5

2-Spin Systems on Regular Graphs

In this chapter, we consider the following class of counting problems. An input k-regular graph $G = (V, E)$ is given, where every $e \in E$ is labeled with a symmetric edge function $g : \{0, 1\}^2 \to \mathbb{C}$. We allow self-loops and parallel edges in G, where each self-loop contributes 2 to the degree of the incident vertex. We present a dichotomy theorem for spin systems on k-regular graphs. For simplicity and for what turns out to be sufficient in terms of logical dependence from later chapters, we will restrict our proofs to $k = 3$ and $k = 4$. As a spin system, the vertices of the graph represent Boolean variables. The edge function g takes 0-1 inputs from its incident vertices and outputs arbitrary (algebraic) values in $\mathbb{C}$. The problem is to compute the partition function

$$Z(G) = \sum_{\sigma : V \to \{0,1\}} \prod_{\{u,v\} \in E} g(\sigma(u), \sigma(v)).$$

For example, if g is the Boolean OR function represented by the matrix $\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$, then $Z(G)$ counts the number of vertex covers on a k-regular graph G.

A spin system can also be defined for a general domain $[q]$, for $q > 2$, where each vertex takes one of q possible values. But in Volume I of this book we focus on the Boolean domain $q = 2$. A 2-spin system is a special case of #CSP where there is a single symmetric binary constraint function. A 2-spin system on a k-regular graph is the further restriction that every variable appears k times. Equivalently, we may view this as a bipartite Holant problem Holant$(=_k \mid g)$. We treat the binary g as a generator (contravariant) on the right side, and the EQUALITY $(=_k)$ of arity k as a recognizer (covariant) on the left side. The main difference between general Holant problems and #CSP is that EQUALITY functions of arbitrary arity are *presumed* to be present in #CSP. For spin systems on k-regular graphs, we assume the presence of $=_k$, and a single symmetric edge function g. When EQUALITY gates of arbitrary arity are freely available

https://doi.org/10.1017/9781107477063.006 Published online by Cambridge University Press

in possible inputs, it is technically easier to prove #P-hardness. Two important techniques, called *stretching* and *thickening*, require the availability of EQUALITY gates of arbitrary arity (equivalently, vertices of arbitrarily high degrees). Stretching replaces an edge by a path, which requires binary EQUALITY gates. Thickening replaces an edge by multiple parallel edges, which requires EQUALITY of arbitrary arity. Proving #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 #P-hard for general graphs, but is solvable in polynomial time when restricted to k-regular graphs.

We denote the symmetric edge function g by $[x, y, z]$, where $x = g(0, 0)$, $y = g(0, 1) = g(1, 0)$ and $z = g(1, 1)$. Functions will also be called gates or signatures. (For VERTEX COVER , the corresponding function is the OR gate, and is denoted by the signature $[0, 1, 1]$.) The dichotomy theorem presented in this chapter gives a complexity classification of $Z(G)$ on k-regular graphs G in terms of the signature $g = [x, y, z]$, where $x, y, z \in \mathbb{C}$. Note that a self-loop with a binary edge function $g = [x, y, z]$ amounts to a unary vertex weight function $[x, z]$.

First, if $y = 0$, it is easy to compute $Z(G)$ in polynomial time. Assume $y \neq 0$. We may normalize g and set $y = 1$. The main theorem of this chapter is the following.

Theorem 5.1. *Suppose $a, b \in \mathbb{C}$, $k \geq 3$, and let $X = ab$ and $Y = a^k + b^k$. Then $Z(G)$ with $g = [a, 1, b]$ for input k-regular graphs G is* #P-hard *except in the following four cases, for which the problem is in P.*

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

(The same statement holds for Holant$(=_k \mid [a, 1, b], \Delta_0, \Delta_1)$*, and when it is #P-hard a reduction exists that does not use Lemma 3.13.)*

If we restrict the input to planar k-regular graphs, then these four cases are solvable in P, as well as a fifth case, $Y^2 = 4X^k$. The problem remains #P-hard *in all other cases.*

Given a binary symmetric function g, if #CSP(g) is tractable, then of course the 2-spin system $Z(G)$ is also tractable with g on k-regular graphs. Cases 1 to 4 correspond to tractable cases of #CSP by the product type $\mathscr{P}$ (Definition 3.2) and the affine type $\mathscr{A}$ (Definition 3.6), possibly after a holographic transformation. Furthermore, over planar graphs, there is an additional set of tractable cases that are #P-hard over general (nonplanar) k-regular graphs, and

https://doi.org/10.1017/9781107477063.006 Published online by Cambridge University Press

these consist entirely of suitable holographic transformations from matchgate computable problems. Finally, everything else is #P-hard, even for planar k-regular graphs. (For #CSP problems, this planar tractable case will be classified in Chapter 8.)

We can parameterize the space by (a, b) and also equivalently by (X, Y). The region defined by cases 1 to 4 in Theorem 5.1 will be called region I. In terms of the categories of tractability for #CSP (cf. Theorem 3.7), case 1 is degenerate, case 2 together with $y = 0$ in $[x, y, z]$ before normalization corresponds to the product type, and cases 3 and 4 correspond to affine binary signatures, including possibly a suitable holographic transformation. Region II is defined to be $Y^2 = 4X^k$ but $X \notin \{0, \pm 1\}$. It can also be specified by $Y^2 = 4X^k$, minus the intersection with region I. It is worth noting that $Y^2 = 4X^k$ specifies precisely those signatures that under a suitable holographic transformation both $=_k$ and g are realizable as standard matchgate signatures. The remaining space is called region III.

Definition 5.2. In terms of (a, b), region I consists of

1. $ab = 1$ (degenerate),
2. $a = b = 0$ (disequality),
3. $ab = -1$ and $a^{2k} = b^{2k}$ (combining cases 3 and 4 in Theorem 5.1).

Region II consists of $a^k = b^k$, minus the intersection with region I. Region III consists of all remaining $(a, b) \in \mathbb{C}^2$.

The union of regions I and II is specified by $X = 1$ or $Y^2 = 4X^k$ or $(X, Y) = (-1, 0)$. In terms of (a, b), this union is $ab = 1$ or $a^k = b^k$ or $[ab = -1$ and $a^{2k} = b^{2k}]$.

We can restate this theorem in terms of a and b. Note that $Y^2 = 4X^k$ is equivalent to $a^k = b^k$.

Theorem 5.3. *Suppose $a, b \in \mathbb{C}$ and $k \geq 3$. Then $Z(G)$ with $g = [a, 1, b]$ for input k-regular graphs G is* #P-hard *except in the following categories, for which the problem is in P.*

1. $ab = 1$.
2. $a = b = 0$.
3. $ab = -1$ *and* $a^{2k} = b^{2k}$.

(The same statement holds for Holant$(=_k | [a, 1, b], \Delta_0, \Delta_1)$*, and when it is #P-hard a reduction exists that does not use Lemma 3.13.)*

https://doi.org/10.1017/9781107477063.006 Published online by Cambridge University Press

If we restrict the input to planar k-regular graphs, then these three categories are solvable in P, as well as a fourth category, $a^k = b^k$. The problem remains #P-hard *in all other cases.*

Exercise: Prove that Theorem 5.1 and Theorem 5.3 are equivalent.

Prove that case 3 of Theorem 5.3 is equivalent to $ab = -1$ and $a^{4k} = 1$, as well as $ab = -1$ and $b^{4k} = 1$. Prove that if k and k' are relatively prime, then the tractability conditions of #CSP($[a, 1, b]$) in Theorem 3.7 and that of $Z(G)$ in Theorem 5.3, combined for both k-regular and k'-regular graphs, are equivalent.

We will prove this dichotomy for the cases $k = 3$ and $k = 4$. For technical reasons, the situations for odd and even k are slightly different. But we will proceed in a similar fashion in both cases. We will first establish tractability, in region I for general (not necessarily planar) graphs, and in region II for planar graphs. The main task is to show everything else is #P-hard. For 3-regular graphs, we will first prove that these problems are #P-hard in region II for general graphs (where the problem is tractable when restricted to planar graphs as input). Then we move on to prove #P-hardness within region III, where the problem is #P-hard even for planar graphs. For 4-regular graphs the order is reversed. The main theme in the #P-hardness proof is to show that we can interpolate all unary (or "virtually unary") signatures. After that, in essence, we appeal to ideas and results from the framework of Holant* problems.

To prove this theorem, several new proof techniques are introduced.

1. We present a general approach to interpolate all unary signatures. This involves a recursive iteration gadget, a starter gadget (in some cases), and an analysis of eigenvalues and eigenvectors.
2. We introduce a method to construct gadgets that carry out iterations at a higher dimension, and then collapse it to a lower dimension for the purpose of constructing (virtual) unary signatures. This involves a starter gadget, a recursive iteration gadget, and a finisher gadget. We prove a lemma that guarantees that among polynomially many iterations, some subset of them will be sufficient for interpolation to succeed.
3. Algebraic symmetrization. We derive an expression of $Z(G)$ over k-regular graphs as a graph polynomial, whose degree is reduced by taking symmetry into account. This symmetry enables us to draw connections between different problems, and also reduces the size and complexity of various polynomials that will be analyzed.
4. Eigenvalue shifted pairs. These are coupled pairs of gadgets whose transition matrices differ by δI, where $\delta \neq 0$. They have shifted eigenvalues, and by

https://doi.org/10.1017/9781107477063.006 Published online by Cambridge University Press

analyzing where they may fail individually, we can show that *jointly* they succeed.

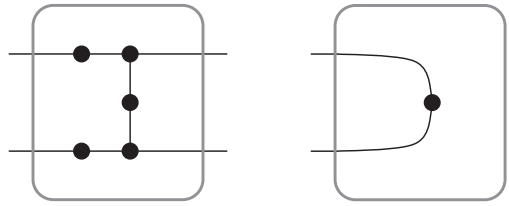
5. Anti-gadgets. These are also coupled pairs of gadgets, but in which one gadget has the algebraic effect of canceling out a portion of the other gadget, resulting in a "virtual gadget" with desirable algebraic properties.
6. Gadget syzygy. This is a trio of gadgets that in their alignment we can prove they conjointly succeed.
7. Symmetrizer gadgets. Some of our constructions produce signatures with desirable properties, but they are not necessarily symmetric. If symmetric signatures are required, then gadgets can be used to introduce symmetry in the underlying graph, thereby guaranteeing that the signatures produced from the construction are also symmetric.

When the dichotomy was first proved [CLX11, KC10, CK13, CK12], an additional important idea was to use Tarski's decidability theorem for a real closed fields [Tar51, BOKR86, BPR06] and prove the desired result by a substantial amount of symbolic computation. In the present chapter, we have at least formally eliminated symbolic computation that must require machine verification. However, many constructions in this chapter are found computationally. The fact that they work as stated can be verified by hand with some work, and they have also been verified via computer programs. Symbolic computation remains a valuable tool for exploration and as a proof technique.

Our spin system is the same problem as Holant$(=_k \mid [a, 1, b])$, which we will abbreviate as $\mathrm{Hol}_k(a, b)$. In this edge–vertex incidence graph view, the input instances are $(2, k)$-regular bipartite graphs. Throughout this chapter, all $(2, k)$-regular bipartite graphs are arranged with generators (contravariant tensors) on the degree-2 side (right-hand side (RHS)) and recognizers (covariant tensors) on the degree-k side (left-hand side (LHS)).

For convenience, in this chapter we further designate dangling edges as *leading* edges if they are internally connected to a binary generator $g = [a, 1, b]$, or *trailing* edges if they are internally connected to a recognizer $=_k$. We will draw $\mathcal{F}$-gates with leading edges protruding from the left and trailing edges from the right. These $\mathcal{F}$-gates can be composed by merging leading edges of one $\mathcal{F}$-gate with trailing edges of another, respecting the underlying recognizer and generator bipartite structure. 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 $2^m \times 2^n$ matrix, where the rows and columns are indexed by the 0-1 assignments to the leading and trailing edges respectively. 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

https://doi.org/10.1017/9781107477063.006 Published online by Cambridge University Press



(a) A recursive gadget (b) A starter gadget

Figure 5.1. Examples of binary recursive and starter gadgets.

by multiplying the two original matrices together. In particular, an $\mathcal{F}$-gate with only leading edges would be viewed as a column vector, representing a generator, and then merging with an $\mathcal{F}$-gate having 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 generator signatures into $\mathcal{F}$-gates with arity-m generator signatures. Furthermore, the $\mathcal{F}$-gates in this chapter will transform symmetric signatures to signatures that are also symmetric. This implies that there exists an equivalent $(m+1) \times (n+1)$ matrix that operates directly on vectors written in symmetric signature notation. We will henceforth identify the transition matrix with the $\mathcal{F}$-gate itself.

We define some specific types of $\mathcal{F}$-gates. An *arity-r starter gadget* is an $\mathcal{F}$-gate with no trailing edges and r leading edges, representing an arity-r generator. An *arity-r recursive gadget* is an $\mathcal{F}$-gate with r trailing edges and r leading edges. Figure 5.1 gives an example.

When we speak of an $\mathcal{F}$-gate (where $\mathcal{F} = \mathcal{R} \cup \mathcal{G}$) or gadget M being constructible *in the context of* Holant($\mathcal{R} \mid \mathcal{G}$), we mean that the underlying graph of M has a bipartite structure, where vertices in one partition are labeled with signatures from $\mathcal{R}$ and vertices in the other partition from $\mathcal{G}$. In other words, M can appear within an input instance of Holant($\mathcal{R} \mid \mathcal{G}$) without violating any structural bipartite constraints. When we say a generator (or recognizer) is constructible in the context of Holant($\mathcal{R} \mid \mathcal{G}$), we mean that an $\mathcal{F}$-gate is constructible in that context, and that all dangling edges are internally incident to generators (or recognizers). When we say that a sequence of signatures is efficiently constructible in the context of some Holant problem, we mean that a sequence of $\mathcal{F}$-gates having those signatures can be constructed in that context, and that the first n of these can be built in time polynomial in n. When we say that a generator g (or recognizer r) can be efficiently *simulated* in the context of Holant($\mathcal{R} \mid \mathcal{G}$), we mean that Holant($\mathcal{R} \mid \mathcal{G} \cup \{g\}$) $\leq_{\mathrm{T}}^{\mathrm{P}}$ Holant($\mathcal{R} \mid \mathcal{G}$) or Holant($\mathcal{R} \cup \{r\} \mid \mathcal{G}$) $\leq_{\mathrm{T}}^{\mathrm{P}}$ Holant($\mathcal{R} \mid \mathcal{G}$), respectively.

https://doi.org/10.1017/9781107477063.006 Published online by Cambridge University Press

We use Arg to denote the principal value of a complex argument, i.e., $\mathrm{Arg}(z) \in (-\pi, \pi]$ for all nonzero $z \in \mathbb{C}$, such that $z = |z|e^{\mathrm{i}\,\mathrm{Arg}(z)}$. We say that a square nonsingular matrix M has finite projective order if there exists a positive integer j, such that $M^j = \lambda I$ for some (nonzero) $\lambda \in \mathbb{C}$. Otherwise, M has infinite projective order. A nonsingular M has finite projective order iff for some positive integers $i \neq j$, $M^i = \lambda M^j$ for some (nonzero) $\lambda \in \mathbb{C}$.

5.1 3-Regular Graphs

5.1.1 Tractability in Regions I and II

Recall that for 3-regular graphs, region I is specified by $X = 1$ or $(X, Y) \in \{(0, 0), (-1, 0), (-1, \pm 2\mathrm{i})\}$. Region II is specified by $Y^2 = 4X^3$ but $X \notin \{0, \pm 1\}$. The union of regions I and II is specified by $X = 1$ or $Y^2 = 4X^3$ or $(X, Y) = (-1, 0)$.

The next lemma introduces the technique of algebraic symmetrization. We show that over 3-regular graphs, the Holant value is expressible as a polynomial $P(X, Y)$ with integer coefficients, where $X = ab$ and $Y = a^3 + b^3$. This change of variable, from (a, b) to (X, Y), is important in two ways. First, it allows us to derive tractability and hardness results more easily. It draws a connection between problems that may appear unrelated, but the tractability, and respectively hardness, of one problem implies the other. Second, it facilitates the proof of hardness by reducing the degree of the polynomials involved. Such a reduction in degree also makes symbolic computation more feasible, although we do not use this particular approach here.

Lemma 5.4. *Let G be a 3-regular graph. Then there exists a polynomial $P_G(\cdot, \cdot)$ with two variables and integer coefficients such that for any signature grid Ω having underlying graph G, if the edge function is $[a, 1, b]$, then $Z(G) = P_G(ab, a^3 + b^3)$.*

Proof. Consider any 0-1 vertex assignment σ with a nonzero valuation. If σ' is the complement assignment switching every 0 and 1 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 in this case i is the number of edges, $j = 0$, 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

https://doi.org/10.1017/9781107477063.006 Published online by Cambridge University Press

0-1 assignment is obtainable from the all-0 assignment by a sequence of switches, the conclusion $i \equiv j \pmod 3$ follows.

Now $a^i b^j + a^j b^i = (ab)^{\min(i,j)}(a^{3\ell} + b^{3\ell})$, for some $\ell \geq 0$ and a simple induction

$$a^{3(\ell+1)} + b^{3(\ell+1)} = (a^{3\ell} + b^{3\ell})(a^3 + b^3) - (ab)^3(a^{3(\ell-1)} + b^{3(\ell-1)})$$

shows that the partition function $Z(G)$ is a polynomial $P_G(ab, a^3 + b^3)$ with integer coefficients. □

Corollary 5.5. *If $X = -1$ and $Y \in \{0, \pm 2\mathrm{i}\}$, then $\mathrm{Hol}_3(a, b)$ is in P.*

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

We now list all the cases where $\mathrm{Hol}_3(a, b)$ is computable in polynomial time.

Theorem 5.6. *If any of the following four conditions is true, then $\mathrm{Hol}_3(a, b)$ is solvable in polynomial time:*

1. $X = 1$,
2. $X = Y = 0$,
3. $X = -1$ *and* $Y \in \{0, \pm 2\mathrm{i}\}$
4. $Y^2 = 4X^3$ *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 $Y \in \{0, \pm 2\mathrm{i}\}$ then by Corollary 5.5 we are done. If we restrict the input to planar graphs and $4X^3 = Y^2$ (equivalently, $a^3 = b^3$), holographic algorithms with matchgates from Chapter 4 can be applied. Indeed, if $ab = 0$ then $a = b = 0$ and this is case 2, which is tractable even for general graphs. Suppose $ab \neq 0$, and let $\omega = a/b$. We apply a holographic transformation defined by $T = \begin{bmatrix} 1 & 0 \\ 0 & \omega \end{bmatrix}$; then $(=_3)T^{\otimes 3} = (=_3)$, and $(T^{-1})^{\otimes 2}[1, \frac{1}{a}, \frac{b}{a}] = [1, \frac{b}{a^2}, 1]$, using $a^3 = b^3$. Then under a further holographic transformation by $\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$, both $(=_3)$ and any $[1, c, 1]$ are simultaneously realizable by matchgates. (This can be directly verified, but

https://doi.org/10.1017/9781107477063.006 Published online by Cambridge University Press

a more systematic approach is to use the theory developed in Chapter 4, in particular Theorem 4.33.) □

We note that the first three tractable cases also hold for Holant($=_3$|$[a, 1, b]$, Δ_0, Δ_1). Also note that diagonal (or antidiagonal) holographic transformations do not change $\{\Delta_0, \Delta_1\}$ up to a nonzero constant.

The main task in Section 5.1 is to prove that all remaining problems are #P-hard for 3-regular graphs.

5.1.2 Planar Tractable Region II Is #P-hard for General Graphs

In this subsection we get acquainted with our technique of proving hardness for Holant problems over regular graphs. Our specific application at the moment is to prove that $\mathrm{Hol}_3(a, b)$ is #P-hard assuming $a^3 = b^3$ and $X \notin \{-1, 0, 1\}$. (By Theorem 5.6, $\mathrm{Hol}_3(a, b)$ is tractable under these assumptions when the input is restricted to planar graphs.) We first make the following simplifying observation: Instead of working under $a^3 = b^3$, we may as well assume $a = b$.

