Holographic Reduction, Interpolation and Hardness

Jin-Yi Cai[*] Pinyan Lu[†] Mingji Xia[‡]

Abstract

We prove a dichotomy theorem for a class of counting problems expressible by Boolean signatures. The proof methods are holographic reductions and interpolations. We show that interpolatability provides a universal strategy to prove #P-hardness for this class of problems. For these problems whenever holographic reductions followed by interpolations fail to prove #P-hardness, we can show that the problems are actually solvable in polynomial time.

1 Introduction

The study of counting problems and their classifications are a major theme in computational complexity theory. Some counting problems are computable in P, while others appear hard. Valiant introduced the class #P to capture most of these counting problems [17]. Some well known examples of this class of problems are counting perfect matchings, or counting vertex covers. Over the past several years a uniform framework to address a large class of counting problems has emerged [6, 11, 2].

Consider the problem of counting all vertex covers on a graph $G = (V, E)$. One way to express this problem is as follows: We will consider all 0-1 assignments σ of the vertex set V, and for every edge $(x, y) \in E$ we assign an OR function on two bits. This is represented by its truth table $F = (0, 1, 1, 1)$, and is called a "signature". Then σ is a vertex cover iff $\prod_{(x,y)\in E} F(\sigma(x), \sigma(y)) = 1$, and the total number of vertex covers is $\sum_\sigma \prod_{(x,y)\in E} F(\sigma(x), \sigma(y))$.

This framework can be generalized to the so-called H-colorings or H-homomorphisms [11]. Here H is a fixed directed or undirected graph (with possible self loops) given by a Boolean adjacency matrix. A mapping $\sigma : V(G) \to V(H)$ is a homomorphism iff for every edge $(x, y) \in E(G)$, $H(\sigma(x), \sigma(y)) = 1$. Then the quantity $\sum_\sigma \prod_{(x,y)\in E(G)} H(\sigma(x), \sigma(y))$ counts the number of H-homomorphisms. Vertex cover is the special case where the two-vertex graph $H = (\{0, 1\}, \{(0, 1), (1, 0), (1, 1)\})$. Dichotomy theorems for H-coloring problems with undirected graphs H and directed acyclic graphs H are given in [11] and [10] respectively.

When it comes to matchings or perfect matchings, the more natural framework will be to consider assignments to the edge set of G instead of the vertex set, and the "evaluation" F happens at each vertex, which is either a Boolean OR function (for matchings) or the EXACT-ONE function (for perfect matchings). Thus a Boolean assignment σ of E is a matching (resp. a perfect matching) iff at every vertex v the assignment σ at the incident edges $E(v)$ evaluates to 1 according to F, and the sum $\sum_{\sigma \text{ on } E} \prod_{v\in V} F(\sigma \mid_{E(v)})$ is the total number of matchings or perfect matchings, respectively.

We remark that assigning values on edges can be viewed as a generalization of assigning values on vertices. To see this, let's temporarily consider the following further generalization where we assign a value at each *end* of an edge $e = (x, y)$, i.e., we assign a value $\sigma(e, x)$ and $\sigma(e, y)$. Then we may assign

[*] University of Wisconsin-Madison, and Radcliffe Institute, Harvard University jyc@cs.wisc.edu

[†] Tsinghua University lpy@mails.tsinghua.edu.cn

[‡] Institute of Software, Chinese Academy of Sciences, xmjljx@gmail.com

an "evaluation" function F at each edge as well as at each vertex. The overall evaluation is done for all $v \in V$ and all $e \in E$, and the sum over all σ of products over all v and e, $\sum_\sigma \prod_{v,e} F$, is then *the counting problem*. In this set-up, evaluating over vertex assignments is the special case where F at each vertex is the Equality function, and evaluating over edge assignments is the special case where F at each edge is the Equality function. However, we claim that this further generalization can be easily simulated by the following construction, which remains in the framework of edge assignments: Replace each edge by a path of length two and introduce a new vertex of degree 2 in the middle. This substitution makes G a bipartite graph, where every vertex on one side (the new vertices) has degree 2. In this paper we will study our counting problems in the framework of edge assignments.

It turns out that studying counting problems in this framework has a close connection with holographic algorithms and reductions. Holographic algorithms have been introduced by Valiant [19]. This beautiful theory has two main ingredients. The first is the use of matchgates to encode computations, which allows a P-time computation over planar graphs using the FKT method [12, 13] in terms of Pfaffians. The second ingredient is to use linear algebra to create exponential sums of perfect matchings in a "holographic mix", and achieve exponential cancelations in the process. In [5] we have introduced another family of P-time computable primitives called Fibonacci gates. Holographic transformations with Fibonacci gates also create exponential cancelations to yield P-time algorithms.

In this paper we take a broader perspective, by considering which counting problems are in P and which are #P-complere in the framework discussed above. In order to obtain clearly stated results we restrict our attention here to the class of 2-3 regular graphs. A 2-3 regular graph is a bipartite graph $G = (U, V, E)$, where $\deg(u) = 2$ and $\deg(v) = 3$ for all $u \in U$ and $v \in V$. As indicated above, evaluating over edge assignments for this class of graphs already encompasses all 3-regular graphs. The reason for this restriction is that (a) in this simplest case we can already show #P-completeness, and (b) we can exhibit a dichotomy theorem. In principle our results can be generalized to non-Boolean assignments and signatures on arbitrary graphs. However a dichotomy theorem will be more difficult.

Our main technical contributions are as follows. Over the class of 2-3 regular graphs we will consider each vertex $u \in U$ (resp. $v \in V$) is given a Boolean signature, $[x_0, x_1, x_2]$ (resp. $[y_0, y_1, y_2, y_3]$). This notation (see [19]) means that at $u \in U$ of degree 2, a Boolean function F takes the value x_0, x_1 and x_2 respectively when the Hamming weight of the Boolean assignment at its two incident edges are $0, 1$ and 2 respectively. The meaning of the signature $[y_0, y_1, y_2, y_3]$ at $v \in V$ is similar. We denote by $\#[x_0, x_1, x_2]|[y_0, y_1, y_2, y_3]$ the counting problem over all 2-3 regular graphs using these signatures. Our starting point is the observation that both $\#[0, 1, 1]|[1, 0, 0, 1]$ and $\#[1, 0, 1]|[1, 1, 0, 0]$ are #P-complete. (Perceptive readers will notice that $\#[0, 1, 1]|[1, 0, 0, 1]$ is just counting vertex covers, and $\#[1, 0, 1]|[1, 1, 0, 0]$ is counting matchings, both over 3-regular graphs [21].) To consider a general counting problem $\#[x_0, x_1, x_2]|[y_0, y_1, y_2, y_3]$, we apply *holographic reductions* to transform either the signature $[1, 0, 0, 1]$ or the signature $[1, 1, 0, 0]$ to the signature $[y_0, y_1, y_2, y_3]$. This uses some signature theory of holographic algorithms [3, 4]. Under this holographic reduction, the signatures $[0, 1, 1]$ or $[1, 0, 1]$ respectively are transformed to some new signature $[x'_0, x'_1, x'_2]$. This transformation will be an invertible map which shows that the counting problem $\#[x'_0, x'_1, x'_2]|[y_0, y_1, y_2, y_3]$ has the same complexity as either $\#[0, 1, 1]|[1, 0, 0, 1]$ or $\#[1, 0, 1]|[1, 1, 0, 0]$, thus #P-complete.

Next we try to show that our given signature pairs $[x_0, x_1, x_2]$ and $[y_0, y_1, y_2, y_3]$ can simulate $[x'_0, x'_1, x'_2]$. To do this we develop an algebraic lemma, and apply the powerful technique of *interpolation* initiated by Valiant [17]. The lemma gives a sufficient condition for this interpolation to succeed. The proof of this lemma uses some basic Galois theory. The actual interpolation is accomplished by a couple of versatile combinatorial gadgets. (But the theory is strong enough that the particular gadgets are almost generic; see more discussions in the Appendix.) When this interpolation succeeds, we will have proved that the counting problem $\#[x_0, x_1, x_2] \mid [y_0, y_1, y_2, y_3]$ is #P-complete. All our hardness results are proved by this single universal strategy.

Along the way we will discover that for certain cases of signature pairs $[x_0, x_1, x_2]$ and $[y_0, y_1, y_2, y_3]$ this hardness proof via interpolation does not work. Then we will see that these cases are in fact computable in P. They come in three categories: (1) They can be solved by matchgates over planar graphs; (2) They can be solved by Fibonacci gates over general graphs; and (3) Some special cases solvable in P for obvious reasons. This gives us a dichotomy theorem. To sum up we show that *interpolatability implies hardness*. In the class of problems we considered the converse is also true, namely failure to interpolate also implies solvability in P. It appears that there are deeper connections between interpolatability and hardness in general. Some additional results and proofs are given in the Appendix.

2 Definitions and Background

A *signature grid* $\Omega = (G, \mathcal{F})$ is a tuple, where $G = (V, E)$ is a graph, and each $v \in V(G)$ is assigned a function $F_v \in \mathcal{F}$. A Boolean assignment σ for every $e \in E$ gives an evaluation $\prod_{v \in V} F_v(\sigma \mid_{E(v)})$, where $E(v)$ denotes the incident edges of v. The counting problem on the instance Ω is to compute

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

(The term Holant was first introduced by Valiant in [19] to denote a related exponential sum.) We can view each function F_v as a truth table, and then we can represent it by a vector in $\mathbf{F}^{2^{d(v)}}$, or a tensor in $(\mathbf{F}^2)^{\otimes d(v)}$. This is called a *signature*.

