Holographic Algorithms: From Art to Science

Jin-Yi Cai *
Computer Sciences Department
University of Wisconsin
Madison, WI 53706, USA
jyc@cs.wisc.edu

Pinyan Lu †
Computer Sciences Department
Tsinghua University
Beijing, 100084, P. R. China
lpy@mails.tsinghua.edu.cn

ABSTRACT

We develop the theory of holographic algorithms. We define a basis manifold and give characterizations of algebraic varieties of realizable symmetric generators and recognizers on this manifold. We present a polynomial time decision algorithm for the simultaneous realizability problem. Using the general machinery we are able to give unexpected holographic algorithms for some counting problems, modulo certain Mersenne type integers. These counting problems are #P-complete without the moduli. Going beyond symmetric signatures, we define d-admissibility and d-realizability for general signatures, and give a characterization of 2-admissibility.

Categories and Subject Descriptors:
F. Theory of Computation.
F.2 Analysis of Algorithms and Problem Complexity.
General Terms:
Algorithms, Theory.
Keywords:
Holographic algorithms, matchgates, signatures.

1. INTRODUCTION

It has become more or less an article of faith among theoretical computer scientists that the *conjecture* P $\neq$ NP holds. Certainly there are good reasons to believe this assertion, not the least of which is the fact that the usual algorithmic paradigms seem unable to handle any of the NP-hard problems. Such statements are made credible by decades of in-depth study of these methodologies.

To be sure, there are some "surprising" polynomial time algorithms for problems which, on appearance, would seem to require exponential time. One such example is to count the number of perfect matchings in a planar graph (the FKT method) [18, 19, 25]. In [27, 29] Valiant introduced *holographic algorithms*—a truly original algorithmic design technique. Computation in these algorithms is expressed and interpreted through a choice of linear basis vectors in an exponential "holographic" mix, and then it is carried out by the FKT method via the Holant Theorem. This methodology has produced polynomial time algorithms for a variety of problems ranging from restrictive versions of Satisfiability, Vertex Cover, to other graph problems such as edge orientation and node/edge deletion. No polynomial time algorithms were known for any of these problems, and some minor variations are known to be NP-hard.

These holographic algorithms are quite unusual compared to other kinds of algorithms (except perhaps quantum algorithms). At the heart of the computation is a process of introducing and then canceling exponentially many computational fragments. Invariably the success of this methodology on a particular problem boils down to finding a certain "exotic" object represented by a *signature*.

For example, Valiant showed [32] that the restrictive SAT problem $\#_7$Pl-Rtw-Mon-3CNF (counting the number of satisfying assignments of a planar read-twice monotone 3CNF formula, modulo 7) is solvable in P. The same problem #Pl-Rtw-Mon-3CNF without mod 7 is known to be #P-complete; the problem mod 2, $\#_2$Pl-Rtw-Mon-3CNF, is known to be $\oplus$P-complete (thus NP-hard). The surprising tractability mod 7 is due to the existence of an unexpected signature over $\mathbf{Z}_7$.

These signatures are specified by families of algebraic equations. These families of equations are typically exponential in size. Finding a solution will imply the solvability of a problem in P. In his "Accidental Algorithm" paper [32] Valiant makes the case that "the situation with the P = NP question is not dissimilar to that of other unresolved enumerative conjectures in mathematics. The possibility that accidental or freak objects in the enumeration exist cannot be discounted." However, dealing with such algebraic equations can be difficult due to the exponential size. So far the successes have been an expression of *artistic* inspirations.

To sustain our belief in P $\neq$ NP, we must start to develop a systematic understanding of the capabilities of holographic algorithms. Some may consider the problems such as $\#_7$Pl-Rtw-Mon-3CNF that have been solved in this framework a little contrived. But the point is that when we surveyed potential algorithmic approaches with P vs. NP in mind, these algorithms were not part of the repertoire. Presumably the same "intuition" for P $\neq$ NP would have applied equally to $\#_7$Pl-Rtw-Mon-3CNF and to $\#_2$Pl-Rtw-Mon-3CNF. Thus,

*Supported by NSF CCR-0511679.

†Supported by the National Natural Science Foundation of China Grant 60553001 and the National Basic Research Program of China Grant 2007CB807900, 2007CB807901.

STOC'07, June 11–13, 2007, San Diego, California, USA.

Valiant suggested in [29], "any proof of P $\neq$ NP may need to explain, and not only to imply, the unsolvability" of NP-hard problems using this approach.

While finding "exotic" solutions such as the signature for $\#_7$Pl-Rtw-Mon-3CNF is inspired artistry, the situation with ever more complicated algebraic constraints on such signatures (for other problems) can quickly overwhelm such an artistic approach (as well as a computer search). At any rate, failure to find such solutions to a particular algebraic system yields no proof that such solutions do not exist, and it generally does not give us any insight as to why. We need a more *scientific* understanding. The aim of this paper is to build toward such an understanding.

We have achieved a complete account of the realizable symmetric signatures. Using this we can show why the modulus 7 happens to be *the* modulus that works for $\#_7$Pl-Rtw-Mon-3CNF. Underlying this is the fact that 7 is 2^3-1, and for any odd prime p, any prime factor q of the Mersenne number 2^p-1 has $q \equiv \pm 1 \bmod 8$, and therefore 2 is a quadratic residue in $\mathbf{Z}_q$. Generalizing this, we show that $\#_{2^k-1}$Pl-Rtw-Mon-kCNF is in P for all $k \geq 3$ (the problem is trivial for $k \leq 2$). Furthermore, no suitable signatures exist for any modulus other than factors of 2^k-1 for this problem.

