}.$$

The matrix above has entry $(x_r/y_r)^c$ at row r and column c. Due to pairwise linear independence of $[x_r, 0, y_r]$, x_r/y_r is pairwise distinct for $0 \leq r \leq n$. Hence this is a Vandermonde system of full rank. Therefore the initial feasible linear system has full rank and we can solve it for the c_i values. With these values in hand, we calculate $\mathrm{Holant}_\Omega = \sum_{0 \leq i \leq n} c_i x^i y^{n-i}$ directly, completing the reduction. □

The new interpolation construction is depicted in Figure 5.1. Gadget M is a unary recursive gadget, and gadget A exists merely to ensure that the signature of the construction is symmetric before applying a finisher gadget. The proof idea is essentially the same as Lemma 19. A set of infinitely many pairwise linearly independent binary symmetric signatures are produced and one of a set of finisher gadgets is used to collapse them into a lower dimension while preserving a polynomial fraction of pairwise linearly independent signatures. The main difference is that the binary signatures are produced in a circular way by a unary recursive gadget instead of in a linear way by a binary recursive gadget. The use of unary gadgets also means that this construction will be useful primarily when X and Y are not both real.

Earlier, we saw how to use finisher gadgets top finish off a binary recursive construction that started with a starter gadget, and a pure unary recursive constrution. Now we show how to give a similar construction using unary recursive gadgets built in a circular pattern (see Figure 5.1). This uses a binary starter gadget instead of a unary starter gadget, avoiding the parity issue when k is even.

Lemma 51. *Suppose that the following gadgets can be built using complex-valued signatures from a finite generator set $\mathcal{G}$ and a finite recognizer set $\mathcal{R}$.*

1. *A unary recursive gadget with nonsingular transition matrix M, for which $M/\det(M)$ is not cyclic.*

2. *A binary starter gadget with nondegenerate signature $[z_0, z_1, z_2]$, such that AM^k is symmetric for all $k \geq 0$ where $A = \begin{bmatrix} z_0 & z_1 \\ z_1 & z_2 \end{bmatrix}$.*

3. *Three finisher gadgets with rank 2 matrices $F', F'', F''' \in \mathbb{C}^{3\times 3}$, where the intersection of the row spaces of F', F'', and F''' is trivial.*

Then for any $x, y \in \mathbb{C}$, $\#\mathcal{G} \mid \mathcal{R} \cup \{[x, 0, y]\} \leq_{\mathrm{T}}^{\mathrm{P}} \#\mathcal{G} \mid \mathcal{R}$.

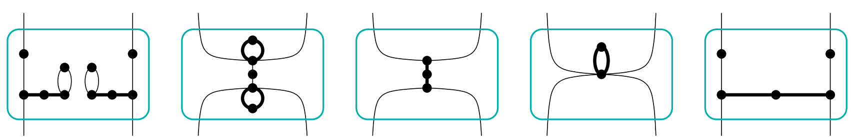
Proof. The construction begins with gadget A: designate one dangling edge to be the "fixed" leading edge, and call this $\mathcal{F}$-gate N_0. Recursively, $\mathcal{F}$-gate N_{k+1} is defined to be N_k connected to gadget M in such a way that the trailing edge of M is merged with the non-fixed leading edge of N_k. Note that for $k > k'$ there is no scalar $\lambda \in \mathbb{C}$ such that $\lambda AM^k = AM^{k'}$, otherwise since A and M are both nonsingular, we get $\lambda M^{k-k'} = I$, contradicting the assumption that $M/\det(M)$ is not cyclic. So the $\mathcal{F}$-gates defined by any such AM^k and $AM^{k'}$ have symmetric signatures, and these signatures are pairwise linearly independent. This implies the polynomial time algorithm $\mathcal{A}$ required by Lemma 50, and we are done. □

5.1.2 A set of general-purpose finisher gadgets

For every recursive gadget presented in this chapter, the existence of a corresponding binary starter gadget is trivial. Condition (2) of Lemma 51 follows directly by creating symmetry in the underlying graph (see Figure 5.1, for example). Note that while this isn't necessarily possible in general, it follows trivially for all of the unary recursive gadgets we use here. Also, the fact that the starter gadget A has a nonsingular recurrence matrix follows from the fact that the recurrence matrix M is nonsingular and can be written as $M^{-1} = AB$ for some matrix B. As for condition (3), we will construct an explicit set of finisher gadgets which is completely general, in the sense that if we do not have a finisher gadget for some $a, b \in \mathbb{C}$, then $\text{Pl-Hol}_k(a, b)$ is in P.

The discovery of these finisher gadgets is guided by the finisher gadgets in Chapter 4. For uniformity of presentation, all finisher gadgets are the 2-leading-edge variety (note that gadget F_1

is a natural adaptation of gadget F_1 from the previous chapter). Gadgets F_3 and M_2 are identical to gadgets F_2 and M_1 in the previous chapter. Gadgets F_1, F_3, and M_2 can already be used to form good finisher gadget sets whenever $k \geq 3$, $X \notin \{0, 1\}$, and $a^k \neq b^k$ (see Lemmas 36 and refp3:finisherEven). In the previous chapter, $\text{Pl-Hol}_k(a, b)$ was proved to be $\#\text{P-hard}$ when $X = 0$ and $Y \neq 0$ by a direct gadget reduction from problems that were already known to be $\#\text{P-hard}$ at that point. Presently, we show that there is no fundamental limitation of finisher gadgets when $X = 0$ and $Y \neq 0$. Gadgets M_1 and F_2 can be used to form a standard finisher gadget set for this case. The introduction of self-loops on a finisher gadget seems to render it useless when $X = 0$. Following the heuristic preference for smaller gadgets, F_2 is the natural choice, particularly since it is defined for both odd and even k. From similar reasoning, we get gadget M_1. Calculating the transition matrices by hand and doing the remaining calculations with the aid of symbolic computation, we find that a finisher gadget set built from these two gadgets handles the remaining case completely.



(a) Gadget M_1 (b) Gadget F_1 (c) Gadget F_2 (d) Gadget F_3 (e) Gadget M_2

Figure 5.2 Gadgets used to construct finisher gadget sets. Bold edge pairs indicate that the gadget is generalized to higher degrees by replacing that length 2 path with several length 2 paths in parallel.

Lemma 52. *Consider $\#\mathcal{G} \mid \mathcal{R}$ and suppose $[a, 1, b] \in \mathcal{G}$, $=_k \in \mathcal{R}$, $k \geq 3$, $X \neq 1$, $a^k \neq b^k$, and it is not the case that $X = Y = 0$. Then there is an explicit set of finisher gadgets which satisfies condition (3) of Lemma 51.*

Proof. We break this into 3 different cases: $X = 0$, $X \neq 0$ when k is odd, and $X \neq 0$ when k is even. We build a finisher gadget set for each of these 3 cases using five "primitive" gadgets (see Figure 5.2). In every case, we will demonstrate that our finisher gadgets (say, F', F'', and F''') have row spaces with trivial intersection. Let v_1, v_2, and v_3 (resp.) denote the cross products of the first and last row vectors of F', F'', and F''' (resp.) and let $\operatorname{cross}(F', F'', F''')$ denote the 3 by 3 matrix with v_1, v_2, and v_3 as its first, second, and third rows. We claim that if $\det(\operatorname{cross}(F', F'', F''')) \neq 0$, then the row spaces of F', F'', and F''' have trivial intersection. To see this, suppose v is a complex vector in the intersection of the row spaces of F', F'', and F'''. Then v_1, v_2, and v_3 are all orthogonal to v, but since $\det(\operatorname{cross}(F', F'', F''')) \neq 0$, it follows that v_1, v_2, and v_3 are linearly independent and they span the conjugate vector $\overline{v}$ which is then also orthogonal to v. This means $|v|^2 = v\overline{v} = 0$, and that $v = 0$.

We now calculate the matrices of the primitive gadgets.

$$F_2 = \begin{bmatrix} a^{k-2} & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & b^{k-2} \end{bmatrix}, M_2 = \begin{bmatrix} a^k & 2a & b^{k-2} \\ a^{k-1} & 1+ab & b^{k-1} \\ a^{k-2} & 2b & b^k \end{bmatrix}$$

$$F_1 = \begin{bmatrix} a^{k-2} & 0 & a^{(k-3)/2}b^{(k-3)/2} \\ 0 & 0 & 0 \\ a^{(k-3)/2}b^{(k-3)/2} & 0 & b^{k-2} \end{bmatrix}, F_3 = \begin{bmatrix} a^{(k-4)/2} & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & b^{(k-4)/2} \end{bmatrix}$$

$$M_1 = \begin{bmatrix} (a^k+ab)^2 & 2(a^k+ab)(a+b^{k-1}) & (a+b^{k-1})^2 \\ a(a^{k-1}+b)^2 & (1+ab)(a^{k-1}+b)(a+b^{k-1}) & b(a+b^{k-1})^2 \\ (a^{k-1}+b)^2 & 2(a^{k-1}+b)(ab+b^k) & (ab+b^k)^2 \end{bmatrix}$$

Suppose $X \neq 0$ and k is odd. We will use gadgets F_1 and M_2; let $F = F_1$, $F' = F_1M_2$, and $F'' = F_1M_2^2$. Note $\det(M_2) = X^{k-2}(X-1)^3 \neq 0$ and F_1 has a 2 by 2 submatrix with determinant $X^{k-3}(X-1) \neq 0$, so F, F', and F'' have rank 2 (and they each have a middle row of all zeros, inherited from F_1), hence they are all finisher gadgets. The determinant of the matrix of cross products is $4X^{4k-11}(X-1)^7(a^k - b^k) \neq 0$, so the row spaces of these finisher gadgets have trivial intersection, as required.

Now suppose $X \neq 0$ and k is even. We will use gadgets F_3 and M_2; let $F = F_3$, $F' = F_3M_2$, and $F'' = F_3M_2^2$. We have $\det(M_2) = X^{k-2}(X-1)^3 \neq 0$ and F_3 has a 2 by 2 submatrix with determinant $X^{(k-4)/2} \neq 0$, so F, F', and F'' have rank 2 (and they each have a middle row of all zeros, inherited from F_3), hence they are all finisher gadgets. The determinant of the matrix of cross products is $4X^{5k/2-8}(X-1)^4(a^k-b^k) \neq 0$, so the row spaces of these finisher gadgets have trivial intersection.

Finally, suppose $X = 0$ and $Y \neq 0$. We will use gadgets F_2 and M_1; let $F = F_2$, $F' = F_2M_1$, and $F'' = F_2M_1^2$. Then $\det(M_1) = (X-1)^3(X + X^{k-1} + Y)^3 = -Y^3 \neq 0$ and F_2 has a 2 by 2 submatrix with determinant $X^{k-2} - 1 \neq 0$, so F, F', and F'' have rank 2 (and they each have a middle row of all zeros, inherited from F_2), hence they are all finisher gadgets. The determinant of the matrix of cross products is $4(X-1)^4(Y + X + X^{k-1})^5(a^k - b^k)(Y + 2X)(X^{k-2} - 1)^3 = -4Y^6(a^k - b^k) \neq 0$, so the row spaces of these finisher gadgets have trivial intersection, and we are done. □

To connect the circular gadget interpolation method with a hardness result, we reduce from COUNTING VERTEX COVERS on k-regular graphs, using Lemma 38 from Chapter 4. This implies a result which is more directly usable.

Theorem 19. *Suppose that the following gadgets can be built using generator* $[a, 1, b]$ *and recognizer* $=_k$*, where* $k \geq 3$*,* $X \neq 1$*,* $a^k \neq b^k$*, and it is not the case that* $X = Y = 0$*.*

1. *A planar unary recursive gadget with nonsingular transition matrix* M*, whose eigenvalues have distinct norm.*
2. *A planar binary starter gadget with nondegenerate signature* $[z_0, z_1, z_2]$*, such that* AM^k *is symmetric for all* $k \geq 0$ *where* $A = \begin{bmatrix} z_0 & z_1 \\ z_1 & z_2 \end{bmatrix}$.

Then $\text{Pl-Hol}_k(a, b)$ *is* $\#\text{P-hard}$.

Proof. Suppose matrices M and A satisfy the conditions above. Then all positive powers of M have eigenvalues of distinct norm, so there cannot be a positive integer k and $d \in \mathbb{C}$ for which $M^k = dI$. By Lemma 52 we have a set of finisher gadgets that satisfies condition (3) of Lemma 51, and A already satisfies condition (2) of Lemma 51. Then for any $x, y \in \mathbb{C}$, $\#\mathcal{G} \mid \mathcal{R} \cup \{[x, 0, y]\} \leq_T^P \#\mathcal{G} \mid \mathcal{R}$, so $\#\mathcal{G} \mid \mathcal{R}$ is $\#\text{P-hard}$ by Lemma 38. □

5.2 Classification of problems

In this section we show that $\mathrm{Hol}_k(a,b)$ is $\#\mathrm{P}\text{-hard}$ unless Theorem 20 indicates it is in P.

Theorem 20. *If any of the following four conditions is true, then* $\mathrm{Hol}_k(a,b)$ *and* Pl-$\mathrm{Hol}_k(a,b)$ *are both solvable in* P*:*

1. $X = 1$
2. $X = 0$ *and* $Y = 0$
3. $X = -1$ *and* $Y = 0$
4. $X = -1$ *and* $Y^2 = 4X^k$

If $Y^2 = 4X^k$ *then* Pl-$\mathrm{Hol}_k(a,b)$ *is solvable in* P.

This is done by constructing recursive gadgets for k-regular graphs for all $k \geq 3$, and applying Lemmas 51 and 52. We will work in terms of $(2,k)$-regular graphs, and let $X = ab$ and $Y = a^k + b^k$ throughout. When we speak of a gadget, we really mean a member of a family of gadgets, each one for a specific k; all gadgets we use can be generalized to an arbitrary degree $k \geq 4$ (though most gadget families are restricted to even or odd parity). We will use the following results from Chapter 3.

Lemma 53. *If both roots of the complex polynomial* $x^2 + Bx + C$ *have the same norm, then* $B|C| = \overline{B}C$ *and* $B^2\overline{C} = \overline{B}^2C$*. If further* $B \neq 0$ *and* $C \neq 0$*, then* $\mathrm{Arg}(B^2) = \mathrm{Arg}(C)$.