As discussed in the previous section, many important counting problems can be viewed as computing Holant_Ω for appropriate signatures at each vertex, such as counting (perfect) matchings and counting vertex covers. Many counting problems not directly defined in terms of graphs can also be formulated as holant problems, e.g., the #SAT problem.

In this paper we will mainly consider symmetric signatures. A signature is called symmetric, if each signature entry only depends on the Hamming weight of the input. The signatures we defined above for matching or perfect matching or Boolean OR all have this property. We use a more compact notation $[f_0, f_1, \ldots, f_n]$ to denote a symmetric signature on n inputs, where f_i is the value on inputs of weight i.

2.1 $\mathcal{F}$-Gate

A signature from $\mathcal{F}$ at a vertex is considered a basic realizable function. Instead of a single vertex, we can use graph fragments to generalize this notion. An $\mathcal{F}$-gate Γ is a pair $(H, \mathcal{F})$, where $H = (V, E, D)$ is a graph with some dangling edges D. (See Figure 1 for one example.) Other than these dangling edges, an $\mathcal{F}$-gate is the same as a signature grid. The role of dangling edges is similar to that of external nodes in Valiant's notion [18], however we allow more than one dangling edges for a node. In $H = (V, E, D)$ each node is assigned a function in $\mathcal{F}$ (we do not consider "dangling" leaf nodes at the end of a dangling edge among these), E are the regular edges, denoted as $1, 2, \ldots, m$, and D are the dangling edges, denoted as $m+1, m+2, \ldots, m+n$. Then we can define a function for this $\mathcal{F}$-gate $\Gamma = (H, \mathcal{F})$,

$$\Gamma(y_1, y_2, \ldots, y_n) = \sum_{x_1 x_2 \cdots x_m \in \{0,1\}^m} H(x_1 x_2 \cdots x_m y_1 y_2 \cdots y_n),$$

where $(y_1, y_2, \ldots, y_n) \in \{0,1\}^n$ denotes an assignment on the dangling edges and $H(x_1 x_2 \cdots x_m y_1 y_2 \cdots y_n)$ denotes the value of the signature grid on an assignment of all edges. We will also call this function the signature of the $\mathcal{F}$-gate Γ. An $\mathcal{F}$-gate can be used in a signature grid as if it is just a single node with the particular signature. We note that even for a very simple signature set $\mathcal{F}$, the signatures for all $\mathcal{F}$-gates can be quite complicated and expressive. Matchgate signatures are an example.

2.2 Holographic Reduction

To introduce the idea of holographic reductions, it is convenient (but not necessary) to consider bipartite graphs. We note that this is without loss of generality. For any general graph, we can make it bipartite by adding an additional vertex on each edge, and for each new vertex by giving it the EQUALITY function $(1, 0, 0, 1)$ on 2 inputs (in symmetric notation $[1, 0, 1]$.)

We use $\#\mathcal{G}|\mathcal{R}$ to denote all the counting problems, expressed as holant problems on bipartite graphs $H = (U, V, E)$, where each signature for a vertex in U or V is from $\mathcal{G}$ or $\mathcal{R}$, respectively. An input instance of the holant problem is a signature grid and is denoted as $\Omega = (H, \mathcal{G}|\mathcal{R})$. Signatures in $\mathcal{G}$ are called generators, which are denoted by column vectors (or contravariant tensors); signatures in $\mathcal{R}$ are called recognizers, which are denoted by row vectors (or covariant tensors) [8].

One can perform (contravariant and covariant) tensor transformations on the signatures, which may produce exponential cancelations in tensor spaces. We will define a simple version of holographic reductions, which are invertible. Suppose $\#\mathcal{G}|\mathcal{R}$ and $\#\mathcal{G}'|\mathcal{R}'$ are two holant problems defined for the same family of graphs, and $T = [\mathbf{n}, \mathbf{p}] \in \mathbf{GL}_2(\mathbf{C})$ is a basis. We say that there is a holographic reduction from $\#\mathcal{G}|\mathcal{R}$ to $\#\mathcal{G}'|\mathcal{R}'$, if the *contravariant* transformation $G' = T^{\otimes g}G$ and the *covariant* transformation $R = R'T^{\otimes r}$ map $G \in \mathcal{G}$ to $G' \in \mathcal{G}'$ and $R \in \mathcal{R}$ to $R' \in \mathcal{R}'$, where G and R have arity g and r respectively. (Notice the reversal of directions when the transformation $T^{\otimes n}$ is applied. This is the meaning of *contravariance* and *covariance.*)

Theorem 2.1 (Holant Theorem)**.** *Suppose there is a holographic reduction from $\#\mathcal{G}|\mathcal{R}$ to $\#\mathcal{G}'|\mathcal{R}'$ mapping signature grid Ω to Ω', then*

$$\mathrm{Holant}_{\Omega} = \mathrm{Holant}_{\Omega'}.$$

The proof of this theorem follows from general principles of contravariant and covariant tensors [8].

In particular, for invertible holographic reductions from $\#\mathcal{G}|\mathcal{R}$ to $\#\mathcal{G}'|\mathcal{R}'$, one problem is in P iff the other one is, and similarly one problem is #P-complete iff the other one is also.

2.3 Related Work

Our counting problems are closely related to Constrained Satisfaction Problems (CSP). A uniform treatment of CSP is given in [7] by Creignou, Khanna and Sudan. Many counting problems can be formulated as $\#\mathcal{G}|\mathcal{R}$. When $\mathcal{R}$ is fixed to be the set of EQUALITY of all arities, $\#\mathcal{G}|\mathcal{R}$ are called #Weighted CSP problems. The following table lists some known dichotomy theorems about the complexity of some subclasses of #Weighted CSP.

Type of variables	The range of function value	The arity of functions	The number of functions	Name in literature	Reference
Boolean	Boolean	arbitrary	arbitrary	#Boolean CSP	[6]
any finitary	Boolean	two	one symmetric	#H-coloring	[11]
any finitary	non-negative rational	two	one symmetric	partition function	[2]
any finitary	Boolean	two	one unsymmetric acyclic	#H-coloring	[10]
Boolean	non-negative rational	arbitrary	arbitrary	#Weighted Boolean CSP	[9]

Obviously, #Weighted CSP generalizes both #H-colorings and #Weighted Boolean CSP, but unfortunately, there is no dichotomy theorem. Some partial results are given in [1]. When $\mathcal{G}$ and $\mathcal{R}$ contain some functions other than EQUALITY, $\#\mathcal{G}|\mathcal{R}$ become our graph counting problems, which is not expressible as #Weighted CSP. See [15] for some results for these problems.

3 Interpolation Method

Polynomial interpolation is a powerful tool in the study of counting problems initiated by Valiant [17] and further developed by Vadhan, Dyer and Greenhill [15, 11]. We discuss the interpolation method we will use in this paper.

Let $\Omega = (G, \mathcal{F})$ be a signature grid. Suppose $g \in \mathcal{F}$ is a symmetric signature with arity 2, and we denote it as $[x, y, z]$. Thus $g(00) = x$, $g(01) = g(10) = y$ and $g(11) = z$. Let V_g be the subset of vertices assigned g in Ω. Suppose $|V_g| = n$. Then the holant value Holant_Ω can be expressed as

$$\text{Holant}_\Omega = \sum_{i+j+k=n} c_{i,j,k} x^i y^j z^k, \tag{1}$$

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

Now suppose $\{f_s\}$ is a sequence of symmetric functions of arity 2, with signatures $[x_s, y_s, z_s]$, for $s = 0, 1, \ldots$. If we replace each occurrence of g by f_s in Ω we get a new signature grid Ω_s with

$$\text{Holant}_{\Omega_s} = \sum_{i+j+k=n} c_{i,j,k} x_s^i y_s^j z_s^k. \tag{2}$$

Note that the same set of values $c_{i,j,k}$ occur. We can treat $c_{i,j,k}$ in (2) as a set of unknowns in a linear system. The idea of interpolation is to find a suitable sequence $\{f_s\}$ such that we can evaluate Holant_{Ω_s}, and then to find all $c_{i,j,k}$ by solving a linear system (2).

In this paper, the sequence $\{f_s\}$ will be constructed recursively using a suitable gadget. Let $\mathcal{F}' = \mathcal{F} - \{g\}$. A sequence of $\mathcal{F}'$-gates N_s will be constructed, such that its signature is f_s. Recursively from the construction, f_s will be symmetric. Let this signature be denoted by $[x_s, y_s, z_s]$, then the construction will yield a linear recurrence:

$$\begin{bmatrix} x_s \\ y_s \\ z_s \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} \begin{bmatrix} x_{s-1} \\ y_{s-1} \\ z_{s-1} \end{bmatrix}. \tag{3}$$

Let A denote the 3×3 matrix. This A will be independent of s. Suppose A has distinct eigenvalues α, β and γ, and $A = T^{-1}\text{diag}(\alpha, \beta, \gamma)T$, where the rows of T are the row eigenvectors of A.