When designing a holographic algorithm for any particular problem, the essential step is to decide whether there is a basis for which certain signatures of both generators and recognizers can be simultaneously realized (a quick review of terminologies is given in Section 2.) Frequently these signatures are symmetric signatures. Our understanding of symmetric signatures has advanced to the point where it is possible to give a polynomial time algorithm to decide the simultaneous realizability problem. If a matchgate has arity n, the signature has size 2^n. However for symmetric signatures we have a compact form, and the running time of the decision algorithm is measured in n. Followed from this structural understanding we can give (i) a complete account of all the previous successes of holographic algorithms using symmetric signatures [29, 5, 32]; (ii) generalizations such as $\#_{2^k-1}$Pl-Rtw-Mon-kCNF and a similar problem for Vertex Cover, when this is possible; and (iii) a proof when this is not possible. This should be considered an important step in our understanding of holographic algorithms, from *art* to *science*.

In order to investigate realizability of signatures, we found it useful to introduce a basis manifold $\mathcal{M}$, which is defined to be the set of all possible bases modulo an equivalence relation. This is a useful language for the discussion of symmetric signatures; it becomes essential for the general signatures. We define the notions of d-admissibility and d-realizability. To be d-admissible is to have a d-dimensional solution subvariety in $\mathcal{M}$, satisfying all the parity requirements. These are part of the requirements for the bases to satisfy in order to be realizable. To be d-realizable is to have a d-dimensional solution subvariety in $\mathcal{M}$ for all realizability requirements, which include the parity requirements as well as the *useful Grassmann-Plücker identities* [5, 28], called the matchgate identities. To have 0-realizability is a necessary condition. But to get holographic algorithms one needs simultaneous realizability of both generators and recognizers. This is accomplished by having a non-empty intersection of the respective subvarieties for the realizability of generators and recognizers. And this tends to be accomplished by having d-realizability (which implies d-admissibility), for $d \geq 1$, on at least one side. Therefore it is important to investigate d-realizability and d-admissibility for $d \geq 1$. We give a complete characterization of 2-admissibility. We also have some general results concerning 1-admissibility and on 1- or 2-realizable families. These will be reported in the future.

This paper is organized as follows. In Section 3 we define the basis manifold $\mathcal{M}$ which will be used to express our results throughout. In Section 4 we describe our results on simultaneous realizability of recognizers and generators, culminating in the polynomial time decision procedure. In Section 5 we describe our results on $\#_{2^k-1}$Pl-Rtw-Mon-kCNF and on Vertex Cover. Further illustrations of the power of the general machinery are given in Section 6. In Section 7 we go beyond symmetric signatures, and give some general results regarding d-admissibility and d-realizability.

2. SOME BACKGROUND

In this section we review some definitions and results. More details can be found in [27, 29, 28, 5, 4, 3, 30, 31].

Let $G = (V, E, W)$, $G' = (V', E', W')$ be weighted undirected planar graphs. A *generator matchgate* Γ is a tuple (G, X) where $X \subset V$ is a set of external *output* nodes. A *recognizer matchgate* Γ' is a tuple (G', Y) where $Y \subset V'$ is a set of external *input* nodes. The external nodes are ordered counter-clock wise on the external face. Γ is called an odd (resp. even) matchgate if it has an odd (resp. even) number of nodes.

Each matchgate is assigned a *signature* tensor. A generator Γ with m output nodes is assigned a contravariant tensor $\mathbf{G} \in V_0^m$ of type $\binom{m}{0}$. This tensor under the standard basis $\mathbf{b}$ has the form

$$\sum G^{i_1 i_2 \dots i_m} \mathbf{b}_{i_1} \otimes \mathbf{b}_{i_2} \otimes \cdots \otimes \mathbf{b}_{i_m},$$

where $G^{i_1 i_2 \dots i_m} = \text{PerfMatch}(G - Z)$, is the sum of products of matching edge weights over all perfect matchings $\text{PerfMatch}(G - Z) = \sum_M \prod_{(i,j) \in M} w_{ij}$, and Z is the subset of the output nodes having the characteristic sequence $\chi_Z = i_1 i_2 \dots i_m$. Similarly a recognizer Γ' with m input nodes is assigned a covariant tensor $\mathbf{R} \in V_m^0$ of type $\binom{0}{m}$. This tensor under the standard (dual) basis $\mathbf{b}^*$ has the form

$$\sum R_{i_1 i_2 \dots i_m} \mathbf{b}^{i_1} \otimes \mathbf{b}^{i_2} \otimes \cdots \otimes \mathbf{b}^{i_m},$$

where $R_{i_1 i_2 \dots i_m} = \text{PerfMatch}(G' - Z)$, and Z is the subset of the input nodes having $\chi_Z = i_1 i_2 \dots i_m$.

In particular, $\mathbf{G}$ transforms as a contravariant tensor, and $\mathbf{R}$ transforms as a covariant tensor, under a basis transformation.

A signature is symmetric, if each entry only depends on the Hamming weight of the index. This notion is invariant under basis transformations. A symmetric signature is denoted by $[\sigma_0, \sigma_1, \dots, \sigma_m]$.

A *matchgrid* $\Omega = (A, B, C)$ is a weighted planar graph consisting of a disjoint union of: a set of g generators $A = (A_1, \dots, A_g)$, a set of r recognizers $B = (B_1, \dots, B_r)$, and a set of f connecting edges $C = (C_1, \dots, C_f)$, where each C_i edge has weight 1 and joins an output node of a generator with a input node of a recognizer, so that every input and output node in every constituent matchgate has exactly one such incident connecting edge.