Definition 2. *A pair of nonsingular square matrices* M *and* M' *is called an* Eigenvalue Shifted Pair (ESP) *if* $M' = M + \delta I$ *for some nonzero* $\delta \in \mathbb{C}$*, and* M *has distinct eigenvalues.*

Corollary 6. *Let* M *and* M' *be an Eigenvalue Shifted Pair of* 2 *by* 2 *matrices. If both* M *and* M' *have eigenvalues of equal norm, then there exists* $r, s \in \mathbb{R}$ *such that* $\mathrm{tr}(M) = r\delta$ *(possibly* 0*) and* $\det(M) = s\delta^2$.

In the previous chapter, we already proved a dichotomy for $\mathrm{Hol}_k(a,b)$ when X and Y are both real, so we only need to consider the case where X and Y are not both real. Even k and odd k are considered separately.

5.2.1 Discussion of methodology

We reiterate that the second condition of the Theorem 19 is trivially satisfied provided the recursive gadget M can be viewed as the composition of two symmetric binary $\mathcal{F}$-gates; one with both dangling edges incident to generator vertices and one with both dangling edges incident to recognizer vertices. Then for some symmetric matrices A and B we have $M = BA$, and $(AM^k)^{\mathrm{T}} = (M^{\mathrm{T}})^k A^{\mathrm{T}} = (A^{\mathrm{T}} B^{\mathrm{T}})^k A^{\mathrm{T}} = (AB)^k A = A(BA)^k = AM^k$, so the construction produces symmetric signatures exclusively with A as a starter gadget. At this point it would be natural to conjecture that anything not covered by Theorem 18 (repeated below for reference) is $\#\mathrm{P}\text{-hard}$, and if this is true we just need to find the unary recursive gadgets to prove it.

Nevertheless, it turns out that it isn't just a matter of searching out a few gadgets and working out the details. The approach varies considerably for even and odd k, with odd k requiring little in terms of new insight.

When k is odd, we already have $k = 3$ as a starting point from Chapter 3. It turns out that with some modifications, the main ESP from that chapter (Lemma 26) can be generalized to all odd $k \geq 5$ by adding self-loops to each recognizer vertex. Most of the remaining gadgets used to prove the main result in Chapter 3 also generalize by this same transformation. Even so, this was a significant undertaking since the recurrence matrices of the recursive gadgets were determined by hand calculations (and verified for small k by computer computation). During this process, it was noted that the ESP of Lemma 30 is unnecessary when the natural generalization of the trace coincidence of Lemma 31 is applied first. This results in a slightly cleaner proof.

When k is even, it is a different story. To this point, we have used ESPs to get statements of the form "assuming X and Y are not both real, this problem is $\#\mathrm{P}\text{-hard}$ unless one of the following equations holds". If we attempt to apply the same ESP to even k, we turn out with something that is much less cleanly stated, the problem being with the "assuming X and Y are not both real" part. Such a statement would normally come from the cancelization of different polynomials that have been related (the determinant, trace, and eigenvalue shift), which simplify to get something like "$X - 1 = r$ for some $r \in \mathbb{R}$". In this case we instead get something more complicated, like TODO.

Furthermore, an attempt to find ESPs based on gadgets with more vertices suffered from the same problem, and the fact that it is less common to get nice cancellations involving larger gadgets.

In some sense, this is a repeat of the struggle that originally drove the discovery of ESPs. In chapter 3, we had a system of equations (corresponding to the failure sets of various gadgets), and we wanted to explicitly characterize the set of points for which at least one of the equations did not hold. This situation was exacerbated by the fact that these equations were written in terms of the complex argument of a polynomial, which is difficult to manipulate. What makes an ESP so special is that it has algebraic properties that line up in *just the right way* to simplify these confounding conditions to something comprehensible. Informally, we will use the term *syzygy* to describe any system of algebraic conditions that align in *exactly* the right way to produce an algebraic system that is far simpler. For example, equations 4.1 and 4.2 of Lemma 42 are complicated when considered individually. However, when combined, they form a syzygy that miraculously proves $\#\mathrm{P}$-hardness for almost everything that is required for the dichotomy result of Chapter 4. Now we are faced with the situation where the ESPs produce similar difficult algebraic conditions (mixed equations in complex and real variables), and we want some kind of new syzygy to grapple with this.

Such a syzygy was discovered through the examination of the coincidence graphs for various k. For each $k \geq 4$, a *chain* of ESPs exist, where the second gadget in one ESP has the same trace as the first gadget in the next ESP, and so on for some number of ESPs depending on k. The syzygy is a *pair* of Eigenvalue Shifted Pairs, as the matching traces are precisely the coincidence needed to prove a comprehensible result. Once this is done, the remaining special cases not addressed by the syzygy can be proved (laboriously) by introducing gadgets customized to deal with each such condition. The discovery of these remaining gadgets follows a similar progression as in Chapter 4. For each remaining condition, computer search and human observation are used to find gadgets that prove $\#\mathrm{P}$-hardness for small k, the gadget family is extrapolated to all k, and the transition matrix and other relevant terms calculated.

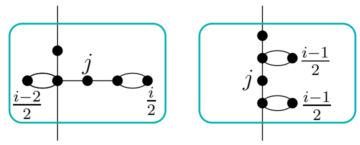
In the course of all of this, a condition was encountered that was resilient to proof (Lemma 60). This was solved using another szygy, this one composed of three gadgets. It is worth discussing in some detail how the gadgets for this Lemma were uncovered.

Recall that for a unary recursive gadget M, the main failure condition is $\mathrm{Arg}(B^2) = \mathrm{Arg}(C)$, where the characteristic polynomial of M is $x^2 + Bx + C$. Then $\mathrm{tr}(M) = -B$ and $\det(M) = C$. Technically, we must be assured that B and C are nonzero before using the failure condition in the form $\mathrm{Arg}(B^2) = \mathrm{Arg}(C)$, but the argument condition is the more challenging one to satisfy; in the worst case $B \neq 0$ and $C \neq 0$ translate to special cases that can be handled afterwords. Thus, when searching for gadgets, we just examine $\frac{B^2}{C}$ in factored form. Assuming that B and C are both nonzero, the gadget only fails when $\frac{B^2}{C}$ is a positive real number, which is why it is so valuable to find gadgets for which this is something simple (such as $\frac{B^2}{C} = (X-1)^2$). In the setting of Lemma 60, no such gadgets were found. A manual search ensued for a set of gadgets that combine together to give a simple condition, such as $\frac{B^2}{C} \cdot \frac{C'}{B'^2} = (X-1)^2$. The polynomial $\frac{B^2}{C}$ is often complicated even for relatively small gadgets, so a set of three gadgets were isolated for which $\frac{B^2}{C}$ was relatively simple in factored form. By combining these terms to cancel common factors, a syzygy was revealed that dealt with this outstanding condition nicely.

The twist in this story is that this three-gadget syzygy didn't apply just to the special case where $X^3 = 1$, but practically all settings of X and Y. Even more astonishingly, whenever the "special cases" of a zero-valued trace or determinant occured for one of the gadgets, one of the other two handled that subcase cleanly. We will give the earlier, more prolonged proof in the next section (which may be skipped without loss of continuity), and the direct proof by the syzygy in the following section. The relative size of these proofs is tribute to the incredible proving power wielded by this syzygy.

5.2.2 Recursive gadgets for $\mathrm{Pl}\text{-}\mathrm{Hol}_k(a, b)$ when k is even, using ESP-chains

For even k, we start by introducing *pairs* of Eigenvalue Shifted Pairs that share a common trace. Let gadget $\mathcal{M}_{i,j}$ be defined as in Figure 5.2.2 for all positive integers i and nonegative integers j,



(a) Gadget $\mathcal{M}_{i,j}$ when i is even (b) Gadget $\mathcal{M}_{i,j}$ when i is odd

Figure 5.3 Gadgets that form an ESP-chain. Labels indicate the number of length-2 paths in parallel.

where $i + j = k$. Then if i is odd,

$$\begin{aligned}\mathcal{M}_{i,j} &= \begin{bmatrix} a & 1 \\ 1 & b \end{bmatrix} \begin{bmatrix} a^{(i-1)/2} & 0 \\ 0 & b^{(i-1)/2} \end{bmatrix} \begin{bmatrix} a^j & 1 \\ 1 & b^j \end{bmatrix} \begin{bmatrix} a^{(i-1)/2} & 0 \\ 0 & b^{(i-1)/2} \end{bmatrix} \\ &= \begin{bmatrix} a^k + a^{(i-1)/2}b^{(i-1)/2} & a^{(i+1)/2}b^{(i-1)/2} + b^{k-1} \\ a^{k-1} + a^{(i-1)/2}b^{(i+1)/2} & a^{(i-1)/2}b^{(i-1)/2} + b^k \end{bmatrix}.\end{aligned}$$

If i is even,

$$\begin{aligned}\mathcal{M}_{i,j} &= \begin{bmatrix} a & 1 \\ 1 & b \end{bmatrix} \begin{bmatrix} a^{k-1} + a^{i/2-1}b^{i/2} & 0 \\ 0 & b^{k-1} + a^{i/2}b^{i/2-1} \end{bmatrix} \\ &= \begin{bmatrix} a^k + a^{i/2}b^{i/2} & a^{i/2}b^{i/2-1} + b^{k-1} \\ a^{k-1} + a^{i/2-1}b^{i/2} & a^{i/2}b^{i/2} + b^k \end{bmatrix}.\end{aligned}$$

Let $X = ab$ and $Y = a^k + b^k$. We note that if i is odd then $i < k$ and $j > 0$ then $\mathcal{M}_{i+1,j-1} - \mathcal{M}_{i,j} = (X^{(i+1)/2} - X^{(i-1)/2})I = X^{(i-1)/2}(X-1)I$. If i is even then $\operatorname{tr}(\mathcal{M}_{i,j}) = Y + 2X^{i/2} = \operatorname{tr}(\mathcal{M}_{i+1,j-1})$. This leads to a chain of gadgets where each pair in the chain either forms an ESP or has a common trace, alternately. If i is odd then $\det(\mathcal{M}_{i,j}) = X^{i-1}(X-1)(X^j-1)$, and if i is even then $\det(\mathcal{M}_{i,j}) = X^{i/2-1}(X-1)(X^{i/2+j} + X^{i/2} + Y)$.

Lemma 54. *Suppose i is an odd positive integer, $j \geq 3$ is an integer, $X \neq 0$, $X^j \neq 1$, $X^{j-2} \neq 1$, $Y + 2X^{(i+1)/2} \neq 0$, $X^{(i+1)/2+j-1} + X^{(i+1)/2} + Y \neq 0$, $X^{(i+3)/2+j-3} + X^{(i+3)/2} + Y \neq 0$, $(Y+2X^{(i-1)/2})^2 - 4X^{i-1}(X-1)(X^j-1) \neq 0$, and $(Y+2X^{(i+1)/2})^2 - 4X^{i+1}(X-1)(X^{j-2}-1) \neq 0$, and it is not the case that both X and Y are real valued. Then gadget $\mathcal{M}_{i,j}$, $\mathcal{M}_{i+1,j-1}$, $\mathcal{M}_{i+2,j-2}$,* *or* $\mathcal{M}_{i+3,j-3}$ *is a* $(i+j)$*-regular unary recursive gadget with nonzero eigenvalues with distinct norm.*

Proof. First we verify $(\mathcal{M}_{i,j}, \mathcal{M}_{i+1,j-1})$ is an eigenvalue shifted pair.

1. $\mathcal{M}_{i+1,j-1} - \mathcal{M}_{i,j} = X^{(i-1)/2}(X-1)I$ and $X^{(i-1)/2}(X-1) \neq 0$
2. $\det(\mathcal{M}_{i,j}) = X^{i-1}(X-1)(X^j-1) \neq 0$
3. $\det(\mathcal{M}_{i+1,j-1}) = X^{(i-1)/2}(X-1)(X^{(i+1)/2+j-1} + X^{(i+1)/2} + Y) \neq 0$
4. $\operatorname{tr}(\mathcal{M}_{i,j})^2 - 4\det(\mathcal{M}_{i,j}) = (Y + 2X^{(i-1)/2})^2 - 4X^{i-1}(X-1)(X^j-1) \neq 0$

Next we do the same for $(\mathcal{M}_{i+2,j-2}, \mathcal{M}_{i+3,j-3})$.

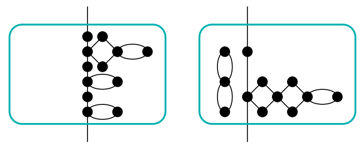
1. $\mathcal{M}_{i+3,j-3} - \mathcal{M}_{i+2,j-2} = X^{(i+1)/2}(X-1)I$ and $X^{(i+1)/2}(X-1) \neq 0$
2. $\det(\mathcal{M}_{i+2,j-2}) = X^{i+1}(X-1)(X^{j-2}-1) \neq 0$
3. $\det(\mathcal{M}_{i+3,j-3}) = X^{(i+1)/2}(X-1)(X^{(i+3)/2+j-3} + X^{(i+3)/2} + Y) \neq 0$
4. $\operatorname{tr}(\mathcal{M}_{i+2,j-2})^2 - 4\det(\mathcal{M}_{i+2,j-2}) = (Y + 2X^{(i+1)/2})^2 - 4X^{i+1}(X-1)(X^{j-2}-1) \neq 0$

We claim that some $M \in \{\mathcal{M}_{i,j}, \mathcal{M}_{i+1,j-1}, \mathcal{M}_{i+2,j-2}, \mathcal{M}_{i+3,j-3}\}$ has eigenvalues with distinct norm. Otherwise, Corollary 6 indicates that there exists $r, s \in \mathbb{R}$ such that $rX^{(i-1)/2}(X-1) = \operatorname{tr}(\mathcal{M}_{i+1,j-1}) = Y + 2X^{(i+1)/2} = \operatorname{tr}(\mathcal{M}_{i+2,j-2}) = sX^{(i+1)/2}(X-1)$, hence $r = sX$ and $X = r/s \in \mathbb{R}$ (note that $s \neq 0$ because $Y + 2X^{(i+1)/2} \neq 0$). Furthermore, $Y + 2X^{(i+1)/2} = sX^{(i+1)/2}(X-1)$ so $Y = sX^{(i+1)/2}(X-1) - 2X^{(i+1)/2} \in \mathbb{R}$. □

These pairs of Eigenvalue Shifted Pairs are quite useful, and using several of them in conjunction provides an easy way to prove #P-hardness when k is sufficiently large. However, for smaller k there are fewer ESPs in the chain, so we will need to follow a different line of reasoning. We will use the setting $i = k-3$ and $j = 3$, so the cases remaining after applying this pair of ESPs will be dealt with presently.