Lemma 5.7. *Suppose $Y^2 = 4X^3$ (equivalently, $a^3 = b^3$). Then there exist $a', b' \in \mathbb{C}$ such that $a' = b'$, $a'b' = X$, and $(a')^3 + (b')^3 = Y$.*

Proof. If $X = 0$ then $Y = 0$ and $a = b = 0$ so we are already done. Otherwise, $X \neq 0$ implies $a \neq 0$ and we may set $a' = b' = b^2a^{-1}$ so that $a'b' = (b^2a^{-1})^2 = b^4a^{-2} = ab = X$ and $(a')^3 + (b')^3 = b^6a^{-3} + b^6a^{-3} = a^3 + b^3 = Y$. □

A recurring theme we will see for proving hardness in this chapter is

1. Obtain an infinite set of pairwise linearly independent signatures.
2. If necessary, project the signatures down to a lower dimension while retaining pairwise linear independence.
3. Use an interpolation argument to simulate *any* signature in that lower dimensional space.

The ability to simulate any signature in the lower dimensional space will lead to a reduction to prove #P-hardness. By "lower dimension" we usually mean unary signatures (i.e., a signature sequence of the form $[x_j, y_j]$ for $j \geq 0$). However, in some circumstances (such as for $\mathrm{Hol}_3(a, a)$), it is impossible to do so without sacrificing pairwise linear independence:

Lemma 5.8. *Let $\mathcal{F}$ be a set of signatures each satisfying the complementary invariance property, namely its value remains unchanged under the complement of all input bits. Then any $\mathcal{F}$-gate has this same property.*

https://doi.org/10.1017/9781107477063.006 Published online by Cambridge University Press

Proof. For any $f \in \mathcal{F}$, if σ and σ' are complementary assignments to its inputs, then they take the same value $f\,|_\sigma = f\,|_{\sigma'}$. If σ and σ' are complementary assignments to the dangling edges of an $\mathcal{F}$-gate, by complementing the assignments to all internal edges, we have a 1-1 correspondence of all terms defining the signature sum of the $\mathcal{F}$-gate under σ with those under σ', and each pair of corresponding terms has the same value. □

Corollary 5.9. *If $\mathcal{F} = \{[a, 1, a], =_k\}$ for some positive integer k, then any arity 1 or arity 2 $\mathcal{F}$-gate has a signature of the form $[x, x]$ or $[x, y, x]$ respectively.*

Proof. Immediate from Lemma 5.8. □

Given this knowledge, we aim to produce a sequence of "virtual unary" signatures rather than actual unary signatures in such cases. Specifically, we will obtain pairwise linearly independent signatures of the form $[x_j, y_j, x_j]$ instead of $[x_j, y_j]$. Owing to the symmetry exhibited in these binary signatures, we will be able to carry out interpolation without projecting them down to a lower dimension.

Unary Recursive Construction

Given a unary recursive gadget M, we can chain j copies of M together (merging the leading edges of one copy with the trailing edges of the next) to arrive at an arity-2 $\mathcal{F}$-gate with signature M^j. We want such a sequence $\{M^j\}_{j\geq 0}$ of signatures to be pairwise linearly independent.

Lemma 5.10. *Let M be a nonsingular square matrix. Then M has infinite projective order if and only if $\{M^j\}_{j\geq 0}$ are pairwise linearly independent. In particular, if M is the transition matrix for some arity-r recursive gadget, then M has infinite projective order if and only if $\{M^j\}_{j\geq 0}$ is a sequence of pairwise linearly independent signatures.*

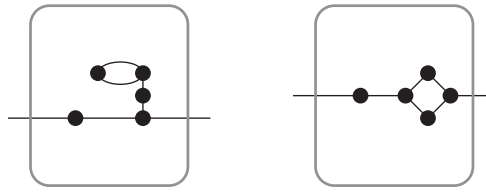
Proof. Immediate from definitions. □

The eigenvalues of M give us a convenient way to check that this sequence of $\mathcal{F}$-gates really has the property that the signatures M^j are pairwise linearly independent. In other words, we are reducing the problem of generating a sequence of pairwise linearly independent signatures to a test in terms of eigenvalues.

Lemma 5.11. *Let $M \in \mathbb{C}^{r\times r}$ be a nonsingular matrix, where the ratio of two of its eigenvalues is not a root of unity. Then $\{M^j\}_{j\geq 0}$ is a sequence of pairwise linearly independent matrices.*

Proof. We write $M = TJT^{-1}$ in its Jordan normal form, where T is invertible, and J is a triangular matrix with all eigenvalues of M appearing on its diagonal.

https://doi.org/10.1017/9781107477063.006 Published online by Cambridge University Press



(a) Gadget M_1 (b) Gadget M_2

Figure 5.2. A useful pair of unary recursive gadgets.

Suppose that M has finite projective order. Then for some $m > 0$ we have $M^m = \lambda I$ for some nonzero $\lambda \in \mathbb{C}$. Then $T^{-1}J^mT = \lambda I$ and hence $J^m = \lambda I$. So $\alpha^m = \beta^m$ for all eigenvalues α and β of M. This is a contradiction. We conclude that M has infinite projective order and by Lemma 5.10 $\{M^j\}_{j\geq 0}$ is a sequence of pairwise linearly independent signatures. □

Suppose $a = b$. Depending on the value of a and our gadget M, the sequence $\{M^j\}_{j\geq 0}$ may or may not be pairwise linearly independent, but we will show that for every $[a, 1, a]$ that does not correspond to a tractable case, there exists some unary recursive gadget with this property. There is a technical detail in the interpolation step; we will want these $\mathcal{F}$-gates to take the place of generator signatures in a signature grid to preserve the bipartite structure of the graph. To address this, we tack on an extra degree-2 vertex labeled with the generator $[a, 1, a]$, making the full gadget a binary generator.

Lemma 5.12. *Suppose $a = b$ and $a^4 \notin \{0, 1\}$. Then there exists a unary recursive gadget M for which the generator sequence $\{M^j g\}_{j\geq 0}$ is pairwise linearly independent, where $g = \begin{bmatrix} a & 1 \\ 1 & a \end{bmatrix}$ is a genarator $\mathcal{F}$-gate having a single vertex.*

Proof. Suppose the real part of a is nonzero, and consider gadget M_1 (see Figure 5.2),

$$M_1 = \begin{bmatrix} a^3 + a^2 & a^2 + a \\ a^2 + a & a^3 + a^2 \end{bmatrix}.$$

The eigenvalues of M_1 are $a(a + 1)^2$ and $a(a^2 - 1)$, both of which are nonzero. Their ratio is $\frac{a+1}{a-1}$, which is not a root of unity, as $|a + 1| \neq |a - 1|$. Note that $|a + 1| = |a - 1|$ consists of exactly those values a on the imaginary line $\mathrm{i}\mathbb{R}$.

Now assume the real part of a is 0, and consider gadget M_2 (see Figure 5.2),

$$M_2 = \begin{bmatrix} a^3 + 1 & a^2 + a \\ a^2 + a & a^3 + 1 \end{bmatrix}.$$

https://doi.org/10.1017/9781107477063.006 Published online by Cambridge University Press

The eigenvalues are $(a+1)(a-1)^2$ and $(a+1)(a^2+1)$, both nonzero. The ratio of these is $\frac{a^2-2a+1}{a^2+1}$. Since a is purely imaginary, a^2+1 is real-valued. Since a is furthermore nonzero and belongs to $\mathrm{i}\mathbb{R}$, $|a^2+1-2a| > |a^2+1|$ and thus $\frac{a^2-2a+1}{a^2+1}$ is not a root of unity.

By Lemma 5.11, we have a unary recursive gadget M for which $\{M^j\}_{j\geq 0}$ is a sequence of pairwise linearly independent signatures. Pairwise linear independence is preserved under invertible linear transformations defined by g on the set $\{M^j\}_{j\geq 0}$. As $M^j \mapsto M^j g$ is an invertible linear transformation, where $g = \begin{bmatrix} a & 1 \\ 1 & a \end{bmatrix}$, we conclude that $\{M^j g\}_{j\geq 0}$ is also pairwise linearly independent. □

Exercise: Compute the signature matrices of gadgets M_1 and M_2 for edge function $[a, 1, b]$. Note that $M_1 - M_2 = (ab-1)I$. Setting $a = b$ as in Lemma 5.12, verify that the signature matrices are as stated.

Interpolation and Reduction

Suppose we have a sequence of pairwise linear independent $\{[x_j, y_j, x_j]\}_{j\geq 0}$ of generators. We show how to simulate *any* generator of the form $[x, y, x]$.

Lemma 5.13. *Let $k \geq 3$ be fixed and suppose that in the context of* $\mathrm{Hol}_k(a, b)$ *we can efficiently construct a sequence of pairwise linearly independent generators of the form $\{[x_j, y_j, x_j]\}_{j\geq 0}$. Then for any $x, y \in \mathbb{C}$ we can efficiently simulate the generator $[x, y, x]$.*

Proof. Let Ω be a bipartite signature grid for the problem Holant($\mathcal{R} \mid \mathcal{G} \cup \{[x, y, x]\}$), and suppose the generator $[x, y, x]$ occurs n times in Ω. We stratify the Holant sum according to how many times the generator $[x, y, x]$ evaluates to x. Collecting these terms together, we write $\mathrm{Holant}_\Omega = \sum_{j=0}^{n} c_j x^j y^{n-j}$, where c_j is the sum over all edge assignments of the product of signature evaluations other than the n copies of $[x, y, x]$, subject to the restriction that exactly j of the edge pairs connecting to $[x, y, x]$ are assigned both 0's or both 1's.

We construct a sequence of bipartite signature grids Ω_i for the problem Holant($\mathcal{R} \mid \mathcal{G}$), by replacing each occurrence of $[x, y, x]$ with a copy of an $\mathcal{F}$-gate with signature $[x_i, y_i, x_i]$, for $i = 0, 1, \ldots, n$. (By omitting at most one element from our sequence and relabeling, we assume that $y_i \neq 0$ for all i.) Note that the bipartite structure is maintained, and the Holant of Ω_i evaluates to $\sum_{j=0}^{n} c_j x_i^j y_i^{n-j}$, where the same c_j's appear in this sum, for all i. By oracle queries to Holant($\mathcal{R} \mid \mathcal{G}$), we obtain a Vandermonde system where c_j are

https://doi.org/10.1017/9781107477063.006 Published online by Cambridge University Press

the unknowns.

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

Note that this Vandermonde system has full rank iff $[x_j, y_j, x_j]$ are pairwise linearly independent, namely x_j/y_j are pairwise distinct. Solving this linear system for c_j $(0 \le j \le n)$ yields the answer to $\text{Holant}_\Omega = \sum_{j=0}^{n} c_j x^j y^{n-j}$. □

Now we will use the interpolatation result to simulate the signature $[1, 0, 1]$, in order to get a reduction from $\text{Holant}(=_1, =_2, =_3, \ldots \mid [a, 1, a])$, namely $\#\text{CSP}([a, 1, a])$, to prove #P-hardness.

Lemma 5.14. *Suppose the parameters (a, b) are in region II; equivalently, suppose $X, Y \in \mathbb{C}$, $a^3 = b^3$, and $X \notin \{0, 1, -1\}$. Then $\text{Hol}_3(a, b)$ is* #P-hard.

The same statement holds for $\text{Holant}(=_3 \mid [a, 1, b], \Delta_0, \Delta_1)$, and a reduction exists that does not use Lemma 3.13 when it is #P-hard.

Proof. By Lemmas 5.7 and 5.4 we may assume that $a = b$. Since $X \notin \{0, \pm 1\}$ and $a = b$ we know $a^4 = (ab)^2 \notin \{0, 1\}$. We have a sequence of pairwise linearly independent generator signatures from Lemma 5.12, and by Corollary 5.9 they all have the form $[x, y, x]$. Therefore by Lemma 5.13 we can efficiently simulate generator signature $[1, 0, 1]$. We also know from the dichotomy theorem for Boolean #CSP problems, Theorem 3.7, that $\#\text{CSP}([a, 1, a])$ is #P-hard. We have a reduction from $\#\text{CSP}([a, 1, a])$, which is by definition $\text{Holant}(\{=_1, =_2, =_3, \ldots, \} \mid [a, 1, a])$.

$$\begin{aligned} \text{Holant}(\{=_1, =_2, =_3, \ldots, \} \mid [a, 1, a]) &\le_{\text{T}} \text{Holant}(=_3 \mid \{[a, 1, a], [1, 0, 1]\}) \\ &\le_{\text{T}} \text{Holant}(=_3 \mid [a, 1, a]). \end{aligned}$$

In the first step, we can use $(=_2) = [1, 0, 1]$ on the RHS and $(=_3)$ on the LHS to simulate $(=_k)$, for any k. The second step is by interpolation.

For $\text{Holant}(=_3 \mid [a, 1, b], \Delta_0, \Delta_1)$, we cannot apply Lemma 5.7, and we give an alternative proof using a diagonal holographic transformation. Let $\omega = a/b$; then $\omega^3 = 1$. By a holographic transformation $T = \begin{bmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{bmatrix}$ the EQUALITY $(=_3)$ is transformed to $(=_3)T^{\otimes 3} = (=_3)$, we have

https://doi.org/10.1017/9781107477063.006 Published online by Cambridge University Press

$(T^{-1})^{\otimes 2}[a, 1, b] = [a/\omega^2, 1, b\omega^2]$, as seen by its matrix form

$$\begin{bmatrix} \omega^{-1} & 0 \\ 0 & \omega \end{bmatrix} \begin{bmatrix} a & 1 \\ 1 & b \end{bmatrix} \begin{bmatrix} \omega^{-1} & 0 \\ 0 & \omega \end{bmatrix} = \begin{bmatrix} a/\omega^2 & 1 \\ 1 & b\omega^2 \end{bmatrix}.$$

Meanwhile T keeps $\{\Delta_0, \Delta_1\}$ invariant up to a nonzero constant. Note that $a/\omega^2 = b\omega^2$, with the same X and Y. □

Exercise: For any $k \geq 1$, construct a gadget that has signature $(=_k)$ on the LHS, using $(=_2)$ on the RHS and $(=_3)$ on the LHS. For what values of d and d' in place of 2 and 3 can one construct $(=_k)$ for all $k \geq 1$?

5.1.3 Hardness in Region III Where $(X, Y) \notin \mathbb{R} \times \mathbb{R}$

Recall that region III is the complement of the union of regions I and II, which is specified by $X \neq 1$ and $Y^2 \neq 4X^3$ (equivalently $a^3 \neq b^3$) and $(X, Y) \neq (-1, 0)$.

So far, we have seen one complete iteration of the general strategy we use in this chapter. We devised a scheme to produce an infinite set of pairwise linearly independent (virtual) unary signatures, found some gadgets to implement that scheme, used interpolation to simulate *any* such (virtual) unary signature, and applied that result to complete a reduction from a known #P-hard problem to prove #P-hardness. We will continue to develop the theory to make our tools applicable to wider classes of problems. Specifically, in this subsection we will prove #P-hardness for $\text{Hol}_3(a, b)$, subject to the restrictions that $(X, Y) \notin \mathbb{R} \times \mathbb{R}$, $a^3 \neq b^3$, and $X \neq 1$. To prove #P-hardness for region III, we must use planar gadgets and use an initial problem to reduce from that is #P-hard even for planar graphs.

Unary Recursive Construction with Starter Gadgets

As before, we first seek to produce a sequence of pairwise linearly independent signatures. We expand on the unary recursive construction by introducing a *starter gadget*. The following lemma is stated in terms of vectors and matrices so that we can reuse it for region II of $\text{Hol}_4(a, b)$ later on.

Lemma 5.15. *Let $M \in \mathbb{C}^{2\times 2}$ be a nonsingular matrix with infinite projective order, and let $s \in \mathbb{C}^2$ be a vector that is not orthogonal to any row eigenvector of M; i.e., the dot product with any row eigenvector of M is nonzero. Then $\{M^j s\}_{j\geq 0}$ is a sequence of pairwise linearly independent vectors in $\mathbb{C}^2$.*

Proof. Suppose that M is diagonalizable and we write $M = T^{-1}JT$, where $J = \begin{bmatrix} \alpha & 0 \\ 0 & \beta \end{bmatrix}$ and the rows of T are the row eigenvectors of M. As M is nonsingular,

https://doi.org/10.1017/9781107477063.006 Published online by Cambridge University Press

we have $\alpha\beta \neq 0$. We know by assumption that $Ts = \begin{bmatrix} x \\ y \end{bmatrix}$ for some $x, y \in \mathbb{C}$, where $xy \neq 0$. Then

$$M^j s = T^{-1}\begin{bmatrix} \alpha^j & 0 \\ 0 & \beta^j \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix} = T^{-1}\begin{bmatrix} x & 0 \\ 0 & y \end{bmatrix}\begin{bmatrix} \alpha^j \\ \beta^j \end{bmatrix}.$$

The vectors $\begin{bmatrix} \alpha^j \\ \beta^j \end{bmatrix}$ are pairwise linearly independent since $\frac{\alpha}{\beta}$ is not a root of unity, and this property is preserved by the invertible linear transformation $T^{-1}\begin{bmatrix} x & 0 \\ 0 & y \end{bmatrix}$, so $\{M^j s\}_{j\geq 0}$ is a sequence of pairwise linearly independent vectors.

Now suppose that M is not diagonalizable. Then we write the Jordan normal form of M as $M = T^{-1}JT$, where $J = \begin{bmatrix} \alpha & 0 \\ 1 & \alpha \end{bmatrix}$ and the first row of T is a row eigenvector corresponding to α. We know by assumption that $Ts = \begin{bmatrix} x \\ y \end{bmatrix}$ for some $x, y \in \mathbb{C}$, where $x \neq 0$. Then

$$M^j s = T^{-1}J^j Ts = \alpha^j T^{-1}\begin{bmatrix} 1 & 0 \\ j\alpha^{-1} & 1 \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix} = \alpha^j T^{-1} v_j,$$

where the vectors $v_j = \begin{bmatrix} x \\ j\alpha^{-1}x + y \end{bmatrix}$ are pairwise linearly independent. This uses the fact that $x \neq 0$. This pairwise linear independence is preserved by the invertible linear transformation T^{-1}; thus after a scalar multiple α^j, the vectors $\alpha^j T^{-1} v_j$ are also pairwise linearly independent. □

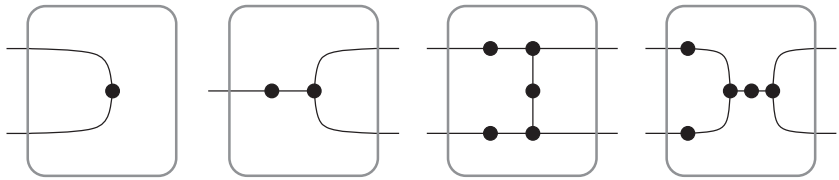
Corollary 5.16. *Let M be a unary recursive gadget with infinite projective order, and let s be a unary starter gadget whose signature is not orthogonal to any row eigenvector of M. Then the sequence $\{M^j s\}_{j\geq 0}$ has pairwise linearly independent generator signatures.*

Proof. Immediate. □

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 corollary. It is easy to see that $ab = 1$ is a tractable case, as $[a, 1, b] = [a, 1, a^{-1}]$ is degenerate. Recall that $a^3 = b^3$ essentially corresponds to region II.

Theorem 5.17. *In the context of* $\mathrm{Hol}_3(a, b)$ *let $a, b \in \mathbb{C}$ such that $ab \neq 1$ and $a^3 \neq b^3$, and let M be a unary recursive gadget with infinite projective order. Then there exists a starter gadget s (also in the context of* $\mathrm{Hol}_3(a, b)$*) such*

https://doi.org/10.1017/9781107477063.006 Published online by Cambridge University Press



(a) Gadget M_3 (b) Gadget M_4 (c) Gadget M_5 (d) Gadget M_6

Figure 5.3. Gadgets for constructing general-purpose starter gadgets.

that $\{M^j s\}_{j\geq 0}$ *is a sequence of pairwise linearly independent unary generator signatures.*

Proof. Let M_3, M_4, M_5, and M_6 be defined as in Figure 5.3. We calculate their signature matrices

$$v = M_3 = \begin{bmatrix} a \\ 1 \\ b \end{bmatrix}, \quad M_4 = \begin{bmatrix} a & 0 & 1 \\ 1 & 0 & b \end{bmatrix}, \quad M_5 = \begin{bmatrix} a^3 & 2a & b \\ a^2 & ab+1 & b^2 \\ a & 2b & b^3 \end{bmatrix},$$

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

Note that these matrices operate directly on symmetric signatures, e.g., the middle column of M_5 corresponds to the sum of the assignments of 01 and 10 on the trailing edges.