Let $(u, v, w)^{\mathrm{T}} = T(x_0, y_0, z_0)^{\mathrm{T}}$ be the inner products of the row eigenvectors with the initial values. Then

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

Let $B = T^{-1}\text{diag}(u, v, w)$. B is non-singular iff $uvw \neq 0$, which we will assume in the following. It follows that

$$\begin{bmatrix} x_s \\ y_s \\ z_s \end{bmatrix}^{\otimes n} = B^{\otimes n} \begin{bmatrix} \alpha^s \\ \beta^s \\ \gamma^s \end{bmatrix}^{\otimes n}. \tag{4}$$

The rows and columns of $B^{\otimes n}$ are indexed by $t_1 t_2 \cdots t_n \in \{1, 2, 3\}^n$. There are 3^n equalities in (4). Let $\kappa = \{1^i 2^j 3^k \mid i + j + k = n\}$ be the set of "types" for all $t_1 t_2 \cdots t_n$, and $|\kappa| = \binom{n+2}{2}$. Define an equivalence relation on the indices, $t_1 t_2 \cdots t_n \sim t'_1 t'_2 \cdots t'_n$ if they have the same numbers of 1's and 2's and 3's. We identify the equivalence classes with κ.

Define $\widehat{B^{\otimes n}}$ to be the $3^n \times \binom{n+2}{2}$ matrix obtained from $B^{\otimes n}$ by adding all columns in each equivalence class. We claim that this matrix $\widehat{B^{\otimes n}}$ has full column rank $\binom{n+2}{2}$. This is easy to see, since any non-trivial linear combination of the columns of $\widehat{B^{\otimes n}}$ can be also obtained as a non-trivial linear combination of the columns of $B^{\otimes n}$, which is non-singular. The crucial point is that $\widehat{B^{\otimes n}}$ is obtained from $B^{\otimes n}$ by adding all columns within each class in a *disjoint partition* of columns.

Next we claim that there are exactly $\binom{n+2}{2}$ distinct rows in $\widehat{B^{\otimes n}}$, and if we select a set of $\binom{n+2}{2}$ distinct representatives to form a new $\binom{n+2}{2} \times \binom{n+2}{2}$ matrix $\widetilde{B^{\otimes n}}$, it is of full rank. We only need to prove that if $t_1 t_2 \cdots t_n \sim t'_1 t'_2 \cdots t'_n$ then the two rows of $\widehat{B^{\otimes n}}$ indexed by $t_1 t_2 \cdots t_n$ and $t'_1 t'_2 \cdots t'_n$ are the same. Since $t_1 t_2 \cdots t_n \sim t'_1 t'_2 \cdots t'_n$, there is a permutation σ such that σ maps $t_1 t_2 \cdots t_n$ to $t'_1 t'_2 \cdots t'_n = t_{\sigma(1)} t_{\sigma(2)} \cdots t_{\sigma(n)}$. If we perform a simultaneous permutation of rows and columns of $B^{\otimes n}$ by σ, the entries $(B^{\otimes n})_{t_1 t_2 \cdots t_n, c_1 c_2 \cdots c_n} = B_{t_1,c_1} B_{t_2,c_2} \cdots B_{t_n,c_n}$ is mapped to $(B^{\otimes n})_{t_{\sigma(1)} t_{\sigma(2)} \cdots t_{\sigma(n)}, c_{\sigma(1)} c_{\sigma(2)} \cdots c_{\sigma(n)}} = B_{t_{\sigma(1)},c_{\sigma(1)}} B_{t_{\sigma(2)},c_{\sigma(2)}} \cdots B_{t_{\sigma(n)},c_{\sigma(n)}} = B_{t_1,c_1} B_{t_2,c_2} \cdots B_{t_n,c_n}$. That is, a simultaneous permutation of rows and columns of $B^{\otimes n}$ by σ leaves it invariant. But the permutation of the columns by σ certainly induces a permutation within each equivalence class of κ, and thus keeps its sum invariant. It follows that the two rows of $\widehat{B^{\otimes n}}$ indexed by $t_1 t_2 \cdots t_n$ and $t'_1 t'_2 \cdots t'_n$ are the same. Since $\widehat{B^{\otimes n}}$ has full column rank $\binom{n+2}{2}$, $\widetilde{B^{\otimes n}}$ also has full rank $\binom{n+2}{2}$ (and exactly $\binom{n+2}{2}$ distinct rows).

Now we return to the linear system (2), for $0 \le s < \binom{n+2}{2}$. If we consider this as a linear equation system with unknowns $c_{i,j,k}$, indexed by κ, it has a coefficient matrix which is the product of $\widetilde{B^{\otimes n}}$ with a Vandermonde matrix $\mathbf{V}$. The rows of $\mathbf{V}$ are indexed by κ and columns are indexed by $0 \le s < \binom{n+2}{2}$. The entry of $\mathbf{V}$ at $(1^i 2^j 3^k, s)$ is $(\alpha^i \beta^j \gamma^k)^s$. This Vandermonde matrix will be of full rank if all entries $\alpha^i \beta^j \gamma^k$ are distinct.

We summarize this as follows:

Theorem 3.1. *Suppose the recurrence matrix A of the construction N_s satisfies*

1. $\det(A) \neq 0$,
2. *The initial signature $[x_0, y_0, z_0]$ is not orthogonal to any row eigenvector of A, and*
3. *For all $(i,j,k) \in \mathbf{Z}^3 - \{(0,0,0)\}$ with $i + j + k = 0$, $\alpha^i \beta^j \gamma^k \neq 1$.*

Then all $c_{i,j,k}$ in (1), where $1^i 2^j 3^k \in \kappa$, can be computed in polynomial time.

4 Interpolatability Implies Hardness

Definition 4.1. *For $n \ge 2$, a signature $[x_0, x_1, \ldots, x_n]$ is called non-degenerate if*

$$\operatorname{rank} \begin{bmatrix} x_0 & \ldots & x_{n-1} \\ x_1 & \ldots & x_n \end{bmatrix} = 2.$$

A signature $[x_0, x_1, \ldots, x_n]$ is degenerate iff it is of the form $[s^0 t^n, s^1 t^{n-1}, \ldots, s^n t^0]$, for some s and t.

Lemma 4.1. *For any non-degenerate signature $[y_0, y_1, y_2, y_3]$, there exists a symmetric signature $[x_0, x_1, x_2]$ of arity two, such that $\#[x_0, x_1, x_2]|[y_0, y_1, y_2, y_3]$ is #P-Complete. Furthermore this remains true even for planar graphs.*

Proof: Our starting point is that $\#[0,1,1]|[1,0,0,1]$ and $\#[1,0,1]|[1,1,0,0]$ are both #P-Complete. The first problem is simply counting the number of vertex covers for 3-regular graphs; while the second is to count the number of (not necessarily perfect) matchings for 3-regular graphs [21]. We remark that both of them remain #P-Complete even for planar graphs.

Our technique here is to use the theory of holographic reductions. Given a non-degenerate signature $[y_0, y_1, y_2, y_3]$, we can give a parameterization in terms of a homogeneous 2nd order recurrence relation. There are three cases: $y_i = \alpha_1^{3-i}\alpha_2^i + \beta_1^{3-i}\beta_2^i$, where $\alpha_1\beta_2 - \alpha_2\beta_1 \neq 0$; $y_i = Ai\alpha^{i-1} + B\alpha^i$, where $A \neq 0$; or $y_i = A(3-i)\alpha^{2-i} + B\alpha^{3-i}$, where $A \neq 0$. The last case can be viewed as the reversal of the second case, so we will omit the proof for this case. Note that for any non-degenerate signature one of these parameterizations is always possible. (In the expression $i\alpha^{i-1}$, if $\alpha = 0$, we take the convention that $i\alpha^{i-1} = 0, 1, 0, 0$ for $i = 0, 1, 2, 3$ respectively.)

For the first case, under the basis $T = \begin{bmatrix} \alpha_1 & \beta_1 \\ \alpha_2 & \beta_2 \end{bmatrix}$, signature $[1, 0, 0, 1]$ becomes $[y_0, y_1, y_2, y_3]$. This is the result of the contravariant transformation $(y_0, y_1, y_1, y_2, y_1, y_2, y_2, y_3)^{\mathrm{T}} = T^{\otimes 3}(1, 0, 0, 0, 0, 0, 0, 1)^{\mathrm{T}}$. Under the same basis, $[0, 1, 1]$ undergoes the covariant transformation $(x_0, x_1, x_1, x_2) = (0, 1, 1, 1)(T^{-1})^{\otimes 2}$, to become a new symmetric signature $[x_0, x_1, x_2]$. So by the holographic reduction the complexity of $\#[x_0, x_1, x_2]|[y_0, y_1, y_2, y_3]$ and $\#[0, 1, 1]|[1, 0, 0, 1]$ is the same. Since $\#[0, 1, 1]|[1, 0, 0, 1]$ is #P-Complete, we know that $\#[x_0, x_1, x_2]|[y_0, y_1, y_2, y_3]$ is also #P-Complete.

For the second case, we choose the following basis $T = \begin{bmatrix} 1 & \frac{B-1}{3} \\ \alpha & A + \frac{B-1}{3}\alpha \end{bmatrix}$. Then under the contravariant transformation $(y_0, y_1, y_1, y_2, y_1, y_2, y_2, y_3)^{\mathrm{T}} = T^{\otimes 3}(1, 1, 1, 0, 1, 0, 0, 0)^{\mathrm{T}}$, the signature $[1, 1, 0, 0]$ becomes $[y_0, y_1, y_2, y_3]$. Under the same basis, $[1, 0, 1]$ undergoes the covariant transformation $(x_0, x_1, x_1, x_2) = (1, 0, 0, 1)(T^{-1})^{\otimes 2}$, to become a new symmetric signature $[x_0, x_1, x_2]$. (We chose these basis transformations not "out of blue", but rather they are informed by an underlying signature theory of holographic algorithms [3, 4]. But for brevity of exposition we state these transformations *as is* without discussing the background. They can be directly verified, albeit a bit tedious.)