Lemma 55. *If* $X = 0$ *and* $Y \notin \mathbb{R}$ *then gadget* $\mathcal{M}_{1,k-1}$ *has a transition matrix with nonzero eigenvalues of distinct norm.*

Proof. We get $\mathrm{tr}[\mathcal{M}_{1,k-1}] = Y + 2$ and $\det[\mathcal{M}_{1,k-1}] = 1$, so if the eigenvalues of $\mathcal{M}_{1,k-1}$ have equal norm then by Lemma 53, $2 + Y = 2 + \overline{Y}$ and $Y \in \mathbb{R}$. $\square$

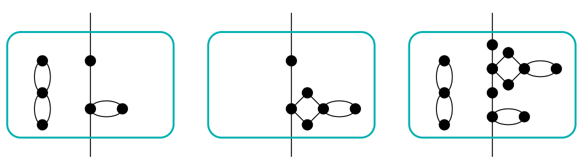


(a) Gadget M_3 (b) Gadget M_4

Figure 5.4 Some recursive gadgets for even k. These are both generalized to higher degrees by adding length 2 cycles to the recognizer vertices.

Lemma 56. *Suppose $Y = -2X^{(k-2)/2}$. Then gadget M_3 has nonzero eigenvalues with distinct norm, unless X and Y are both real numbers.*

Proof. We calculate that $\mathrm{tr}(M_3) = 4X^{k-2} + 2X^{k-1} - 2X^k + X^{(k-4)/2}Y + 3X^{(k-2)/2}Y + Y^2$ and $\det(M_3) = (X-1)^3 X^{3k/2-4}(X^{k/2+1} + X^{k/2-1} + Y)$. Under the condition $Y = -2X^{(k-2)/2}$, we find that $(\mathrm{tr}(M_3))^2 = 4(X-1)^4 X^{2k-6}(1+X)^2 \neq 0$ and $\det(M_3) = (X-1)^4 X^{2k-5}(1+X) \neq 0$, hence by Lemma 53, if gadget M_3 has eigenvalues of equal norm, then $\mathrm{Arg}(4X+4) = \mathrm{Arg}(X)$, $X \in \mathbb{R}$, and $Y = -2X^{(k-2)/2} \in \mathbb{R}$. $\square$



(a) Gadget M_5 (b) Gadget M_6 (c) Gadget M_7

Figure 5.5 A three-gadget syzygy. All gadgets pictured here are shown for $k = 4$, but are generalized to all even $k \geq 4$ by adding any number of length-2 cycles to the degree-4 vertices

Lemma 57. *Suppose $Y = -X^{(k-2)/2} - X^{(k+2)/2}$. Then gadget M_5 has nonzero eigenvalues with distinct norm, unless X and Y are both real numbers.*

Proof. We calculate that $\mathrm{tr}(M_5) = 2X^{k/2} + Y$ and $\det(M_5) = (X-1)X^{(k-2)/2}(2X^{k/2}+Y)$. Under the condition $Y = -X^{(k-2)/2} - X^{(k+2)/2}$, we find that $(\mathrm{tr}(M_5))^2 = (X-1)^4X^{k-2} \neq 0$ and $\det(M_5) = -(X-1)^3X^{k-2} \neq 0$, hence by Lemma 53, if gadget M_5 has eigenvalues of equal norm, then $\mathrm{Arg}(X-1) = \mathrm{Arg}(-1)$, $X \in \mathbb{R}$, and $Y = -X^{(k-2)/2} - X^{(k+2)/2} \in \mathbb{R}$. □

Lemma 58. *Suppose either $Y = -2X^{k/2}$ or $(Y + 2X^{(k-2)/2})^2 = 4X^{k-2}(X-1)^2$. Then gadget M_6 has nonzero eigenvalues with distinct norm, unless X and Y are both real numbers.*

Proof. We calculate that $\mathrm{tr}(M_6) = 2X^{(k-2)/2} + Y$ and $\det(M_6) = (X-1)X^{k/2-2}(X^{k/2+1} + X^{k/2-1} + Y)$. Supposing $Y = -2X^{k/2}$, we find that $(\mathrm{tr}(M_6))^2 = 4(X-1)^2X^{k-2} \neq 0$ and $\det(M_6) = (X-1)^3X^{k-3} \neq 0$, hence by Lemma 53, if gadget M_6 has eigenvalues of equal norm, then $\mathrm{Arg}(4X) = \mathrm{Arg}(X-1)$, $X \in \mathbb{R}$, and $Y = -2X^{k/2} \in \mathbb{R}$.

Now suppose $(Y + 2X^{(k-2)/2})^2 = 4X^{k-2}(X-1)^2$, so $Y = \pm 2X^{(k-2)/2}(X-1) - 2X^{(k-2)/2}$ and $(\mathrm{tr}(M_6))^2 = 4(X-1)^2X^{k-2} \neq 0$. If $X \in \mathbb{R}$ then $Y \in \mathbb{R}$, so we may assume that $X \notin \mathbb{R}$. If $Y = 2X^{(k-2)/2}(X-1) - 2X^{(k-2)/2}$ then $\det(M_6) = (X-1)^2X^{k-3}(3+X) \neq 0$, hence by Lemma 53, Gadget M_6 has eigenvalues with distinct norm, since otherwise $\mathrm{Arg}(4X) = \mathrm{Arg}(3+X)$ and $X \in \mathbb{R}$. Similarly, if $Y = -2X^{(k-2)/2}(X-1) - 2X^{(k-2)/2}$ then $\det(M_6) = (X-1)^3X^{k-3} \neq 0$ and by Lemma 53, gadget M_6 has eigenvalues of distinct norm, since otherwise $\mathrm{Arg}(4X) = \mathrm{Arg}(X-1)$ and $X \in \mathbb{R}$. □

Lemma 59. *Suppose $(Y + 2X^{(k-4)/2})^2 = 4X^{k-4}(X-1)(X^3-1)$. Then either gadget M_7 or gadget M_4 has nonzero eigenvalues with distinct norm, unless $X \in \mathbb{R}$ and $Y \in \mathbb{R}$.*

Proof. If $X \in \mathbb{R}$ then $4X^{k-4}(X-1)(X^3-1) \geq 0$ so $Y + 2X^{(k-4)/2} \in \mathbb{R}$ and $Y \in \mathbb{R}$, hence we may now assume that $X \notin \mathbb{R}$. We calculate the following.

$$
\begin{aligned}
\mathrm{tr}(M_7) &= -(2X^{k/2}+Y)(-2X^{k/2-1} + X^{k/2} - X^{k/2-2} - Y) \\
\mathrm{tr}(M_4) &= -(2X^{k/2}+Y)(-2X^{k/2-1} + X^{k/2} - X^{k/2-2} - Y) \\
\det(M_7) &= (X-1)^2X^{k-3}(2X^{k/2}+Y)(X^{(k+2)/2} + X^{k/2-1} + Y) \\
\det(M_4) &= (X-1)X^{k/2-5}(2X^{k/2}+Y)(X^k + 2X^{1+k} + 2X^{2+k} - 2X^{3+k} + X^{4+k} + \\
&\quad X^{k/2+1}Y + 2X^{(k+4)/2}Y + X^{k/2+3}Y + X^3Y^2)
\end{aligned}
$$

Note that these gadgets have identical trace. Let S denote $(Y+2X^{(k-4)/2})^2-4X^{k-4}(X-1)(X^3-1)$, which is zero by assumption, and then $\det(M_4)=\det(M_4)-SX^n(X-1)(Y+2X^{n+2})=(X-1)^2X^{k-4}(X+3)(2X^{k/2}+Y)(X^{(k+2)/2}+X^{k/2-1}+Y)$, which we claim is nonzero. If it were equal to zero, as $X\notin\mathbb{R}$, this would force either $Y=***$ or $Y=***$. If $Y=-2X^{k/2}$ then $S=4(X-1)^2X^{k-3}$ and if $Y=-X^{k/2+1}-X^{k/2-1}$ then $S=(X-1)^2X^{k-2}(1+X)^2$, which are incompatible with $X\notin\mathbb{R}$ and $S=0$. These facts also imply that $\det(M_7)\neq 0$. Similarly, $\mathrm{tr}(M_7)\neq 0$ since otherwise $Y=-2X^{k/2-1}+X^{k/2}-X^{k/2-2}$ but then $S=-3(X-1)^2X^{k-4}(1+X)^2$. Applying Lemma 53 twice, $\mathrm{Arg}(\det(M_7))=\mathrm{Arg}(\mathrm{tr}(M_7)^2)=\mathrm{Arg}(\mathrm{tr}(M_4)^2)=\mathrm{Arg}(\det(M_4))$. However, this would imply $\mathrm{Arg}(X)=\mathrm{Arg}(3+X)$ and $X\in\mathbb{R}$, so we conclude that either M_7 or M_4 has nonzero eigenvalues with distinct norm. □

Lemma 60. *Suppose $X^3=1$ but $X\neq 1$. Then either gadget M_5, gadget M_6, or gadget M_7 has nonzero eigenvalues with distinct norm.*

Proof. We start by calculating the trace and determinant of all three gadgets.

$$\begin{aligned}
\mathrm{tr}(M_5) &= 2X^{k/2}+Y\\
\mathrm{tr}(M_6) &= 2X^{k/2-1}+Y\\
\mathrm{tr}(M_7) &= (2X^{k/2}+Y)(2X^{k/2-1}-X^{k/2}+X^{k/2-2}+Y)\\
\det(M_5) &= (X-1)X^{k/2-1}(2X^{k/2}+Y)\\
\det(M_6) &= (X-1)X^{k/2-2}(X^{k/2-1}+X^{k/2+1}+Y)\\
\det(M_7) &= (X-1)^2X^{k-3}(2X^{k/2}+Y)(X^{k/2-1}+X^{k/2+1}+Y)
\end{aligned}$$

We claim that if any one of these traces or determinants is zero, then one of the other two gadgets has nonzero eigenvalues with distinct norm. For instance, if $Y=-2X^{k/2}$, then $\mathrm{tr}(M_6)=-2(X-1)X^{(k-2)/2}$ and $\det(M_6)=(X-1)^3X^{k-3}$ so by Lemma 53, if gadget M_6 had eigenvalues with equal norm then we would have $\mathrm{Arg}(4X)=\mathrm{Arg}(X-1)$ and $X\in\mathbb{R}$. Similarly, if $Y=-2X^{k/2-1}$ then $\mathrm{tr}(M_7)=-2(X-1)^2X^{k-3}(1+X)$ and $\det(M_7)=2(X-1)^4X^{2k-5}(1+X)$ and Lemma 53 implies that gadget M_7 has eigenvalues with unequal norm since $\mathrm{Arg}(2(1+X))=\mathrm{Arg}(X)$ and $X\in\mathbb{R}$ otherwise. If $Y=-X^{k/2+1}-X^{k/2-1}$ then $\mathrm{tr}(M_5)=-(X-1)^2X^{(k-2)/2}$ and

$\det(M_5) = -(X-1)^3 X^{k-2}$ and by Lemma 53 gadget M_5 has eigenvalues with unequal norm because otherwise $\operatorname{Arg}(1-X) = \operatorname{Arg}(1)$ and $X \in \mathbb{R}$. Finally, if $Y = -2X^{k/2-1} + X^{k/2} - X^{k/2-2}$ then $\operatorname{tr}(M_5) = (X-1)X^{(k-4)/2}(1+3X)$ and $\det(M_5) = (X-1)^2 X^{k-3}(1+3X)$ and again by Lemma 53 gadget M_5 has eigenvalues with unequal norm since $\operatorname{Arg}(1+3X) = \operatorname{Arg}(X)$ and $X \in \mathbb{R}$ otherwise.

Now we may assume that each trace and determinant is nonzero. If all three gadgets fail to have eigenvalues with distinct norm, then Lemma 53 indicates that $\frac{\operatorname{tr}^2(M)}{\det(M)} \in \mathbb{R}^+$ for each $M \in \{M_5, M_6, M_7\}$. Supposing this is the case, we observe that $\frac{X^{-k/2+1}(2X^{k/2}+Y)}{X-1} = \frac{\operatorname{tr}^2(M_5)}{\det(M_5)} \in \mathbb{R}$ and $\frac{X^{k/2-2}(X^2-1)}{2X^{k/2-1}+Y} = \sqrt{\frac{\operatorname{tr}^2(M_7)\det(M_6)\det(M_5)}{\operatorname{tr}^2(M_5)\operatorname{tr}^2(M_6)\det(M_7)}} + 1 \in \mathbb{R}$. Note that for either possible setting of X under consideration, these conditions form a pair of affine linear subspaces in the complex plane which intersect only when $Y = -2X^{k/2-1}$, but we have already established that gadget M_7 has nonzero eigenvalues of distinct norm in this case. □

In summary, when $k \geq 4$ is even we have a nonsingular unary recursive gadget with eigenvalues of distinct norm for every setting of X and Y unless $X = 1$ (degenerate) or X and Y are both real (which is handled by [6]).

5.2.3 Recursive gadgets for $\text{Pl-Hol}_k(a,b)$ when k is even, using a 3-gadget syzygy

Our goal here is to construct recursive gadgets for all even $k \geq 4$, provided $X \neq 1$ and that X and Y are not both real (note that this excludes $X = -1$ with $Y = \pm 2$, which is tractable for even k). First we deal with a special case of $X = 0$, both for even and odd k.