The 2×2 matrices $[M_4M_5v\ M_4v]$ and $[M_4M_6v\ M_4v]$ both have determinant $(a^3 - b^3)(ab-1)^2$, whereas $\det([M_4M_5v\ M_4M_6v]) = (a^3 - b^3)(ab-1)^3$, so the vectors M_4v, M_4M_5v, and M_4M_6v are pairwise linearly independent provided that $ab \neq 1$ and $a^3 \neq b^3$. The set of vectors that are orthogonal by dot product to at least one row eigenvector of the given matrix $M \in \mathbb{C}^{2\times 2}$ can be expressed as a union of at most two one-dimensional linear subspaces. By the pigeonhole principle, this union cannot contain three pairwise linearly independent vectors. Hence at least one element of $\{M_4M_5v, M_4M_6v, M_4v\}$ is not orthogonal to any row eigenvector of M. The corresponding starter gadget can be used with M in a recursive construction and we get a sequence of pairwise linearly independent unary generator signatures by Corollary 5.16. □

Exercise: Verify the signature matrices for gadgets M_3, M_4, M_5, and M_6 are as stated. Notice that these matrices are in a form that can be directly applied to symmetric signatures. Give a simple explanation that the middle columns of M_4 and M_6 are both 0.

https://doi.org/10.1017/9781107477063.006 Published online by Cambridge University Press

We make two remarks:

1. For a nonzero vector $s \in \mathbb{C}^2$, and a nonsingular matrix $M \in \mathbb{C}^{2\times 2}$, the condition that s is not a column eigenvector of M is equivalent to $\det[s\, Ms] \neq 0$, which is also equivalent to the condition that s is not orthogonal by dot product to any row eigenvector of M.
2. A sufficient condition for a nonsingular matrix $M \in \mathbb{C}^{2\times 2}$ to have infinite projective order is that the ratio of the eigenvalues is not a root of unity, which in turn is implied by the two eigenvalues having different norms.

Interpolation with Starter Gadgets

Since Theorem 5.17 already produced a sequence of unary generators (provided a suitable unary recursive gadget is given), there is no need to project it down to a lower dimension. Thus, the plan is to show that we can interpolate any unary generator, along similar lines to Lemma 5.13. However, we will prove it for recognizer signatures of the form $[x, 0, y]$ instead, since this allows us to reuse this lemma later on. Note that we can easily convert from generators of the form $[x, y]$ to recognizers of the form $[x, 0, y]$ by attaching a single vertex with recognizer $=_3$.

Lemma 5.18. *Let $k \geq 3$ be fixed and suppose that in the context of $\mathrm{Hol}_k(a, b)$, we can efficiently construct a sequence of pairwise linearly independent recognizers of the form $\{[x_j, 0, y_j]\}_{j\geq 0}$. Then for any $x, y \in \mathbb{C}$ we can efficiently simulate recognizer $[x, 0, y]$.*

Proof. By ignoring at most one signature in the sequence $\{[x_j, 0, y_j]\}_{j\geq 0}$ and relabeling the indices, we assume that each y_j is nonzero. Let Ω be a bipartite signature grid for the problem Holant$(\mathcal{R} \cup \{[x, 0, y]\} \mid \mathcal{G})$. Suppose recognizer $[x, 0, y]$ occurs n times in Ω. Dropping terms that evaluate to 0, we stratify the Holant sum according to how many times the signature $[x, 0, y]$ evaluates to x. Collecting these terms together, we write $\mathrm{Holant}_\Omega = \sum_{j=0}^{n} c_j x^j y^{n-j}$, where c_j is the sum over all edge assignments of the product of signature evaluations other than the n copies of $[x, 0, y]$, subject to the restriction that exactly j of the edge pairs connecting to $[x, 0, y]$ are both assigned 0, and exactly $n - j$ of the edge pairs connecting to $[x, 0, y]$ are both assigned 1.

We construct a sequence of bipartite signature grids Ω_i for the Holant problem Holant$(\mathcal{R} \mid \mathcal{G})$, by replacing each occurrence of $[x, 0, y]$ with a copy of an $\mathcal{F}$-gate with signature $[x_i, 0, y_i]$, for $i = 0, 1, \ldots, n$. This has the effect of replacing each occurrence of $[x, 0, y]$ by pairwise linearly independent signatures. Note that the bipartite structure is maintained. By oracle queries to Holant$(\mathcal{R} \mid \mathcal{G})$, we obtain a nonsingular Vandermonde system where c_j are the

https://doi.org/10.1017/9781107477063.006 Published online by Cambridge University Press

unknowns. Solving this linear system for c_j $(0 \le j \le n)$ yields the answer to $\text{Holant}_\Omega = \sum_{j=0}^{n} c_j x^j y^{n-j}$. □

When we apply Theorem 5.17, we will show that the eigenvalues of M have unequal norm. The following lemma gives a concrete way to test this, by examining the characteristic polynomial of M.

Lemma 5.19. *If the roots of a polynomial $x^2 - Bx + C \in \mathbb{C}[x]$ 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* $\text{Arg}(B^2) = \text{Arg}(C)$.

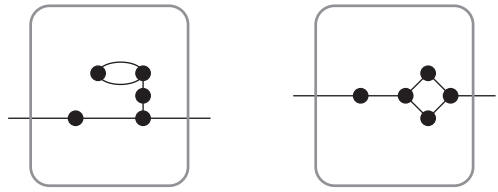
Proof. If the roots have equal norm, then for some $a, b \in \mathbb{C}$ with $|a| = |b| = 1$, and nonnegative $r \in \mathbb{R}$, we can write $x^2 - Bx + C = (x - ra)(x - rb)$, so $B|C| = r(a + b)r^2 = r(a^{-1} + b^{-1})r^2 ab = \overline{B}C$. Squaring both sides and dividing by C, we have $B^2\overline{C} = \overline{B}^2 C$ (note that 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, $\text{Arg}(B^2) = \text{Arg}(C)$. □

Eigenvalue Shifted Pairs and Other Gadgetry

Given any fixed $a, b \in \mathbb{C}$ for which $\text{Hol}_3(a, b)$ happens to be #P-hard, it is usually a straightforward process of trial and error of using Lemma 5.19 to find a unary recursive gadget with infinite projective order, so as to satisfy the conditions of Theorem 5.17. This would be fine if we were only aiming to prove hardness of a small finite number of problems. However, given some particular unary recursive gadget, there will inevitably be some settings of a and b that do not work. It is natural to add more gadgets to the mix, but the coefficients of the characteristic polynomial of M are themselves polynomials in a and b. Also, the degrees of these polynomials can get rather high and somewhat cumbersome (depending on the size of the gadget M). Algebraic symmetrization can help by reducing the complexity of the polynomials involved, but then we are still left with the question: Given two polynomials $p(X, Y)$ and $q(X, Y)$, under which settings of $X, Y \in \mathbb{C}$ is it the case that $\text{Arg}(p(X, Y)) = \text{Arg}(q(X, Y))$? Moreover, given many such pairs of polynomials, how can we be assured that all relevant X and Y are "covered" by one or more gadgets?

We now introduce a technique called *eigenvalue shifted pairs*, or ESPs for short, to address this problem. Suppose we have unary recursive gadgets M and M', and suppose the eigenvalues of M are those of M' shifted by some complex number δ. Then unless δ "lines up just right," at least one of the two matrices will have eigenvalues with unequal norm, which is just what we need.

https://doi.org/10.1017/9781107477063.006 Published online by Cambridge University Press



(a) Gadget M_1 (b) Gadget M_2

Figure 5.4. An eigenvalue-shifted pair of gadgets.

Definition 5.20. 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. For example, the transition matrices of gadgets M_1 and M_2 (Figure 5.4) differ only by $ab - 1$ along the main diagonal, and form an ESP for all $a, b \in \mathbb{C}$, except when $ab = 1$ (these are the same gadgets we saw earlier in Figure 5.2). Before we make use of this ESP, we state a technical lemma so we can describe the conditions under which an ESP *doesn't* work.

Lemma 5.21. *Suppose* $\alpha, \beta, \delta \in \mathbb{C}$, $|\alpha| = |\beta|$, $\alpha \neq \beta$, $\delta \neq 0$, *and* $|\alpha + \delta| = |\beta + \delta|$. *Then there exist* $r, s \in \mathbb{R}$ *such that* $r\delta = \alpha + \beta$ *and* $s\delta^2 = \alpha\beta$.

Proof. After a rotation in the complex plane, namely multiplying α, β, δ by some $e^{i\theta}$, 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 get $\overline{\delta} = \delta$; therefore $\delta \in \mathbb{R}$. □

Corollary 5.22. *Let* M *and* M' *be an eigenvalue shifted pair of* 2×2 *matrices. If* M *and* M' *have the property that both eigenvalues have the same norm, then* $\mathrm{tr}(M)/\delta \in \mathbb{R}$ *and* $\det(M)/\delta^2 \in \mathbb{R}$.

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 $|\alpha + \delta| = |\beta + \delta|$. By Definition 5.20, $\alpha \neq \beta$ and $\delta \neq 0$. Then by Lemma 5.21, there exist r and $s \in \mathbb{R}$ such that $\mathrm{tr}(M) = \alpha + \beta = r\delta$ and $\det(M) = \alpha\beta = s\delta^2$, hence $\mathrm{tr}(M)/\delta \in \mathbb{R}$ and $\det(M)/\delta^2 \in \mathbb{R}$. □

We now apply an ESP to prove that for most settings (a, b), the problem $\mathrm{Hol}_3(a, b)$ is #P-hard.

https://doi.org/10.1017/9781107477063.006 Published online by Cambridge University Press

Lemma 5.23. *Suppose X and Y are not both real, $X \neq \pm 1$, $X^2 + X + Y \neq 0$, and $4(X-1)^2(X+1) \neq (Y+2)^2$. Then either gadget M_1 or gadget M_2 has nonzero eigenvalues with distinct norm.*

Proof. The transition matrices are $M_1 = \begin{bmatrix} a^3+ab & a+b^2 \\ a^2+b & ab+b^3 \end{bmatrix}$ and $M_2 = \begin{bmatrix} a^3+1 & a+b^2 \\ a^2+b & b^3+1 \end{bmatrix}$, so $M_1 = M_2 + (X-1)I$, and the eigenvalue shift is nonzero. $\operatorname{tr}(M_2) = Y+2$. Checking the determinants, $\det(M_2) = (X-1)^2(X+1) \neq 0$ and $\det(M_1) = (X-1)(X^2+X+Y) \neq 0$. Also, $\operatorname{tr}(M_2)^2 - 4\det(M_2) = (Y+2)^2 - 4(X-1)^2(X+1) \neq 0$, so the eigenvalues of M_2 are distinct. Therefore by Corollary 5.22, either M_1 or M_2 has nonzero eigenvalues of distinct norm unless

$$Y + 2 = \operatorname{tr}(M_2) = r(X-1) \text{ and } (X-1)^2(X+1) = \det(M_2) = s(X-1)^2$$

for some $r, s \in \mathbb{R}$. Then we would have $X = s - 1 \in \mathbb{R}$ and $Y = r(X-1) - 2 \in \mathbb{R}$. □

The case where $X \in \mathbb{R}$ and $Y \in \mathbb{R}$ will require different techniques, so we put it aside for now and focus on the remaining three cases in this subsection, where X and Y are not both real and the following conditions hold. Note that $X = 1$ is tractable by Theorem 5.6 and we exclude that.

1. $X = -1$ or
2. $X^2 + X + Y = 0$ or
3. $4(X-1)^2(X+1) = (Y+2)^2$

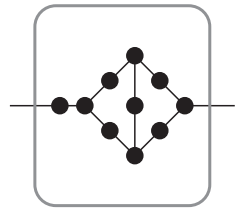
Having a specific condition such as $X = -1$ or $X^2 + X + Y = 0$ introduces fortuitous cancellations, making it possible to use individual gadgets rather than ESPs. The following gadgets were selected by a trial and error process, using a computer to assist with the search.

Gadgets M_1 and M_7 (see Figure 5.5) can be used to deal with the $X = -1$ case. Recall that any setting of a and b such that $X = -1$ and $Y = \pm 2\mathrm{i}$ is tractable by Theorem 5.6.

Lemma 5.24. *If $X = -1$, $Y \neq \pm 2\mathrm{i}$, and $Y \notin \mathbb{R}$, then either gadget M_1 or gadget M_7 has a transition matrix with nonzero eigenvalues with distinct norm.*

Proof. Suppose $|Y| \neq 2$, $Y \notin \mathbb{R}$. Under the assumption $X = -1$, $\det(M_1) = -2Y \neq 0$ and $\operatorname{tr}(M_1) = Y - 2$, so $\operatorname{tr}(M_1) \cdot |\det(M_1)| - \overline{\operatorname{tr}(M_1)} \cdot \det(M_1) = (Y-2) \cdot |-2Y| + (\overline{Y}-2)(2Y) = 2Y \cdot |Y| - 4|Y| + 2|Y|^2 - 4Y = 2(|Y|-2)(|Y|+Y) \neq 0$. Thus $\overline{\operatorname{tr}(M_1)} \cdot \det(M_1) \neq \operatorname{tr}(M_1) \cdot |\det(M_1)|$ and by Lemma 5.19, M_1 has (nonzero) eigenvalues with distinct norm.

https://doi.org/10.1017/9781107477063.006 Published online by Cambridge University Press



Gadget M_7

Figure 5.5. A unary recursive gadget.

Now suppose $|Y| = 2$, but $Y \neq \pm 2\mathrm{i}$ and $Y \notin \mathbb{R}$.

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

Under the assumption $X = -1$, we have $\det(M_7) = -16Y \neq 0$. Substituting $\overline{Y} = 4/Y$,

$$\begin{aligned} &\mathrm{tr}(M_7)^2\overline{\det(M_7)} - \overline{\mathrm{tr}(M_7)}^2 \det(M_7) \\ &\quad = -16(Y - \overline{Y}) \cdot (-16 + 8Y\overline{Y} + 8Y^2\overline{Y} + Y^3\overline{Y} + 8Y\overline{Y}^2 + Y^2\overline{Y}^2 + Y\overline{Y}^3) \\ &\quad = \frac{-64(Y - \overline{Y})(Y^2 + 4)(Y^2 + 8Y + 4)}{Y^2} \\ &\quad \neq 0. \end{aligned}$$

Note that $|Y^2 + 4| \leq 8 < |8Y| = 16$. Hence $\mathrm{tr}(M_7)^2\overline{\det(M_7)} \neq \overline{\mathrm{tr}(M_7)}^2 \det(M_7)$ and the eigenvalues of M_7 (which are nonzero) have distinct norm by Lemma 5.19. □

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 5.25. *If $X^2 + X + Y = 0$ and $X \notin \mathbb{R}$ then the transition matrix of gadget M_8 has nonzero eigenvalues with distinct norm.*

Proof. Gadget M_8 is defined in Figure 5.6.

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

https://doi.org/10.1017/9781107477063.006 Published online by Cambridge University Press

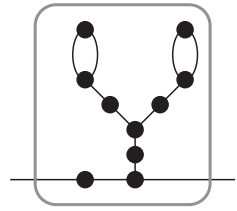


Figure 5.6. A unary recursive gadget.

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

$$-X^2(X-1)^5.$$

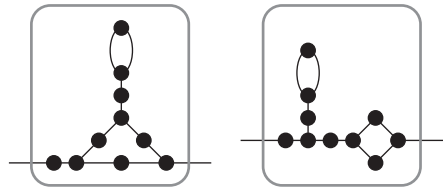
Exercise: Verify that the displayed polynomial is congruent to $-X^2(X-1)^5$ mod $X^2 + X + Y$.

Similarly, the trace, which is $-2X^3 + 6X^2 + 3XY + Y^2 + Y$, also factors into $X(X-1)^3$. Since $X \notin \mathbb{R}$, we have $\det(M_8) \neq 0$, $\operatorname{tr}(M_8) \neq 0$, and $(1 - X)\det(M_8) = \operatorname{tr}(M_8)^2$. Therefore $\operatorname{Arg}(\det(M_8)) \neq \operatorname{Arg}(\operatorname{tr}(M_8)^2)$ for otherwise X is real, and we conclude by Lemma 5.19 that the eigenvalues of M_8 (which are nonzero) have distinct norm. □

The condition $4(X-1)^2(X+1) = (Y+2)^2$ is somewhat resilient to individual unary recursive gadgets, so we take advantage of another interesting coincidence: two gadgets with transition matrices that have identical trace. In the following lemma, we may assume $X^2 + X + Y \neq 0$ due to Lemma 5.25. We will also assume $X \notin \mathbb{R}$ in this lemma for technical reasons. The case of $X \in \mathbb{R}$ and $Y \notin \mathbb{R}$ will be easy to clean up afterwards.

Lemma 5.26. *Suppose $X \notin \mathbb{R}$, and further assume that $X^2 + X + Y \neq 0$ and $4(X-1)^2(X+1) = (Y+2)^2$. Then the transition matrix of either unary recursive gadget M_9 or unary recursive gadget M_{10} has nonzero eigenvalues with distinct norm.*

https://doi.org/10.1017/9781107477063.006 Published online by Cambridge University Press



(a) Gadget M_9 (b) Gadget M_{10}

Figure 5.7.

Proof. Gadgets M_9 and M_{10} are defined in Figure 5.7. The transition matrices are

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

$$M_{10} = \begin{bmatrix} a^6 + a^4b + 2a^3 + a^2b^2 + 2ab + b^3 & a^4 + a^3b^2 + a^2b + 2ab^3 + a + b^5 + b^2 \\ a^5 + 2a^3b + a^2b^3 + a^2 + ab^2 + b^4 + b & a^3 + a^2b^2 + ab^4 + 2ab + b^6 + 2b^3 \end{bmatrix}.$$

Let R denote $(Y+2)^2 - 4(X-1)^2(X+1)$. The main diagonals of M_9 and M_{10} are identical, so $\mathrm{tr}(M_9) = \mathrm{tr}(M_{10})$. Furthermore, $\mathrm{tr}(M_9) = \mathrm{tr}(M_9) - R = (X-1)(2X^2+Y)$. Clearly $X - 1 \neq 0$, since $X \notin \mathbb{R}$. If $2X^2 + Y = 0$, then substituting $Y = -2X^2$ into $4(X-1)^2(X+1) = (Y+2)^2$ would yield $X(X-1)^2(X+1) = 0$, again impossible by $X \notin \mathbb{R}$. So $\mathrm{tr}(M_9) \neq 0$. Next, $\det(M_{10}) = (X-1)^3(X+1)(X^2+X+Y)$ and $\det(M_9) = \det(M_9) - R(X-1)^2 = (X-1)^3(X+4)(X^2+X+Y)$, so these are both nonzero. If both M_9 and M_{10} have eigenvalues with equal norm, then applying Lemma 5.19 twice, $\mathrm{Arg}(\det(M_9)) = \mathrm{Arg}(\mathrm{tr}(M_9)^2) = \mathrm{Arg}(\mathrm{tr}(M_{10})^2) = \mathrm{Arg}(\det(M_{10}))$. However, this would imply $\mathrm{Arg}(X+4) = \mathrm{Arg}(X+1)$ and $X \in \mathbb{R}$, so we conclude that either M_9 or M_{10} has nonzero eigenvalues with distinct norm. □

We have already seen a gadget that can handle the remaining case.