Let $\mathbf{G} = \bigotimes_{i=1}^{g} \mathbf{G}(A_i)$ be the tensor product of all the generator signatures, and let $\mathbf{R} = \bigotimes_{j=1}^{r} \mathbf{R}(B_j)$ be the tensor

product of all the recognizer signatures. Then Holant(Ω) is defined to be the contraction of the two product tensors, under some basis $\boldsymbol{\beta}$, where the corresponding indices match up according to the f connecting edges in C.

The remarkable Holant Theorem is

THEOREM 2.1 (VALIANT). *For any matchgrid Ω over any basis $\boldsymbol{\beta}$, let G be its underlying weighted graph, then*

$$\text{Holant}(\Omega) = \text{PerfMatch}(G).$$

A development of Valiant's framework with covariant and contravariant tensors and a proof of the Holant Theorem using these concepts can be found in [4].

The FKT algorithm can compute the perfect matching polynomial PerfMatch(G) for a planar graph in polynomial time. This algorithm gives an orientation of the edges of the planar graph, which assigns a ± 1 factor to each edge weight. It then evaluates the Pfaffian of the skew-symmetric matrix of the graph.

Pfaffians satisfy the Grassmann-Plücker identities [24]. A set of so-called *useful* Grassmann-Plücker identities have been proved to characterize planar matchgate signatures [28, 3, 5]. These are called Matchgate Identities.

Matchgate computations also have interesting connections to quantum computing, in particular, what fragments of quantum computation can be simulated classically (cf. [27] and Knill-Gottesman theorem [13]. See also [1, 21, 10].) In this paper we will not discuss this connection.

We state some theorems from [6], which will be used.

THEOREM 2.2. *(Thm. 3 in [6], p. 436) A symmetric signature $[x_0, x_1, \ldots, x_n]$ for a recognizer is realizable under the basis $\boldsymbol{\beta} = [n, p] = \left[\binom{n_0}{n_1}, \binom{p_0}{p_1}\right]$* iff *it takes one of the following forms:*
Form 1: there exist (arbitrary) constants λ, s, t and ϵ where $\epsilon = \pm 1$, such that for all $i, 0 \le i \le n$,

$$x_i = (sn_0 + tn_1)^{n-i}(sp_0 + tp_1)^i + \epsilon(sn_0 - tn_1)^{n-i}(sp_0 - tp_1)^i. \quad (1)$$

Form 2: there exist (arbitrary) constants λ,such that for all $i, 0 \le i \le n$,

$$x_i = \lambda[(n-i)n_0(p_1)^i(n_1)^{n-1-i} + ip_0(p_1)^{i-1}(n_1)^{n-i}]. \quad (2)$$

Form 3: there exist (arbitrary) constants λ,such that for all $i, 0 \le i \le n$,

$$x_i = \lambda[(n-i)n_1(p_0)^i(n_0)^{n-1-i} + ip_1(p_0)^{i-1}(n_0)^{n-i}]. \quad (3)$$

A similar theorem for generators (Thm. 4 in [6], p. 437) will also be used, but we omit the statement here.

THEOREM 2.3. *(Thm. 5 in [6], p. 438) A symmetric signature $[x_0, x_1, \cdots, x_n]$ is realizable on some basis of size 1 iff there exists three constants a, b, c(not all zero), such that $\forall k, 0 \le k \le n-2$,*

$$ax_k + bx_{k+1} + cx_{k+2} = 0. \quad (4)$$

The following two simple lemmas are used in the proof of Lemma 4.5 and 4.6. We omit their proofs.

LEMMA 2.1. *Suppose a sequence x_i ($i = 0, 1, \ldots, n$, where $n \ge 3$) has the following form: $x_i = A\alpha^i + B\beta^i$, ($AB \ne 0, \alpha \ne \beta$), then the representation is unique. That is, if $x_i = A'(\alpha')^i + B'(\beta')^i$, ($i = 0, 1, \ldots, n$, $n \ge 3$), then $A' = A, B' = B, \alpha' = \alpha, \beta' = \beta$ or $A' = B, B' = A, \alpha' = \beta, \beta' = \alpha$.*

LEMMA 2.2. *Suppose a sequence x_i ($i = 0, 1, \ldots, n$, where $n \ge 3$) has the following form: $x_i = Ai\alpha^{i-1} + B\alpha^i$, ($A \ne 0$), then the representation is unique. That is, if $x_i = A'i(\alpha')^{i-1} + B'(\alpha')^i$, ($i = 0, 1, \ldots, n$, $n \ge 3$), then $A' = A, B' = B, \alpha' = \alpha$.*

3. THE BASIS MANIFOLD

In holographic algorithms, computations are expressed in terms of a set of linear basis vectors of dimension 2^k, where k is called the size of the basis. In almost all cases [29, 3], the successful design of a holographic algorithm was accomplished by a basis of size 1. In [32], initially Valiant used a basis of size 2 to show $\#_7$Pl-Rtw-Mon-3CNF $\in$ P. Then it was pointed out in [6] that even in that case the same can be done with a basis of size 1. Subsequently we were able to prove that *every* holographic algorithm using a basis of size 2 can be efficiently simulated by another holographic algorithm using a basis of size 1 [7].

However trying to extend this collapse to arbitrary dimensions we encountered significant difficulties, mainly due to matchgate identities. (At the time of submission of the present paper, we thought we had overcome that difficulty; but we didn't.) Finally this universal collapse was achieved [8]. (See also [9].) The final proof uses many crucial ideas from [7], but we had to do much more. The upshot is that higher dimensional bases *do not* extend the reach of holographic algorithms. Therefore, we will develop our theory exclusively with bases of size 1; but our results are universally applicable.