Lemma 61. *If $X = 0$ and $Y \notin \mathbb{R}$ then gadget $\mathcal{M}_{1,k-1}$ has a transition matrix with nonzero eigenvalues of distinct norm.*

Proof. We get $\operatorname{tr}[\mathcal{M}_{1,k-1}] = Y + 2$ and $\det[\mathcal{M}_{1,k-1}] = 1$, so if the eigenvalues of $\mathcal{M}_{1,k-1}$ have equal norm then by Lemma 53, $2 + Y = 2 + \overline{Y}$ and $Y \in \mathbb{R}$. □

Lemma 62. *Suppose $X \notin \{0,1\}$, and it is not the case that X and Y are both real. Then either gadget M_5, gadget M_6, or gadget M_7 has nonzero eigenvalues with distinct norm.*

Proof. We start by calculating the trace and determinant of all three gadgets.

$$\begin{aligned}
\operatorname{tr}(M_5) &= 2X^{k/2} + Y \\
\operatorname{tr}(M_6) &= 2X^{k/2-1} + Y \\
\operatorname{tr}(M_7) &= (2X^{k/2} + Y)(2X^{k/2-1} - X^{k/2} + X^{k/2-2} + Y) \\
\det(M_5) &= (X-1)X^{k/2-1}(2X^{k/2} + Y) \\
\det(M_6) &= (X-1)X^{k/2-2}(X^{k/2-1} + X^{k/2+1} + Y) \\
\det(M_7) &= (X-1)^2 X^{k-3}(2X^{k/2} + Y)(X^{k/2-1} + X^{k/2+1} + Y)
\end{aligned}$$

Note that if $X = -1$ then $Y \notin \mathbb{R}$, $\det(M_5) \neq 0$, $\operatorname{tr}(M_5) \neq 0$, and $\frac{\operatorname{tr}^2(M_5)}{\det(M_5)} = \frac{2X^{k/2}+Y}{(X-1)X^{k/2-1}} \notin \mathbb{R}$ so we are done by Lemma 53; thus we will assume that $X \neq -1$ throughout. We claim that if any one of these traces or determinants is zero, then one of the other two gadgets has nonzero eigenvalues with distinct norm. For instance, if $Y = -2X^{k/2}$, then $\operatorname{tr}(M_6) = -2(X-1)X^{(k-2)/2}$ and $\det(M_6) = (X-1)^3 X^{k-3}$ so by Lemma 53, if gadget M_6 had eigenvalues with equal norm then we would have $\operatorname{Arg}(4X) = \operatorname{Arg}(X-1)$ and $X, Y \in \mathbb{R}$. Similarly, if $Y = -2X^{k/2-1}$ then $\operatorname{tr}(M_7) = -2(X-1)^2 X^{k-3}(1+X)$ and $\det(M_7) = 2(X-1)^4 X^{2k-5}(1+X)$ and Lemma 53 implies that gadget M_7 has eigenvalues with unequal norm since $\operatorname{Arg}(2(1+X)) = \operatorname{Arg}(X)$ and $X, Y \in \mathbb{R}$ otherwise. If $Y = -X^{k/2+1} - X^{k/2-1}$ then $\operatorname{tr}(M_5) = -(X-1)^2 X^{(k-2)/2}$ and $\det(M_5) = -(X-1)^3 X^{k-2}$ and by Lemma 53 gadget M_5 has eigenvalues with unequal norm because otherwise $\operatorname{Arg}(1-X) = \operatorname{Arg}(1)$ and $X, Y \in \mathbb{R}$. Finally, if $Y = -2X^{k/2-1} + X^{k/2} - X^{k/2-2}$ then $\operatorname{tr}(M_5) = (X-1)X^{(k-4)/2}(1+3X)$ and $\det(M_5) = (X-1)^2 X^{k-3}(1+3X)$ and again by Lemma 53 gadget M_5 has eigenvalues with unequal norm since $\operatorname{Arg}(1+3X) = \operatorname{Arg}(X)$ and $X, Y \in \mathbb{R}$ otherwise.

Now we may assume that each trace and determinant is nonzero. If all three gadgets fail to have eigenvalues with distinct norm, then Lemma 53 indicates that $\frac{\operatorname{tr}^2(M)}{\det(M)} \in \mathbb{R}^+$ for each $M \in \{M_5, M_6, M_7\}$. Supposing this is the case, we observe that $\frac{2X^{k/2}+Y}{X^{k/2-1}(X-1)} = \frac{\operatorname{tr}^2(M_5)}{\det(M_5)} \in \mathbb{R}$ and $\frac{\operatorname{tr}^2(M_7)\det(M_6)\det(M_5)}{\operatorname{tr}^2(M_5)\operatorname{tr}^2(M_6)\det(M_7)} = \frac{(2X^{k/2-1}-X^{k/2}+X^{k/2-2}+Y)^2}{(2X^{k/2-1}+Y)^2} = (1 - \frac{X^{k/2-2}(X^2-1)}{2X^{k/2-1}+Y})^2$, hence $\frac{X^{k/2-2}(X^2-1)}{2X^{k/2-1}+Y} \in \mathbb{R}$.

Fix $X \notin \{0, \pm 1\}$, and this defines two lines on the Y-plane as s and t vary over $\mathbb{R}$:

$$\begin{aligned} Y &= -2X^{k/2} + r \cdot X^{k/2-1}(X-1) \\ Y &= -2X^{k/2-1} + s \cdot X^{k/2-2}(X^2-1). \end{aligned}$$

The slopes are not equal, because otherwise we would have $X^{k/2-2}(X^2-1) = X^{k/2-1}(X-1)$ and since $X \notin \{0, 1\}$ we would get $X + 1 = X$. Thus for any $X \notin \{0, \pm 1\}$, these two lines intersect at a unique point Y, which is given by $Y = -2X^{k/2-1}$ (this can be verified by substituting $r = 2$ and $s = 0$), but we have already established that gadget M_7 has nonzero eigenvalues of distinct norm in this case. $\square$

5.2.4 Recursive gadgets for $\text{Pl-Hol}_k(a, b)$ when k is odd

Now we construct recursive gadgets for all odd $k \geq 5$, ($k = 3$ was done in Chapter 3) provided $X \neq 1$, X and Y are not both real, and if $X = -1$ then $Y \neq \pm 2\mathfrak{i}$. We start with an ESP for all odd $k \geq 3$. This is a natural generalization of the main ESP in Chapter 3.

Lemma 63. *Suppose* $X \notin \{0, 1, -1\}$, $X^{(k+1)/2} + X^{(k-1)/2} + Y \neq 0$, *and* $(Y + 2X^{(k-3)/2})^2 \neq 4X^{k-3}(X-1)(X^2-1)$. *Then either gadget* $\mathcal{M}_{k-2,2}$ *or gadget* $\mathcal{M}_{k-1,1}$ *has nonzero eigenvalues with distinct norm, unless* X *and* Y *are both real numbers.*

Proof. The transition matrices are

$$\begin{aligned} \mathcal{M}_{k-2,2} &= \begin{bmatrix} a^k + a^{(k-3)/2}b^{(k-3)/2} & a^{(k-1)/2}b^{(k-3)/2} + b^{k-1} \\ a^{k-1} + a^{(k-3)/2}b^{(k-1)/2} & a^{(k-3)/2}b^{(k-3)/2} + b^k \end{bmatrix}, \\ \mathcal{M}_{k-1,1} &= \begin{bmatrix} a^k + a^{(k-1)/2}b^{(k-1)/2} & a^{(k-1)/2}b^{(k-1)/2-1} + b^{k-1} \\ a^{k-1} + a^{(k-1)/2-1}b^{(k-1)/2} & a^{(k-1)/2}b^{(k-1)/2} + b^k \end{bmatrix}. \end{aligned}$$

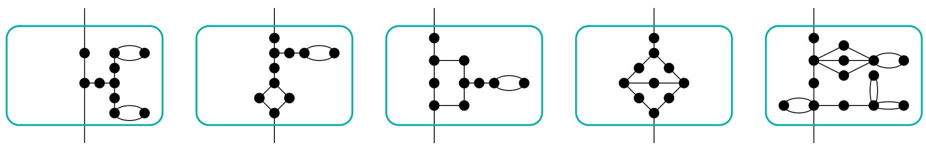
These form an ESP:

1. $\mathcal{M}_{k-1,1} - \mathcal{M}_{k-2,2} = X^{(k-3)/2}(X-1)I$ and $X^{(k-3)/2}(X-1) \neq 0$
2. $\det(\mathcal{M}_{k-2,2}) = X^{k-3}(X-1)^2(X+1) \neq 0$
3. $\det(\mathcal{M}_{k-1,1}) = X^{(k-3)/2}(X-1)(X^{(k+1)/2} + X^{(k-1)/2} + Y) \neq 0$

4. $\mathrm{tr}(\mathcal{M}_{k-2,2})^2 - 4\det(\mathcal{M}_{k-2,2}) = (Y + 2X^{(k-3)/2})^2 - 4X^{k-3}(X-1)^2(X+1) \neq 0$

By Corollary 6, either $\mathcal{M}_{k-1,1}$ or $\mathcal{M}_{k-2,2}$ has nonzero eigenvalues of distinct norm unless $Y + 2X^{(k-3)/2} = \mathrm{tr}(\mathcal{M}_{k-2,2}) = rX^{(k-3)/2}(X-1)$ and $X^{k-3}(X-1)^2(X+1) = \det(\mathcal{M}_{k-2,2}) = sX^{k-3}(X-1)^2$ for some $r, s \in \mathbb{R}$. Then we would have $X + 1 = s$ so $X = s - 1 \in \mathbb{R}$, and futhermore $Y = rX^{(k-3)/2}(X-1) - 2X^{(k-3)/2} \in \mathbb{R}$. □

Now we deal with the exceptional cases.



(a) Gadget M_8 (b) Gadget M_9 (c) Gadget M_{10} (d) Gadget M_{11} (e) Gadget M_{12}

Figure 5.6 Recursive gadgets for odd k. Shown here for $k = 3$ and (for gadget M_{12}) $k = 5$. These are all generalized to higher odd degrees by adding length 2 cycles to the degree 3 (or 5) vertices.

Lemma 64. *Suppose $X^{(k+1)/2} + X^{(k-1)/2} + Y = 0$. Then gadget M_8 has nonzero eigenvalues with distinct norm, unless X and Y are both real numbers.*

Proof. We calculate that $\mathrm{tr}(M_8) = Y^2 + YX^{(k-3)/2} + 3YX^{(k-1)/2} + 6X^{k-1} - 2X^k$ and

$$\begin{aligned}\det(M_8) &= (X-1)X^{(k-23)/2}(X^{(3k+15)/2} + 11X^{(3k+17)/2} - 5X^{(3k+19)/2} + X^{(3k+21)/2} + 3X^{k+8}Y \\ &\quad +10X^{k+9}Y - X^{k+10}Y + X^{(k+17)/2}Y^2 + 5X^{(k+19)/2}Y^2 + X^{10}Y^3).\end{aligned}$$

Miraculously, under the condition $X^{(k+1)/2} + X^{(k-1)/2} + Y = 0$, we find that $\mathrm{tr}(M_8) = X^{k-2}(X-1)^3 \neq 0$ and $\det(M_8) = -X^{2(k-2)}(X-1)^5 \neq 0$, hence by Lemma 53, if gadget M_8 had eigenvalues of equal norm, then $1 - X \in \mathbb{R}$, $X \in \mathbb{R}$, and $Y = -X^{(k+1)/2} - X^{(k-1)/2} \in \mathbb{R}$, but by assumption this is not the case. □

Lemma 65. *Suppose $X \notin \mathbb{R}$ and $(Y + 2X^{(k-3)/2})^2 = 4X^{k-3}(X-1)(X^2-1)$. Then either gadget M_9 or gadget M_{10} has nonzero eigenvalues with distinct norm.*

Proof. We calculate the following.

$$\begin{aligned}
\operatorname{tr}(M_9) &= 4X^{k-2} + 2X^{k-1} - 2X^k + 3X^{(k-3)/2}Y + X^{(k-1)/2}Y + Y^2 \\
\operatorname{tr}(M_{10}) &= 4X^{k-2} + 2X^{k-1} - 2X^k + 3X^{(k-3)/2}Y + X^{(k-1)/2}Y + Y^2 \\
\det(M_9) &= (X-1)^3X^{(3k-9)/2}(1+X)(X^{(k+1)/2} + X^{(k-1)/2} + Y) \\
\det(M_{10}) &= (X-1)^2X^{k-3}(3X^{k-1} + X^{k+1} + 3X^{(k-1)/2}Y + X^{(k+1)/2}Y + Y^2)
\end{aligned}$$

Note that these gadgets have identical trace. First, $\det(M_9)$ is nonzero, since substituting $Y = -X^{(k-1)/2} - X^{(1+k)/2}$ into $(Y+2X^{(k-3)/2})^2 - 4X^{k-3}(X-1)(X^2-1)$, we get $(X-1)^2X^{k-1} \neq 0$. Next, let S denote $(Y + 2X^{(k-3)/2})^2 - 4X^{k-3}(X-1)(X^2-1)$, which is zero by assumption, and then $\det(M_{10}) = \det(M_{10}) - S(X-1)^2X^{k-3} = (X-1)^3X^{(3k-9)/2}(X+4)(X^{(k+1)/2} + X^{(k-1)/2} + Y) \neq 0$. Finally, $\operatorname{tr}(M_9) = \operatorname{tr}(M_9) - S = (X-1)X^{(k-3)/2}(2X^{(1+k)/2} + Y) \neq 0$. Now applying Lemma 53 twice, if both gadgets fail to have eigenvalues with distinct norm, then $\operatorname{Arg}(\det(M_9)) = \operatorname{Arg}(\operatorname{tr}(M_9)^2) = \operatorname{Arg}(\operatorname{tr}(M_{10})^2) = \operatorname{Arg}(\det(M_{10}))$. However, this would imply $\operatorname{Arg}(X+4) = \operatorname{Arg}(X+1)$ and $X \in \mathbb{R}$, so we conclude that either M_9 or M_{10} has nonzero eigenvalues with distinct norm. □

Lemma 66. *Suppose $X \in \mathbb{R}$, $Y \notin \mathbb{R}$, and $(Y + 2X^{(k-3)/2})^2 = 4X^{k-3}(X-1)(X^2-1)$. Then gadget M_{11} has nonzero eigenvalues with distinct norm.*

Proof. First note that $X \notin \{0,1\}$, because otherwise $(Y+2X^{(k-3)/2})^2 = 4X^{k-3}(X-1)(X^2-1)$ would imply $Y \in \mathbb{R}$. We calculate the following.

$$\begin{aligned}
\operatorname{tr}(M_{11}) &= Y^2 + 2X^{(k-3)/2}(3X^{1+(k-3)/2} - X^{3+(k-3)/2} + 2Y) \\
\det(M_{11}) &= (X-1)^3X^{\frac{3}{2}(k-3)}(X^{1+(k-3)/2} + 2X^{2+(k-3)/2} + X^{3+(k-3)/2} + 2Y)
\end{aligned}$$

Let S denote $(Y+2X^{(k-3)/2})^2 - 4X^{k-3}(X-1)(X^2-1)$, which is zero by assumption. Incredibly, $\operatorname{tr}(M_{11}) = \operatorname{tr}(M_{11}) - S = 2X^{k-2}(X-1)^2$, which is real and nonzero, and since $X \in \mathbb{R} - \{0,1\}$ and $Y \notin \mathbb{R}$, we know $\det(M_{11}) \neq 0$. Then by Lemma 53, gadget #2 has eigenvalues with distinct norm unless $\det(M_{11}) \in \mathbb{R}$, but this would imply $Y \in \mathbb{R}$. □

Now we deal with $X = -1$, which consists of two subcases.