Lemma 5.27. *Suppose $X \in \mathbb{R}$ and $Y \notin \mathbb{R}$, and further assume that $4(X-1)^2(X+1) = (Y+2)^2$. Then the transition matrix of unary recursive gadget M_7 has nonzero eigenvalues with distinct norm.*

Proof. Note that $X < -1$, lest Y be real valued. Let R denote $(Y+2)^2 - 4(X-1)^2(X+1)$ as before. We find that $\mathrm{tr}(M_7) = \mathrm{tr}(M_7) - R = 2X(X-1)^2 \neq 0$. We calculate that $\det(M_7) = (X-1)^3(X+2X^2+X^3+2Y)$, and we claim this is also nonzero. Otherwise, we would have $Y = -(X+2X^2+X^3)/2$, and from $X \in \mathbb{R}$ we would have $Y \in \mathbb{R}$, a contradiction. Now $\mathrm{tr}^2(M_7) = 4X^2(X-1)^4 \in \mathbb{R}$,

https://doi.org/10.1017/9781107477063.006 Published online by Cambridge University Press

so $\mathrm{tr}^2(M_7)/\det(M_7) \notin \mathbb{R}$ follows from $X \in \mathbb{R}$ and $Y \notin \mathbb{R}$. We conclude by Lemma 5.19 that M_7 has nonzero eigenvalues with distinct norm. □

Now we sum up the results of the previous lemmas. Recall that if $X = 1$ or $(X, Y) = (-1, \pm 2\mathrm{i})$ then $\mathrm{Hol}_3(a, b)$ is tractable.

Lemma 5.28. *Suppose that it is not the case that both X and Y are real valued. Also assume that $X \neq 1$ and $(X, Y) \neq (-1, \pm 2\mathrm{i})$. Then in the context of $\mathrm{Hol}_3(a, b)$ there exists a unary recursive gadget M for which the eigenvalues are both nonzero and have distinct norm.*

Proof. We know by Lemma 5.23 that either gadget M_1 or M_2 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. $X = -1$,
2. $X^2 + X + Y = 0$, or
3. $4(X - 1)^2(X + 1) = (Y + 2)^2$.

First suppose $X = -1$. Then Y is not real valued and $Y \neq \pm 2\mathrm{i}$, so we get a transition matrix of the required form by Lemma 5.24. If $X^2 + X + Y = 0$ we have $X \notin \mathbb{R}$ (otherwise we would have $X, Y \in \mathbb{R}$), and we have the requirement satisfied by Lemma 5.25. Now we may assume $X^2 + X + Y \neq 0$ and suppose $4(X - 1)^2(X + 1) = (Y + 2)^2$. If $X \notin \mathbb{R}$ then by Lemma 5.26 we are done; otherwise $X \in \mathbb{R}$ but $Y \notin \mathbb{R}$ so we are done by Lemma 5.27. □

Corollary 5.29. *Suppose $a, b \in \mathbb{C}$ are such that it is not the case that both X and Y are real valued. Also assume $X \neq 1$ and $4X^3 \neq Y^2$ (equivalently, $a^3 \neq b^3$). Then in the context of $\mathrm{Hol}_3(a, b)$ we can efficiently simulate any recognizer signature of the form $[x, 0, y]$.*

Proof. For any such $a, b \in \mathbb{C}$, we have a unary recursive gadget M by Lemma 5.28 whose transition matrix has nonzero eigenvalues of distinct norm. Then M has infinite projective order, and by Theorem 5.17, we can efficiently construct a sequence of pairwise linearly independent unary generators $[x_j, y_j]$. By attaching an additional vertex labeled with recognizer $=_3$, these become pairwise linearly independent signatures of the form $[x_j, 0, y_j]$. Therefore by Lemma 5.18 we can efficiently simulate any recognizer of the form $[x, 0, y]$. □

Applying Unary Signatures to Prove #P-hardness

The ability to simulate unary signatures (or "virtual unary" signatures) will give us a reduction from Vertex Cover. Note that counting Vertex Cover on

https://doi.org/10.1017/9781107477063.006 Published online by Cambridge University Press

k-regular graphs is just Holant($=_k$| [0, 1, 1]). Counting VERTEX COVER is #P-hard even when the input is restricted to k-regular planar graphs. We remark that for $k \geq 6$, any k-regular planar graph must have self-loops or multiple edges. This follows from Euler's formula $V - E + F = 2$.

Lemma 5.30. *Counting* VERTEX COVERS *on k-regular planar multigraphs (with self-loops and parallel edges) is* #P-hard *for $k \geq 3$.*

Proof. We will give a reduction from counting VERTEX COVERS on 3-regular planar graphs, which is known to be #P-hard [XZZ07]. If k is odd, we can easily reduce from the given 3-regular planar graph $G = (V, E)$ to a k-regular planar graph by using a gadget consisting of a single vertex incident with $(k-1)/2$ self-loops and one dangling edge. Connect $k - 3$ copies of this gadget to every vertex $v \in V$. Owing 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 where k is even. The gadget is similar, consisting of a single vertex incident with $(k-2)/2$ self-loops and two dangling edges. 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 we will argue that the vertices in V can be paired in such a way that the gadgets can be introduced while preserving planarity. We do this in two steps. First, we show that there exists a pairing of vertices in which the distance between each pair is ≤ 2. After that we show that planarity is preserved when we add edges of the gadgets according to such a pairing.

We may assume that G is connected, so fix any spanning tree T of G, and note that T has an even number of vertices as G does and the degree of every vertex in T is ≤ 3. It is then sufficient to argue that such a pairing exists in T, because distance measured in G is no more than that measured in T. If there exist adjacent vertices u and v in T such that $\deg(u) = 1$ and $\deg(v) \leq 2$, then we pair u with v. Otherwise, every leaf node is incident with a vertex of degree 3, implying that there exists a vertex t that is adjacent to at least two leaf nodes u and v, and we pair these two leaf nodes together. (To see that such a vertex t exists, fix any node r and make T a rooted tree with root r. Let u be a leaf of maximum depth. As the number of vertices is even, hence more than one, $u \neq r$ and u has a parent t. We have $\deg(t) = 3$, since no neighbor of u has degree ≤ 3. Thus t has another child v. This v must be a leaf by the maximum depth of u.)

https://doi.org/10.1017/9781107477063.006 Published online by Cambridge University Press

In any case, after removing u and v and their incident edges, we are left with an induced subtree T' with an even number of vertices and for which every vertex has degree ≤ 3. This implies a simple recursive algorithm that finds a pairing where paired vertices have distance (on tree T) ≤ 2.

Given such a pairing, we may further assume that there are no pairs (u, v) and (s, t) such that the distance between both pairs is 2 and (u, s, v, t) is a path in G; otherwise we may instead pair u with s and v with t, resulting in two pairs of adjacent vertices. Now for every pair (u, v) of paired vertices, fix a minimal length path in G between them. Draw all gadgets in a neighborhood of the path connecting each pair. Clearly this can be done preserving planarity if (u, v) has distance 1. For (u, v) having distance 2, let the chosen path be (u, s, v). Then s must have degree 3; otherwise s must be paired with some t and (u, s, v, t) or (t, u, s, v) is a path in G. Let the third edge incident to s be (s, w). The gadgets for (u, v) are drawn on the opposite side of (s, w). Note that s is paired with some vertex t through a path (s, w, t) not involving u or v, and causes no edge crossings with the gadgets drawn between u and v. Moreover, gadgets that are drawn along a path involving u or v also introduce no crossings with the gadgets between u and v (they do not connect to s, and the drawing was defined in such a way that they do not cross the path (u, s, v)). Hence planarity is preserved. □

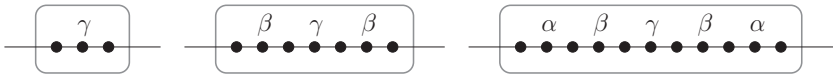
The #P-hardness reduction in Lemma 5.30 is direct from Vertex Covers on 3-regular planar graphs; thus clearly it does not use the pinning lemma (Lemma 3.13).

For future reference, we record the planar pairing construction in the proof of Lemma 5.30 separately. The proof also works for multigraphs allowing loops and parallel edges.

Lemma 5.31. *For any 3-regular planar multigraph $G = (V, E)$, with $V = \{v_1, \ldots, v_n\}$, one can find in polynomial time a pairing $M = \{\{v_{i_1}, v_{i_2}\}, \ldots, \{v_{i_{n-1}}, v_{i_n}\}\}$, i.e., a partition of V into disjoint pairs, such that $(V, E \cup M)$ is a planar multigraph, where $E \cup M$ is the multiset formed by disjoint union.*

The ability to simulate all unary signatures is what will allow us to prove #P-hardness, although technically we will use "virtual unary" recognizers of the form $[x, 0, y]$. The next lemma says that if we are considering $\mathrm{Hol}_k(a, b)$, then other than on a one-dimensional curve $ab = 1$ and an isolated point $(a, b) = (0, 0)$ we get a reduction from Vertex Cover by using virtual unary recognizers. As we have seen, the problem $\mathrm{Hol}_k(a, b)$ is tractable on the curve $ab = 1$ and at $(a, b) = (0, 0)$.

https://doi.org/10.1017/9781107477063.006 Published online by Cambridge University Press



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

Figure 5.8. Gadgets used to simulate the [0,1,1] signature.

Lemma 5.32. *Suppose $k \geq 3$ and $(a, b) \in \mathbb{C}^2$ satisfies $ab \neq 1$ and $(a, b) \neq (0, 0)$, and assume that for any fixed $m \geq 1$, and any $x_j, y_j \in \mathbb{C}$ $(1 \leq j \leq m)$,*

$$\text{Holant}(\{=_k, [x_1, 0, y_1], \ldots, [x_m, 0, y_m]\} \mid [a, 1, b]) \leq_{\text{T}} \text{Holant}(=_k \mid [a, 1, b]).$$

Then

$$\text{Holant}(=_k \mid [0, 1, 1]) \leq_{\text{T}} \text{Holant}(=_k \mid [a, 1, b])$$

and $\text{Holant}(=_k \mid [a, 1, b])$ *is* #P-hard.

The same statement holds for $\text{Holant}(=_k \mid [a, 1, b], \Delta_0, \Delta_1)$*, and a #P-hardness reduction exists that does not use Lemma 3.13.*

Proof. Assume $ab \neq 1$ and $(a, b) \neq (0, 0)$. Since $\text{Hol}_k(0, 1)$ is the same problem as $\text{Holant}(=_k \mid [0, 1, 1])$, i.e., counting Vertex Cover on k-regular graphs, which is #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 5.8. Each gadget will have recognizer signatures of the type $[x, 0, y]$ assigned to the labeled vertices and the generator $[a, 1, b]$ assigned to the unlabeled vertices.

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

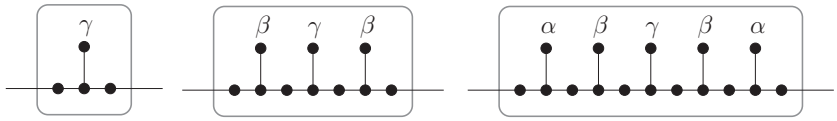
If $ab \neq 0$ and $ab \neq -1$, then we use gadget 3 in Figure 5.8, and we set its signatures to be

$$\alpha = [-b/(ab - 1), 0, a/(ab - 1)] \sim [-b, 0, a],$$
$$\beta = [-a^{-2}, 0, b^{-1}(1 + ab)^{-1}], \quad \text{and}$$
$$\gamma = [(ab + 1)/(1 - ab), 0, -a^2(ab + 1)/(1 - ab)] \sim [1, 0, -a^2].$$

Here we use the notation $\sim$ to mean up to a nonzero multiplier. Calculating the resulting signature of gadget 3 using matrix product, we find that it is $[0, 1, 1]$ as desired.

If $ab = 0$ then assume without loss of generality that $a = 0$ and $b \neq 0$ (we can do this because $\text{Hol}_k(0, 1) = \text{Hol}_k(1, 0)$ – also note that $\text{Hol}_k(1, 0)$ is the

https://doi.org/10.1017/9781107477063.006 Published online by Cambridge University Press



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

Figure 5.9. Alternate depiction of gadgets 1 through 3.

problem of counting INDEPENDENT SET on k-regular graphs). This time we use gadget 1, setting $\gamma = [b, 0, b^{-1}]$. Then gadget 1 simulates a generator signature $[b^{-1}, 1, 2b]$. But since this signature fits the criteria of case 1 above, we are done by a reduction from case 1.

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

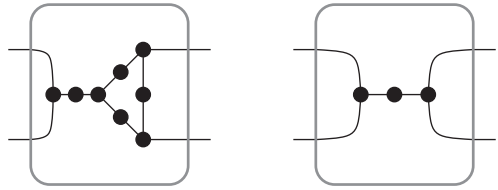
Corollary 5.33. *Suppose $a, b \in \mathbb{C}$ are such that X and Y are not both real valued. Also assume $X \neq 1$ and $4X^3 \neq Y^2$ (equivalently, $a^3 \neq b^3$). Then* $\mathrm{Holi}_3(a, b)$ *is* #P-hard*, even when restricted to planar graphs as input.*

The same statement holds for $\mathrm{Holant}(=_3 | [a, 1, b], \Delta_0, \Delta_1)$*, and a #P-hardness reduction exists that does not use Lemma 3.13.*

Proof. Immediate from Corollary 5.29 and Lemma 5.32. Note that all constructions preserve planarity. □

The proof of Lemma 5.32 is a good demonstration of the power of having all unary signatures. However, the particular choices of the (virtual) unary signatures α, β, γ may appear mysterious. Some explanations will demystify this. As indicated earlier, each signature of the form $[x, 0, y]$ as a recognizer is obtained by connecting a copy of $=_3$ to a unary generator $[x, y]$. The more detailed and direct depiction of gadgets 1 to 3 is in Figure 5.9 with unary signatures. We have seen a similar proof in the dichotomy for Holant* problems, where there were gadgets that resemble "growing weeds." The matrix form of a signature $u = [x, 0, y]$ is diagonal $D_u = \begin{bmatrix} x & 0 \\ 0 & y \end{bmatrix}$. Gadget 3 (in either Figure 5.8c or Figure 5.9c) has the signature $(gD_\alpha g)D_\beta(gD_\gamma g)D_\beta(gD_\alpha g)$, expressed as a matrix product, where $g = \begin{bmatrix} a & 1 \\ 1 & b \end{bmatrix}$. If $D = \begin{bmatrix} x & 0 \\ 0 & y \end{bmatrix}$ then $gDg = \begin{bmatrix} a^2x + y & ax + by \\ ax + by & x + b^2y \end{bmatrix}$, and it can be made a diagonal matrix if we choose $(x, y) \sim (-b, a)$, which is what we did for D_α. On the other hand, if we take $y = -a^2x$

https://doi.org/10.1017/9781107477063.006 Published online by Cambridge University Press



(a) A finisher gadget (b) Another finisher gadget

Figure 5.10. Examples of finisher gadgets.

then gDg has the form $g_1 = x(1-ab)\begin{bmatrix} 0 & a \\ a & 1+ab \end{bmatrix}$, which is what we did for D_γ. Our goal is to realize $\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$. With a diagonal $D' \sim \begin{bmatrix} 1/a & 0 \\ 0 & 1/(1+ab) \end{bmatrix}$, $D'g_1D' = D'(gD_\gamma g)D'$ takes the form $g_2 = \lambda\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$. We need the outside factors $gD_\alpha g$ to provide a proper bipartite form, so that gadget 3 constructed in the end is a generator. Thus the strategy is to choose γ such that $gD_\gamma g$ has the form g_1, choose α such that $gD_\alpha g$ takes a diagonal form D''. We assume D'' is invertible and choose $D_\beta \sim (D'')^{-1}D'$. Note that we can choose D_β to be an arbitrary diagonal matrix of the form $\begin{bmatrix} x & 0 \\ 0 & y \end{bmatrix}$, in particular any given $(D'')^{-1}D'$, and because these matrices are diagonal they commute $(D'')^{-1}D' = D'(D'')^{-1}$. Thus $(gD_\alpha g)D_\beta(gD_\gamma g)D_\beta(gD_\alpha g) = D'(gD_\gamma g)D'$ takes the form g_2.

5.1.4 Hardness in Region III Where $(X, Y) \in \mathbb{R} \times \mathbb{R}$

Recall that region III is specified by $X \neq 1$, $Y^2 \neq 4X^3$ (equivalently $a^3 \neq b^3$) and $(X, Y) \neq (-1, 0)$. In this subsection we further assume $(X, Y) \in \mathbb{R} \times \mathbb{R}$.

Interpolation

We now introduce a new type of gadget called a finisher gadget, and adapt our interpolation techniques to the scenario with binary recursive gadgets and finisher gadgets. A finisher gadget has two sets of two dangling edges all connected internally to recognizers. See Figure 5.10 for two examples. It can transform a binary symmetric generator to a binary symmetric recognizer. Symmetry is guaranteed by the symmetry of the underlying graph of the gadget. They have the additional property that one set of two dangling edges (depicted as protruding from the left) are connected to a single $=_k$. These finisher gadgets will be represented by 3×3 matrices with middle row identically 0, and thus

https://doi.org/10.1017/9781107477063.006 Published online by Cambridge University Press

rank at most 2. This extension is necessary to treat the case in region III where $(X, Y) \in \mathbb{R} \times \mathbb{R}$, and it is also a natural place to introduce the idea of iterating at a higher dimensional space, which affords more flexibility, and then apply a *projection* down to a lower dimension. The most crucial lemma is Lemma 5.36, which amounts to an exchange of quantifiers. But first we establish tools for binary recursive gadgets as we did for unary recursive gadgets.

Lemma 5.34. *Let $M \in \mathbb{C}^{3\times 3}$ be a nonsingular binary recursive gadget with infinite projective order. Let $s \in \mathbb{C}^3$ be a binary starter gadget such that s is not orthogonal to any row eigenvector of M. Then $\{M^j s\}_{j\geq 0}$ is a sequence of pairwise linearly independent generator signatures.*

Proof. The form of $M^j s$ defines generator signatures, where both s and M are expressed for symmetric signatures.

Let $M = T^{-1}JT$, where J is the Jordan normal form for M, and let $u, v, w \in \mathbb{C}$ be determined by $[u\ v\ w]^{\mathrm{T}} = Ts$. Suppose J is diagonal, let $B = T^{-1}\operatorname{diag}(u, v, w)$, and then

$$M^j s = T^{-1}J^j Ts = T^{-1}\begin{bmatrix}\alpha^j & 0 & 0\\ 0 & \beta^j & 0\\ 0 & 0 & \gamma^j\end{bmatrix}\begin{bmatrix}u\\ v\\ w\end{bmatrix}$$
$$= T^{-1}\begin{bmatrix}u & 0 & 0\\ 0 & v & 0\\ 0 & 0 & w\end{bmatrix}\begin{bmatrix}\alpha^j\\ \beta^j\\ \gamma^j\end{bmatrix} = B\begin{bmatrix}\alpha^j\\ \beta^j\\ \gamma^j\end{bmatrix}.$$

There is a pair of eigenvalues of M for which the ratio is not a root of unity (otherwise, we would have some j for which $M^j = \lambda I$ for some nonzero λ). Then the sequence of vectors $[\alpha^j\ \beta^j\ \gamma^j]^{\mathrm{T}}$ are pairwise linearly independent, and since pairwise linear independence is preserved under multiplication by the nonsingular matrix B (note $uvw \neq 0$), we conclude that $\{M^j s\}_{j\geq 0}$ is pairwise linearly independent.

If M has two Jordan blocks, then we have

$$M^j s = T^{-1}J^j Ts = T^{-1}\begin{bmatrix}\alpha^j & 0 & 0\\ j\alpha^{j-1} & \alpha^j & 0\\ 0 & 0 & \beta^j\end{bmatrix}\begin{bmatrix}u\\ v\\ w\end{bmatrix},$$

where $uw \neq 0$. If M has one Jordan block, then

$$M^j s = T^{-1}J^j Ts = T^{-1}\begin{bmatrix}\alpha^j & 0 & 0\\ j\alpha^{j-1} & \alpha^j & 0\\ \binom{j}{2}\alpha^{j-2} & j\alpha^{j-1} & \alpha^j\end{bmatrix}\begin{bmatrix}u\\ v\\ w\end{bmatrix},$$

https://doi.org/10.1017/9781107477063.006 Published online by Cambridge University Press

where $u \neq 0$. Either way, we have

$$M^j s = T^{-1} J^j T s = T^{-1} \begin{bmatrix} \alpha^j & 0 & 0 \\ j\alpha^{j-1} & \alpha^j & 0 \\ * & * & * \end{bmatrix} \begin{bmatrix} u \\ v \\ w \end{bmatrix}$$
$$= \begin{bmatrix} u\alpha^j \\ uj\alpha^{j-1} + v\alpha^j \\ * \end{bmatrix} = u\alpha^j \begin{bmatrix} 1 \\ j/\alpha + v/u \\ * \end{bmatrix}.$$

The determinant of the 2×2 matrix $\det \begin{bmatrix} 1 & 1 \\ j/\alpha + v/u & i/\alpha^i + v/u \end{bmatrix} = \frac{i-j}{\alpha} \neq 0$. Hence $\{M^j s\}_{j \geq 0}$ is a sequence of pairwise linearly independent signatures. □

We will not construct general-purpose binary starter gadgets (as we did for unary starter gadgets). Instead, we will test starter gadgets individually, using the following lemma.