We will identify the set of 2-dim bases $\left[\binom{n_0}{n_1}, \binom{p_0}{p_1}\right]$ with $\text{GL}_2(\mathbf{F})$. Over the complex field $\mathbf{F} = \mathbf{C}$, it has (complex) dimension 4. Similarly for $\mathbf{F} = \mathbf{R}$. However, the following simple Proposition 4.3 of [29] shows that the essential underlying structure has only dimension 2.

PROPOSITION 3.1 (VALIANT). *[29] If there is a generator (recognizer) with certain signature for size one basis $\{(n_0, n_1), (p_0, p_1)\}$ then there is a generator (recognizer) with the same signature for size one basis $\{(xn_0, yn_1), (xp_0, yp_1)\}$ or $\{(xn_1, yn_0), (xp_1, yp_0)$ for any $x, y \in \mathbf{F}$, and $xy \ne 0$.*

This leads to the following definition of an equivalence relation:

DEFINITION 3.1. *Two bases $\boldsymbol{\beta} = [n, p] = \left[\binom{n_0}{n_1}, \binom{p_0}{p_1}\right]$ and $\boldsymbol{\beta'} = [n', p'] = \left[\binom{n'_0}{n'_1}, \binom{p'_0}{p'_1}\right]$ are equivalent, denoted by $\boldsymbol{\beta} \sim \boldsymbol{\beta'}$, iff there exist $x, y \in \mathbf{F}^*$ such that $n'_0 = xn_0, p'_0 = xp_0, n'_1 = yn_1, p'_1 = yp_1$ or $n'_0 = xn_1, p'_0 = xp_1, n'_1 = yn_0, p'_1 = yp_0$.*

THEOREM 3.1. *$\text{GL}_2(\mathbf{F})/\sim$ is a two dimensional manifold (for $\mathbf{F} = \mathbf{C}$ or $\mathbf{R}$).*

We call this the *basis manifold* $\mathcal{M}$. For $\mathbf{F} = \mathbf{R}$, it can be shown that topologically $\mathcal{M}$ is a Möbius strip. From now

on we identify a basis $\boldsymbol{\beta}$ with its equivalence class containing it. When it is permissible, we use the dehomogenized coordinates $\begin{pmatrix}1 & x\\ 1 & y\end{pmatrix}$ to represent a point (i.e., a basis class) in $\mathcal{M}$. We will assume char.$\mathbf{F} \neq 2$.

4. SIMULTANEOUS REALIZABILITY OF SYMMETRIC SIGNATURES

In [6], we gave a complete characterization of all the realizable symmetric signatures (Thm. 3, 4, 5 in [6]). These tell us exactly what signatures can be realized over *some* bases. However, to construct a holographic algorithm, one needs to realize some generators and recognizers simultaneously. In terms of $\mathcal{M}$, a given generator (recognizer) defines a (possibly empty) subvariety which consists of all the bases over which it is realizable. Then simultaneous realizability is equivalent to a non-empty intersection of these subvarieties. Thus we have to go beyond [6]. For every signature which is realizable according to Theorem 2.3, we need to determine the subvariety where it is realizable.

DEFINITION 4.1. *Let $B_{gen}(G)$ (resp. $B_{rec}(R)$) be the set of all possible bases in $\mathcal{M}$ for which a symmetric signature G for a generator (resp. R for a recognizer) is realizable.*

Since the identical zero signature is realizable in every basis, we will assume the signature is non-zero in the following discussion.

4.1 Realizability of Recognizers

The following Lemmas give a complete and mutually exclusive list of realizable symmetric signatures for recognizers.

LEMMA 4.1.

$$B_{rec}([a^n, a^{n-1}b, \ldots, b^n]) = \left\{ \left[\begin{pmatrix} a \\ n_1 \end{pmatrix}, \begin{pmatrix} b \\ p_1 \end{pmatrix} \right] \in \mathcal{M} \middle| \, n_1, p_1 \in \mathbf{F} \right\}.$$

Remark: Every signature of arity 1 is in this form.

Proof: If $n = 1$, the standard signature can and can only be $(\lambda, 0)$ or $(0, \lambda)$ (where λ is arbitrary). So the signature over the basis $\left[\begin{pmatrix} n_0 \\ n_1 \end{pmatrix}, \begin{pmatrix} p_0 \\ p_1 \end{pmatrix} \right]$ is $(\lambda n_0, \lambda p_0)$ or $(\lambda n_1, \lambda p_1)$. Since we require the signature to be (a, b), all the possible bases as expressed in $\mathcal{M}$ are $\left[\begin{pmatrix} a \\ n_1 \end{pmatrix}, \begin{pmatrix} b \\ p_1 \end{pmatrix} \right]$, where n_1, p_1 are arbitrary, except $ap_1 - bn_1 \neq 0$.