It follows from holographic reductions the complexity of $\#[x_0, x_1, x_2]|[y_0, y_1, y_2, y_3]$ and $\#[1, 0, 1]|[1, 1, 0, 0]$ is the same. Since $\#[1, 0, 1]|[1, 1, 0, 0]$ is #P-Complete, $\#[x_0, x_1, x_2]|[y_0, y_1, y_2, y_3]$ is also #P-Complete.

□

This lemma directly gives the following theorem:

Theorem 4.1. *If $[y_0, y_1, y_2, y_3]$ is non-degenerate, and if $[x_0, x_1, x_2]|[y_0, y_1, y_2, y_3]$ can be used to interpolate all symmetric signatures of arity 2, then $\#[x_0, x_1, x_2]|[y_0, y_1, y_2, y_3]$ is #P-Complete.*

This theorem gives a sufficient condition for $\#[x_0, x_1, x_2]|[y_0, y_1, y_2, y_3]$ to be hard. In the next section, we will prove an algebraic lemma that guarantees this interpolatability, and then in Section 6 we use this theorem to prove all the hardness results for Boolean symmetric signatures.

5 An Algebraic Lemma

Fix a signature set $\mathcal{F}$. Our general recursive construction of a series of gadgets is depicted in Fig. 2. Every gadget N_s will have arity 2. (In this paper we restrict to interpolations for signatures of arity 2. But the general theory can be applied to arbitrary arity.) The first gadget is just a vertex with some signature in $\mathcal{F}$. The key of this construction is the $\mathcal{F}$-gate $\mathcal{A}$ in Fig. 2 with arity 4. The specific $\mathcal{A}$'s we will use are depicted in Fig. 3 and 4. In each step, we will connect a copy of $\mathcal{A}$ to make a new gadget. In order to make use of Theorem 3.1, we choose our $\mathcal{F}$-gate $\mathcal{A}$ such that all the signatures are symmetric. We denote by $[x_s, y_s, z_s]$ the signature of the s-th gadget. Then there is a linear recursive relation in the constructed gadgets, that is, $(x_s, y_s, z_s)^{\mathrm{T}} = A(x_{s-1}, y_{s-1}, z_{s-1})^{\mathrm{T}}$ for some matrix A as in (3). We can use the same A because the matrix is completely determined by the $\mathcal{F}$-gate $\mathcal{A}$.

According to Theorem 3.1, the interpolatability of the signature requires three conditions, of which the main condition is: For no $i, j, k \in \mathbf{Z}$ with $i + j + k = 0$, other than the trivial $(0, 0, 0)$, do we have

$$\alpha^i \beta^j \gamma^k = 1. \tag{5}$$

This condition ensures that a Vandermonde matrix is non-singular. Let $f(x)$ be the characteristic polynomial of A. The following algebraic lemma gives a sufficient condition that condition (5) is satisfied. The proof of this lemma uses some basic Galois theory. Due to space limitation, we present its proof in the Appendix.

Lemma 5.1. *Let $f(x) = x^3 + c_2x^2 + c_1x + c_0 \in \mathbf{Q}[x]$ be a given polynomial with rational coefficients. It is decidable in polynomial time whether any non-trivial solution to (5) exists, where α, β and γ are its roots, and if so, find all solutions (in terms of a short basis of the lattice). If f is irreducible, except of the form $x^3 + c$ for some $c \in \mathbf{Q}$, there are no non-trivial solutions to (5).*

6 Boolean Symmetric Signatures

In this section, we give a dichotomy theorem for all counting problems of the form $\#[x_0, x_1, x_2]|[y_0, y_1, y_2, y_3]$, where each $x_i, y_j \in \{0, 1\}$. Such signatures are called Boolean symmetric signatures [3]. This family of signatures is particularly important because they have clear combinatorial meanings and many combinatorial constraints can be described by these signatures.

By flipping all 0's and 1's, we see that the problem $\#[x_2, x_1, x_0]|[y_3, y_2, y_1, y_0]$ always has the same complexity as the problem $\#[x_0, x_1, x_2]|[y_0, y_1, y_2, y_3]$. So we will only consider one problem for each pair. In the following we only enumerate problems $\#[x_0, x_1, x_2]|[y_0, y_1, y_2, y_3]$, where we let (1) $x_0 \geq x_2$, and (2) if $x_0 = x_2$, then $y_0 \geq y_3$, and (3) if $x_0 = x_2$ and $y_0 = y_3$, then $y_1 \geq y_2$. Also when we consider a signature $[y_0, y_1, y_2, y_3]$ we also consider its reversal, in particular in terms of expressibility as a second order recurrence relation involving its eigenvalues. We also will only implicitly verify the other conditions in Theorem 3.1, and not mention it explicitly, i.e., we will only focus explicitly on the condition (5).

6.1 The Tractable Cases

First if at least one side of the signatures is degenerate, then the holant Holant_Ω can be computed in polynomial time. The degenerate Boolean signatures of arity 2 are: $[0, 0, 0], [0, 0, 1], [1, 0, 0], [1, 1, 1]$; and the degenerate Boolean signatures of arity 3 are: $[0, 0, 0, 0], [0, 0, 0, 1], [1, 0, 0, 0], [1, 1, 1, 1]$. These problems are all trivially solvable; e.g., for $\#[x_0, x_1, x_2]|[1, 1, 1, 1]$, the holant is completely decomposed as a product over identical disjoint paths of length 2, i.e., $\prod_{v \in V:\deg(v)=3}(x_0 + 2x_1 + x_2)$. From now on, we discuss non-degenerate Boolean signatures and rule out these 8 signatures.

Some holants evaluate to 0 by a cardinality argument. For example, in the counting problem $\#[0, 1, 0]|[0, 1, 0, 0]$, signature $[0, 1, 0]$ requires that exactly half of all edges have value 1, while the signature $[0, 1, 0, 0]$ requires that exactly one third of edges have value 1. This is a contradiction. So there are no feasible solutions and the output of the counting problem is 0. These infeasible cases include the following problems: $\#[0, 1, 0]|[1, 1, 0, 0]$, $\#[0, 1, 0]|[0, 1, 0, 0]$, $\#[1, 1, 0]|[0, 0, 1, 1]$, $\#[1, 1, 0]|[0, 0, 1, 0]$.

Similarly, the following two problems are both tractable: $\#[1, 0, 1]|[1, 0, 0, 1]$ and $\#[0, 1, 0]|[1, 0, 0, 1]$, proved by an easy connectivity argument.

The remaining tractable cases are those which can be solved by holographic algorithms with Fibonacci gates [5]. They are $\#[0, 1, 0]|[1, 0, 1, 0]$,$\#[1, 0, 1]|[1, 0, 1, 0]$, $\#[1, 0, 1]|[1, 1, 0, 1]$ and $\#[1, 1, 0]|[1, 1, 0, 1]$, where the recurrences are $f_{i+2} = 0 \cdot f_{i+1} + f_i$ for the first two, and $f_{i+2} = (-1) \cdot f_{i+1} + f_i$ for the last two. It is proved in [5] that $f_{i+2} = m \cdot f_{i+1} + f_i$ can all be reduced by holographic reductions to the basic Fibonacci gates $f_{i+2} = f_{i+1} + f_i$.

6.2 Tractable for Planar Graphs but Hard in General

This class contains 3 members: $\#[1,0,1]|[0,1,0,0]$, $\#[1,0,1]|[0,1,1,0]$ and $\#[0,1,0]|[0,1,1,0]$. The problem $\#[1,0,1]|[0,1,0,0]$ is counting perfect matchings in a 3-regular graph (Problem PM). The second one, $\#[1,0,1]|[0,1,1,0]$ is a special edge coloring problem we studied in [5]; let's call it Problem COLOR (this is not the usual Graph Coloring problem). The third problem $\#[0,1,0]|[0,1,1,0]$ is an Ising problem studied by Valiant in [19] (Problem ICE). For planar graphs, all these three problems are polynomial time computable by holographic algorithms with matchgates.

In [5] (Theorem 7.1), we proved that $\#[1,0,1]|[0,1,1,0]$ (Problem COLOR) is #P-complete for general graphs. Next, to prove $\#[0,1,0]|[0,1,1,0]$ (Problem ICE) is #P-complete we use $\#[0,1,0]|[0,1,1,0]$ (Problem COLOR) to interpolate all signatures of the form $[a,b,a]$, the proof can be found in the Appendix. Then the fact that $\#[1,0,1]|[0,1,1,0]$ (Problem COLOR) is #P-complete implies that $\#[0,1,0]|[0,1,1,0]$ (Problem ICE) is #P-complete, by an adaptation of Theorem 4.1.

The #P-hardness for Problem PM is proved in [17].

6.3 The Hard Cases (Hard even for Planar Graphs)

In this section, we make use of the tools we developed in Sections 4 and Section 5 to prove hardness for all the remaining problems.