Lemma 5.35. *Suppose $M \in \mathbb{C}^{m \times m}$ and $s \in \mathbb{C}^m$. If* $\det([s \; Ms \; M^2 s \cdots M^{m-1} s]) \neq 0$ *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 since $vM^i s = \lambda^i vs = 0$ we have $v[s \; Ms \cdots M^{m-1} s] = 0$, but $v \neq 0$, so this is a contradiction. □

The next lemma is crucial.

Lemma 5.36. *Suppose $\{m_i\}_{i \geq 0}$ is a series of pairwise linearly independent column vectors in $\mathbb{C}^3$. Let F', F'', and $F''' \in \mathbb{C}^{3 \times 3}$ be matrices of rank 2 where* $\ker(F')$, $\ker(F'')$, *and* $\ker(F''')$ *are linearly independent. Then for every n, there exists some $S \subseteq \{i \mid 0 \leq i \leq n^3\}$, and some $F \in \{F', F'', F'''\}$, such that $|S| \geq n$ and vectors in $\{Fm_i \mid i \in S\}$ are* pairwise *linearly independent.*

Proof. Let $j > i \geq 0$ be integers, let $N = [m_i \; m_j] \in \mathbb{C}^{3 \times 2}$, then $\text{rank}(N) = 2$ and $\dim(\text{Im}(N)) = 2$. Since $\ker(F')$, $\ker(F'')$, and $\ker(F''')$ are linearly independent of $\mathbb{C}^3$, we can let $F \in \{F', F'', F'''\}$ such that $\ker(F) \cap \text{Im}(N) = \{0\}$. Then $FN \in \mathbb{C}^{3 \times 2}$ has rank 2, hence Fm_i and Fm_j are linearly independent.

Each $F \in \{F', F'', F'''\}$ defines a coloring of the set $K = \{0, 1, \ldots, n^3\}$ as follows: color $i \in K$ with the linear subspace spanned by Fm_i. Assume for a contradiction that for each $F \in \{F', F'', F'''\}$ there are not n pairwise linearly independent vectors among $\{Fm_i : i \in K\}$. Then, including possibly the 0-dimensional space $\{0\}$, there can be at most n distinct colors assigned by each

https://doi.org/10.1017/9781107477063.006 Published online by Cambridge University Press

$F \in \{F', F'', F'''\}$. By the pigeonhole principle, some i and j with $0 \le i < j \le n^3$ must receive the same color for all $F \in \{F', F'', F'''\}$. This is a contradiction and we are done. □

We remark that Lemma 5.36 amounts to an exchange of quantifiers. As shown in the first paragraph of the proof, the antecedent of the lemma says that for every pair of distinct m_i and m_j from a sequence of pairwise linearly independent $\{m_i\}_{i\ge 0}$, there exists a finisher $F \in \{F', F'', F'''\}$ such that Fm_i and Fm_j are linearly independent. This is a $\forall\exists$ type condition. Then the consequent of the lemma says that there is a single $F \in \{F', F'', F'''\}$ that produces an arbitrarily large set of pairwise linearly independent $\{Fm_i \mid i \in S\}$. This is an $\exists\forall$ type statement (there exist a large S among the first $n^{O(1)}$ many i's and a single F, such that F works for all m_i from S.) The cost of this exchange of quantifiers is that we may have to look at polynomially more vectors in the original list $\{m_i\}_{i\ge 0}$, and we may not know in advance which subset S would work. As we will see, both caveats are harmless in our intended application of this lemma.

In the following lemma we use binary finisher gadgets. Recall that such a gadget has two sets of two dangling edges each, both sets are connected internally to recognizer signatures, and both dangling edges of one set (depicted as protruding from the left) are connected internally to a single EQUALITY signature. The two dangling edges of the other set (depicted as protruding from the right) are to be merged with the two leading edges of a binary recursive gadget. Thus these finisher gadgets have 3×3 transition matrices that have an identically 0 middle row. They transform a generator signature to a recognizer signature.

Lemma 5.37. *Suppose that the following gadgets can be built using complex-valued signatures from a finite generator set $\mathcal{G}$ and a finite recognizer set $\mathcal{R}$.*

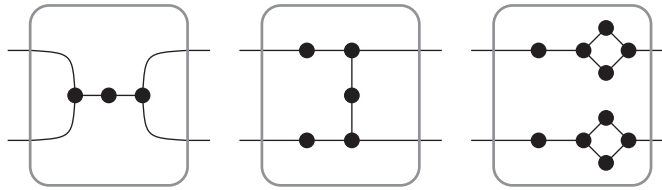
1. *A nonsingular binary recursive gadget M with infinite projective order*
2. *A binary starter gadget s where* $\det([s\ Ms\ M^2 s]) \ne 0$
3. *Three binary finisher gadgets with rank 2 transition matrices $F_1, F_2, F_3 \in \mathbb{C}^{3\times 3}$, for which* $\ker(F_1)$, $\ker(F_2)$, *and* $\ker(F_3)$ *are linearly independent*

Then for any $x, y \in \mathbb{C}$, $\text{Holant}(\mathcal{R} \cup \{[x, 0, y]\} \mid \mathcal{G}) \le_{\text{T}}^{\text{P}} \text{Holant}(\mathcal{R} \mid \mathcal{G})$. *This reduction does not use Lemma 3.13.*

Proof. By Lemma 5.35 we know that s is not orthogonal to any row eigenvector of M, so $\{M^j s\}_{j\ge 0}$ is a sequence of pairwise linearly independent vectors by Lemma 5.34. We will efficiently find a subsequence of pairwise linearly independent recognizers from the sequence

$$\{F_1 M^j s, F_2 M^j s, F_3 M^j s \mid j \ge 0\}.$$

https://doi.org/10.1017/9781107477063.006 Published online by Cambridge University Press



(a) Gadget M_{11} (b) Gadget M_5 (c) Gadget M_{12}

Figure 5.11. Gadgets for constructing finisher gadgets.

By design both sets of dangling edges of each finisher gadget are internally incident to recognizers, making this a list of recognizer signatures of the form $[*, 0, *]$. We can greedily pick a large subset of pairwise linear independent recognizers from the above list in polynomial time. Start with the empty subset, we test each successive signature for pairwise linear independence with all previously chosen signatures, and append it to our subsequence if it passes the test. Note that a signature is eliminated in this process iff it is a multiple of a previously chosen signature. By Lemma 5.36, we will have collected the first n signatures in this process by considering only $0 \leq j \leq n^3$ among the list. Indeed if at the end of this process we end up having collected fewer than n pairwise linearly independent recognizers, then for all $0 \leq j \leq n^3$, every F_1M^js, F_2M^js and F_3M^js is a multiple of some chosen signature. But then some two distinct members of the set S of size $|S| \geq n$ guaranteed by Lemma 5.36 must be independently dependent, a contradiction. Then by Lemma 5.18, for any $x, y \in \mathbb{C}$ we can efficiently simulate recognizer $[x, 0, y]$. □

Now we explicitly construct some finisher gadgets.

Lemma 5.38. *Suppose $X \neq 1$ and $a^3 \neq b^3$. Then in the context of* $\mathrm{Hol}_3(a, b)$ *there exist three binary finisher gadgets with rank 2 transition matrices $F_1, F_2, F_3 \in \mathbb{C}^{3\times 3}$, for which* $\ker(F_1)$, $\ker(F_2)$, *and* $\ker(F_3)$ *are linearly independent.*

Proof. We start first with the case where $ab \neq 0$. Using the simplest possible choice for a finisher gadget M_{11} (Figure 5.11), we get

$$M_{11} = \begin{bmatrix} a & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & b \end{bmatrix}.$$

We calculate that

$$M_5 = \begin{bmatrix} a^3 & 2a & b \\ a^2 & ab+1 & b^2 \\ a & 2b & b^3 \end{bmatrix}.$$

https://doi.org/10.1017/9781107477063.006 Published online by Cambridge University Press

We build two more finisher gadgets F' and F'' using gadgets M_{11} and M_5 so that $F' = M_{11}M_5$ and $F'' = M_{11}M_5^2$. Since M_{11} has rank 2 and M_5 is nonsingular (note $\det(M_5) = ab(ab-1)^3$), it follows that F' and F'' also have rank 2. Now to show that the kernels of M_{11}, F' and F'' are linearly independent, we check that the cross products of the first and last row vectors of M_{11}, F', and F'' (denoted respectively by v, v', and v'') are linearly independent. Note that M_{11} has an identically 0 middle row, so the cross product of the first row and the third row spans the kernel $\{x \in \mathbb{C}^3 \mid M_{11}x = 0\}$. The same is true for F' and F''. The cross products of the first and last row vectors of M_{11}, F', and F'' are respectively, $[0, 1-ab, 0]$, $(ab-1)^2[2b^2, -ab(ab+1), 2a^2]$, and

$$(ab-1)^3[2b(a^2b^3+a^2+ab^2+b^4),$$
$$-ab(a^3b^3+2a^3+2a^2b^2+ab+2b^3), 2a(a^4+a^3b^2+a^2b+b^2)].$$

As $ab \neq 1$, to see that these three vectors are linearly independent, it suffices to verify that the 2×2 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 $a \neq 0$, $b \neq 0$, we just need to 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 kernels of M_{11}, F', and F'' are linearly independent 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 $b = 0$.

$$M_{12} = \begin{bmatrix} a^6+2a^3+1 & 2a^4+2a & a^2 \\ a^5+a^2 & 2a^3+1 & a \\ a^4 & 2a^2 & 1 \end{bmatrix}.$$

Composing M_{11} with M_{12}, we get a finisher gadget with matrix $M_{11}M_{12}$, which has rank 2 since M_{11} has rank 2 and $\det(M_{12}) = 1$. It is also straightforward to see that $F' = M_{11}M_5$ has rank 2, as

$$F' = \begin{bmatrix} a^4+a & 2a^2 & 0 \\ 0 & 0 & 0 \\ a^3 & 2a & 0 \end{bmatrix}$$

using $b = 0$. The cross products of the first and last rows of M_{11}, F', and $M_{11}M_{12}$ are $[0, 1, 0]$, $[0, 0, 2a^2]$, and $[-2a, 2a^3+1, -2a^2(1+a)(a^2-a+1)]$

https://doi.org/10.1017/9781107477063.006 Published online by Cambridge University Press

respectively. Then the matrix of cross products is clearly nonsingular, and we conclude that for any $a, b \in \mathbb{C}$, we have three finisher gadgets satisfying our requirement. □

Corollary 5.39. *Let $a, b \in \mathbb{C}$ such that $X \neq 1$ and $a^3 \neq b^3$. Suppose that in the context of $\mathrm{Hol}_3(a, b)$, there exists a nonsingular binary recursive gadget M with infinite projective order and a binary starter gadget s where $\det([s\, Ms\, M^2 s]) \neq 0$. Then $\mathrm{Hol}_3(a, b)$ is* #P-hard.

The same statement holds for $\mathrm{Holant}(=_3 | [a, 1, b], \Delta_0, \Delta_1)$*, and a #P-hardness reduction exists that does not use Lemma 3.13.*

Proof. Immediate from Lemmas 5.38, 5.37, and 5.32. □

Applying Interpolation with Anti-gadgets

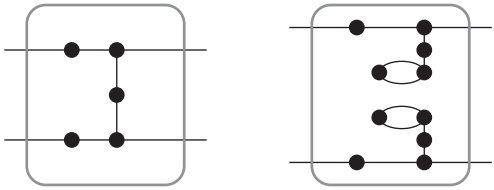
Now we will construct specific recursive gadgets to handle the special case of region III when X and Y are real valued: $(X, Y) \in \mathbb{R} \times \mathbb{R}$. We have $X \neq 1$, $Y^2 \neq 4X^3$ (equivalently $a^3 \neq b^3$) and $(X, Y) \neq (-1, 0)$. We will first set $X \neq 0, \pm 1$. There are two cases depending on whether $X + X^2 + Y = 0$. After that we consider $X = -1$ (but $Y \neq 0$) or $X = 0$ (but $Y \neq 0$).

We will introduce the idea of an *anti-gadget* in the next lemma. In a typical reduction from one problem to another in complexity theory, one often designs various gadgets. A reduction starts from an instance of the first problem and constructs an instance of the second problem that may contain a polynomial number of copies of the gadget. But the notion of containing a *negative* number of copies of a gadget seems meaningless. However, the *effect* of including an anti-gadget will indeed be the same as introducing a negative copy of a gadget in a reduction. More precisely, the effect of an anti-gadget, when expressed in algebraic terms, is the same as *erasing* the presence of some other gadget fragment. It is *as if* we managed to include a negative copy of a certain gadget.

We will see that anti-gadget greatly simplifies our work in finding a recursive gadget with infinite projective order. Effectively, we can use one gadget to "cancel out" a portion of another gadget, leaving a "virtual gadget" with a diagonal signature matrix – ideal for our purposes, as it is straightforward to analyze.

Lemma 5.40. *Let $a, b \in \mathbb{C}$ such that $X, Y \in \mathbb{R}$, and assume that $X \notin \{0, 1, -1\}$, $a^3 \neq b^3$, and $X^2 + X + Y \neq 0$. Then $\mathrm{Hol}_3(a, b)$ is* #P-hard. *The same statement holds for* $\mathrm{Holant}(=_3 | [a, 1, b], \Delta_0, \Delta_1)$*, and a #P-hardness reduction exists that does not use Lemma 3.13.*

https://doi.org/10.1017/9781107477063.006 Published online by Cambridge University Press



(a) Gadget M_5 (b) Gadget M_{13}

Figure 5.12. An anti-gadget pair.

Proof. We begin this proof with binary recursive gadget

$$M_5 = \begin{bmatrix} a^3 & 2 & a & b \\ a^2 & ab+1 & & b^2 \\ a & 2b & & b^3 \end{bmatrix}.$$

as depicted in Figure 5.12. Taking determinant, we find $\det(M_5) = X(X-1)^3 \neq 0$. If we let s be the simplest possible binary starter gadget consisting of a single vertex (Figure 5.3(a), Gadget M_3), then $\det([s\ M_5 s\ M_5^2 s]) = -(a^3-b^3)(ab-1)^4 \neq 0$. If M_5 has infinite projective order, then all criteria for Corollary 5.39 are met, and $\mathrm{Hol}_3(a,b)$ is #P-hard.

Now suppose that M_5 has finite projective order, and we let $i \in \mathbb{Z}^+$ and nonzero $\lambda \in \mathbb{C}$ such that $M_5^i = \lambda I$. Then chaining $i-1$ copies of gadget M_5 together, we have an explicit construction for a gadget with signature $M_5^{i-1} = \lambda M_5^{-1}$.

The gadget M_{13} (see Figure 5.12) has a 4×4 signature matrix obtained as a tensor product of the 2×2 matrix of $M_1 = \begin{bmatrix} a(a^2+b) & a+b^2 \\ a^2+b & (a+b^2)b \end{bmatrix}$. Expressed for symmetric signatures, we have

$$M_{13} = \begin{bmatrix} a^2A^2 & 2aAB & B^2 \\ aA^2 & (ab+1)AB & bB^2 \\ A^2 & 2bAB & b^2B^2 \end{bmatrix},$$

where $A = a^2+b$ and $B = a+b^2$.

Then concatenating the gadget with signature M_5^{i-1} and a copy of M_{13}, we have

$$M = M_5^{i-1} M_{13} = \lambda \begin{bmatrix} \alpha & 0 & 0 \\ 0 & AB & 0 \\ 0 & 0 & \beta \end{bmatrix},$$

where $\alpha = \frac{A^2}{a} = \frac{(a^2+b)^2}{a}$ and $\beta = \frac{B^2}{b} = \frac{(a+b^2)^2}{b}$. Note that $AB = (a^2+b)(a+b^2) = X^2+X+Y \neq 0$ and $X \neq 0$ by assumption. It follows that

https://doi.org/10.1017/9781107477063.006 Published online by Cambridge University Press

$\det(M) = \lambda^3\alpha\beta AB = \lambda^3(AB)^3/X \neq 0$, so M is nonsingular. We prove that M has infinite projective order, by showing that some two eigenvalues among $\{\alpha, \beta, AB\}$ have distinct norm. Suppose $|\alpha| = |\beta|$, then $|\alpha\beta X| = |\alpha|^2|X| \neq |\alpha|^2$ since $X \in \mathbb{R}$ and $X \neq \pm 1$. But $|\alpha\beta X| = |AB|^2$ and so $|\alpha| \neq |AB|$. Finally, we check that $\det([s\ Ms\ M^2s]) = \lambda^3(a^3 - b^3)(X-1)^3(X^2 + X + Y) \neq 0$, where $s = [a\ 1\ b]^{\mathrm{T}}$. Hence we apply Corollary 5.39 again and conclude that $\mathrm{Hol}_3(a, b)$ is #P-hard. □

The following test is a straightforward way to verify that a matrix has infinite projective order, by looking at the characteristic polynomial.

Lemma 5.41. *If all roots of the complex polynomial $x^3 - Bx^2 + Cx - D$ have the same norm, then $C|C|^2 = \overline{B}|B|^2D$.*

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

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

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

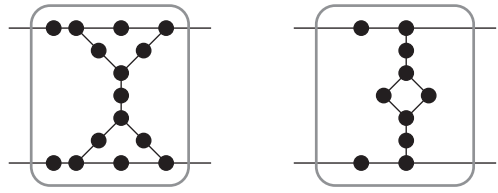
Lemma 5.42. *Suppose $X, Y \in \mathbb{R}$, $X^2 + X + Y = 0$, $a^3 \neq b^3$, and $X \notin \{0, 1, -1\}$. Then $\mathrm{Hol}_3(a, b)$ is* #P-hard. *The same statement holds for* Holant$(=_3 |\ [a, 1, b], \Delta_0, \Delta_1)$*, and a #P-hardness reduction exists that does not use Lemma 3.13.*

Proof. We first verify that $\det(M_5) = X(X-1)^3 \neq 0$. Next we show that M_5 has infinite projective order. The characteristic polynomial of M_5 is $x^3 - Bx^2 + Cx - D$, where $B = X + Y + 1 = 1 - X^2, C = (X-1)(X^2 + X + Y) = 0$, and $D = X(X-1)^3$. Thus $B, C, D \in \mathbb{R}$ and by Lemma 5.41 it is sufficient to observe $C^3 - B^3D = X(X-1)^6(X+1)^3 \neq 0$. We also have $\det([s\ M_5s\ M_5^2s]) = -(a^3 - b^3)(ab - 1)^4 \neq 0$ as required by Corollary 5.39, where s is the single-vertex starter gadget. □

We are left with two cases: $X = -1$ (but $Y \neq 0$) or $X = 0$ (but $Y \neq 0$).

Lemma 5.43. *Suppose $X = -1$, $a^3 \neq b^3$, and $Y \in \mathbb{R}$ but $Y \neq 0$. Then $\mathrm{Hol}_3(a, b)$ is* #P-hard. *The same statement holds for* Holant$(=_3 |\ [a, 1, b], \Delta_0, \Delta_1)$*, and a #P-hardness reduction exists that does not use Lemma 3.13.*

https://doi.org/10.1017/9781107477063.006 Published online by Cambridge University Press



(a) Gadget M_{14} (b) Gadget M_{15}

Figure 5.13. Binary recursive gadgets.