Lemma 67. *If the degree $k \geq 5$ is odd, $X = -1$, $|Y| \neq 2$, and $Y \notin \mathbb{R}$, then gadget $\mathcal{M}_{2,k-2}$ has a transition matrix with nonzero eigenvalues of distinct norm.*

Proof. We get $\operatorname{tr}[\mathcal{M}_{2,k-2}] = Y - 2$ and $\det[\mathcal{M}_{2,k-2}] = (XY + X^2 + X^k) - (X + X^{k-1} + Y) = -2Y$, so if $\mathcal{M}_{2,k-2}$ does not have nonzero eigenvalues with distinct norm then by Lemma 53, $(Y-2) \cdot |-2Y| = \operatorname{tr}(\mathcal{M}_{2,k-2}) \cdot |\det(\mathcal{M}_{2,k-2})| = \overline{\operatorname{tr}(\mathcal{M}_{2,k-2})} \cdot \det(\mathcal{M}_{2,k-2}) = -(\overline{Y} - 2)(2Y)$, so it follows that $(|Y| - 2)(|Y| + Y) = 0$, which is a contradiction. □

Lemma 68. *If the degree $k \geq 3$ is odd, $X = -1$, $|Y| = 2$, and $Y \neq \pm 2\mathrm{i}$, then the transition matrix of unary gadget M_{12} has nonzero eigenvalues with distinct norm.*

Proof. Under these conditions, $\det(M_{12}) = -4Y^2 \neq 0$ and $\operatorname{tr}(M_{12}) = 4 + Y^2 \neq 0$. If the eigenvalues of M_{12} have identical norm then by Lemma 53, $(4 + Y^2) \cdot |-4Y^2| = \operatorname{tr}(M_{12}) \cdot |\det(M_{12})| = \overline{\operatorname{tr}(M_{12})} \cdot \det(M_{12}) = (4 + \overline{Y}^2) \cdot (-4Y^2)$, and from this it follows that $4Y(\overline{Y} + Y)(4 + |Y|^2) = 0$, which cannot be true. □

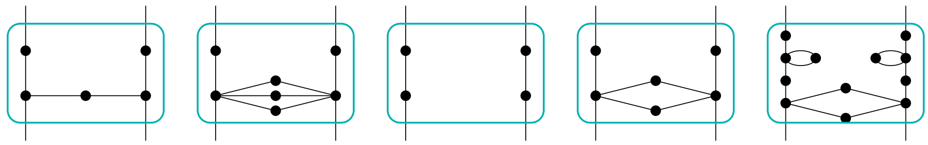
The $X = 0$ case is dispatched with by Lemma 55, so for every odd $k \geq 5$ and for every setting of X and Y, we now have a nonsingular unary recursive gadget with eigenvalues of distinct norm unless $X = 1$, $(X, Y) = (-1, \pm 2i)$, or X and Y are both real. The $k = 3$ case is covered in Chapter 3.

5.2.5 Recursive gadgets for $\operatorname{Hol}_k(a, b)$

Although Pl-$\operatorname{Hol}_k(a, b)$ is in P when $a^k = b^k$ (equivalently, $Y^2 = 4X^k$), it turns out that $\operatorname{Hol}_k(a, b)$ is $\#\mathrm{P}$-hard in this case — except for the tractable subcases $X \in \{0, \pm 1\}$. So this needs to be proved separately, and we do so presently.

Lemma 69. *Suppose $k \geq 3$, $a^k = b^k$ and $X \notin \{0, \pm 1\}$. Then we can efficiently simulate a set of pairwise linearly independent signatures of the form $[x, y, x]$, and $\operatorname{Hol}_k(a, b)$ is $\#\mathrm{P}$-hard.*

Proof. The $k = 3$ case is established in Chapter 3 so we prove it for $k \geq 4$. Before arguing the gadget construction, we will transform the problem $\operatorname{Hol}_k(a, b)$ in such a way that it has the form $\#[c, 1, c] \mid r$ for some $c \in \mathbb{C}$ and some symmetric signature r. Becuase of this additional symmetry



(a) Gadget M_{13} (b) Gadget M_{14} (c) Gadget M_{15} (d) Gadget M_{16} (e) Gadget M_{17}

Figure 5.7 Recursive gadgets for $\mathrm{Hol}_k(a, b)$. Each gadget here is shown for a degree 2 through 5, but these are all generalized to higher degrees by adding length 2 cycles to the recognizer vertices.

in the generator signature, binary recursive gadgets will be represented with 2 by 2 matrices, along the lines of Lemma 4 in Chapter 3.

First suppose k is odd. We know ba^{-1} is a k^{th} root of unity (a and b are not zero), so we let $\omega \in \mathbb{C}$ such that $\omega^k = 1$ and $\omega^4 = ba^{-1}$ (squaring is a permutation on the k^{th} roots of unity, since k is odd). Then let $T = \begin{bmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{bmatrix}$ be a basis for a holographic reduction, and we calculate $[a\omega^2, 1, a\omega^2]^{\mathrm{T}} = [a\omega^2, 1, b\omega^{-2}]^{\mathrm{T}} = T^{\otimes 2}[a, 1, b]^{\mathrm{T}}$ and $[1, 0, 0, \ldots, 0, 1] = [1, 0, 0, \ldots, 0, 1](T^{-1})^{\otimes k}$, so $\mathrm{Hol}_k(a, b)$ is equivalent to $\mathrm{Hol}_k(a\omega^2, a\omega^2)$. Furthermore, since X is unchanged by this holographic transformation, we may now assume that $a = b$. We will show that for every $a \notin \{0, \pm 1, \pm \mathrm{i}\}$, either M_{13} or M_{14} is 1) nonsingular, 2) doesn't have $s = [a\ 1]^{\mathrm{T}}$ as a column eigenvector, and 3) has eigenvalues with distinct norm (using Lemma 53). By Lemma 4, these conditions are sufficient to prove $\mathrm{Hol}_k(a,a)$ is #P-hard.

$$M_{13} = \begin{bmatrix} a^{2k-5}+a^{2k-3} & 2a^{2k-5} \\ 2a^{2k-4} & a^{2k-6}+a^{2k-4} \end{bmatrix}, \qquad M_{14} = \begin{bmatrix} a^{2k-7}+a^{2k-5} & 2a^{2k-9} \\ 2a^{2k-6} & a^{2k-10}+a^{2k-8} \end{bmatrix}$$

$$\begin{aligned}
\mathrm{tr}[M_{13}] &= a^{2k-6}(a+1)(a^2+1) \neq 0 \\
\det[M_{13}] &= (a-1)^2a^{4k-11}(a+1)^2 \neq 0 \\
\mathrm{tr}[M_{14}] &= a^{2k-10}(a+1)(a^2+1)(a^2-a+1) \\
\det[M_{14}] &= (a-1)^2a^{4k-17}(a+1)^2 \neq 0 \\
\frac{\mathrm{tr}^2[M_{13}]}{\det[M_{13}]} &= \frac{(a^2+1)^2}{(a-1)^2a} \\
\frac{\mathrm{tr}^2[M_{14}]}{\det[M_{14}]} &= \frac{\left(1+a^2\right)^2\left(1-a+a^2\right)^2}{(-1+a)^2a^3} \\
\det([M_{13}s,s]) &= -(a-1)a^{2k-5}(a+1)^2 \neq 0 \\
\det([M_{14}s,s]) &= -(a-1)a^{2k-9}(a+1)^2(a^2-a+1)
\end{aligned}$$

If $a^2-a+1=0$ then $\frac{\mathrm{tr}^2[M_{13}]}{\det[M_{13}]} = \frac{(a^2+1)^2}{a(a-1)^2} = -1 \notin \mathbb{R}^+$ and since $X \notin \{0,1\}$ we already have both $\det[M_{13}] \neq 0$ and $\det([M_{13}s,s]) \neq 0$. Therefore we may assume that $a^2-a+1 \neq 0$, and in particular $\mathrm{tr}[M_{14}] \neq 0$ and $\det([M_{14}s,s]) \neq 0$. Now suppose that both M_{13} and M_{14} fail to have eigenvalues of distinct norm. Then $\frac{\left(1+a^2\right)^2}{(-1+a)^2a}$ and $\frac{\left(1+a^2\right)^2\left(1-a+a^2\right)^2}{(-1+a)^2a^3}$ are both positive real, so $\frac{(-1+a)^2a}{\left(1+a^2\right)^2} \cdot \frac{\left(1+a^2\right)^2\left(1-a+a^2\right)^2}{(-1+a)^2a^3} = \frac{(1-a+a^2)^2}{a^2}$ is also positive real, hence $r = \frac{1-a+a^2}{a}$ is real. From this it follows that $a^{-1}+a = r+1 \in \mathbb{R}$, so either $a \in \mathbb{R}$ or $|a|=1$. (This is easy to see geometrically, but symbolically, let $a = re^{\mathrm{i}t}$ where $r = |a|$. Then $\Im(a+1/a) = r\sin t + 1/r\sin(-t) = (r-1/r)\sin t$, which is 0 iff either $r=1$ or t is an integer multiple of π.) Suppose $a \notin \mathbb{R}$ and $|a|=1$, then $|\sqrt{a}|=1$ and $\sqrt{a} \notin \mathbb{R}$ hence $\sqrt{a}-1/\sqrt{a}$ is purely imaginary and nonzero. Then $(a-1)^2/a = (\sqrt{a}-1/\sqrt{a})^2$ is negative real, and we already know $(a^{-1}+a)^2$ is positive real, but then $\frac{(a^{-1}+a)^2}{(a-1)^2/a} = \frac{\left(1+a^2\right)^2}{(-1+a)^2a}$ is negative real which is a contradiction.

Now suppose k is even. Let ω be a $4k^{\text{th}}$ root of unity such that $a\omega^4 = b$. Then let $T = \begin{bmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{bmatrix}$ be a basis for a holographic reduction, and we calculate $[a\omega^2\ 1\ 1\ a\omega^2]^{\mathrm{T}} = [a\omega^2\ 1\ 1\ b\omega^{-2}]^{\mathrm{T}} = T^{\otimes 2}[a\ 1\ 1\ b]^{\mathrm{T}}$ and $[\omega^{-k}\ 0\ 0\ \ldots 0\ \omega^k] = [1\ 0\ 0\ \ldots 0\ 1](T^{-1})^{\otimes k}$, so $\mathrm{Hol}_k(a,b)$ is equivalent to

$\#[a\omega^2, 1, a\omega^2] \mid [\omega^{-k}\ 0\ 0\ \ldots 0\ \omega^k]$. Multiplying each entry of the recognizer signature by a fixed nonzero constant does not change the complexity of the problem, and $\omega^k \in \{\pm 1, \pm \mathrm{i}\}$, so the problem is equivalent to $\#[a\omega^2, 1, a\omega^2] \mid [1, 0, 0, \ldots 0, \pm 1]$. We will first consider the case of $\#[a\omega^2, 1, a\omega^2] \mid =_k$; the transformation leaves X invariant so we will now assume $a = b$. We will use gadgets M_{15} and M_{16}.

$$M_{15} = \begin{bmatrix} a^{k-2} + a^k & 2a^{k-1} \\ 2a^{k-1} & a^{k-2} + a^k \end{bmatrix}, \qquad M_{16} = \begin{bmatrix} a^{k-2} + a^k & 2a^{k-3} \\ 2a^{k-1} & a^{k-4} + a^{k-2} \end{bmatrix}$$

$$\begin{aligned}
\mathrm{tr}[M_{15}] &= 2a^{k-2}(a^2+1) \neq 0 \\
\det[M_{15}] &= (a-1)^2 a^{2k-4}(a+1)^2 \neq 0 \\
\mathrm{tr}[M_{16}] &= a^{k-4}(1+a^2)^2 \neq 0 \\
\det[M_{16}] &= (a-1)^2 a^{2k-6}(1+a)^2 \neq 0 \\
\frac{\mathrm{tr}^2[M_{15}]}{\det[M_{15}]} &= \frac{4(1+a^2)^2}{(-1+a)^2(1+a)^2} \\
\frac{\mathrm{tr}^2[M_{16}]}{\det[M_{16}]} &= \frac{(1+a^2)^4}{(-1+a)^2 a^2 (1+a)^2} \\
\det([M_{15}s, s]) &= -2(a-1)a^{k-1}(1+a) \neq 0 \\
\det([M_{16}s, s]) &= -(a-1)a^{k-3}(1+a)(1+a^2) \neq 0
\end{aligned}$$

The only condition that might fail for these gadgets is that the eigenvalues have distinct norm. If M_{15} fails to have eigenvalues of distinct norm, then $\frac{4\left(1+a^2\right)^2}{(-1+a)^2(1+a)^2}$ is positive real, and $r = \frac{4(1+a^2)}{(a^2-1)}$ is real, but then $\frac{8}{(a^2-1)} = r - 4 \in \mathbb{R}$ and a must either be real or purely imaginary. If a is real, then the problem is already known to be $\#\mathrm{P}$-hard unless $a \in \{0, \pm 1\}$ [6]. If a is purely imaginary, then $\frac{(1+a^2)^4}{a^2(a^2-1)^2}$ is negative real, meaning that gadget M_{16} has eigenvalues of distinct norm, and we are done.