Here we go over all cases of the form $\#[0,1,0]|[y_0,y_1,y_2,y_3]$ (note that there are two cases for each listed case by symmetry). The first hard case is $\#[0,1,0]|[1,1,1,0]$. We will consider instead its flipped case $\#[0,1,0]|[0,1,1,1]$. Over planar graphs (we are assuming planarity in this subsection) this is called #Pl-Rtw-Opp-3CNF—Satisfiability of planar 3CNF formulae where each variable occurs twice and in opposite signs. We note that #Pl-Rtw-Mon-3CNF [20] is #P-complete and $\oplus$Pl-Rtw-Mon-3CNF is $\oplus$P-complete, while $\#_7$Pl-Rtw-Mon-3CNF is P-time computable. Here we use Theorem 4.1 to prove that #Pl-Rtw-Opp-3CNF is also #P-complete.

We use the gadget in Figure 3 to construct recursively an arity 2 gate N_i using the signatures $[0,1,0]|[0,1,1,1]$. This means that in the construction, every node of degree two (resp. three) is assigned a signature $[0,1,0]$ (resp. $[0,1,1,1]$).

Obviously, the signatures $[a_i,b_i,c_i]$ for N_i are all symmetric. It takes some computation, but it can be verified that the following recursive relation holds:

$$\begin{bmatrix} a_i \\ b_i \\ c_i \end{bmatrix} = \begin{bmatrix} 48 & 136 & 96 \\ 28 & 88 & 68 \\ 16 & 56 & 48 \end{bmatrix} \begin{bmatrix} a_{i-1} \\ b_{i-1} \\ c_{i-1} \end{bmatrix}.$$

The characteristic polynomial is $x^3 - 184x^2 + 1600x - 512$. It is easy to verify that it is irreducible over $\mathbf{Q}[x]$. Then by Lemma 5.1, we know that this family of gadgets can be used for interpolation. As a result, $\#[0,1,0]|[0,1,1,1]$ is #P-complete.

The next hard case is $\#[0,1,0]|[1,1,0,1]$. This is called #Pl-Rtw-Opp-$F_{0,1,3}$-SAT in the notation of [21]. In [21], they proved that #Pl-Rtw-Mon-$F_{0,1,3}$-SAT is P-time computable and if one does not restrict the occurrence of the variables, then #Pl-Rtw-$F_{0,1,3}$-SAT is #P-complete. Here we improve this result by showing that #Pl-Rtw-Opp-$F_{0,1,3}$-SAT remains #P-complete.

If we use the same gadget as above, we have the following recursive relation:

$$\begin{bmatrix} a_i \\ b_i \\ c_i \end{bmatrix} = \begin{bmatrix} 8 & 8 & 0 \\ 8 & 12 & 4 \\ 8 & 16 & 8 \end{bmatrix} \begin{bmatrix} a_{i-1} \\ b_{i-1} \\ c_{i-1} \end{bmatrix}.$$

Unfortunately this matrix is singular and therefore we cannot use this recursive construction to do interpolation.

However we can use another gadget (Figure 4). Here again each vertex of degree 2 (resp. 3) shown in Figure 4 is assigned a signature $[0, 1, 0]$ (resp. $[1, 1, 0, 1]$).

Then we have a recursive relation:

$$\begin{bmatrix} a_i \\ b_i \\ c_i \end{bmatrix} = \begin{bmatrix} 0 & 2 & 0 \\ 1 & 1 & 1 \\ 2 & 2 & 0 \end{bmatrix} \begin{bmatrix} a_{i-1} \\ b_{i-1} \\ c_{i-1} \end{bmatrix}.$$

The characteristic polynomial is $x^3 - x^2 - 4x - 4$. It is easy to verify that it is irreducible over $\mathbf{Q}[x]$, and by Lemma 5.1, we know that this family of gadgets can be used for interpolation. As a result, $\#[0, 1, 0]|[1, 1, 0, 1]$ and $\#[0, 1, 0]|[1, 0, 1, 1]$ are #P-complete.

We summarize our treatment of problems of the form $\#[0, 1, 0]|[y_0, y_1, y_2, y_3]$: The cases where $[y_0, y_1, y_2, y_3] = [0, 0, 0, 0], [0, 0, 0, 1], [1, 0, 0, 0], [1, 1, 1, 1]$ are trivial signatures. The pair $[0, 0, 1, 0]$, $[0, 1, 0, 0]$ and the pair $[0, 0, 1, 1]$, $[1, 1, 0, 0]$ are both trivial by a counting argument. The pair $[0, 1, 0, 1]$ and $[1, 0, 1, 0]$ are solvable in P by Fibonacci gates. The Problem ICE $\#[0, 1, 0]|[0, 1, 1, 0]$ is solvable in P for planar graphs, but #P-complete for general graphs. The pair where $[y_0, y_1, y_2, y_3] = [0, 1, 1, 1]$ and $[1, 1, 1, 0]$ are #P-complete, dealt with as #Pl-Rtw-Opp-3CNF. The case $[1, 0, 0, 1]$ is trivial by a connectivity argument. Finally the pair $[1, 0, 1, 1]$ and $[1, 1, 0, 1]$ are #P-complete, dealt with as #Pl-Rtw-Opp-$F_{0,1,3}$-SAT. This completes all 16 cases of $\#[0, 1, 0]|[y_0, y_1, y_2, y_3]$.

All hard cases of the form $\#[1, 0, 1]|[y_0, y_1, y_2, y_3]$ have been proved in [21] using a different proof. We can reprove them in our framework to give a uniform treatment, but we omit the details here. In the Appendix we prove all the hardness results of the form $\#[1, 1, 0]|[y_0, y_1, y_2, y_3]$.

To recap for the side $[x_0, x_1, x_2]$ of arity 2, the cases $[0, 0, 0]$, $[0, 0, 1]$, $[1, 0, 0]$ and $[1, 1, 1]$ are trivial. The case $[0, 1, 0]$ is discussed above in detail. The proof for the pair $[0, 1, 1]$ and $[1, 1, 0]$ is presented in the Appendix. The case $[1, 0, 1]$ has been done in [21].

To sum up, we have the following table (we removed entries for degenerate signatures). In the table "T" means that it is computable in P-time by some trivial reasons; "F" means that it is computable in P-time by holographic algorithms with Fibonacci gates; "P" means that it is computable in P-time for planar graphs (by holographic algorithms with matchgates) but #P-complete for general graphs; and "H" means that it is #P-complete even for planar graphs.

$f_2 \mid g_3$	$[0, 1, 0]$	$[1, 0, 1]$	$[1, 1, 0]$
$[0, 0, 1, 0]$	T	P	T
$[0, 0, 1, 1]$	T	H	T
$[0, 1, 0, 0]$	T	P	H
$[0, 1, 0, 1]$	F	F	H
$[0, 1, 1, 0]$	P	P	H
$[0, 1, 1, 1]$	H	H	H
$[1, 0, 0, 1]$	T	T	H
$[1, 0, 1, 0]$	F	F	H
$[1, 0, 1, 1]$	H	F	H
$[1, 1, 0, 0]$	T	H	H
$[1, 1, 0, 1]$	H	F	F
$[1, 1, 1, 0]$	H	H	H

Theorem 6.1. *Every counting problem $\#[x_0, x_1, x_2]|[y_0, y_1, y_2, y_3]$, where $[x_0, x_1, x_2]$ and $[y_0, y_1, y_2, y_3]$ are Boolean signatures, is either (a) in P; or (b) #P-complete but solvable in P for planar graphs; or (c) #P-complete even for planar graphs. The results are summarized in the table (with some trivial cases removed.)*

Acknowledgments

We gratefully acknowledge helpful comments by Xi Chen, Madhu Sudan, Endre Szemeredi, Les Valiant and Avi Wigderson.

References

[1] Andrei A. Bulatov, Vctor Dalmau: Towards a dichotomy theorem for the counting constraint satisfaction problem. Inf. Comput. 205(5): 651-678 (2007)

[2] Andrei A. Bulatov, Martin Grohe: The complexity of partition functions. Theor. Comput. Sci. 348(2-3): 148-186 (2005)

[3] J-Y. Cai and Pinyan Lu. On Symmetric Signatures in Holographic Algorithms. In the proceedings of STACS 2007, LNCS Vol 4393, pp 429–440. Also available at Electronic Colloquium on Computational Complexity Report TR06-135.

[4] J-Y. Cai and Pinyan Lu. Holographic Algorithms: From Art to Science. In the proceedings of STOC 2007, pp 401-410.

[5] J-Y. Cai, Pinyan Lu and Mingji Xia. Holographic Algorithms by Fibonacci Gates. Submitted to FOCS 2008.

[6] Nadia Creignou, Miki Hermann: Complexity of Generalized Satisfiability Counting Problems. Inf. Comput. 125(1): 1-12 (1996)

[7] N. Creignou, S. Khanna and M. Sudan. Complexity classifications of boolean constraint satisfaction problems. SIAM Monographs on Discrete Mathematics and Applications. 2001.

[8] C. T. J. Dodson and T. Poston. *Tensor Geometry*, Graduate Texts in Mathematics 130, Second edition, Springer-Verlag, New York, 1991.

[9] Martin E. Dyer, Leslie Ann Goldberg, Mark Jerrum: The Complexity of Weighted Boolean #CSP CoRR abs/0704.3683: (2007)

[10] Martin E. Dyer, Leslie Ann Goldberg, Mike Paterson: On counting homomorphisms to directed acyclic graphs. J. ACM 54(6): (2007)

[11] Martin E. Dyer, Catherine S. Greenhill: The complexity of counting graph homomorphisms. Random Struct. Algorithms 17(3-4): 260-289 (2000)

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

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

[14] Lenstra, A. K.; Lenstra, H. W.; and Lovasz, L. ”Factoring Polynomials with Rational Coefficients.” Math. Ann. 261, 515-534, 1982.