Now we assume $n > 1$, then it is easy to show that this signature must be generated from Form 1 of Theorem 2.2. In this form, we must have $b(sn_0 + tn_1) = a(sp_0 + tp_1)$ and $b(sn_0 - tn_1) = a(sp_0 - tp_1)$. It follows that $bsn_0 = asp_0$ and $btn_1 = atp_1$. Because at least one of a, b is non-zero, if $st \neq 0$, we have $n_0p_1 - n_1p_0 = 0$. But this is not allowed. So we must have $s = 0$ or $t = 0$, (but not both $s = 0$ and $t = 0$, o.w., the signature is identically 0). In either cases, all the possible bases are $\left[\begin{pmatrix} a \\ n_1 \end{pmatrix}, \begin{pmatrix} b \\ p_1 \end{pmatrix} \right] \in \mathcal{M}$, where n_1, p_1 are arbitrary, subject to $ap_1 - bn_1 \neq 0$. □

LEMMA 4.2.

$$B_{rec}([x_0, x_1, x_2]) = \left\{ \left[\begin{pmatrix} n_0 \\ n_1 \end{pmatrix}, \begin{pmatrix} p_0 \\ p_1 \end{pmatrix} \right] \in \mathcal{M} \mid \right.$$
$$\left. \begin{array}{c} x_0p_1^2 - 2x_1p_1n_1 + x_2n_1^2 = 0, x_0p_0^2 - 2x_1p_0n_0 + x_2n_0^2 = 0 \\ or \quad x_0p_0p_1 - x_1(n_0p_1 + n_1p_0) + x_2n_0n_1 = 0 \end{array} \right\}.$$

Proof: Under the equivalence relation, we can assume $n_0p_1 - n_1p_0 = 1$.

Then $\left[\begin{pmatrix} n_0 \\ n_1 \end{pmatrix}, \begin{pmatrix} p_0 \\ p_1 \end{pmatrix} \right]^{-1} = \left[\begin{pmatrix} p_1 \\ -n_1 \end{pmatrix}, \begin{pmatrix} -p_0 \\ n_0 \end{pmatrix} \right]$. So the standard signature of $[x_0, x_1, x_2]$ is $[x_0p_1^2 - 2x_1p_1n_1 + x_2n_1^2, x_0p_0p_1 - x_1(n_0p_1 + n_1p_0) + x_2n_0n_1, x_0p_0^2 - 2x_1p_0n_0 + x_2n_0^2]$. The fact that the only constraint of a standard signature of arity 2 is the parity constraint completes the proof. □

In the following the matchgate arity n is ≥ 3.

LEMMA 4.3. *Let $\lambda_1 \neq 0$. Suppose $p = $ char.$\mathbf{F}$ $\not| n$, then*

$$B_{rec}([0, 0, \ldots, 0, \lambda_1, \lambda_2]) = \left\{ \left[\begin{pmatrix} 0 \\ n\lambda_1 \end{pmatrix}, \begin{pmatrix} 1 \\ \lambda_2 \end{pmatrix} \right] \right\}.$$

For $p|n$ and $\lambda_2 = 0$,

$$B_{rec}([0, \ldots, 0, \lambda_1, 0]) = \left\{ \left[\begin{pmatrix} 0 \\ n_1 \end{pmatrix}, \begin{pmatrix} 1 \\ p_1 \end{pmatrix} \right] \in \mathcal{M} \middle| \, n_1, p_1 \in \mathbf{F} \right\}.$$

For $p|n$ and $\lambda_2 \neq 0$, $B_{rec}([0, 0, \ldots, 0, \lambda_1, \lambda_2]) = \emptyset$.

Proof: Its reversal signature $[\lambda_2, \lambda_1, 0, \ldots, 0]$ is a special case of Lemma 4.6 (setting $\alpha = 0$ in Lemma 4.6). □

LEMMA 4.4. *For any scalars α, A, B, where $AB \neq 0$,*

$$B_{rec}([A, A\alpha, A\alpha^2, \ldots, A\alpha^n + B]) =$$
$$\left\{ \left[\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} \alpha + \omega \\ \alpha - \omega \end{pmatrix} \right] \middle| \, \omega^n = \pm \frac{B}{A} \right\}.$$

Proof: Its reversal signature $[A\alpha^n + B, A\alpha^{n-1}, \ldots, A\alpha, A]$ is a spacial case of Lemma 4.5. (This proof assumes $\alpha \neq 0$. For $\alpha = 0$, it can be directly verified.) □

Other cases of Theorem 2.3 have the property that the a, b and c (in the statement of Theorem 2.3) are unique up to a scaling factor and $c \neq 0$. So we have a unique characteristic equation $cx^2 + bx + a = 0$, which has two roots α and β. (For arbitray a, b, c, α and β are general too.) Corresponding to $\alpha \neq \beta$, we have the following lemma:

LEMMA 4.5. *For any scalars α, β, A and B, where $AB \neq 0$ and $\alpha \neq \beta$,*

$$B_{rec}([A\alpha^i + B\beta^i | i = 0, 1, \ldots, n]) =$$
$$\left\{ \left[\begin{pmatrix} 1 + \omega \\ 1 - \omega \end{pmatrix}, \begin{pmatrix} \alpha + \beta\omega \\ \alpha - \beta\omega \end{pmatrix} \right] \middle| \, \omega^n = \pm \frac{B}{A} \right\}.$$

Remark: We denote $0^0 = 1$.