Proof. As before, $\det(M_5) = X(X-1)^3 \neq 0$. Looking at the characteristic polynomial $x^3 - Bx^2 + Cx - D$ of M_5, we have $C^3 - B^3D = -16Y^3 \neq 0$, so by Lemma 5.41 there are eigenvalues for which the ratio is not a root of unity and the matrix has infinite projective order. Once again, $\det([s\ M_5 s\ M_5^2 s]) = -(a^3 - b^3)(ab-1)^4 \neq 0$, where s is the single-vertex starter gadget, and by Corollary 5.39 we are done. □

Lemma 5.44. *Suppose* $X = 0$ *and* $Y \in \mathbb{R}$ *but* $Y \neq 0$. *Then* $\mathrm{Hol}_3(a, b)$ *is* #P-hard. *The same statement holds for* $\mathrm{Holant}(=_3 | [a, 1, b], \Delta_0, \Delta_1)$, *and a #P-hardness reduction exists that does not use Lemma 3.13.*

Proof. Gadgets M_{14} and M_{15} are depicted in Figure 5.13. Let $M = M_{14}$. Under the condition $X = 0$, we have $\det(M) = Y^3 \neq 0$, and also

$$C^3 - B^3D = 2Y^6(3L^2 + 1) \neq 0,$$

where we let $L = Y^2 + 6Y + 8$ and the characteristic polynomial of M is $x^3 - Bx^2 + Cx - D$. Also, $\det([s\ Ms\ M^2 s]) = 2Y^2(a^3 - b^3)(Y+3)$, where s is the single-vertex starter gadget, so by Corollary 5.39 we are done unless $Y = -3$ (note $a^3 \neq b^3$ because either a or b is 0, but not both).

For $X = 0$ and $Y = -3$ we let $M = M_{15}$ and then we have $\det(M) = 6 \neq 0$, $C^3 - B^3D = 21 \neq 0$, and

$$\det([s\ Ms\ M^2 s]) = -(X-1)^6(X+1)(a^3 - b^3)(Y+2) \neq 0. \qquad \square$$

Finally we are ready to prove the main theorem of Section 5.1: Theorem 5.1 for the case $k = 3$.

Proof of Theorem 5.1 Restricted to $k = 3$

Proof. Tractability (for region I and for region II on planar inputs) is given by Theorem 5.6. Intractability is given by Lemma 5.14 for region II. For region III, where X and Y are not both real valued, we have Corollary 5.33. For region III, where X and Y are both real, we appeal to Lemmas 5.44, 5.43, 5.42, and 5.40 as follows. For $X = 0$ we have Lemma 5.44; for $X = -1$ we have

https://doi.org/10.1017/9781107477063.006 Published online by Cambridge University Press

Lemma 5.43. For the remaining cases we have Lemma 5.40 if $X^2 + X + Y \neq 0$, and Lemma 5.42 if $X^2 + X + Y = 0$. □

5.2 4-Regular Graphs

5.2.1 Tractability in Regions I and II

Recall that for 4-regular graphs, region I is specified by $X = 1$ or $(X, Y) \in \{(0, 0), (-1, 0), (-1, \pm 2)\}$. Region II is specified by $Y^2 = 4X^4$ but $X \notin \{0, \pm 1\}$. The union of regions I and II is specified by $X = 1$ or $Y^2 = 4X^4$ or $(X, Y) = (-1, 0)$.

We will show that X and Y capture the complexity of $\text{Hol}_4(a, b)$, just as we did for $\text{Hol}_3(a, b)$. This will be slightly more involved, since in the case of $\text{Hol}_4(a, b)$ it is not true that the Holant is an integer polynomial in X and Y; there can be an extra factor $a^2 + b^2$. This factor appears precisely when the number of vertices in the graph is odd (which can never happen in a 3-regular graph). We start with a version of Lemma 5.4 adapted to any k.

Lemma 5.45. *Let G be a k-regular graph with n vertices. Then there exists a polynomial $P_G(\cdot, \cdot)$ with two variables and integer coefficients such that, for any signature grid Ω having underlying graph G, $Z(G) = P_G(ab, a^3 + b^3)$ (if n is even) and $Z(G) = (a^{k/2} + b^{k/2})P(ab, a^k + b^k)$ (if n is odd), for any edge function $[a, 1, b]$.*

Proof. In the edge–vertex bipartite view, the partition function $Z(G)$ is the value Holant_Ω in the Holant problem $\text{Holant}(=_k | [a, 1, b])$. First note that if k and n are both odd then no k-regular graph exists on n vertices, as kn is twice the number of edges, 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

https://doi.org/10.1017/9781107477063.006 Published online by Cambridge University Press

$\ell \geq 0$, 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 $P_G(ab, a^k + b^k)$ 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 5.46. *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* $\text{Holant}_\Omega = 0$.

Corollary 5.47. *Let $a', b' \in \mathbb{C}$ such that $a'b' = X$ and $(a')^k + (b')^k = Y$. Then $\text{Hol}_k(a, b)$ is polynomial time computable (respectively, is* #P-hard*) if and only if $\text{Hol}_k(a', b')$ is polynomial time computable (is* #P-hard*).*

Proof. Consider an input instance Ω for $\text{Hol}_k(a, b)$. If n is even then the claim is obvious. Suppose there are an odd number of vertices, and let Ω' be a copy of Ω with an additional vertex having $k/2$ self-loops. Then

$$\text{Holant}_{\Omega'} = (a^{k/2} + b^{k/2})\text{Holant}_\Omega. \tag{5.1}$$

If $a^{k/2} + b^{k/2} \neq 0$ we can easily obtain Holant_Ω from $\text{Holant}_{\Omega'}$ and vice versa. If $a^{k/2} + b^{k/2} = 0$ then both $\text{Holant}_\Omega = 0$ (by Corollary 5.46) and $\text{Holant}_{\Omega'} = 0$ (by (5.1). Thus the complexity of $\text{Hol}_k(a, b)$ is captured by input instances with an even number of vertices, for which the Holant can be expressed as a function of X and Y. □

Now we specialize to $k = 4$. We first list the tractable cases of $\text{Hol}_4(a, b)$.

Theorem 5.48. *For any $a, b \in \mathbb{C}$, $\text{Hol}_4(a, b)$ is solvable in polynomial time if any of the following four conditions are true.*

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

https://doi.org/10.1017/9781107477063.006 Published online by Cambridge University Press

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 $T = \begin{bmatrix} 1 & 0 \\ 0 & a^{-1} \end{bmatrix}$, we get $(T^{-1})^{\otimes 2} g = [a, a, -a]^{\mathrm{T}}$ and $(=_4)T^{\otimes 4} = [1, 0, 0, 0, a^{-4}]$, where $g = [a, 1, -a^{-1}]^{\mathrm{T}}$ (note that the form of 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 Holant$(=_4 \mid g)$ is equivalent in complexity to Holant$([1, 0, 0, 0, a^{-4}] \mid [1, 1, -1])$, and the problem Holant$(\{[1, 0, 0, 0, a^{-4}], [1, 1, -1]\})$ is tractable if $a^4 \in \{1, -1, \mathrm{i}, -\mathrm{i}\}$, by families $\mathscr{F}_1$ and $\mathscr{F}_3$ in Chapter 3. It is easy to see that $a^4 = \pm 1$ or $\pm \mathrm{i}$ is equivalent to $Y = a^4 + (-a^{-1})^4 = a^4 + a^{-4}$ is equal to ± 2 or 0. Finally, if $Y^2 = 4X^4$, then $a^4 = b^4$ and holographic algorithms using matchgates can be applied when the input graph is planar (see Chapter 4 and the proof of Theorem 5.6). □

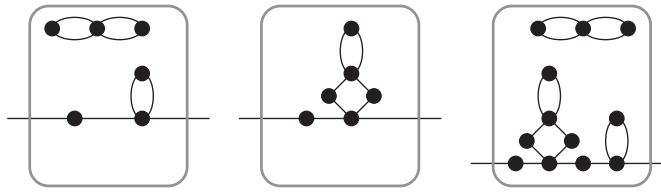
We note that the first three tractable cases also hold for Holant$(=_4 \mid [a, 1, b], \Delta_0, \Delta_1)$, and diagonal holographic transformations do not change $\{\Delta_0, \Delta_1\}$ up to a nonzero constant.

5.2.2 Hardness in Region III

Recall that for 4-regular graphs, region III is the complement of the union of regions I and II, which is specified by $X \neq 1$ and $Y^2 \neq 4X^4$ (equivalently $a^4 \neq b^4$) and $(X, Y) \neq (-1, 0)$. To prove #P-hardness in region III, we must use planar gadgets, and reduce from a problem that is #P-hard for planar graphs.

For $\mathrm{Hol}_3(a, b)$, we were able to make use of constructions consisting of a unary starter gadget together with iterations of a unary recursive gadget. However, in the context of $\mathrm{Hol}_4(a, b)$ the signature of any $\mathcal{F}$-gate has an even arity. This can be seen by adding up mod 2 all arities of signatures in the $\mathcal{F}$-gate, and noting that every internal edge is counted twice in this sum. So we cannot construct unary starter gadgets. However, we would still like to make use of some nice unary recursive gadgets, such as those we will see in Lemma 5.49. One alternative is to leave off the unary starter gadget, and consider the iterated unary recursive gadgets, which have two dangling edges, as constructions of binary signatures. However, these signatures, like unary recursive gadgets, have one dangling edge e internally incident to a generator and one dangling edge e' internally incident to a recognizer, and are not symmetric. To get around this difficulty, we introduce some gadgets for the sole purpose of transforming the construction into a sequence of *symmetric* binary signatures. Symmetry of the signatures constructed will be guaranteed by the symmetry in the underlying graph fragment ($\mathcal{F}$-gate).

https://doi.org/10.1017/9781107477063.006 Published online by Cambridge University Press



(a) Gadget M_{16} (b) Gadget M_{17} (c) Gadget M_{18}

Figure 5.14. A gadget syzygy.

In the next lemma we introduce a new idea of gadget construction – *syzygy* – a trio of gadgets that work in concert, and their alignment produces their success.

Lemma 5.49. *Suppose either $X \notin \mathbb{R}$, or both $Y \notin \mathbb{R}$ and $X \neq 0, 1$. Then in the context of $\mathrm{Hol}_4(a, b)$, there exists a unary recursive gadget M and a gadget A such that $\{M^j A\}_{j\geq 0}$ is a sequence of pairwise linearly independent symmetric binary generator signatures.*

Proof. The gadgets M_{16}, M_{17}, and M_{18} are depicted in Figure 5.14. The matrices for these gadgets are as follows.

$$M_{16} = \begin{bmatrix} a^4 + a^2b^2 & a^2b + b^3 \\ a^3 + ab^2 & a^2b^2 + b^4 \end{bmatrix}, \qquad M_{17} = \begin{bmatrix} a^4 + ab & a + b^3 \\ a^3 + b & ab + b^4 \end{bmatrix},$$

$$M_{18} = \begin{bmatrix} a^8 + a^6b^2 + a^5b + a^4 + 2a^3b^3 + a^2b^2 + ab^5 & a^6b + a^4b^3 + 2a^3b^2 + a^2b^5 + 2ab^4 + b^7 \\ a^7 + 2a^4b + a^5b^2 + 2a^2b^3 + a^3b^4 + ab^6 & a^5b + a^2b^2 + 2a^3b^3 + b^4 + ab^5 + a^2b^6 + b^8 \end{bmatrix}.$$

We begin by calculating the trace and determinant of each gadget in the trio of gadgets M_{16}, M_{17}, and M_{18}:

$$\begin{aligned} \mathrm{tr}(M_{16}) &= 2X^2 + Y \\ \mathrm{tr}(M_{17}) &= 2X + Y \\ \mathrm{tr}(M_{18}) &= (2X^2 + Y)(-X^2 + 2X + Y + 1) \\ \det(M_{16}) &= X(X-1)(2X^2 + Y) \\ \det(M_{17}) &= (X-1)(X^3 + X + Y) \\ \det(M_{18}) &= X(X-1)^2(X^3 + X + Y)(2X^2 + Y). \end{aligned}$$

We note that $M_{18} = M_{17}M_{16}$.

https://doi.org/10.1017/9781107477063.006 Published online by Cambridge University Press

We will show that if any one of these traces or determinants is 0, then another one of the three gadgets has nonzero eigenvalues of distinct norms. Since $X \neq 0, 1$ in any case, the only possibilities for any of these traces or determinants to be 0 are

$$2X^2 + Y = 0, \quad \text{or} \quad 2X + Y = 0, \quad \text{or} \quad X^3 + X + Y = 0,$$
$$\text{or} \quad -X^2 + 2X + Y + 1 = 0.$$

First we note that if any of these four equations is satisfied, then $X \notin \mathbb{R}$, for either it is by direct hypothesis of the lemma, or it is by $Y \notin \mathbb{R}$ and then by the equation.

Now we consider the four equations. If $2X^2 + Y = 0$ then $\operatorname{tr}(M_{17}) = -2X(X-1) \neq 0$, $\det(M_{17}) = X(X-1)^3 \neq 0$, and the ratio $\frac{\operatorname{tr}^2(M_{17})}{\det(M_{17})} = \frac{4X}{X-1} \notin \mathbb{R}^+$. If $2X + Y = 0$ then $\operatorname{tr}(M_{18}) = -2X(X-1)^2(X+1) \neq 0$, $\det(M_{18}) = 2X^3(X-1)^4(X+1) \neq 0$, and the ratio $\frac{\operatorname{tr}^2(M_{18})}{\det(M_{18})} = \frac{2(X+1)}{X} \notin \mathbb{R}^+$. If $X^3 + X + Y = 0$ then $\operatorname{tr}(M_{16}) = -X(X-1)^2 \neq 0$, $\det(M_{16}) = -X^2(X-1)^3 \neq 0$, and the ratio $\frac{\operatorname{tr}^2(M_{16})}{\det(M_{16})} = -X + 1 \notin \mathbb{R}^+$. Finally, suppose $-X^2 + 2X + Y + 1 = 0$. Then $\operatorname{tr}(M_{16}) = (X-1)(3X+1) \neq 0$, $\det(M_{16}) = X(X-1)^2(3X+1) \neq 0$, and the ratio $\frac{\operatorname{tr}^2(M_{16})}{\det(M_{16})} = \frac{3X+1}{X} \notin \mathbb{R}^+$. In each case, by Lemma 5.19 one of the gadgets M_{16}, M_{17}, or M_{18} has nonzero eigenvalues of distinct norm.

Now suppose each trace and determinant is nonzero, and suppose all three gadgets fail to have eigenvalues with distinct norm. Then Lemma 5.19 implies that $\frac{\operatorname{tr}^2(M_i)}{\det(M_i)} \in \mathbb{R}^+$ for each M_i. In particular, we claim that in this case $X \neq -1$. Otherwise, by hypothesis $Y \notin \mathbb{R}$ since $X = -1 \in \mathbb{R}$, and yet $\operatorname{tr}(M_{16}) = Y + 2$, $\det(M_{16}) = 2(Y+2)$, and $\frac{\operatorname{tr}^2(M_{16})}{\det(M_{16})} = (Y+2)/2 \in \mathbb{R}^+$; this is a contradiction.

We write $\frac{\operatorname{tr}^2(M_{18})\det(M_{16})\det(M_{17})}{\det(M_{18})\operatorname{tr}^2(M_{16})\operatorname{tr}^2(M_{17})} = \frac{\left(-X^2+2X+Y+1\right)^2}{(2X+Y)^2} = \left(1 - \frac{(X-1)(X+1)}{2X+Y}\right)^2$. The cancelation and its factorization as a square all follow from the fact that $\det(M_{18}) = \det(M_{16})\det(M_{17})$. Hence $\frac{(X-1)(X+1)}{2X+Y}$ is real valued. Furthermore, $\frac{(X-1)(X+1)}{2X+Y}$ is nonzero since $X \neq 1$ in either case of the hypothesis and $X \neq -1$ by the proof above. Thus $\frac{2X+Y}{(X-1)(X+1)}$ is well defined and real-valued. We also know that $\frac{2X^2+Y}{X(X-1)} = \frac{\operatorname{tr}^2(M_{16})}{\det(M_{16})} \in \mathbb{R}^+$, so there exist r and $s \in \mathbb{R}$ (both nonzero) such that

$$Y = r(X-1)(X+1) - 2X, \tag{5.2}$$
$$Y = sX(X-1) - 2X^2.$$

Setting these two expressions of Y equal to each other and refactoring, we get

$$(X-1)(r - (s-2-r)X) = 0;$$

https://doi.org/10.1017/9781107477063.006 Published online by Cambridge University Press

therefore $r = (s - 2 - r)X$, but since $r \neq 0$, we get $X \in \mathbb{R}$, and by (5.2), we also get $Y \in \mathbb{R}$. This contradiction establishes that one of the gadgets – M_{16}, M_{17}, or M_{18} – has nonzero eigenvalues of distinct norms. By Lemma 5.11, the powers of one of M_{16}, M_{17}, or M_{18} are pairwise linearly independent. Equivalently, it has infinite projective order by Lemma 5.10.

Now we show that in each case, for the chosen unary recursive gadget M, there exists a gadget A such that M^jA are signature matrices of symmetric binary generator signatures, for all nonnegative integer j. We take g to be a gadget consisting of a single generator vertex with matrix

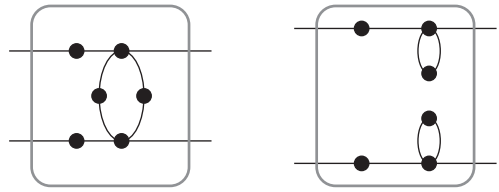
$$g = \begin{bmatrix} a & 1 \\ 1 & b \end{bmatrix}.$$

If $M = M_{16}$ or $M = M_{17}$, then by the symmetry in the gadget design each function M^jg is a symmetric binary generator signature. Hence we take $A = g$ in these cases. For gadget M_{18}, we set $A = M_{17}g$, and again we get the desired graph symmetry. We know g is nonsingular, as $X \neq 1$. For any case where we need to apply M_{18}, we also have M_{18} is nonsingular. (This includes the case when $2X + Y = 0$, where we explicitly verified that $\det(M_{18}) \neq 0$, and when we supposed all three traces and determinants are nonzero.) However, $M_{18} = M_{17}M_{16}$, so it follows that $M_{17}g$ is also nonsingular in such a case. In any case, applying the nonsingular linear transformation defined by A: $M^j \mapsto M^jA$, does not change the fact that we have a sequence of pairwise linearly independent signatures, and these are symmetric binary generators by design. □

In the next three lemmas we will do the same thing as in Lemma 5.49 to produce a sequence of pairwise linearly independent symmetric binary generator signatures, in the case $X \in \mathbb{R}$. Note that we will avoid tractable cases; thus we will exclude the case $X = 1$ or $(X, Y) = (0, 0)$, $(-1, 0)$ or $(-1, \pm 2)$. In Lemmas 5.50 and 5.51, the generators will be constructed using the technique of a binary recursive gadget and a starter gadget, rather than a unary recursive gadget that is symmetrized as in Lemma 5.49. Thus these generator signatures will be expressed as column vectors in $\mathbb{C}^3$ rather than the matrix form in $\mathbb{C}^{2\times 2}$ as in Lemma 5.49. However, in terms of their functionality as generator signatures there is no difference.

Lemma 5.50. *Suppose $X \in \mathbb{R} - \{-1, 0, 1\}$ and $a^4 \neq b^4$. Then there is a nonsingular binary recursive gadget $M \in \mathbb{C}^{3\times 3}$ and a starter gadget $s \in \mathbb{C}^3$ for which $\{M^js\}_{j\geq 0}$ is a sequence of pairwise linearly independent symmetric binary generator signatures.*

https://doi.org/10.1017/9781107477063.006 Published online by Cambridge University Press



(a) Gadget M_{19} (b) Gadget M_{20}

Figure 5.15. Binary recursive gadgets.