[15] Salil P. Vadhan: The Complexity of Counting in Sparse, Regular, and Planar Graphs. SIAM J. Comput. 31(2): 398-427 (2001)

[16] L. Trevisan, G. B. Sorkin, M. Sudan and D. P. Williamson. Gadgets, Approximation, and Linear Programming. SIAM J. on Computing, 29 (6): 2074–2097, 2000.

[17] L. G. Valiant: The Complexity of Computing the Permanent. Theor. Comput. Sci. 8: 189-201 (1979)

[18] Leslie G. Valiant: Quantum Circuits That Can Be Simulated Classically in Polynomial Time. SIAM J. Comput. 31(4): 1229-1254 (2002)

[19] L. G. Valiant. Holographic Algorithms (Extended Abstract). In *Proc. 45th IEEE Symposium on Foundations of Computer Science*, 2004, 306–315. A more detailed version appeared in ECCC Report TR05-099.

[20] L. G. Valiant. Accidental Algorithms. In *Proc. 47th Annual IEEE Symposium on Foundations of Computer Science* 2006, 509–517.

[21] Mingji Xia, Peng Zhang, Wenbo Zhao: Computational complexity of counting problems on 3-regular planar graphs. Theor. Comput. Sci. 384(1): 111-125 (2007)

7 Figures

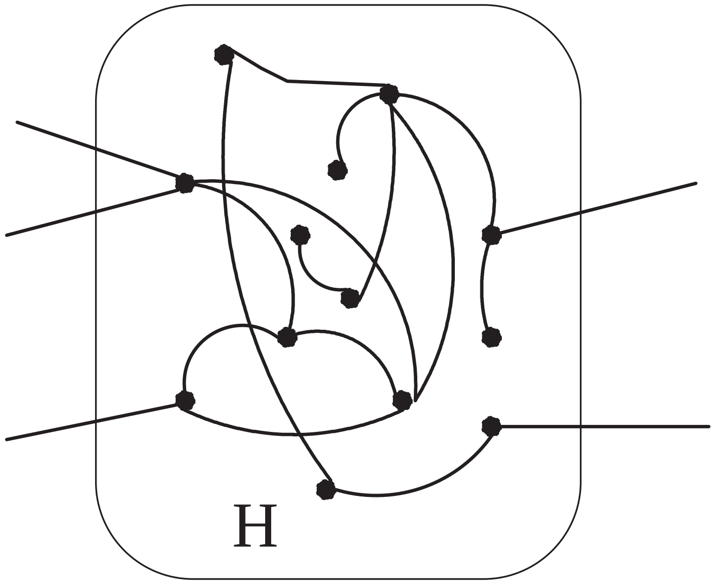

Figure 1: An example of $\mathcal{F}$-gate with five dangling edges.

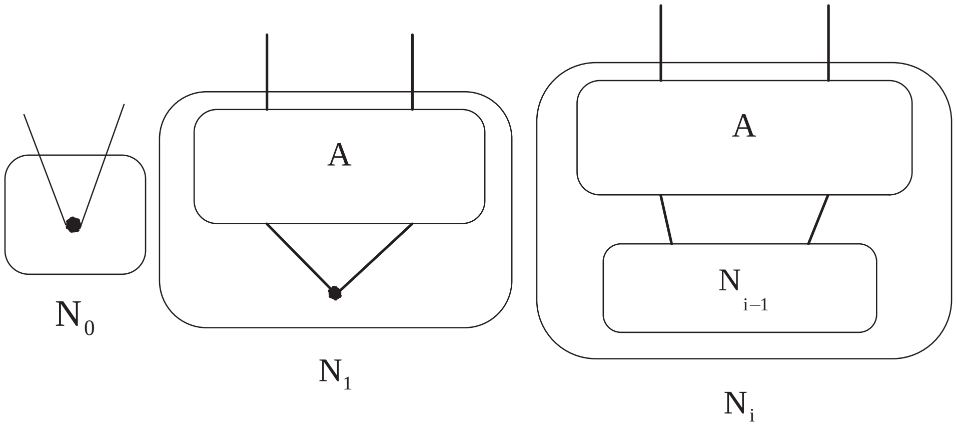

Figure 2: Recursive construction

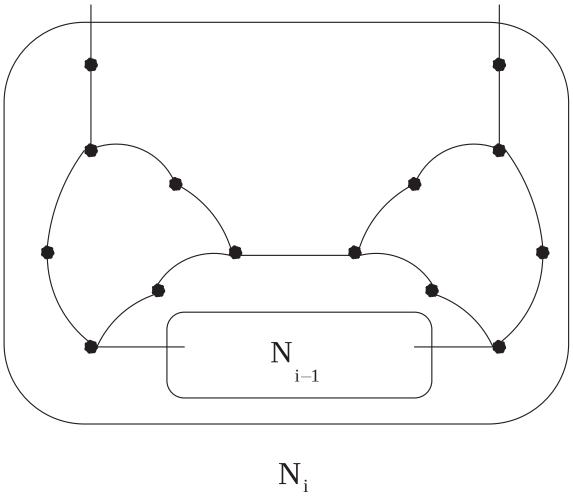

Figure 3: Gadget 1.

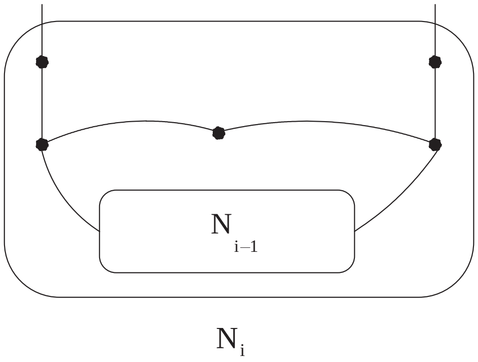

Figure 4: Gadget 2.

Appendix

8 More Hardness Results

In this section, we go over all the cases of the form $\#[1,1,0]|[y_0,y_1,y_2,y_3]$.

First we remark that it has already been noted in Section 6 that the following problems $\#[1,1,0]|[0,0,1,0]$ and $\#[1,1,0]|[0,0,1,1]$ are trivial by a counting argument. Also the problem $\#[1,1,0]|[1,1,0,1]$ is solvable in P by Fibonacci gates.

Now we discuss hardness. All the proofs here will be given by the same proof technique, using the two gadgets in Figures 3 and 4.

The first problem we consider is $\#[1,1,0]|[0,1,0,0]$. Using gadget 2 in Figures 4 we derive the following recursive relation:

$$\begin{bmatrix} a_i \\ b_i \\ c_i \end{bmatrix} = \begin{bmatrix} 3 & 4 & 1 \\ 1 & 3 & 1 \\ 0 & 2 & 1 \end{bmatrix} \begin{bmatrix} a_{i-1} \\ b_{i-1} \\ c_{i-1} \end{bmatrix}.$$

The characteristic polynomial is $x^3 - 7x^2 + 9x - 1$. It is easy to verify that it is irreducible over $\mathbf{Q}[x]$. Then by Lemma 5.1, we know that interpolation succeeds. Hence, $\#[1,1,0]|[0,1,0,0]$ is #P-complete.

In the following, the reasoning in each case is identical. We will only list the problem, the gadget used, the recursive relation from N_{i-1} to N_i, and the characteristic polynomial.

Problem $\#[1,1,0]|[0,1,0,1]$. We use gadget 2 and get:

$$\begin{bmatrix} a_i \\ b_i \\ c_i \end{bmatrix} = \begin{bmatrix} 3 & 6 & 3 \\ 1 & 3 & 2 \\ 0 & 2 & 1 \end{bmatrix} \begin{bmatrix} a_{i-1} \\ b_{i-1} \\ c_{i-1} \end{bmatrix}.$$

The characteristic polynomial is $x^3 - 7x^2 + 5x + 3$.

Problem $\#[1,1,0]|[0,1,1,0]$. We use gadget 2 and get:

$$\begin{bmatrix} a_i \\ b_i \\ c_i \end{bmatrix} = \begin{bmatrix} 5 & 14 & 8 \\ 1 & 6 & 5 \\ 0 & 2 & 3 \end{bmatrix} \begin{bmatrix} a_{i-1} \\ b_{i-1} \\ c_{i-1} \end{bmatrix}.$$

The characteristic polynomial is $x^3 - 14x^2 + 39x - 14$.

Problem $\#[1,1,0]|[0,1,1,1]$. We use gadget 1 and get:

$$\begin{bmatrix} a_i \\ b_i \\ c_i \end{bmatrix} = \begin{bmatrix} 477 & 2120 & 2332 \\ 125 & 634 & 778 \\ 32 & 186 & 259 \end{bmatrix} \begin{bmatrix} a_{i-1} \\ b_{i-1} \\ c_{i-1} \end{bmatrix}.$$

The characteristic polynomial is $x^3 - 1370x^2 + 105835x - 352450$.

Problem $\#[1,1,0]|[1,0,0,1]$ is Matching.

Problem $\#[1,1,0]|[1,0,1,0]$. We use gadget 2 and get:

$$\begin{bmatrix} a_i \\ b_i \\ c_i \end{bmatrix} = \begin{bmatrix} 3 & 6 & 3 \\ 2 & 3 & 1 \\ 1 & 2 & 0 \end{bmatrix} \begin{bmatrix} a_{i-1} \\ b_{i-1} \\ c_{i-1} \end{bmatrix}.$$

The characteristic polynomial is $x^3 - 6x^2 - 8x - 3$.