Proof: From $A + B = x_0, A\alpha + B\beta = x_1$, we can solve uniquely for A and B. We have $AB \neq 0$; otherwise $\{x_i\}$ has the form $\{a^ib^{n-i}\}$, which has been dealt with in Lemma 4.1. So from Lemma 2.1, we know that the representation is unique. But from form 1 of Theorem 2.2, we know that

$$x_i = (sn_0 + tn_1)^n \left(\frac{sp_0 + tp_1}{sn_0 + tn_1} \right)^i + \epsilon(sn_0 - tn_1)^n \left(\frac{sp_0 - tp_1}{sn_0 - tn_1} \right)^i.$$

So $(sn_0 + tn_1)^n = A$, $\frac{sp_0 + tp_1}{sn_0 + tn_1} = \alpha$, $\epsilon(sn_0 - tn_1)^n = B$, $\frac{sp_0 - tp_1}{sn_0 - tn_1} = \beta$, (exchanging notations A with B, and α with β if necessary.) So $\left[\begin{pmatrix} sn_0 \\ tn_1 \end{pmatrix}, \begin{pmatrix} sp_0 \\ tp_1 \end{pmatrix} \right] = \left[\begin{pmatrix} a + b \\ a - b \end{pmatrix}, \begin{pmatrix} a\alpha + b\beta \\ a\alpha - b\beta \end{pmatrix} \right]$, where $a^n = A, b^n = B$. Since $\alpha \neq \beta$, we know $st \neq 0$. So $\left[\begin{pmatrix} n_0 \\ n_1 \end{pmatrix}, \begin{pmatrix} p_0 \\ p_1 \end{pmatrix} \right] \sim \left[\begin{pmatrix} sn_0 \\ tn_1 \end{pmatrix}, \begin{pmatrix} sp_0 \\ tp_1 \end{pmatrix} \right]$. This completes the proof. □

Corresponding to $\alpha = \beta$, we have the following lemma:

LEMMA 4.6. *For any scalars α, A and B, let $p = \text{char.}\mathbf{F}$ and let $A \neq 0$.*
Case 1: $p = 0$ or $p \not| n$.

$$B_{rec}([Ai\alpha^{i-1} + B\alpha^i]) = \left\{ \left[\binom{1}{B}, \binom{\alpha}{nA + B\alpha} \right] \right\}.$$

Case 2: $p|n$ and $x_0 = 0$. In this case, $B = 0$ and the signature is of the form $[Ai\alpha^{i-1}] = [0, A, 2A\alpha, \ldots]$. Then,

$$B_{rec}([Ai\alpha^{i-1}]) = \left\{ \left[\binom{1}{n_1}, \binom{\alpha}{p_1} \right] \in \mathcal{M} \middle| n_1, p_1 \in \mathbf{F} \right\}.$$

Case 3: $p|n$ and $x_0 \neq 0$. Then it is not realizable.

Remark: If $\alpha = 0$, and $i = 0$, we still denote $i\alpha^{i-1} = 0$. Also $\alpha^i = 0^0 = 1$.
Proof: In Case 1, from $B = x_0, A + B\alpha = x_1$, we can solve uniquely for A, B. We have $A \neq 0$, so Lemma 2.2 applies. From Lemma 2.2, we know that the representation is unique. From form 2 of Theorem 2.2 (form 3 will give an equivalent basis), we know that $x_i = (n_1p_0 - n_0p_1)n_1^n i \left(\frac{p_1}{n_1}\right)^{i-1} + nn_1^{n-1}\left(\frac{p_1}{n_1}\right)^i$. So $(n_1p_0 - n_0p_1)n_1^n = A$, $\frac{p_1}{n_1} = \alpha, nn_0n_1^{n-1} = B$. Since $n_1 \neq 0$, under the equivalence relation, we can let $n_1 = 1$, then we have the unique solution $n_0 = B/n, p_1 = \alpha, p_0 = A + \frac{B\alpha}{n}$. We omit the proofs for Case 2 and 3. □

4.2 Realizability of Generators

The following Lemmas give a complete and mutually exclusive list of realizable symmetric signatures for generators. They can be proved similarly.

LEMMA 4.7.

$$B_{gen}([a^n, a^{n-1}b, \cdots, b^n]) = \left\{ \left[\binom{n_0}{-b}, \binom{p_0}{a} \right] \middle| n_0, p_0 \in \mathbf{F} \right\}.$$

LEMMA 4.8.

$$B_{gen}([x_0, x_1, x_2]) = \left\{ \left[\binom{n_0}{n_1}, \binom{p_0}{p_1} \right] \in \mathcal{M} \middle| \begin{array}{c} x_0n_0^2 + 2x_1n_0p_0 + x_2p_0^2 = 0, x_0n_1^2 + 2x_1n_1p_1 + x_2p_1^2 = 0 \\ or\ x_0n_0n_1 + x_1(n_0p_1 + n_1p_0) + x_2p_0p_1 = 0 \end{array} \right\}.$$

LEMMA 4.9. *Let $\lambda_1 \neq 0$. Suppose $p = \text{char.}\mathbf{F}$ $\not| n$,*

$$B_{gen}([0, 0, \cdots, 0, \lambda_1, \lambda_2]) = \left\{ \left[\binom{-\lambda_2}{1}, \binom{n\lambda_1}{0} \right] \right\}.$$

For $p|n$ and $\lambda_2 = 0$,

$$B_{gen}([0, \ldots, 0, \lambda_1, 0]) = \left\{ \left[\binom{1}{n_1}, \binom{0}{p_1} \right] \in \mathcal{M} \middle| n_1, p_1 \in \mathbf{F} \right\}.$$

For $p|n$ and $\lambda_2 \neq 0$, $[0, 0, \ldots, 0, \lambda_1, \lambda_2]$ is not realizable.