Now we consider the case where k is even and the transformed problem is of the form $\#[a, 1, a] \mid [1, 0, 0, \ldots 0, -1]$. Again note that we need to prove the problem is hard when $a \notin \{0, \pm 1, \pm \mathrm{i}\}$. For this, we use gadgets M'_{16} and M'_{17} (we use the prime to denote that the recognizer signature is

$[1, 0, 0, \ldots 0, -1]$ rather than $=_k$, to avoid confusion notationally).

$$M'_{16} = \begin{bmatrix} a^{k-2} + a^k & -2a^{k-3} \\ 2a^{k-1} & -a^{k-4} - a^{k-2} \end{bmatrix}, \qquad M'_{17} = \begin{bmatrix} a^{2k} + a^{2k-4} - 2a^{2k-2} & 0 \\ 0 & a^{2k-6} - 2a^{2k-4} + a^{2k-2} \end{bmatrix}$$

$$\begin{aligned}
\mathrm{tr}[M'_{16}] &= (a-1)a^{k-4}(1+a)(1+a^2) \neq 0 \\
\det[M'_{16}] &= -(a-1)^2 a^{2k-6}(1+a)^2 \neq 0 \\
\mathrm{tr}[M'_{17}] &= (a-1)^2 a^{2k-6}(1+a)^2(1+a^2) \neq 0 \\
\det[M'_{17}] &= (a-1)^4 a^{4k-10}(1+a)^4 \neq 0 \\
\frac{\mathrm{tr}^2[M'_{16}]}{\det[M'_{16}]} &= -\frac{(1+a^2)^2}{a^2} \\
\frac{\mathrm{tr}^2[M'_{17}]}{\det[M'_{17}]} &= \frac{(1+a^2)^2}{a^2} \\
\det([M'_{16}s, s]) &= -(a-1)^2 a^{k-3}(1+a)^2 \neq 0 \\
\det([M'_{17}s, s]) &= (a-1)^3 a^{2k-5}(1+a)^3 \neq 0
\end{aligned}$$

Clearly, $\frac{(1+a^2)^2}{a^2}$ and $-\frac{(1+a^2)^2}{a^2}$ cannot both be positive real, so either gadget M'_{16} or gadget M'_{17} has eigenvalues of distinct norm, and we are done. □

5.2.6 A dichotomy for $\mathrm{Hol}_k(a, b)$ and Pl-$\mathrm{Hol}_k(a, b)$

We have shown the following.

Theorem 21. *If any of the following four conditions is true, then* $\mathrm{Hol}_k(a, b)$ *and* Pl-$\mathrm{Hol}_k(a, b)$ *are both solvable in* P*:*

1. $X = 1$
2. $X = 0$ *and* $Y = 0$
3. $X = -1$ *and* $Y = 0$
4. $X = -1$ *and* $Y^2 = 4X^k$

If $Y^2 = 4X^k$ *then* Pl-$\mathrm{Hol}_k(a, b)$ *is solvable in* P. *In none of the above conditions apply, then* $\mathrm{Hol}_k(a, b)$ *(respectively,* Pl-$\mathrm{Hol}_k(a, b)$*) is* $\#\mathrm{P}$-hard.

Chapter 6

A dichotomy for graphs with mixed degrees and a symmetric complex-valued edge function

Note that although the complexity of $\mathrm{Hol}_k(a,b)$ and $\mathrm{Pl\text{-}Hol}_k(a,b)$ both depend on k, they do so in a simple way. This makes it easy to give a dichotomy for $\#[x_0,x_1,x_2] \mid \mathcal{R}$ for any $\mathcal{R} \subseteq \{=_3,=_4,=_5,\dots\}$ and $x_i \in \mathbb{C}$. Using the techniques developed in this thesis, this can be extended to any $\mathcal{R} \subseteq \{=_1,=_2,=_3,\dots\}$, and we finish with this more general result.

6.1 The final result

Lemma 70. *Let $S \subseteq \{3,4,5,\dots\}$ be nonempty, $\mathcal{R} = \{=_k : k \in S\}$, and $d = \gcd(S)$. Then $\#[x_0,x_1,x_2] \mid \mathcal{R}$ is $\#\mathrm{P}$-hard, whether or not the input is restricted to planar graphs, for any $x_i \in \mathbb{C}$ unless one of the following conditions holds (in which case the problem is in FP):*

1. $x_0x_2 = x_1^2$
2. $x_0 = x_2 = 0$
3. $x_1 = 0$
4. $x_0x_2 = -x_1^2$ *and* $x_0^{4d} = x_1^{4d}$
5. *the input is restricted to planar graphs and* $x_0^d = x_2^d$

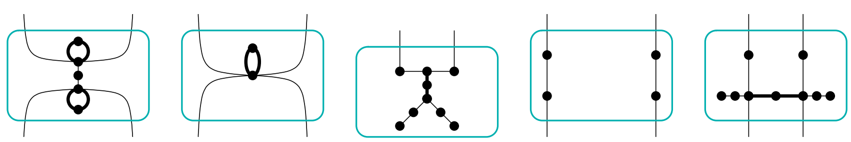
Proof. If $x_0x_2 = x_1^2$ then the signature $[x_0,x_1,x_2]$ is degenerate, and may be equivalently treated as a pair of unary signatures, hence the problem is trivially solvable in FP. If $x_0 = x_2 = 0$ then the problem is in FP by a 2-coloring argument. If $x_1 = 0$ then the problem is in FP by a connectivity argument. Now assume $x_1 \neq 0$. If $x_0x_2 = -x_1^2$ and $x_0^{4d} = x_1^{4d}$ we will first transform the problem using a holographic reduction. Under the basis $T = \begin{bmatrix} 1 & 0 \\ 0 & \frac{x_0}{x_1} \end{bmatrix}$, we get $T^{\otimes 2} g = [x_0, x_0, x_0, x_0^2 x_2 x_1^{-2}]^{\mathrm{T}} = [x_0, x_0, x_0, -x_0]^{\mathrm{T}}$ where $g = [x_0, x_1, x_1, x_2]^{\mathrm{T}}$ and for every $r \in \mathcal{R}$ we have $r(T^{-1})^{\otimes k} = [1, 0, 0, \ldots, 0, (\frac{x_1}{x_0})^k] = [1, 0, 0, \ldots, 0, \mathfrak{i}^j\}]$ for some integers j and $k \geq 3$. Multiplying a signature by a nonzero constant does not change the complexity of the problem, so we may assume we have the generator signature $[1, 1, -1]$ in place of $[x_0, x_0, -x_0]$. Then the problem is tractable in FP by signature families $\mathcal{F}_1$ and $\mathcal{F}_3$ in [4]. If the input is restricted to planar graphs and $x_0^d = x_2^d$, then holographic algorithms using matchgates can be applied (see [7], Lemmas 4.4 and 4.8).

Now assume the negation of the 5 conditions above, and this will directly imply the negation of the conditions of Theorem 21 with respect to some $=_k \in \mathcal{R}$. First, $X = ab = x_0 x_2 x_1^{-2} \neq 1$ so condition 1 does not hold. Next, if both x_0 and x_2 are nonzero then $X = ab = x_0 x_2 x_1^{-2} \neq 0$, but if only one is nonzero then $a^k + b^k \neq 0$ for any $k \geq 3$ hence condition 2 does not hold. Now we focus on conditions 3 and 4 of Theorem 21. On one hand, $Y = 0$ can be equivalently understood as $(\frac{a}{b})^k = -1$, and since $X = -1$ this becomes $a^{2k} = (-1)^{k+1}$. On the other hand, if $Y^2 = 4X^k$ then $(a^k - b^k)^2 = Y^2 - 4X^k = 0$, hence $a^k = b^k$, but under $X = -1$ this is $a^{2k} = (-1)^k$. Hence conditions 3 and 4 of Theorem 21 can be equivalently summed up as "$ab = -1$ and $a^{4k} = 1$". In the present notation, this is "$x_0 x_2 = -x_1^2$ and $x_0^{4k} = x_1^{4k}$", but we know that either $x_0 x_2 \neq -x_1^2$ or $x_0^{4d} \neq x_1^{4d}$ hence there exists an integer $k \in S$ such that $x_0^{4k} \neq x_1^{4k}$, and conditions 3 and 4 of Theorem 21 do not hold. Finally, if the input is restricted to planar graphs then there exists $k \in S$ such that $x_0^k \neq x_2^k$. Then $(\frac{x_0}{x_1})^k \neq (\frac{x_2}{x_1})^k$, so $a^k \neq b^k$, hence $Y^2 - 4X^k = (a^k - b^k)^2 \neq 0$, and the last condition of Theorem 21 does not hold. We conclude that $\#[x_0, x_1, x_2] \mid \mathcal{R}$ is $\#\mathrm{P}$-hard if none of the 5 conditions given above hold. □

Now we aim to extend Lemma 70 to all $\mathcal{R} \subseteq \{=_1, =_2, =_3, \ldots\}$. The polynomial time algorithms of Lemma 70 apply seamlessly to any such $\mathcal{R}$ without modification. Also, it is easy to see that the holant of signature grids where $\mathcal{R} \subseteq \{=_1, =_2\}$ can be computed efficiently, so we will need to add this as a condition to the more general result. We need to resolve what happens when Lemma 70 doesn't immediately imply $\#\mathrm{P}$-hardness, but the algorithms do not apply either. Thus the only interesting question remaining is: what happens when $\mathcal{R}$ has at least one signature from both $\{=_3, =_4, \dots\}$ and $\{=_1, =_2\}$, and either condition 4 or 5 applies to $\mathcal{R} - \{=_1, =_2\}$ but not to $\mathcal{R}$? A prototypical example is $\#[a, 1, -a] \mid \{[=_1, =_4]\}$, where $a^2 \notin \{0, \pm 1\}$ and the input is restricted to planar graphs. Before we begin, we take a look at how our proof techniques relate to this question.

The interpolation method of Lemma 51 has two essential ingredients: 1) an infinite set of pairwise linearly independent symmetric binary signatures is simulated, and 2) a set of "good" finisher gadgets is applied. If $a^k = b^k$ and $ab \notin \{0, \pm 1\}$ then $[a, 1, b]$ and $=_k$ signatures fulfill the first ingredient for $k \geq 3$ (e.g. this is carried out in the proof of Lemma 69). However, the second ingredient is a problem; it doesn't seem possible to construct "good" finisher gadget sets in this setting, moreover the existence of such a set would imply $FP = \#\mathrm{P}$. However, if we make $=_1$ or $=_2$ available as a recognizer, it may become possible to construct good finisher gadget sets.

When $ab = -1$ and $a^{4k} = 1$ we have the opposite trouble. A good finisher gadget set exists by Lemma 52 in Chapter 5, but to efficiently simulate arbitrarily large sets of pairwise linearly independent symmetric binary signatures would again imply a proof of $FP = \#\mathrm{P}$. So while it would be optimistic to presume to find an efficient construction of such signature sets, it is more realistic to expect this when $=_1$ or $=_2$ recognizers are added to the mix.



(a) Gadget F_1 (b) Gadget F_2 (c) Gadget S_1 (d) Gadget M_1 (e) Gadget M_2

Figure 6.1 Gadgets used for the final dichotomy. Bold edge pairs indicate that the gadget is generalized to higher degrees by replacing that length 2 path with several length 2 paths in parallel.

In the following Lemma, we construct sets of finisher gadgets for $\#\mathcal{G} \mid \mathcal{R}$ in the setting discussed above, so as to satisfy condition (3) of Lemma 51. Gadget M_1 is this simplest possible binary recursive gadget available when $=_2 \in \mathcal{R}$, and it works to build a suitable finisher gadget set together with F_1 or F_2 (depending on the parity of k). Gadget M_2 is a natural choice when $=_1 \in \mathcal{R}$;

we need to use the $=_1$ signature somewhere, but the resulting polynomials have a simpler structure when only one of them is placed on either side.

Lemma 71. *Suppose* $[a, 1, b] \in \mathcal{G}$*,* $ab \notin \{0, \pm 1\}$*,* $=_k \in \mathcal{R}$ *for some* $k \geq 3$*,* $a^k = b^k$*, and either* $=_1 \in \mathcal{R}$ *or* $=_2 \in \mathcal{R}$*. Further assume that* $a \neq b$ *if* $=_1 \in \mathcal{R}$ *and* $a \neq \pm b$ *if* $=_2 \in \mathcal{R}$*. Then* $\#\mathcal{G} \mid \mathcal{R}$ *is* $\#\mathrm{P}\text{-hard}$*, even when restricted to planar graphs as input.*

Proof. Suppose $=_2 \in \mathcal{R}$. We will build finisher gadget sets using gadgets F_1, F_2, and M_1, where in gadget M_1 signature $[a, 1, b]$ is assigned to the vertices incident to the leading edges and $=_2$ is assigned to the vertices incident with the trailing edges.

$$
\begin{aligned}
F_1 &= \begin{bmatrix} a^{k-2} & 0 & a^{(k-3)/2}b^{(k-3)/2} \\ 0 & 0 & 0 \\ a^{(k-3)/2}b^{(k-3)/2} & 0 & b^{k-2} \end{bmatrix}, \\
F_2 &= \begin{bmatrix} a^{(k-4)/2} & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & b^{(k-4)/2} \end{bmatrix}, \\
M_1 &= \begin{bmatrix} a^2 & 2a & 1 \\ a & ab+1 & b \\ 1 & 2b & b^2 \end{bmatrix}
\end{aligned}
$$

Note that F_1 and F_2 are finisher gadgets for odd and even k (respectively) when ≥ 3. Using the same notation as in Lemma 52 in Chapter 5, we find that

$$
\begin{aligned}
\det(\mathrm{cross}(F_1, F_1M_1, F_1M_1^2)) &= 4a^{3k-9}b^{3k-9}(a-b)(a+b)(ab-1)^7 \neq 0 \\
\det(\mathrm{cross}(F_2, F_2M_1, F_2M_1^2)) &= 4a^{3k/2-6}b^{3k/2-6}(a-b)(a+b)(ab-1)^4 \neq 0
\end{aligned}
$$

hence $\{F_1, F_1M_1, F_1M_1^2)\}$ and $\{F_2, F_2M_1, F_2M_1^2\}$ are finisher gadget sets that fill the requirement for odd and even k, respectively.