Problem #[1, 1, 0]|[1, 0, 1, 1]. We use gadget 2 and get:

$$\begin{bmatrix} a_i \\ b_i \\ c_i \end{bmatrix} = \begin{bmatrix} 3 & 8 & 5 \\ 2 & 4 & 1 \\ 1 & 2 & 0 \end{bmatrix} \begin{bmatrix} a_{i-1} \\ b_{i-1} \\ c_{i-1} \end{bmatrix}.$$

The characteristic polynomial is $x^3 - 7x^2 - 11x - 2$.

Problem #[1, 1, 0]|[1, 1, 0, 0]. We use gadget 2 and get:

$$\begin{bmatrix} a_i \\ b_i \\ c_i \end{bmatrix} = \begin{bmatrix} 8 & 6 & 1 \\ 5 & 5 & 1 \\ 3 & 4 & 1 \end{bmatrix} \begin{bmatrix} a_{i-1} \\ b_{i-1} \\ c_{i-1} \end{bmatrix}.$$

The characteristic polynomial is $x^3 - 14x^2 + 16x - 1$.

Problem #[1, 1, 0]|[1, 1, 1, 0]. We use gadget 1 and get:

$$\begin{bmatrix} a_i \\ b_i \\ c_i \end{bmatrix} = \begin{bmatrix} 7191 & 12618 & 5535 \\ 3816 & 6723 & 2961 \\ 2025 & 3582 & 1584 \end{bmatrix} \begin{bmatrix} a_{i-1} \\ b_{i-1} \\ c_{i-1} \end{bmatrix}.$$

The characteristic polynomial is $x^3 - 15498x^2 + 419904x - 19683$.

In all problems listed above, it is easy to verify that the characteristic polynomial is irreducible over $\mathbf{Q}[x]$. By applying Lemma 5.1, interpolation succeeds, and as a result the corresponding problem is #P-complete.

For some of the problems listed in the table of Section 6, in order to apply Theorem 4.1 we have to consider the reversal signatures $[y_3, y_2, y_1, y_0]$. For all these problems (except one) the reversal does not change the $[x_0, x_1, x_2]$ side at all. But for the last problem #[1, 1, 0] | [1, 1, 1, 0] this reversal gives #[0, 1, 1] | [0, 1, 1, 1]. However in the proof using gadget 1 for this problem, if we reverse all 0's and 1's in edge assignments, we will obtain a linear recurrence for #[0, 1, 1] | [0, 1, 1, 1] with the matrix which is the double reversal of rows and columns of the matrix for #[1, 1, 0] | [1, 1, 1, 0]. Thus it will have the same characteristic polynomial, and the same proof works.

This completes the discussion for the problems of the form #[1, 1, 0]|$[y_0, y_1, y_2, y_3]$.

9 The Proof of the Algebraic Lemma

We now discuss when the condition in (5) is satisfied, and give a proof of Lemma 5.1.

Let $f(x) = x^3 + c_2x^2 + c_1x + c_0 \in \mathbf{Q}[x]$ be a cubic polynomial with rational coefficients. Let α, β and γ be its three roots, and let $\mathbf{F} = \mathbf{Q}(\alpha, \beta, \gamma)$ be the splitting field of f over $\mathbf{Q}$, then $\mathbf{F}$ is a Galois extension of degree $[\mathbf{F} : \mathbf{Q}] \in \{1, 2, 3, 6\}$, depending on whether f has three rational roots, or exactly one rational root, or no rational root.

In the first case where $\alpha, \beta, \gamma \in \mathbf{Q}$, condition (5) is a question on the linear dependence of the exponents of α, β, γ with respect to various prime factors. More precisely, if $p_1, p_2, \ldots, p_m$ are all the prime factors appearing in the numerators and denominators of α, β, γ, and we can write α, β, γ as integer vectors in $\mathbf{Z}^m$, i.e., we write α as $(\mathrm{ord}_{p_1}(\alpha), \ldots, \mathrm{ord}_{p_m}(\alpha))$, and similarly for β and γ, where $\mathrm{ord}_{p_i}(\alpha)$ is the exact order (possibly negative) of the prime p_i which appears in α. Then the set of integer solutions (i, j, k) to (5) is a lattice (possibly trivial, namely just $(0, 0, 0)$). A basis of this lattice exists, consisting of zero or more vectors. If the prime factors p_i are known, then this can be easily computed. But even if the prime factorizations are unknown, a basis exists with absolute values of i, j, k

at most polynomially bounded in the binary input length of α, β, γ. Thus one can directly search and find it (either it is trivial $(0,0,0)$, or a small non-trivial basis is found in polynomial time.)

Next we suppose f has exactly one rational root α and $f(x) = (x-\alpha)g(x)$, where $g(x) \in \mathbf{Q}[x]$ is irreducible in $\mathbf{Q}[x]$. In this case the Galois extension has degree $[\mathbf{F} : \mathbf{Q}] = 2$. If (5) holds for some integers (i, j, k), this gives a relation $\beta^j \gamma^k \in \mathbf{Q}$. We first assume $j \neq k$. As γ is the (real or complex) conjugate $\overline{\beta}$ of β, we have $\beta\overline{\beta} \in \mathbf{Q}$. It follows that for some integer $\ell \neq 0$, $\beta^\ell \in \mathbf{Q}$. By taking reciprocal, clearly we can take $\ell > 0$. There are two cases. (I) If β is real, then $\beta = r + r'\sqrt{s}$ for some rational r, some non-zero rational r' and a positive square-free integer $s > 1$. If $r = 0$, then g is of the form $g(x) = x^2 - c$, for a positive nonsquare c, and in this case, (5) is indeed possible and we can easily find all solutions. Suppose $r \neq 0$. By replacing $\overline{\beta}$ for β, we may assume $rr' > 0$. In this case we claim β^ℓ is never in $\mathbf{Q}$ for $\ell > 0$. This is clearly seen if we collect all the terms in the expansion $(r + r'\sqrt{s})^{2\ell}$ corresponding to an odd power of $r'\sqrt{s}$; it is a positive rational multiple of $\sqrt{s}$ and thus can not be canceled out. (II) If β is not real, then both $\beta^\ell \in \mathbf{Q}$ and $\overline{\beta}^\ell = \beta^\ell \in \mathbf{Q}$. This implies that $(\beta/\overline{\beta})^\ell = 1$ and $\beta/\overline{\beta}$ is an ℓ-th root of unity in the degree 2 extension $\mathbf{F}$. Consider the minimal ℓ, we can assume the root of unity is primitive. If ξ is a t-th primitive root of unity then the cyclotomic polynomial $\Phi_t(x) \in \mathbf{Q}[x]$ is irreducible and is the minimal polynomial of ξ. Then any field $\mathbf{F}$ which contains ξ must have degree $[\mathbf{F} : \mathbf{Q}]$ divisible by $\varphi(t) = \deg \Phi_t$. Since our $[\mathbf{F} : \mathbf{Q}] = 2$, from the formula of the Euler's totient function $\varphi(t)$, it follows that the only possible values for ℓ are $\ell = 1, 2, 3, 4, 6$. $\ell = 1$ is impossible since in that case $\beta = \gamma = \overline{\beta}$, and $g(x)$ has double roots, and therefore not irreducible. $\ell = 2$ means that $\beta = -\overline{\beta}$, and this is the case $g(x) = x^2 + c$ for a rational $c > 0$. In this case (5) is indeed possible, and by a similar analysis as above we can find all the solutions in polynomial time. The case $\ell = 4$ is $\beta = \pm i\gamma$. But by being a conjugate, $\beta = \overline{\gamma}$, it implies that $\beta = \pm|\beta|(1 \pm i)/\sqrt{2}$. By taking the trace, $\pm|\beta|\sqrt{2}$ must be rational. It follows that $\beta = (1 \pm i)r$, for some rational r. Thus g is of the form $g(x) = x^2 - 2rx + 2r^2$. In this case (5) is possible, and all solutions can be found in polynomial time. Next consider the case $\ell = 3$. A similar analysis shows that $\beta = \omega r$ and $\gamma = \overline{\omega} r$ for some rational r. And then g takes the form $g(x) = x^2 + rx + r^2$. Finally for the case of γ/β being a 6th primitive root of unity, we can show by a similar analysis that g takes the form $g(x) = x^2 + 3rx + 3r^2$ for some rational r. Again in this case, all solutions to (5) can be found in polynomial time.

Now we assume $j = k$ in $\beta^j \gamma^k \in \mathbf{Q}$. As $\beta\overline{\beta}$ is indeed rational, the solutions, if they exist, are of the form $\alpha^{-2j}\beta^j\gamma^j = \alpha^{-2j}(\beta\overline{\beta})^j = 1$. This is again a problem on the linear dependence relation on the prime exponents, and can be similarly dealt with as before.

Lemma 9.1. *If $f(x) = x^3 + c_2x^2 + c_1x + c_0 \in \mathbf{Q}[x]$ is reducible over $\mathbf{Q}[x]$, either $(x-\alpha)(x-\beta)(x-\gamma)$ or $(x-\alpha)g(x)$ where g is irreducible, we can find all solutions to (5) in polynomial time. The computation, with the following exceptions, reduces to finding a linear dependence lattice on the exponents of prime factors of rationals. The exceptional cases are those involving roots of unity of order 3, 4 and 6, and where $g(x)$ takes the forms $x^2 + r$, $x^2 + rx + r^2$, $x^2 + 2rx + 2r^2$, or $x^2 + 3rx + 3r^2$, where $r \in \mathbf{Q}$.*

Finally we come to the case where $f(x)$ has no rational root, which is the same as $f(x)$ is irreducible. In this case, the Galois group is either isomorphic to $\mathbf{Z}_3$ or S_3. In either case it is transitive.