LEMMA 4.10. *For any scalars α, A and B, $AB \neq 0$,*

$$B_{gen}([A, A\alpha, A\alpha^2, \cdots, A\alpha^n + B]) = \left\{ \left[\binom{\omega - \alpha}{-\alpha - \omega}, \binom{1}{1} \right] \middle| \omega^n = \pm\frac{B}{A} \right\}.$$

LEMMA 4.11. *For any scalars α, β, A and B, where $AB \neq 0$ and $\alpha \neq \beta$,*

$$B_{gen}(\{A\alpha^i + B\beta^i | i = 0, 1, \cdots, n\}) = \left\{ \left[\binom{\beta\omega - \alpha}{-\alpha - \beta\omega}, \binom{1 - \omega}{1 + \omega} \right] \middle| \omega^n = \pm\frac{B}{A} \right\}.$$

LEMMA 4.12. *For any scalars α, A and B, let $p = \text{char.}\mathbf{F}$ and let $A \neq 0$.*
Case 1: $p = 0$ or $p \not| n$.

$$B_{gen}([Ai\alpha^{i-1} + B\alpha^i]) = \left\{ \left[\binom{nA + B\alpha}{-\alpha}, \binom{-B}{1} \right] \right\}.$$

Case 2: $p|n$ and $x_0 = 0$, in this case, the signature is of the form $[Ai\alpha^{i-1}]$.

$$B_{gen}([Ai\alpha^{i-1}]) = \left\{ \left[\binom{-\alpha}{n_1}, \binom{1}{p_1} \right] \in \mathcal{M} \middle| n_1, p_1 \in \mathbf{F} \right\}.$$

Case 3: $p|n$ and $x_0 \neq 0$. Then it's not realizable.

4.3 Simultaneous Realizability

DEFINITION 4.2. *The Simultaneous Realizability Problem (SRP):*
Input: *A set of symmetric signatures for generators and/or recognizers.*
Output: *A common basis of these signatures if any; "NO" if they are not simultaneously realizable.*

Algorithm:
For every signature $[x_0, x_1, \ldots, x_n]$, check if it satisfies Theorem 2.3. If not, output "NO" and halt.
Otherwise find $B_{gen}([x_0, x_1, \ldots, x_n])$ or $B_{rec}([x_0, x_1, \ldots, x_n])$ according to Lemmas 4.7 to 4.12 or Lemmas 4.1 to 4.6, respectively. Check if these subvarieties have a non-empty intersection.

THEOREM 4.1. *This is a polynomial time algorithm for SRP. (If $p = \text{char.}\mathbf{F}$ is a large prime and is considered part of the input, i.e., input size includes $\log p$, then the problem is in RP.)*

Proof: Checking whether every input signature satisfies Theorem 2.3 can obviously be done in polynomial time. To find the right form and then the right Lemma for a signature which satisfies Theorem 2.3 can also be done in polynomial time as they are mutually exclusive.

Every subvariety of bases from Lemma 4.1 to 4.6 and from Lemma 4.7 to 4.12 is of one of three kinds: a finite set of points (of linear size), a line or a quadratic curve. More precisely, consider recognizers; the situation for generators is similar. Express things in terms of the manifold $\mathcal{M}$ shows that: For Lemma 4.1 we get a line with $x = \text{const}$. For Lemma 4.2 we get a union of two sets. The first is finite, where both x and y satisfy a quadratic polynomial (and by projective closure). Therefore there are at most 4 points in $\mathcal{M}$. The second set is defined by an equation of the form $Axy + B(x + y) + C = 0$, (and by projective closure) where A, B, C are known constants. Note that if we had two sets of this type (from Lemma 4.2 and/or Lemma 4.8) we can eliminate A and get a linear equation.

For Lemma 4.3 we have either a single point for $p|n$ or a line "at infinity". Lemma 4.6 is similar, where we have either

a point or a line $x = \text{const}$. For Lemma 4.4, we get at most n points from the equation $\omega^n = \text{const}$. If we are in $\mathbf{C}$ (more precisely in $\mathbf{Q}$ or an algebraic extension field of $\mathbf{Q}$) then the computation is clearly in P. For fields of finite characteristic, since n is given in unary, the computation is in P, provided p is fixed (or at most $O(\log n)$). For large p (the field size is exponential in n), this can be done in RP. We need to be able to factor the polynomial $X^n = \text{const}$. so that we can do symbolic calculations with a minimal polynomial [2]. □

5. SOME NOT SO ACCIDENTAL ALGORITHMS

In [32], Valiant gave polynomial time algorithms for #$_7$Pl-Rtw-Mon-3CNF and #$_7$Pl-3/2Bip-VC, and he called them "accidental algorithms". In this section, we show how such algorithms can be developed almost "mechanically". This approach has the advantage that one gains more understanding of what can or cannot be accomplished. With this machinery we are able to generalize his result to Pl-Rtw-Mon-kCNF and Pl-k/2Bip-VC, for a general k. We show that there is a unique modulus $2^k - 1$ for which we can design such a holographic algorithm which counts the number of solutions. In the case of $k = 3$, this shows why 7 is special.

5.1 $\#_{2^k-1}$Pl-Rtw-Mon-kCNF

For #Pl-Rtw-Mon-kCNF, we are given a planar formula [16] in kCNF form, where each variable appears positively, and each appears in exactly 2 clauses. The problem is to count the number of satisfying assignments. As noted earlier, this counting problem is #P-complete already for $k = 3$.

Now we wish to replace each variable by a generator with signature $[1, 0, 1]$, and each clause by a recognizer with $[0, 1, 1, \cdots, 1]$ (with k 1's). The symmetric signature $[1, 0, 1]$ corresponds to a consistent truth assignment on two edges leading to clauses, and $[0, 1, 1, \cdots, 1]$ corresponds to a Boolean OR for the clause. If we connect the generators and recognizers in a natural way, by the *Holant Theorem* [29] this would solve #Pl-Rtw-Mon-kCNF in polynomial time (if the signatures are realizable over $\mathbf{Q}$).