Proof. The gadgets M_{19} and M_{20} are depicted in Figure 5.15.

$$M_{19} = \begin{bmatrix} a^4 & 2a & b^2 \\ a^3 & 1+ab & b^3 \\ a^2 & 2b & b^4 \end{bmatrix}$$

$$M_{20} = \begin{bmatrix} a^4 & 2a^2b & b^2 \\ a^3 & ab+a^2b^2 & b^3 \\ a^2 & 2ab^2 & b^4 \end{bmatrix}.$$

We calculate $\det(M_{19}) = X^2(X-1)^3 \neq 0$ and

$$\det([s\ M_{19}s\ M_{19}^2 s]) = -(a^4 - b^4)(X+1)(X-1)^4 \neq 0,$$

where s is the single vertex starter gadget. If gadget M_{19} also has infinite projective order then by Lemmas 5.35 and 5.34 we are done, so assume otherwise. Then for some integer $i \geq 0$ and nonzero $\lambda \in \mathbb{C}$ we have $M_{19}^i = \lambda M_{19}^{-1}$, and we construct the gadget

$$M = M_{19}^i M_{20} = \lambda M_{19}^{-1} M_{20} = \lambda \begin{bmatrix} 1 & 0 & 0 \\ 0 & X & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

This is really an application of the idea of an anti-gadget. Then $M^j s = \lambda^j \operatorname{diag}(1, X^j, 1)[a\ 1\ b]^{\mathrm{T}} = \lambda^j [a\ X^j\ b]^{\mathrm{T}}$. Since $X \in \mathbb{R} - \{-1, 0, 1\}$, we have that $\{M^j s\}_{j\geq 0}$ is a sequence of pairwise linearly independent symmetric binary generator signatures. □

Lemma 5.51. *Suppose $X = -1$ and $Y \in \mathbb{R} - \{-2, 0, 2\}$. Then there is a nonsingular binary recursive gadget $M \in \mathbb{C}^{3\times 3}$ and starter gadget $s \in \mathbb{C}^3$ for which $\{M^j s\}_{j\geq 0}$ is a sequence of pairwise linearly independent symmetric binary generator signatures.*

https://doi.org/10.1017/9781107477063.006 Published online by Cambridge University Press

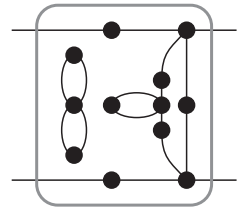


Figure 5.16. A binary recursive gadget.

Proof. The gadget M_{21} is depicted in Figure 5.16.

$$M_{21} = \begin{bmatrix} a^8 + a^5b + a^6b^2 + a^3b^3 & 2a^5 + 4a^3b^2 + 2ab^4 & a^3b + ab^3 + a^2b^4 + b^6 \\ a^7 + a^4b + a^5b^2 + a^2b^3 & a^4 + a^5b + 2a^2b^2 + 2a^3b^3 + b^4 + ab^5 & a^3b^2 + ab^4 + a^2b^5 + b^7 \\ a^6 + a^3b + a^4b^2 + ab^3 & 2a^4b + 4a^2b^3 + 2b^5 & a^3b^3 + ab^5 + a^2b^6 + b^8 \end{bmatrix}.$$

If $X = -1$, then the characteristic polynomial of gadget M_{21} is

$$x^3 - (Y+2)(Y-2)x^2 - 2(Y+2)^2(Y-2)x - 8(Y+2)^2(Y-2),$$

so the determinant is nonzero. By Lemma 5.41, if all roots of the characteristic polynomial have the same norm, then $C^3 = B^3D$ and this amounts to $(Y+2)^2 = -(Y+2)(Y-2)$, but then $Y(Y+2) = 0$, which is not true. Finally, applying Lemma 5.35 to M_{21} and the single-vertex starter gadget s, we get $\det([s\, M_{21}s\, M_{21}^2 s]) = 16Y^2(a^4 - b^4)(Y+2) \neq 0$. □

Lemma 5.52. *Suppose $X = 0$ and $Y \in \mathbb{C} - \{0\}$. Then there exists a unary recursive gadget M and gadgets A and B such that $\{AM^jB\}_{j\geq 0}$ is a sequence of pairwise linearly independent symmetric binary generator signatures.*

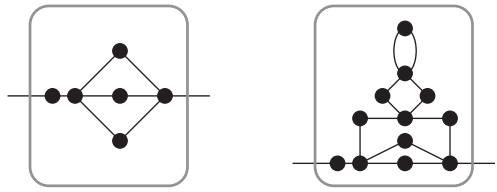
Proof. The gadgets M_{22} and M_{23} are depicted in Figure 5.17.

$$M_{22} = \begin{bmatrix} 1 + a^4 & a + b^3 \\ a^3 + b & 1 + b^4 \end{bmatrix}$$

$$M_{23} = \begin{bmatrix} 2a^4 + a^8 + 2ab + a^5b + a^3b^3 + b^4 & a^5 + 2a^2b + a^3b^2 + b^3 + 2ab^4 + b^7 \\ a^3 + a^7 + 2a^4b + 2ab^2 + a^2b^3 + b^5 & a^4 + 2ab + a^3b^3 + 2b^4 + ab^5 + b^8 \end{bmatrix}.$$

By $X = 0$ and $Y \neq 0$, without loss of generality we assume $a = 0$, and $b \neq 0$.

https://doi.org/10.1017/9781107477063.006 Published online by Cambridge University Press



(a) Gadget M_{22} (b) Gadget M_{23}

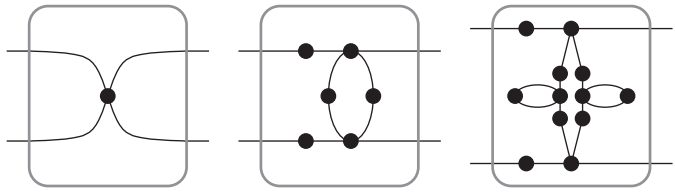
Figure 5.17. Unary recursive gadgets.

First we show the existence of a unary recursive gadget M that has infinite projective order. Under the condition $X = 0$, $\det(M_{22}) = 1$. If gadget M_{22} has infinite projective order then we define $M = M_{22}$ and we are already done. So suppose otherwise. Then for some integer $i \geq 0$ and nonzero $\lambda \in \mathbb{C}$ we have $M_{22}^i = \lambda M_{22}^{-1}$, and we consider the gadget $M = M_{22}^i M_{23} = \lambda M_{22}^{-1} M_{23} = \lambda b^4 \begin{bmatrix} 1 & b^{-1} \\ 0 & 1 \end{bmatrix}$, which is nonsingular. Then $M^j = \lambda^j b^{4j} \begin{bmatrix} 1 & jb^{-1} \\ 0 & 1 \end{bmatrix}$ for any positive integer j, so M has infinite projective order.

Now we show the existence of appropriate gadgets A and B to symmetrize the construction. If $M = M_{22}$, then we set A to be the identity matrix $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ (representing an empty gadget with no vertex and a single straight through edge) and B to be a single generator vertex with one leading edge to be merged with the trailing edge of the recursive gadget, and the other edge becoming a dangling edge. The induced graph symmetry implies that AM^jB is a symmetric binary generator. Furthermore, A and B are nonsingular. If $M = M_{22}^i M_{23}$, then we set A to M_{23} and B to a single generator vertex with one leading edge to be merged with the trailing edge of the recursive gadget, and the other edge becoming a dangling edge. Again, the induced graph symmetry implies that AM^jB is a symmetric binary generator. Furthermore, B is nonsingular, as $X \neq 1$, and A is nonsingular, since if we are using this M as our unary recursive gadget, then we already know that $M_{22}^i M_{23}$ is nonsingular and therefore M_{23} is nonsingular. In any case, the linear transformation $M^j \mapsto AM^jB$ preserves pairwise linear independence, and we have constructed a sequence of pairwise linearly indpendent symmetric binary generator signatures. □

Now we show the existence of a set of general-purpose finisher gadgets. In these finisher gadgets, all dangling edges are internally incident to vertices that are assigned a recognizer signature $(=_4)$. Furthermore, one set of two dangling edges is incident to the same $(=_4)$ vertex. Hence, we are aiming to interpolate recognizer signatures of the form $[*, 0, *]$. These finisher gadgets operate under

https://doi.org/10.1017/9781107477063.006 Published online by Cambridge University Press



(a) Gadget M_{24} (b) Gadget M_{19} (c) Gadget M_{25}

Figure 5.18. Gadgets for building finisher gadgets.

the assumption that the "incoming" gadget has a binary symmetric generator signature. Our finisher gadgets will be expressed as 3×3 matrices (of rank 2), since the incoming signatures are symmetric. The essential property is that for a trio of finisher gadgets, their one-dimensional kernels are linearly independent.

Lemma 5.53. *Let $a, b \in \mathbb{C}$ such that $ab \neq 1$, and $a^4 \neq b^4$. Then in the context of $\mathrm{Hol}_4(a, b)$, there exist three binary finisher gadgets with rank 2 matrices $F, F', F'' \in \mathbb{C}^{3\times 3}$, such that their middle rows are all 0, and the kernels of F, F', and F'' are linearly independent.*

Proof. The gadgets M_{24} and M_{25} are depicted in Figure 5.18.

$$M_{24} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$M_{25} = \begin{bmatrix} a^8 + 2a^5b + a^2b^2 & 2a^5 + 4a^3b^2 + 2ab^4 & a^2 + 2ab^3 + b^6 \\ a^7 + 2a^4b + ab^2 & a^4 + a^5b + 2a^2b^2 + 2a^3b^3 + b^4 + ab^5 & a^2b + 2ab^4 + b^7 \\ a^6 + 2a^3b + b^2 & 2a^4b + 4a^2b^3 + 2b^5 & a^2b^2 + 2ab^5 + b^8 \end{bmatrix}.$$

We will break this proof down into two cases: $X \neq 0$ and $X = 0$. For both cases, we will show the existence of three finisher gadgets for which the (one-dimensional) kernels are linearly independent. Every finisher gadget we utilize in this proof has the property that the middle row of the corresponding transition matrix contains only 0's; hence we can get a nonzero vector v that spans its kernel by calculating the cross product of the first and last rows (provided that the matrix has rank 2). Suppose F, F', and F'' are finisher gadgets and let v_1, v_2, and v_3 denote the respective cross products of the first and last rows of each transition matrix. Then we use $\mathrm{cross}(F, F', F'')$ to denote the matrix whose rows are v_1, v_2, and v_3 (in that order). We can test the linear independence of $\{v_1, v_2, v_3\}$ by verifying the determinant $\det(\mathrm{cross}(F, F', F'')) \neq 0$.

Suppose $X \neq 0$. Let $F = M_{24}$, $F' = M_{24}M_{19}$, $F'' = M_{24}M_{19}^2$. Since M_{24} has rank 2 and $\det(M_{19}) = X^2(X-1)^3 \neq 0$, it follows that F, F', and F'' all have

https://doi.org/10.1017/9781107477063.006 Published online by Cambridge University Press

rank 2. We calculate that $\det(\text{cross}(F, F', F'')) = 4X^2(a^4 - b^4)(X-1)^4 \neq 0$, so the kernels are linearly independent.

Suppose $X = 0$. Without loss of generality we have $a = 0$ and $b \neq 0$ since $a^4 \neq b^4$. Let $F = M_{24}$, $F' = M_{24}M_{25}$, $F'' = M_{24}M_{25}^2$. Then M_{24} has rank 2,

$$\det(M_{25}) = (ab-1)^3(a^3+b)^2(a^2+b^2)^2(a+b^3)^2, \text{ and}$$
$$\det(\text{cross}(F, F', F'')) = 4(ab-1)^4(a^2-b^2)(a^3+b)^2(a^2+b^2)^7 (a+b^3)^2(a^4+2ab+b^4).$$

Under the condition $a = 0$ these polynomials simplify to $-b^{12} \neq 0$ and $-4b^{28} \neq 0$. Therefore F, F', and F'' all have rank 2 and the kernels of F, F', and F'' are linearly independent. □

Corollary 5.54. *Let $a, b \in \mathbb{C}$ be parameters in region III; namely, (a, b) are such that $X \neq 1$, $Y^2 \neq 4X^4$ (equivalently $a^4 \neq b^4$), and $(X, Y) \neq (-1, 0)$. Then* $\text{Hol}_4(a, b)$ *is* #P-hard *even when restricted to planar inputs.*

The same statement holds for $\text{Holant}(=_4 | [a, 1, b], \Delta_0, \Delta_1)$*, and a #P-hardness reduction exists that does not use Lemma 3.13.*

Proof. We have produced a sequence of pairwise linearly independent symmetric binary generator signatures by the following lemmas: If $X \notin \mathbb{R}$, then we have Lemma 5.49 that uses the syzygy construction. Next we assume $X \in \mathbb{R}$ but $X \neq 1$. If further $X \notin \{0, -1\}$, then with $a^4 \neq b^4$, we can apply Lemma 5.50. Suppose $X = 0$, then for all $Y \in \mathbb{C} - \{0\}$, we have Lemma 5.52. Finally suppose $X = -1$. In this case if $Y \notin \mathbb{R}$, then we appeal to Lemma 5.49 again. If $X = -1$ and $Y \in \mathbb{R}$, then by the hypothesis of this corollary, $Y \in \mathbb{R} - \{-2, 0, 2\}$. Then we apply Lemma 5.51.

Now we apply Lemma 5.53 and Lemma 5.36 to the sequence of pairwise linearly independent symmetric binary generator signatures just produced, and obtain a sequence of pairwise linearly independent symmetric binary recognizer signatures of the form $\{[x_1, 0, y_1], \ldots, [x_m, 0, y_m]\}$.

Finally we apply Lemma 5.32. The conclusion of Corollary 5.54 follows. We observe that all reductions use only planar gadgets, and Lemma 5.30 is valid for planar inputs; thus the #P-hardness proved holds over planar instances of $\text{Hol}_4(a, b)$. □

5.2.3 Planar Tractable Region II Is #P-hard for General Graphs

Recall that region II is specified by $Y^2 = 4X^4$ (equivalently $a^4 = b^4$) but $X \notin \{0, \pm 1\}$.

https://doi.org/10.1017/9781107477063.006 Published online by Cambridge University Press

It will be convenient to transform the problem to a setting where generator signatures are of the form $[a, 1, a]$. This can be done with a holographic transformation, and we can also reuse some of our work, using the observation that a sequence of pairwise linearly independent signatures remains so after a holographic transformation.

Lemma 5.55. *Let f and f' be $\mathcal{F}$-gates of arity r, where each dangling edge is internally incident to a vertex labeled with a generator signature. Then the property that f and f' are linearly independent is invariant under holographic reductions.*

Proof. Let $T \in \mathbb{C}^{2\times 2}$ be the basis for a holographic reduction. View the signatures f and f' as column vectors in $\mathbb{C}^{2^r}$ in unsymmetric signature notation. After a holographic reduction under basis T, we get the signatures $\hat{f}$ and $\hat{f}'$, where $[\hat{f}\ \hat{f}'] = (T^{-1})^{\otimes r}[f\ f']$. Since T is invertible, the $2^r \times 2$ block matrix $[f\ f']$ has rank 2 if and only if the $2^r \times 2$ block matrix $[\hat{f}\ \hat{f}']$ has rank 2, i.e., f and f' are linearly independent if and only if $\hat{f}$ and $\hat{f}'$ are linearly independent. □

Lemma 5.56. *Suppose $a^4 = b^4$. Then there exists $c \in \mathbb{C}$ such that the problem* Holant$(=_4 \mid [a, 1, b])$ *is equivalent to the problem* Holant$([1, 0, 0, 0, e] \mid [c, 1, c])$ *under a diagonal holographic reduction, where $ab = c^2$ and $e = \pm 1$. Conversely, given a problem of the form* Holant$([1, 0, 0, 0, e] \mid [c, 1, c])$ *where $c \in \mathbb{C}$ and $e = \pm 1$, there is a diagonal holographic reduction to an equivalent problem* Holant$(=_4 \mid [a, 1, b])$ *for which $ab = c^2$.*

Proof. If $ab = 0$, then $a = b = 0$ by $a^4 = b^4$. In this case, the lemma is trivial. Suppose otherwise, then both $a \neq 0$ and $b \neq 0$.

Let ω be a 16th root of unity such that $a\omega^4 = b$. By the diagonal holographic transformation $T = \begin{bmatrix} \omega^{-1} & 0 \\ 0 & \omega \end{bmatrix}$, we have $(T^{-1})^{\otimes 2}[a, 1, b]^{\mathrm{T}} = [a\omega^2, 1, b\omega^{-2}]^{\mathrm{T}} = [a\omega^2, 1, a\omega^2]^{\mathrm{T}}$, and $[1, 0, 0, 0, 1]T^{\otimes 4} = [\omega^{-4}, 0, 0, 0, \omega^4]$, so $\mathrm{Hol}_4(a, b)$ is equivalent to Holant$([\omega^{-4}, 0, 0, 0, \omega^4] \mid [a\omega^2, 1, a\omega^2])$. Multiplying each entry of a signature by a nonzero value does not change the complexity of the problem, and $\omega^8 \in \{\pm 1\}$, so the problem is equivalent to Holant$([1, 0, 0, 0, \pm 1] \mid [a\omega^2, 1, a\omega^2])$.

Conversely, consider a problem of the form Holant$([1, 0, 0, 0, e] \mid [c, 1, c])$ where $c \in \mathbb{C}$ and $e = \pm 1$. If $e = 1$, then we are already done, so assume $e = -1$. Let $\omega = e^{\pi \mathrm{i}/8}$, and performing a holographic reduction by $T = \begin{bmatrix} \omega^{-1} & 0 \\ 0 & \omega \end{bmatrix}$, we arrive at Holant$([-\mathrm{i}, 0, 0, 0, -\mathrm{i}] \mid [\omega^2 c, 1, \omega^{-2} c])$, which is

https://doi.org/10.1017/9781107477063.006 Published online by Cambridge University Press

equivalent to Holant($=_4$| $[a, 1, b]$), where $a = \omega^2 c$, $b = \omega^{-2} c$, $ab = c^2$, and $a^4 = b^4$. □

We observed in Lemma 5.8 that if all signatures in $\mathcal{F}$ are complement-invariant, then any $\mathcal{F}$-gate that we build with them is also complement-invariant. Although we can't get the same conclusion in the setting of Holant($[1, 0, 0, 0, -1] \mid [a, 1, a]$), there is a similar structural property to observe.

Lemma 5.57. *Let $\mathcal{F} = \{[1, 0, 0, 0, -1], [a, 1, a]\}$. Then any $\mathcal{F}$-gate with an even number of degree-4 vertices has the property that its value remains unchanged under the complement of its inputs.*

Proof. Let $f \in \mathcal{F}$. If σ and σ' are complementary assignments to the edges of f, then their values satisfy $f\,|_\sigma = \pm f\,|_{\sigma'}$, where the sign is -1 if f is the function $[1, 0, 0, 0, -1]$, and the sign is $+1$ if $f = [a, 1, a]$. If σ and σ' are complementary assignments to the dangling edges of an $\mathcal{F}$-gate, by complementing the assignments to all internal edges, we have a 1-1 correspondence of all terms defining the signature sum of the $\mathcal{F}$-gate under σ with those under σ', and since the number of occurrences of $[1, 0, 0, 0, -1]$ is even, each pair of complementary assignments has the same value. □

The following lemma is practically identical to Lemma 5.50, except we carry out the proof in region II. Note we do the analysis with a 2×2 iteration matrix owing to the extra degree of symmetry we have in this setting.