Suppose f has three distinct real roots. In absolute values they must be distinct. Otherwise, say $|\alpha| = |\beta|$. As $f(x)$ is irreducible over a field of characteristic 0, it has no multiple roots. Therefore $\alpha = -\beta$. But then the trace $\alpha + \beta + \gamma = \gamma$ is a rational root, contradicting $f(x)$ being irreducible. If $\alpha^i\beta^j\gamma^k = 1$, where $i + j + k = 0$, and suppose one exponent is 0, say $i = 0$, then $k = -j$. Being a non-trivial solution, $k \neq 0$, and β/γ is a root of unity. Being real, the only possibilities are ±1, both contradicting f being irreducible. If no exponent is 0, then we may assume two of them are positive and one is negative, say, $\alpha^i\beta^j = \gamma^{i+j}$, where $i, j > 0$. By a transitive permutation on the three roots we may assume in the above $|\alpha| < |\beta| < |\gamma|$. This implies that $|\alpha^i\beta^j| < |\gamma^{i+j}|$, a contradiction. Thus when f is irreducible and it has three distinct real roots, there are no non-trivial solutions to (5).

Lemma 9.2. *Let $f(x) = x^3 + c_2x^2 + c_1x + c_0 \in \mathbf{Q}[x]$ be a cubic irreducible polynomial with rational coefficients. If f has three distinct real roots, α, β and γ, then $\forall i, j, k \in \mathbf{Z}, i + j + k = 0$, other than $(0, 0, 0), \alpha^i\beta^j\gamma^k \neq 1$.*

Lastly we consider the case where $f(x)$ is irreducible, but it has exactly one real root (and two complex conjugate roots.) In this case $[\mathbf{F} : \mathbf{Q}] = 6$ and the Galois group is S_3. We now suppose in this case $\alpha^i\beta^j\gamma^k = 1$, and $i + j + k = 0$. We assume at least one pair among the exponents (i, j, k) are distinct integers, for otherwise $i = j = k = 0$ is the trivial case. Let's suppose $i \neq j$. Since the Galois group in this case is S_3, we can assume α is real by a permutation. Also by a permutation we have $\beta^i\alpha^j\gamma^k = 1$. This implies that the ratio β/α is a root of unity. Since f is irreducible, clearly it is not the case that $\alpha = \pm\beta$. Thus we have a certain primitive root of unity of order at least 3 in the field $\mathbf{F}$ of degree $[\mathbf{F} : \mathbf{Q}] = 6$. This leads to the following cases of possible primitive roots of order $7, 9, 14, 18$ in addition to the previous cases of $1, 2, 3, 4, 6$.

We already showed that it must be at least 3. Suppose the order of β/α is 4, i.e., $\beta/\alpha = \pm i$, then, the trace $\alpha + \alpha i - \alpha i = \alpha$ would be rational, a contradiction. Suppose the order of β/α is 6, i.e., $\beta/\alpha = \pm e^{2\pi i/6} = \frac{1}{2} \pm i\frac{\sqrt{3}}{2}$. Again taking trace, we have a contradiction $2\alpha \in \mathbf{Q}$. If a 7th primitive root of unity belongs to $\mathbf{F}$, then there is a cyclic element of the Galois group of order 6, acting on the 7th roots of unity by $x \mapsto x^3$. But clearly the Galois group $\mathrm{Gal}(\mathbf{F}/\mathbf{Q}) = S_3$ has no such element. The situation of a 14th primitive root of unity reduces to that of a 7th primitive root of unity. Similarly, if there is a 9th primitive root of unity belonging to $\mathbf{F}$, then there is a cyclic element of the Galois group of order 6, acting on the 9th roots of unity by $x \mapsto x^2$. Again S_3 has no such element. Also the situation of a 18th primitive root of unity reduces to that of a 9th primitive root of unity.

The only case left is that β/α is a primitive root of unity of order 3, i.e., $\beta/\alpha = \omega$ or $\overline{\omega}$. In this case, the polynomial f must be $x^3 + c$ for some $c \in \mathbf{Q}$ not a cubic power of a rational. In this case there are indeed non-trivial solutions to (5), and again all solutions to (5) can be computed in polynomial time. This finishes all the cases.

We note that for a given $f(x) \in \mathbf{Q}[x]$, one can decide in polynomial time, first its irreducible factorization [14], and then find all solutions to (5) in all the cases discussed above. Thus the criterion of (5) is effective. (In fact factorization of f in this case can be done easier than LLL, e.g., we can use Sturm's sequence and a sufficiently good rational approximation to find its rational roots, if any exists.)

Theorem 9.1. *In all cases, we can decide in polynomial time for $f(x) = x^3 + c_2x^2 + c_1x + c_0 \in \mathbf{Q}[x]$, whether any non-trivial solutions to (5) exists, and if so, find all solutions. In particular if f is irreducible, except of the form $x^3 + c$ for some $c \in \mathbf{Q}$, there are no non-trivial solutions to (5).*

10 Tractable Cases are not Interpolatable

Assuming that P $\neq$ #P, then "interpolatable implies hardness" implies that "tractable cases are not interpolatable". However, in this section, we will unconditionally and algebraically prove that all the known tractable cases, i.e., the degenerate cases, Fibonacci gates, and planar matchgates, indeed cannot be used to do interpolation.

All the proofs are actually unified. Because all the signatures realizable in these tractable cases satisfy some homogeneous identities, such as Matchgate Identities for matchgate signatures.

We will be brief here. Assume for a contradiction that signatures $F_1, F_2, \ldots, F_m$ can be used to interpolate all the signatures of arity n. We assume that K is the number of the target signature involved in the problem. Then the coefficients are exactly all the K-th homogeneous terms of the entries of the signature F_i. Since all the signatures $F_1, F_2, \ldots, F_m$ are realizable, they satisfy some homogeneous identity. We can pad it to a homogeneous identity of degree K and this is a linear dependence among the coefficients of the linear system. Therefore the linear system is degenerate and can not be used to do interpolation.

11 The Proof for a Claim in Subsection 6.2

Theorem 11.1. $\#[0,1,0]|[0,1,1,0]$ *can be used to interpolate all the signatures of the form* $[a,b,a]$.

Proof: The proof technique are similar to that of section 6 and 8. We use gadget 2 for a recursive construction. However all the signatures have the further symmetry that they have the form $[a,b,a]$. We use $[a_i,b_i,a_i]$ to denote the signature of the i-th gadget. Then we have the following recursive relation:

$$\begin{bmatrix} a_i \\ b_i \end{bmatrix} = \begin{bmatrix} 2 & 2 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} a_{i-1} \\ b_{i-1} \end{bmatrix}.$$

Then by the Lemma of Vadhan [15], we can verify that this can be used to interpolate all the signatures of the form $[a,b,a]$.

12 Some Remarks

We make some remarks on the proof methodology. As can be seen all the hardness results in this paper are proved by a uniform method. The general principle is simplification using holographic reductions followed by interpolation. The success of interpolation depends on an algebraic lemma whose proof uses some basic Galois theory, but the actual interpolation using the lemma must be carried out by specific gadgets, case by case.

It is these specific gadgets we wish to comment further. Somewhat unlike a typical NP-hardness proof, here the gadgets are fairly generic, without any particular built-in design purpose. In a typical NP-hardness proof, we usually design a particular gadget with some definite functionality built-in, e.g., as a truth setting component related to a SAT problem. Here there is no apparent custom designed feature, except, since the conditions of the algebraic lemma are fairly general, one expects that a generic gadget will work (if the underlying problem is indeed hard). Whether this is always true remains an interesting question. In forthcoming work we will report some partial results in this direction.

There is another aspect of the proof methodology that is worth commenting. When we design a gadget using e edges for interpolation in this framework, the theory dictates that we must compute the transition matrix from N_s to N_{s+1} for their respective signatures. The computation of this matrix is in fact not a trivial matter, involving 2^e steps in the worst case for each entry. In our proofs we simply presented these matrices as a matter of fact, without giving any efficient way to verify these. This is a marked departure from the practice in typical NP-hardness proofs, where we usually have a built-in structure in the gadget which ensures that there are only a few cases to be examined, in order for us to "understand" the gadget. Here this "understanding" comes at a cost of 2^e steps of computation. If we usually equate NP as a proof system with an efficient verification, then these interpolation proofs fit tenuously at best. One can easily contemplate moderately sized gadgets with over 50 or 100 edges, say, and then to verify a particular gadget works, it may require the computation of 2^{100} steps, far exceeding most cryptosystems such as DES. Moreover these computations are in fact being treated as constants when we use them to prove #P-completeness.

Suppose we arrive at a #P-hardness proof by interpolation using such a gadget, and we can't find a smaller gadget for this purpose. Then are we at a point where we are making a structural distinction of P versus #P-hardness, but the only way we know how to make this distinction is to treat 2^{100}-step computation as a constant, and thus "trivial" according to the usual tenet of complexity theory? We remark that in the paper [16] by Trevisan et. al. a similar situation was discussed, where one had to search in a huge but constant sized space for an optimal gadget.