Now suppose $=_1 \in \mathcal{R}$. Connecting a vertex with signature $=_1$ to a vertex labeled with signature $[a, 1, b]$, we have an $\mathcal{F}$-gate with (generator) signature $[a+1, b+1]$. We will build our finisher gadget sets using gadgets F_1, F_2, and M_2, where gadget M_2 has signature $[a+1, b+1]$ assigned to the degree 1 vertices.

$$M_2 = \begin{bmatrix} a^{k-1}(a+1)^2 & 2a(a+1)^2(b+1)^2 & b^{k-3}(b+1)^2 \\ a^{k-2}(a+1)^2 & (a+1)^2(b+1)^2(ab+1) & b^{k-2}(b+1)^2 \\ a^{k-3}(a+1)^2 & 2b(a+1)^2(b+1)^2 & b^{k-1}(b+1)^2 \end{bmatrix}$$

Some more calculation followed by the substitution $a^k = b^k$ and refactoring shows that under the further assumption $a \neq -1$ and $b \neq -1$,

$$\begin{aligned} \det(\text{cross}(F_1, F_1M_2, F_1M_2^2)) &= 4a^{4k-13}b^{4k-13}(a+1)^8(b+1)^8(ab-1)^7 \cdot \\ &\quad (a^kb + 2a^{k+1}b + a^{k+2}b - ab^k - 2ab^{k+1} - ab^{k+2}) \\ &= 4a^{5k-13}b^{4k-13}(a+1)^8(b+1)^8(ab-1)^8(a-b) \\ &\neq 0 \end{aligned}$$

and similarly

$$\begin{aligned} \det(\text{cross}(F_2, F_2M_2, F_2M_2^2)) &= 4a^{5k/2-10}b^{5k/2-10}(a+1)^8(b+1)^8(ab-1)^4 \cdot \\ &\quad (a^kb + 2a^{k+1}b + a^{k+2}b - ab^k - 2ab^{k+1} - ab^{k+2}) \\ &= 4a^{7k/2-10}b^{5k/2-10}(a+1)^8(b+1)^8(ab-1)^5(a-b) \\ &\neq 0 \end{aligned}$$

hence $\{F_1, F_1M_2, F_1M_2^2)\}$ and $\{F_2, F_2M_2, F_2M_2^2\}$ are finisher gadget sets as required for odd and even k, respectively. Now suppose that either $a = -1$ or $b = -1$ and by symmetry assume without loss of generality that $a = -1$. Then the generator signature $[a+1, b+1]$ is now $[0, b+1]$, and since $ab \neq 1$ we know $b \neq -1$. To simplify notation, we rewrite this generator as $[0, 1]$, recalling that multiplying every entry of a signature by a nonzero number does not change the complexity of the holant problem. The generator $[0, 1]$ also permits the simulation of $[0, 1]$ as a recognizer, by connecting a vertex labeled with recognizer $=_k$ to $k-1$ vertices labeled with generator $[0, 1]$. Finally, connecting a vertex with recognizer $[0, 1]$ to a vertex with generator $[a, 1, b]$, we have simulated generator $[1, b]$. We will use gadget M_2 with signature $[1, b]$ assigned to the degree 1 vertices (which we denote as M_2').

$$M_2' = \begin{bmatrix} a^{k-1} & 2ab & b^{k-1} \\ a^{k-2} & b(ab+1) & b^k \\ a^{k-3} & 2b^2 & b^{k+1} \end{bmatrix}$$

Taking the same approach as before,

$$\begin{aligned} \det(\operatorname{cross}(F_1, F_1 M_2', F_1(M_2')^2)) &= 4a^{4k-13}b^{4k-7}(ab-1)^7(a^k - ab^{1+k}) \\ &= -4a^{5k-13}b^{4k-7}(ab-1)^8 \\ &\neq 0 \\ \det(\operatorname{cross}(F_2, F_2 M_2', F_2(M_2')^2)) &= 4a^{5k/2-10}b^{5k/2-4}(ab-1)^4(a^k - ab^{1+k}) \\ &= -4a^{7k/2-10}b^{5k/2-4}(ab-1)^5 \\ &\neq 0, \end{aligned}$$

hence we have a suitable finisher gadget set in all cases.

Now we just need the existence of an efficiently constructed set of symmetric binary signatures which are pairwise linearly independent. Lemmas 46, 47, and 69 imply that when $a^k = b^k$ and $ab \notin \{0, \pm 1\}$, there is a construction $\{M^i S\}_{i \geq 0}$ which efficiently simulates a set of pairwise linearly independent symmetric binary signatures. Together with the finisher gadgets given above and Lemma 51, this implies that $\#\mathcal{G} \mid \mathcal{R}$ is #P-hard. □

Now we consider $ab = -1$ and $a^{4k} = 1$. When $=_2 \in \mathcal{R}$, we can evade the need for a recursive gadget construction by using a direct reduction instead. The gadget is the simplest possible one to simulate a generator signature.

Lemma 72. *Suppose $[a, 1, b] \in \mathcal{G}$, $ab = -1$, $a^8 \neq 1$, $a^{4k} = 1$, and $=_2, =_k \in \mathcal{R}$ for some $k \geq 3$. Then $\#\mathcal{G} \mid \mathcal{R}$ is* #P-hard*, even when restricted to planar graphs as input.*

Proof. Consider the $\mathcal{F}$-gate in Figure 3.2(a) of Chapter 3, where $\theta = =_2$ and both other vertices are labeled with $[a, 1, b]$. This $\mathcal{F}$-gate simulates the generator signature $[a^2+1, a+b, b^2+1]$, and we claim that $\#[a^2+1, a+b, b^2+1] \mid \{=_2, =_k\}$ is #P-hard. In view of Lemmas 70 and 71, it suffices to show that $a'b' \notin \{0, \pm 1\}$ and $(a')^2 \neq (b')^2$, where $a' = \frac{a^2+1}{a+b}$ and $b' = \frac{b^2+1}{a+b}$ (note $a \neq -b$). We will do this by checking that $(a^2+1)(b^2+1) + c(a+b)^2 \neq 0$ for all $c \in \{0, \pm 1\}$ and that $(a^2+1)^2 \neq (b^2+1)^2$. First, $(a^2+1)(b^2+1) + (a+b)^2 = 1 + 2a^2 + 2ab + 2b^2 + a^2b^2 = 2(a^2+b^2) = 2(a^2+a^{-2}) \neq 0$ since $a^4 \neq -1$. Second, $(a^2+1)(b^2+1) - (a+b)^2 = (ab-1)^2 \neq 0$. Next, $(a^2+1)(b^2+1) = (a^2+1)(a^{-2}+1)$ follows from $a^4 \neq 1$. Finally, $(1+a^2)^2 - (1+b^2)^2 = (a-b)(a+b)(2+a^2+b^2) \neq 0$, since $2+a^2+b^2 = 0$ implies $(a^2+1)^2 = a^4 + 2a^2 + 1 = 0$, and $a = \pm \mathfrak{i}$. $\square$

When we consider $=_1$ instead of $=_2$, such a simple gadget is not possible; at least one vertex of degree k must appear, hence we expect some form of k to appear in the exponents of a and b in the resulting signature from any direct gadget simulation. Once the gadget signature has been calculated, we will be able to simplify appearances of a^k and b^k, since $a^k, b^k \in \{\pm 1, \pm \mathfrak{i}\}$. Hence, in designing this gadget, we keep a couple of things in mind. First, we would like to keep the exponents of a and b in all terms of the resulting polynomials as close as possible to k, because after substitution this will result in low degree polynomials, which are more apt for proving results than high degree polynomials. Secondly, as noted earlier, each application of the recognizer $=_1$ effectively results in the generator $[a+1, b+1]$. We would like to avoid having terms like $(a+1)^k$ in the final signature, so we will aim to minimize use of $=_2$ (without eliminating it completely, of course). These design goals lead us to the gadget family S_1, which turns out to work perfectly.

Lemma 73. *Suppose* $[a, 1, b] \in \mathcal{G}$, $ab = -1$, $a^4 \neq 1$, $a^{4k} = 1$, *and* $=_1, =_k \in \mathcal{R}$ *for some* $k \geq 3$. *Then* $\#\mathcal{G} \mid \mathcal{R}$ *is* $\#\mathrm{P}\text{-hard}$*, even when restricted to planar graphs as input.*

Proof. We will use a direct reduction from problems known to be $\#\mathrm{P}\text{-hard}$ by using gadget S_1, where the unary vertices are labeled with $=_1$.

$$
\begin{aligned}
S_1 &= \begin{bmatrix} m_{1,1} & m_{1,2} \\ m_{2,1} & m_{2,2} \end{bmatrix}, \text{where} \\
m_{1,1} &= 1 + 2a + 2a^2 + a^k + 2a^{1+k} + a^{2+k} + 2a^2 b + a^2 b^2 + b^{-2+k} + 2b^{-1+k} + b^k, \\
m_{1,2} &= a + a^{-1+k} + 2a^k + a^{1+k} + b + 4ab + a^2 b + ab^2 + b^{-1+k} + 2b^k + b^{1+k}, \\
m_{2,1} &= a + a^{-1+k} + 2a^k + a^{1+k} + b + 4ab + a^2 b + ab^2 + b^{-1+k} + 2b^k + b^{1+k}, \\
m_{2,2} &= 1 + a^{-2+k} + 2a^{-1+k} + a^k + 2b + 2b^2 + 2ab^2 + a^2 b^2 + b^k + 2b^{1+k} + b^{2+k}.
\end{aligned}
$$

Suppose that $a^k = \pm 1$, which implies $b^k = -a^k$. A holographic reduction under the basis $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ reverses $[a, 1, b]$ and leaves $=_1$ and $=_k$ unchanged, so we may assume that $a^k = 1$ and $b^k = -1$. Then the signature simplifies to $[2(a+1)^2, 2(a-b-2), 2(b-1)^2]$, and for the purpose of complexity it is equivalent to consider $[(a+1)^2, a-b-2, (b-1)^2]$. We are done by reduction from Lemmas 21 and 71 if we can show that $a'b' \notin \{0, \pm 1\}$ and $a' \neq b'$, where $a' = \frac{(a+1)^2}{a-b-2}$ and $b' = \frac{(b-1)^2}{a-b-2}$ (note that since $|a| = 1$ and $|b| = 1$, $a - b - 2$ would imply $a = 1$ and $b = -1$, which is not true). If we assume $a'b' = -1$ then a little algebra indicates the contradiction

$$
\begin{aligned}
0 &= \Re(5 - 2a + 2a^2 + 2b - 6ab - 2a^2 b + 2b^2 + 2ab^2 + a^2 b^2) \\
&= \Re(5 - 2a + 2a^2 + 2b + 6 + 2a + 2b^2 - 2b + 1) \\
&= 2\Re(6 + a^2 + b^2) \\
&\geq 2 \cdot 4,
\end{aligned}
$$

where the last step follows because $|a| = 1$ and $|b| = 1$. Assuming $a'b' = -1$,

$$
\begin{aligned}
0 &= \Re((ab - 3)(ab - 2a + 2b + 1)) \\
&= 8\Re(a - b) \\
&\neq 0.
\end{aligned}
$$

Also $a'b' = (a+1)^2(b-1)^2 \neq 0$, and finally $(a+1)^2 - (b-1)^2 = (2 + a - b)(a + b) \neq 0$ (note $2 + a - b = 0$ implies $a = -1$ and $b = 1$, which is not the case), so $a' \neq b'$.

Now suppose $a^k = \pm\mathrm{i}$, which implies $b^k = \mathrm{i}$, and let $e = a^k$. The signature is then $[2(e+1)(a^2+1), 4(e-1), 2(e+1)(b^2+1)]$, and dividing by $2(e+1)$ we equivalently consider $[a^2+1, 2e, b^2+1]$, where $2e = 2(e-1)/(e+1)$ because $e = \pm\mathrm{i}$. Now we show that $a'b' \notin \{0, \pm 1\}$ and $a' \neq b'$, where $a' = \frac{a^2+1}{2e}$ and $b' = \frac{b^2+1}{2e}$, or equivalently, $(a^2+1)(b^2+1) \notin \{0, \pm 4\}$ and $a^2 \neq b^2$. First, $(a^2+1)(b^2+1) - 4 = a^2b^2 + a^2 + b^2 - 3 = a^2 + b^2 - 2 \neq 0$ because otherwise $a^2 = b^2 = 1$ and we know $a^2 \neq 1$. Second, $(a^2+1)(b^2+1) + 4 = a^2b^2 + a^2 + b^2 + 5 = a^2 + b^2 + 6 \geq 4 > 0$. Third, $(a^2+1)(b^2+1) = 2 + a^2 + b^2 \neq 0$ since otherwise $a^2 = b^2 = -1$, again contradicting $a^4 \neq 1$. Finally, $a^2 - b^2 = a^4 - a^2b^2 = a^4 - 1 \neq 0$. We conclude that gadget S_1 simulates a symmetric signature g for which $\#g \mid =_k$ is known to be $\#\mathrm{P}$-hard, either by Lemma 21 or Lemma 71, and we are done. □

Now we will prove the final dichotomy theorem of this thesis.