Lemma 5.58. *Consider the problem* Holant($[1, 0, 0, 0, e] \mid [a, 1, a]$)*, where $a^2 \in \mathbb{R} - \{0, \pm 1\}$ and $e = \pm 1$. Then there exists a binary starter gadget s and a binary recursive gadget M such that $\{M^j s\}_{j \geq 0}$ is a sequence of pairwise linearly independent generator signatures of the form $\{[x_j, y_j, x_j]\}_{j \geq 0}$.*

Proof. In this proof, we will use M_{19}, M_{20}, and the single-vertex starter gadget s.

$$M_{19} = \begin{bmatrix} a^4 & 2ae & a^2 \\ a^3 & e + a^2 e & a^3 \\ a^2 & 2ae & a^4 \end{bmatrix}, \quad M_{20} = \begin{bmatrix} a^4 & 2a^3 e & a^2 \\ a^3 & a^2 e + a^4 e & a^3 \\ a^2 & 2a^3 e & a^4 \end{bmatrix}, \quad s = \begin{bmatrix} a \\ 1 \\ a \end{bmatrix}.$$

Let $C = \{[x\ y\ x]^{\mathrm{T}} : x, y \in \mathbb{C}\}$. Then $s \in C$ and C is closed under M_{19} and M_{20}. For this reason, all $\mathcal{F}$-gate signatures in this proof will be in C and we can restrict our attention to the first two entries of each signature. As such, we form

https://doi.org/10.1017/9781107477063.006 Published online by Cambridge University Press

s', M', and M'' as stand-ins for s, M_{19}, and M_{20} (respectively) as follows:

$$s' = \begin{bmatrix} a \\ 1 \end{bmatrix},$$

$$M' = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} a^4 & 2ae & a^2 \\ a^3 & e + a^2 e & a^3 \\ a^2 & 2ae & a^4 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} a^4 + a^2 & 2ae \\ 2a^3 & e + a^2 e \end{bmatrix},$$

$$M'' = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} a^4 & 2a^3 e & a^2 \\ a^3 & a^2 e + a^4 e & a^3 \\ a^2 & 2a^3 e & a^4 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} a^4 + a^2 & 2a^3 e \\ 2a^3 & a^2 e + a^4 e \end{bmatrix}.$$

Note that $M'' = M' \begin{bmatrix} 1 & 0 \\ 0 & a^2 \end{bmatrix}$. First, $\det([s\ M's]) = a(a^2 - 1)(a^2 + e) \neq 0$, so if M' has infinite projective order then we are done by Lemma 5.35 and Lemma 5.15. Now assume otherwise, and since $\det(M') = a^2 e(a^2 - 1)^2 \neq 0$ and M' has finite projective order, there is some integer $i \geq 0$ and nonzero $\lambda \in \mathbb{C}$ for which $M'^i = \lambda M'^{-1}$. Then we construct the gadget $M = M'^i M'' = \lambda M'^{-1} M'' = \lambda \begin{bmatrix} 1 & 0 \\ 0 & a^2 \end{bmatrix}$. Then $M^j s = \lambda^j \operatorname{diag}(1, a^{2j})[a\ 1]^{\mathrm{T}} = \lambda^j [a\ a^{2j}]^{\mathrm{T}}$; hence $\{M^j s\}_{j \geq 0}$ is a sequence of pairwise linearly independent vectors. □

Lemma 5.59. *Consider the problem* Holant([1, 0, 0, 0, e] | [c, 1, c])*, where* $c^2 \notin \mathbb{R}$ *and* $e = \pm 1$*. Then there exists a unary recursive gadget* M *and gadget* A *such that* $\{M^j A\}_{j \geq 0}$ *is a sequence of pairwise linearly independent generator signatures of the form* $\{[x_j, y_j, x_j]\}_{j \geq 0}$.

Proof. By Lemma 5.56 let $a, b \in \mathbb{C}$ such that Holant([1, 0, 0, 0, e] | [c, 1, c]) is equivalent to Holant($=_4$| [a, 1, b]) and $ab = c^2$. Then by Lemma 5.49, since $X = ab = c^2 \notin \mathbb{R}$, we have a recursive unary gadget M and gadget A such that $\{M^j A\}_{j \geq 0}$ is a sequence of pairwise linearly independent symmetric binary generator signatures (in the context of Holant($=_4$| [a, 1, b])). By Lemmas 5.55 and 5.56, this gadget construction also produces a sequence of pairwise linearly independent binary generator signatures in the context of Holant([1, 0, 0, 0, e] | [c, 1, c]). All of the gadgets from Lemma 5.49 have an even number of degree-4 vertices, so by Lemma 5.57 (and Lemma 5.8) the signatures of the $\mathcal{F}$-gates we constructed are invariant under the complement of their inputs. □

The following lemma proves the #P-hardness for $\mathrm{Hol}_4(a, b)$ in region II for general graphs.

https://doi.org/10.1017/9781107477063.006 Published online by Cambridge University Press

Lemma 5.60. *Let* $a, b \in \mathbb{C}$ *such that* $a^4 = b^4$ *and* $ab \notin \{-1, 0, 1\}$. *Then* $\mathrm{Hol}_4(a, b)$ *is* #P-hard. *The same statement holds for* $\mathrm{Holant}(=_4 | [a, 1, b], \Delta_0, \Delta_1)$, *and a #P-hardness reduction exists that does not use Lemma 3.13.*

Proof. By Lemma 5.56 there exists $c \in \mathbb{C}$ and $e = \pm 1$ such that $ab = c^2$ and $\mathrm{Hol}_4(a, b)$ is equivalent to $\mathrm{Holant}([1, 0, 0, 0, e] \mid [c, 1, c])$ by a diagonal holographic transformation. Then $c^2 = ab \notin \{0, \pm 1\}$ and by Lemmas 5.59 and 5.58 we have a sequence of pairwise linearly independent generator signatures of the form $\{[x_j, y_j, x_j]\}_{j \geq 0}$. By Lemma 5.13, we can interpolate generator signature $[1, 1, 1]$, which we use in the following chain of reductions.

$$\begin{aligned}
\mathrm{Hol}_3(ec, ec) &\leq^{\mathrm{P}}_{\mathrm{T}} \mathrm{Holant}([1, 0, 0, e] \mid [c, 1, c]) \\
&\leq^{\mathrm{P}}_{\mathrm{T}} \mathrm{Holant}([1, 0, 0, 0, e] \mid \{[c, 1, c], [1, 1, 1]\}) \\
&\leq^{\mathrm{P}}_{\mathrm{T}} \mathrm{Holant}([1, 0, 0, 0, e] \mid [c, 1, c]) \\
&\leq^{\mathrm{P}}_{\mathrm{T}} \mathrm{Holant}(=_4 | [a, 1, b]).
\end{aligned}$$

To justify this chain of reductions, observe that any instance of $\mathrm{Hol}_3(ec, ec) = \mathrm{Holant}(=_3 | [ec, 1, ec])$ must have an even number of recognizer vertices $=_3$. The first step follows from a diagonal holographic reduction under basis $\begin{bmatrix} 1 & 0 \\ 0 & e \end{bmatrix}$, so that $\mathrm{Hol}_3(ec, ec)$ is equivalent to $\mathrm{Holant}([1, 0, 0, e] \mid [ec, e, ec])$, as $e^2 = 1$, which has the same complexity as $\mathrm{Holant}([1, 0, 0, e] \mid [c, 1, c])$. Note the number of recognizer vertices is unchanged, thus still even. For the next step of the reduction, any pair of vertices with signature $[1, 0, 0, e]$ can be simulated by a pair of vertices with signature $[1, 0, 0, 0, e]$. Simply introduce a vertex with generator signature $[1, 1, 1] = [1, 1]^{\otimes 2}$ and make it adjacent to both recognizer vertices. (This step of the reduction is in general not planar.) The last two steps are carried out by interpolation and by a diagonal holographic reduction. Since $ec \notin \{0, \pm 1, \pm \mathrm{i}\}$, by Lemma 5.14 (also by Theorem 5.1 for the case $k = 3$ already proved at the end of Section 5.1), we know that $\mathrm{Hol}_3(ec, ec)$ is #P-hard and we are done. □

Proof of Theorem 5.1 Restricted to $k = 4$

Proof. Tractability (for regions I and II) is given by Theorem 5.48. Intractability over region II for nonplanar graphs is given by Lemma 5.60. Intractability over region III even for planar graphs is proved in Corollary 5.54. □

https://doi.org/10.1017/9781107477063.006 Published online by Cambridge University Press

We conclude this chapter by giving an equivalent statement of Theorem 5.1 (hence also equivalent to Theorem 5.3), the dichotomy theorem for spin systems on regular-k graphs. Note that in this book we have only proved the cases when $k = 3$ and $k = 4$, and that will be the only cases we will use in what follows. A full proof of Theorem 5.3 can be found in [CK12, CK13, Kow10]. The following equivalent statements are in a transformational form, which are more conceptual than Theorem 5.3, and will be consistent with the general dichotomy expression in Theorem 7.19 in Chapter 7.

Recall the definition of functions of product type $\mathscr{P}$ (Definition 3.2), and functions of affine type $\mathscr{A}$ (Definition 3.6).

Theorem 5.61. *Suppose $x, y, z \in \mathbb{C}$ and $k \geq 3$. Then $Z(G)$ for a spin system on k-regular graphs G with edge function $g = [x, y, z]$ is* #P-hard *except in the following cases, when the problem is in P: There exists a holographic transformation T such that*

1. *$g \in T\mathscr{P}$ and $(=_k)T^{\otimes k} \in \mathscr{P}$, or*
2. *$g \in T\mathscr{A}$ and $(=_k)T^{\otimes k} \in \mathscr{A}$.*

The transformations in the tractable cases can be chosen to be diagonal. The same statement holds for Holant$(=_4 | [a, 1, b], \Delta_0, \Delta_1)$*, and a #P-hardness reduction exists that does not use Lemma 3.13.*

If we restrict the input to planar k-regular graphs, then these are solvable in P, as well as when there exists a holographic transformation T such that $g \in T\mathscr{M}$ and $(=_k)T^{\otimes k} \in \mathscr{M}$, where $\mathscr{M}$ denotes all matchgate signatures. The problem remains #P-hard *in all other cases.*

Proof. We first show that condition 1 is equivalent to $g \in \mathscr{P}$. It is obvious that any $g \in \mathscr{P}$ satisfies condition 1 with $T = I$. Suppose g satisfies condition 1 with T. Since $(=_k)T^{\otimes k} \in \mathscr{P}$ is symmetric and $k \geq 3$, it follows that $(=_k)T^{\otimes k}$ is a Gen-Eq, expressible as $[a, 0]^{\otimes k} + [0, b]^{\otimes k}$, where $ab \neq 0$ because $(=_k)T^{\otimes k}$ is nondegenerate. So $(=_k)(TD)^{\otimes k} = (=_k)$ where $D = \begin{bmatrix} a^{-1} & 0 \\ 0 & b^{-1} \end{bmatrix}$. Let $T_1 = TD = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$. Then

$$[\alpha, \beta]^{\otimes k} + [\gamma, \delta]^{\otimes k} = [1, 0]^{\otimes k} + [0, 1]^{\otimes k}.$$

Dot product with $[-\beta, \alpha]$ and then with $[-\delta, \gamma]$ imply that $\beta\delta[1, 0]^{\otimes(k-2)} + \alpha\gamma[0, 1]^{\otimes(k-2)} = 0$. Since $k \geq 3$, we get $\alpha\gamma = \beta\delta = 0$. So T_1 is either diagonal or antidiagonal since it is nonsingular, thus $T_1\mathscr{P} = \mathscr{P}$. We are also given $g \in T\mathscr{P}$. Since D is diagonal, $D\mathscr{P} = \mathscr{P}$. Thus $g \in T\mathscr{P} = TD\mathscr{P} = T_1\mathscr{P} = \mathscr{P}$.

https://doi.org/10.1017/9781107477063.006 Published online by Cambridge University Press

Clearly, if $y = 0$ in $g = [x, y, z]$ then g is a GEN-EQ, and $g \in \mathscr{P}$. Suppose $y \neq 0$ and we normalize it and write $g = [a, 1, b]$. Then in Theorem 5.3 conditions 1 and 2 correspond to g being degenerate and g being a binary DISEQUALITY. Together these cases are exactly $g \in \mathscr{P}$.

In the following we assume $g \notin \mathscr{P}$. It is easy to verify that condition 3 in Theorem 5.3 is equivalent to $a^{4k} = 1$ and $b = -1/a$. If so, we take $T = \begin{bmatrix} 1 & 0 \\ 0 & a^{-1} \end{bmatrix}$. Then $(=_k)T^{\otimes k} \in \mathscr{A}$, being in the family $\mathscr{F}_1$ of Section 3.2. Furthermore, $(T^{-1})^{\otimes 2}(g) = [a, a, ba^2] = a[1, 1, -1] \in \mathscr{A}$.

Now suppose there exists some T such that $(=_k)T^{\otimes k} \in \mathscr{A}$ and $g \in T\mathscr{A}$. Denote $\mathscr{F}_{123} = \mathscr{F}_1 \cup \mathscr{F}_2 \cup \mathscr{F}_3$ (defined in Section 3.2), then since the signature $(=_k)T^{\otimes k}$ is nondegenerate and symmetric, $(=_k)T^{\otimes k} \in \mathscr{F}_{123}$. By its form, there exists a matrix $M \in \left\{ I, \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \begin{bmatrix} 1 & \mathrm{i} \\ 1 & -\mathrm{i} \end{bmatrix} \right\}$ such that $(=_k)(TM^{-1})^{\otimes k}$ has the form $\lambda \left\{ [1, 0]^{\otimes k} + \mathrm{i}^r [0, 1]^{\otimes k} \right\}$ for some $\lambda \neq 0$ and $r \in \{0, 1, 2, 3\}$. Let $\omega = e^{\frac{r\pi \mathrm{i}}{2k}}$, then $\omega^k = \mathrm{i}^r$. Let $T_1 = TM^{-1} \begin{bmatrix} 1 & 0 \\ 0 & \omega \end{bmatrix}^{-1}$, then $(=_k)T_1^{\otimes k} = \lambda \left\{ [1, 0]^{\otimes k} + [0, 1]^{\otimes k} \right\} = \lambda(=_k)$. We write $T_1 = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$; then

$$[\alpha, \beta]^{\otimes k} + [\gamma, \delta]^{\otimes k} = \lambda \left\{ [1, 0]^{\otimes k} + [0, 1]^{\otimes k} \right\}.$$

Dot product with $[-\beta, \alpha]$ and then with $[-\delta, \gamma]$ imply that $\alpha\gamma = \beta\delta = 0$, as before. So T_1 has the form $\alpha \begin{bmatrix} 1 & 0 \\ 0 & \rho \end{bmatrix}$ or $\alpha X \begin{bmatrix} 1 & 0 \\ 0 & \rho \end{bmatrix}$, where $\alpha \neq 0, X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, and $\rho^k = 1$. It follows that $T = \alpha X' \begin{bmatrix} 1 & 0 \\ 0 & \omega' \end{bmatrix} M$, where $X' = I$ or X, $\omega' = \omega\rho$ and $\omega'^{4k} = 1$.

It is also given that $g \in T\mathscr{A}$. Since $(T^{-1})^{\otimes 2} g$ is a symmetric signature, $(T^{-1})^{\otimes 2} g \in \mathscr{F}_{123}$. By the form of M, $M\mathscr{F}_{123} = \mathscr{F}_{123}$. Hence $\left(\begin{bmatrix} 1 & 0 \\ 0 & \omega' \end{bmatrix}^{-1} X' \right)^{\otimes 2} [a, 1, b] \in \mathscr{F}_{123}$. Then we have $[a\omega', 1, b/\omega'] \in \mathscr{F}_{123}$, or $[b\omega', 1, a/\omega'] \in \mathscr{F}_{123}$. By their forms in Section 3.2, and having assumed $g \notin \mathscr{P}$, we have $ab = -1$ and $a^{4k} = 1$.

Exercise: Suppose $ab = -1$ and $a^{4k} = 1$. Show that there is a diagonal T' of the form $\begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi \mathrm{i}}{4k} s} \end{bmatrix}$, for some integer s, such that $(=_k)T'^{\otimes k} \in \mathscr{A}$ and $(T'^{-1})^{\otimes 2}[a, 1, b] \in \mathscr{A}$. Thus the transformation in the affine case of Theorem 5.61 can be chosen to be diagonal.

https://doi.org/10.1017/9781107477063.006 Published online by Cambridge University Press

Concerning k-regular planar graphs, we show that there exists a holographic transformation T such that $[a, 1, b] \in T\mathscr{M}$ and $(=_k)T^{\otimes k} \in \mathscr{M}$ iff $a^k = b^k$. Suppose $a^k = b^k$. Let $T = DH_2$, where $D = \begin{bmatrix} 1 & 0 \\ 0 & \omega^{-1} \end{bmatrix}$, $\omega = \sqrt{\frac{a}{b}}$ with $\omega^{2k} = 1$, and $H_2 = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$. Then $(=_k)D^{\otimes k} = [1, 0]^{\otimes k} + \omega^{-k}[0, 1]^{\otimes k}$, and $(=_k)T^{\otimes k}$ is a nonzero multiple of $[1, 1]^{\otimes k} \pm [1, -1]^{\otimes k} \in \mathscr{M}$. Also $(D^{-1})^{\otimes 2}[a, 1, b] = [a, \omega, b\omega^2] = [a, \omega, a]$, and $(T^{-1})^{\otimes 2}[a, 1, b]$ has the matrix form

$$\frac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} a & \omega \\ \omega & a \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} a+\omega & 0 \\ 0 & a-\omega \end{bmatrix},$$

which is in $\mathscr{M}$.

Now suppose $T = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$, and both $(=_k)T^{\otimes k} \in \mathscr{M}$ and $[a, 1, b] \in T\mathscr{M}$. By the parity requirements for a matchgate signature $(=_k)T^{\otimes k} = [\alpha, \beta]^{\otimes k} + [\gamma, \delta]^{\otimes k} \in \mathscr{M}$ we have either

$$\alpha^k + \gamma^k = \alpha^{k-2}\beta^2 + \gamma^{k-2}\delta^2 = 0, \tag{5.3}$$

or

$$\alpha^{k-1}\beta + \gamma^{k-1}\delta = \alpha^{k-3}\beta^3 + \gamma^{k-3}\delta^3 = 0. \tag{5.4}$$

First we claim that none of $\alpha, \beta, \gamma, \delta$ can be 0. Suppose $\alpha = 0$, then $\gamma = 0$ or $\gamma^{k-1}\delta = 0$. T is nonsingular, it implies that $\delta = 0$, and $\beta\gamma \neq 0$. But clearly for such a T, $(=_k)T^{\otimes k} \notin \mathscr{M}$ by Theorem 4.11, since $k \geq 3$. Hence $\alpha \neq 0$. By the invariance of $\mathscr{M}$ under $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, the proof that $\alpha \neq 0$ also gives $\beta \neq 0$. By the symmetry between $[\alpha, \beta]$ and $[\gamma, \delta]$ we also have $\gamma\delta \neq 0$.

Then dividing in either set of the equations (5.3) and (5.4), we get $\frac{\alpha^2}{\beta^2} = \frac{\gamma^2}{\delta^2}$. By $\det(T) = \alpha\delta - \beta\gamma \neq 0$, we get

$$\frac{\alpha}{\beta} = -\frac{\gamma}{\delta}. \tag{5.5}$$

From (5.3) we get $(\alpha/\gamma)^k = -1$. From (5.4), we get $(\alpha/\gamma)^{k-1} = -\delta/\beta$, and together with (5.5) we get $(\alpha/\gamma)^k = 1$. Thus $(\alpha/\gamma)^{2k} = 1$ from either (5.3) or (5.4).

It follows that

$$T = \begin{bmatrix} \alpha & \beta \\ \alpha\omega & -\beta\omega \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & \omega \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} \alpha & 0 \\ 0 & \beta \end{bmatrix}$$

for some $\omega^{2k} = 1$.

https://doi.org/10.1017/9781107477063.006 Published online by Cambridge University Press

Now we consider $(T^{-1})^{\otimes 2}[a, 1, b] \in \mathscr{M}$, where T^{-1} takes the form $\begin{bmatrix} x & 0 \\ 0 & y \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & \rho \end{bmatrix}$, where $xy \neq 0$ and $\rho^{2k} = 1$. Then we can calculate the binary signature $(T^{-1})^{\otimes 2}[a, 1, b]$ by its matrix form to get

$$(T^{-1})^{\otimes 2}[a, 1, b] = [x^2(a + 2\rho + b\rho^2), xy(a - b\rho^2), y^2(a - 2\rho + b\rho^2)].$$

By the parity requirements for a matchgate signature, and $xy \neq 0$, we get either $a - b\rho^2 = 0$ or $a + 2\rho + b\rho^2 = a - 2\rho + b\rho^2 = 0$. The latter leads to $\rho = 0$, a contradiction; thus $a = b\rho^2$. Taking k-th power, we get $a^k = b^k$. □

https://doi.org/10.1017/9781107477063.006 Published online by Cambridge University Press