Theorem 22. *Let $S \subseteq \mathbb{Z}^+$ be nonempty, $\mathcal{R} = \{=_k : k \in S\}$, and $d = \gcd(S)$. Then $\#[x_0, x_1, x_2] \mid \mathcal{R}$ is $\#\mathrm{P}$-hard, whether or not the input is restricted to planar graphs, for any $x_i \in \mathbb{C}$ unless one of the following conditions holds (in which case the problem is in FP):*

1. $\mathcal{R} \subseteq \{=_1, =_2\}$
2. $x_0 x_2 = x_1^2$
3. $x_0 = x_2 = 0$
4. $x_1 = 0$
5. $x_0 x_2 = -x_1^2$ *and* $x_0^{4d} = x_1^{4d}$
6. *the input is restricted to planar graphs and* $x_0^d = x_2^d$

Proof. If $\mathcal{R} \subseteq \{=_1, =_2\}$ the problem is trivially solvable in FP. The rest of the polynomial time algorithms apply precisely as before. If $x_0 x_2 = x_1^2$ then the signature $[x_0, x_1, x_2]$ is degenerate, and may be equivalently treated as a pair of unary signatures, hence the problem is trivially solvable in FP. If $x_0 = x_2 = 0$ then the problem is in FP by a 2-coloring argument. If $x_1 = 0$ then the problem is in FP by a connectivity argument. Now assume $x_1 \neq 0$. If $x_0 x_2 = -x_1^2$ and $x_0^{4d} = x_1^{4d}$ we will first transform the problem using a holographic reduction. Under the basis $T = \begin{bmatrix} 1 & 0 \\ 0 & \frac{x_0}{x_1} \end{bmatrix}$, we get $T^{\otimes 2}g = [x_0, x_0, x_0, x_0^2 x_2 x_1^{-2}]^{\mathrm{T}} = [x_0, x_0, x_0, -x_0]^{\mathrm{T}}$ where $g = [x_0, x_1, x_1, x_2]^{\mathrm{T}}$ and for every $r \in \mathcal{R}$ we have $r(T^{-1})^{\otimes k} = [1, 0, 0, \ldots, 0, (\frac{x_1}{x_0})^k] = [1, 0, 0, \ldots, 0, \mathfrak{i}^j\}]$ for some integers j and $k \geq 3$. Multiplying a signature by a nonzero constant does not change the complexity of the problem, so we may assume we have the generator signature $[1, 1, -1]$ in place of $[x_0, x_0, -x_0]$. Then the problem is tractable in FP by signature families $\mathcal{F}_1$ and $\mathcal{F}_3$ in [4]. If the input is restricted to planar graphs and $x_0^d = x_2^d$, then holographic algorithms using matchgates can be applied (see [7], Lemmas 4.4 and 4.8).

Now assume the negation of all 5 conditions in the theorem statement, and we will show that $\#[x_0, x_1, x_2] \mid \mathcal{R}$ is #P-hard. If $\mathcal{R} \subseteq \{=_3, =_4, \ldots\}$ then $\#[x_0, x_1, x_2] \mid \mathcal{R}$ is already #P-hard by Lemma 70 and since $\mathcal{R} \nsubseteq \{=_1, =_2\}$, we may henceforth assume that there exists $k \geq 3$ such that $=_k \in \mathcal{R}$ and either $=_1$ or $=_2$ is also in $\mathcal{R}$. If neither condition 4 nor condition 5 hold with respect to $\mathcal{R} \cap \{=_3, =_4, \ldots\}$,

Now assume the negation of all 5 conditions in the theorem statement, and we will show that $\#[x_0, x_1, x_2] \mid \mathcal{R}$ is #P-hard. Since $\mathcal{R} \nsubseteq \{=_1, =_2\}$ there is at least one EQUALITY signature in $\mathcal{R}$ with arity at least 3. If neither condition 4 nor condition 5 hold with respect to $\mathcal{R}' = \mathcal{R} \cap \{=_3, =_4, \ldots\}$, then $\#[x_0, x_1, x_2] \mid \mathcal{R}$ is already #P-hard, so may assume that either condition 4 or 5 holds true with respect to $\mathcal{R}'$, (but not for $\mathcal{R}$) and that either $=_1$ or $=_2$ is in $\mathcal{R}$. Suppose that $x_0 x_2 \neq -x_1^2$, hence condition 5 must be true with respect to $\mathcal{R}'$. Then since condition 5 is false with respect to $\mathcal{R}$ we know that either $=_2 \in \mathcal{R}$ and $x_0^2 \neq x_2^2$ or $=_1 \in \mathcal{R}$ and $x_0 \neq x_2$. Then $\#[x_0, x_1, x_2] \mid \mathcal{R}$ is #P-hard by Lemma 71. Now suppose $x_0 x_2 = -x_1^2$. We know either condition 4 or 5 is true with respect to $\mathcal{R}'$, but condition 5 implies condition 4 (i.e. $x_0^{4d} = (x_0 x_2)^{2d} = (-x_1^2)^{2d} = x_1^{4d}$), so we can just assume condition 4. Then either $=_2 \in \mathcal{R}$, $(\frac{x_0}{x_1})^8 \neq 1$, and Lemma 72 holds, or $=_1 \in \mathcal{R}$, $(\frac{x_0}{x_1})^4 \neq 1$, and Lemma 73 holds. Either way, the problem is #P-hard, even for planar graphs, and we are done. $\square$

This theorem can also be written in terms of a and b.

Theorem 23. *Let* $S \subseteq \mathbb{Z}^+$ *be nonempty,* $\mathcal{R} = \{=_k : k \in S\}$*, and* $d = \gcd(S)$*. Then* $\#[a, 1, b] \mid \mathcal{R}$ *is* $\#\mathrm{P}$-hard*, whether or not the input is restricted to planar graphs, for all* $a, b \in \mathbb{C}$ *except when any of the following conditions holds (in which case the problem is in* FP*):*

1. $\mathcal{R} \subseteq \{=_1, =_2\}$,
2. $ab = 1$,
3. $a = b = 0$,
4. $ab = -1$ *and* $a^{4k} = 1$,
5. *the input is restricted to planar graphs and* $a^k = b^k$.

Additionally, $\#[a, 0, b] \mid \mathcal{R}$ *is in* FP *for all* $a, b, \in \mathbb{C}$.

Or in terms of X and Y.

Theorem 24. *Let* $S \subseteq \mathbb{Z}^+$ *be nonempty,* $\mathcal{R} = \{=_k : k \in S\}$*, and* $d = \gcd(S)$*. Then* $\#[a, 1, b] \mid \mathcal{R}$ *is* $\#\mathrm{P}$-hard*, whether or not the input is restricted to planar graphs, for all* $a, b \in \mathbb{C}$ *except when any of the following conditions holds (in which case the problem is in* FP*):*

1. $\mathcal{R} \subseteq \{=_1, =_2\}$,
2. $X = 1$,
3. $X = Y = 0$,
4. $X = -1$ *and* $Y = 0$,
5. $X = -1$ *and* $Y^2 = 4X^k$,
6. *the input is restricted to planar graphs and* $Y^2 = 4X^k$.

Additionally, $\#[a, 0, b] \mid \mathcal{R}$ *is in* FP *for all* $X, Y, \in \mathbb{C}$.

LIST OF REFERENCES

[1] L. Blum, F. Cucker, M. Shub, and S. Smale. *Complexity and Real Computation*. Springer-Verlag, New York, 1998.

[2] A. A. Bulatov and V. Dalmau. Towards a dichotomy theorem for the counting constraint satisfaction problem. *Information and Computation*, 205(5):651–678, 2007.

[3] A. A. Bulatov and M. Grohe. The complexity of partition functions. *Theoretical Compututer Science*, 348(2-3):148–186, 2005.

[4] J.-Y. Cai, X. Chen, and P. Lu. Graph homomorphisms with complex values: A dichotomy theorem. *Computing Research Repository*, arXiv:0903.4728v1, 2009.

[5] J.-Y. Cai, S. Huang, and P. Lu. From holant to #CSP and back: Dichotomy for holant^c problems. *Computing Research Repository*, arXiv:1004.0803v1, 2010.

[6] J.-Y. Cai and M. Kowalczyk. A dichotomy for k-regular graphs with $\{0, 1\}$-vertex assignments and real edge functions. In J. Kratochvíl, A. Li, J. Fiala, and P. Kolman, editors, *Theory and Applications of Models of Computation, 7th Annual Conference, TAMC 2010, Prague, Czech Republic, June 7-11, 2010. Proceedings*, volume 6108 of *Lecture Notes in Computer Science*, pages 328–339. Springer, 2010.

[7] J.-Y. Cai and P. Lu. Holographic algorithms: from art to science. In D. S. Johnson and U. Feige, editors, *Proceedings of the 39th Annual ACM Symposium on Theory of Computing, San Diego, California, USA, June 11-13, 2007*, pages 401–410. ACM, 2007.

[8] J.-Y. Cai and P. Lu. On symmetric signatures in holographic algorithms. In W. Thomas and P. Weil, editors, *STACS 2007, 24th Annual Symposium on Theoretical Aspects of Computer Science, Aachen, Germany, February 22-24, 2007, Proceedings*, volume 4393 of *Lecture Notes in Computer Science*, pages 429–440. Springer, 2007.

[9] J.-Y. Cai, P. Lu, and M. Xia. Holographic algorithms by fibonacci gates and holographic reductions for hardness. In *Proceedings: 49th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2008, October 25-28, 2008, Philadelphia, PA, USA*, pages 644–653. IEEE Computer Society, 2008.

[10] J.-Y. Cai, P. Lu, and M. Xia. A computational proof of complexity of some restricted counting problems. In J. Chen and S. B. Cooper, editors, *Theory and Applications of Models of Computation, 6th Annual Conference, TAMC 2009, Changsha, China, May 18-22, 2009. Proceedings*, volume 5532 of *Lecture Notes in Computer Science*, pages 138–149. Springer, 2009.

[11] J.-Y. Cai, P. Lu, and M. Xia. Holant problems and counting CSP. In M. Mitzenmacher, editor, *Proceedings of the 41st Annual ACM Symposium on Theory of Computing, STOC 2009, Bethesda, MD, USA, May 31 - June 2, 2009*, pages 715–724. ACM, 2009.

[12] N. Creignou and M. Hermann. Complexity of generalized satisfiability counting problems. *Information and Computation*, 125(1):1–12, 1996.

[13] N. Creignou, S. Khanna, and M. Sudan. *Complexity Classification of Boolean Constraint Satisfaction Problems*, volume 7 of *SIAM Monographs on Discrete Mathematics and Applications*. Society for Industrial and Applied Mathematics, Philadelphia, PA., 2001.

[14] C. T. J. Dodson and T. Poston. *Tensor geometry; The geometric viewpoint and its uses*. Springer-Verlag, Berlin, Heidelberg, 1991.

[15] M. Dyer, L. A. Goldberg, and M. Jerrum. The complexity of weighted Boolean CSP. *SIAM Journal on Computing*, 38(5):1970–1986, 2009.

[16] M. Dyer, L. A. Goldberg, and M. Paterson. On counting homomorphisms to directed acyclic graphs. *Journal of the ACM*, 54(6):27:1–27:23, 2007.

[17] M. E. Dyer and C. S. Greenhill. The complexity of counting graph homomorphisms. *Random Structures and Algorithms*, 17(3-4):260–289, 2000.

[18] M. Freedman, L. Lovász, and A. Schrijver. Reflection positivity, rank connectivity, and homomorphism of graphs. *JAMS: Journal of the American Mathematical Society*, 20(1):37–51, 2007.

[19] L. A. Goldberg, M. Grohe, M. Jerrum, and M. Thurley. A complexity dichotomy for partition functions with mixed signs. In S. Albers and J.-Y. Marion, editors, *26th International Symposium on Theoretical Aspects of Computer Science, STACS 2009, February 26-28, 2009, Freiburg, Germany, Proceedings*, volume 3 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 493–504, Dagstuhl, Germany, 2009. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.

[20] L. A. Goldberg, S. Kelk, and M. Paterson. The complexity of choosing an H-colouring (nearly) uniformly at random. In *Proceedings of the 34th Annual ACM Symposium on Theory of Computing, STOC 2002, Montreal, Quebec, Canada, May 19-21, 2002*, pages 53–62, New York, May 19–21 2002. ACM Press.

[21] P. Hell and J. Nešetřil. On the complexity of H-coloring. *Journal of Combinatorial Theory, Series B*, 48(1):92–110, 1990.

[22] P. Hell, J. Nešetřil, and X. Zhu. Duality and polynomial testing of tree homomorphisms. *TAMS: Transactions of the American Mathematical Society*, 348(4):1281–1297, 1996.

[23] P. W. Kasteleyn. The statistics of dimers on a lattice. *Physica*, 27(12):1209–1225, 1961.

[24] P. W. Kasteleyn. Graph theory and crystal physics. In F. Harary, editor, *Graph Theory and Theoretical Physics*, pages 43–110, London, 1967. Academic Press.

[25] M. Kowalczyk. Classification of a class of counting problems using holographic reductions. In H. Q. Ngo, editor, *Computing and Combinatorics, 15th Annual International Conference, COCOON 2009, Niagara Falls, NY, USA, July 13-15, 2009, Proceedings*, volume 5609 of *Lecture Notes in Computer Science*, pages 472–485. Springer, 2009.

[26] M. Kowalczyk and J.-Y. Cai. Holant problems for regular graphs with complex edge functions. In J.-Y. Marion and T. Schwentick, editors, *27th International Symposium on Theoretical Aspects of Computer Science, STACS 2010, March 4-6, 2010, Nancy, France*, volume 5 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 525–536. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2010.

[27] L. Lovász. Operations with structures. *Acta Mathematica Academiae Scientiarum Hungaricae*, 18(3-4):321–328, 1967.

[28] A. Tarski. *A Decision Method for Elementary Algebra and Geometry*. Univ. of California Press, Berkeley, CA, 2nd edition, 1951.

[29] H. N. V. Temperley and M. Fisher. Dimer problem in statistical mechanics - an exact result. *Philosophical Magazine*, 6(68):1061–1063, 1961.

[30] S. P. Vadhan. The complexity of counting in sparse, regular, and planar graphs. *SIAM Journal on Computing*, 31(2):398–427, 2001.

[31] L. G. Valiant. The complexity of computing the permanent. *Theoretical Compututer Science*, 8(2):189–201, 1979.

[32] L. G. Valiant. The complexity of enumeration and reliability problems. *SIAM Journal on Computing*, 8(3):410–421, 1979.

[33] L. G. Valiant. Quantum circuits that can be simulated classically in polynomial time. *SIAM Journal on Computing*, 31(4):1229–1254, 2002.

[34] L. G. Valiant. Holographic algorithms. In *Proceedings: 45th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2004, 17–19 October, 2004, Rome, Italy*, pages 306–315. IEEE Computer Society, 2004.

[35] L. G. Valiant. Accidental algorithms. In *Proceedings: 47th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2006, 21-24 October 2006, Berkeley, California, USA*, pages 509–517. IEEE Computer Society, 2006.

[36] M. Xia, P. Zhang, and W. Zhao. Computational complexity of counting problems on 3-regular planar graphs. *Theoretical Compututer Science*, 384(1):111–125, 2007.