Then the question boils down to whether there is a basis in $\mathcal{M}$ where $[1, 0, 1]$ for a generator and $[0, 1, 1, \cdots, 1]$ (with k 1's) for a recognizer can be simultaneously realized. For this, we use our machinery.

From Lemma 4.5, with $A = 1, B = -1, \alpha = 1, \beta = 0$, we have

$$B_{rec}([0, 1, 1, \cdots, 1]) = \left\{ \left[\begin{pmatrix} 1+\omega \\ 1-\omega \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right] \middle| \, \omega^k = \pm 1 \right\}.$$

We look for some $\omega^k = \pm 1$, such that $\left[\begin{pmatrix} 1+\omega \\ 1-\omega \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right] \in B_{gen}([1, 0, 1])$.

According to Lemma 4.8, we want $(1+\omega)^2 + 1 = (1-\omega)^2 + 1 = 0$ or $(1+\omega)(1-\omega) + 1 = 0$.

The first case is impossible, and in the second case we require $\omega^2 = 2$. Together with the condition $\omega^k = \pm 1$, we have $2^k - 1 = 0$. From this we can already see that for every prime $p | 2^k - 1$, $\#_p$Pl-Rtw-Mon-kCNF is computable in polynomial time. In particular this is true for every Mersenne prime $2^q - 1$. More generally we have:

THEOREM 5.1. *There is a polynomial time algorithm for $\#_{2^k-1}$Pl-Rtw-Mon-kCNF. Furthermore, any modulus m for which the appropriate signatures exist must be a divisor of $2^k - 1$.*

Proof: Our discussion above already shows that the modulus $2^k - 1$ is the best we can do. (Formally speaking we should present a generalization of the Holant Theorem [29] over a ring such as $\mathbf{Z}_{2^k-1}$, which we will omit here.) We now give the polynomial algorithms in two cases:

Case 1: k is even.

Over the complex numbers $\mathbf{C}$, from Lemma 4.8, Lemma 4.4, we can see that a generator for $[1, 0, 1]$ and a recognizer for $[1 + \epsilon 2^{k/2}, 1, 1, \cdots, 1]$ (where there are k 1's, and $\epsilon = \pm 1$) are simultaneously realizable in $\boldsymbol{\beta} = \left[\begin{pmatrix} 1+\sqrt{2} \\ 1-\sqrt{2} \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right]$.

Setting $\epsilon = 1$ and replacing each variable by a generator and each clause by a recognizer with the corresponding signatures, we obtain a matchgrid Ω with the underlying weighted planar graph G. Then the Holant Theorem [29] tells us

$$\text{Holant}(\Omega) = \text{PerfMatch}(G). \tag{5}$$

We will denote this value by X.

From the left hand side of (5) we know that X is an integer because every entry in the signatures of generators and recognizers is an integer. Furthermore we have

$$X \equiv \#\text{Pl-Rtw-Mon-}k\text{CNF} \pmod{1 + 2^{k/2}}.$$

From the right hand side of (5) we know that X can be computed in polynomial time using the FKT algorithm for perfect matchings of a planar graph. The planar graph has weights from the subfield $\mathbf{Q}(\sqrt{2}) \subset \mathbf{C}$, which poses no problem to the Pfaffian evaluation of FKT in polynomial time. Therefore $\#_{2^{k/2}+1}$Pl-Rtw-Mon-kCNF can be computed in polynomial time. Similarly, setting $\epsilon = -1$, we can compute $\#_{2^{k/2}-1}$Pl-Rtw-Mon-kCNF in polynomial time.

Since $(2^{k/2}+1, 2^{k/2}-1) = 1$ and $2^k - 1 = (2^{k/2}+1)((2^{k/2}-1)$, we can apply Chinese remaindering to get a polynomial time algorithm for $\#_{2^k-1}$Pl-Rtw-Mon-kCNF.

Case 2: k is odd.

Consider the ring $\mathbf{Z}_{2^k-1}$, and let $r = 2^{(k+1)/2} \in \mathbf{Z}_{2^k-1}$. Then r satisfies $r^2 = 2$ in $\mathbf{Z}_{2^k-1}$. We denote this r by $\sqrt{2}$. Then $1 - (\sqrt{2})^k = 1 - (2^k)^{(k+1)/2} = 0$ in $\mathbf{Z}_{2^k-1}$.

Therefore over this ring $\mathbf{Z}_{2^k-1}$ and with the basis $\boldsymbol{\beta} = \left[\begin{pmatrix} 1+\sqrt{2} \\ 1-\sqrt{2} \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right] = \left[\begin{pmatrix} 1+2^{(k+1)/2} \\ 1-2^{(k+1)/2} \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right]$, we have a generator for $[1, 0, 1]$ and a recognizer for $[0, 1, 1, \cdots, 1]$ (with k 1's) according to Lemma 4.8 and 4.4. As a result, we have a polynomial time algorithm for $\#_{2^k-1}$Pl-Rtw-Mon-kCNF. (It is in this case where k is odd, we need 2 as a quadratic residue in $\mathbf{Z}_p$ for primes $p | 2^k - 1$, as discussed in Section 1.) □

5.2 $\#_{2^k-1}$Pl-k/2Bip-VC

In this problem, we are given a planar bipartite graph with left degree k and right degree 2. We wish to count the number of Vertex Covers mod $2^k - 1$. The counting problem for this class of graphs mod 2 is $\oplus$P-complete and thus NP-hard [32]. Consider an arbitrary subset S of vertices from the right. Every vertex v on the left *either* has all its k adjacent vertices in S, in which case there are exactly two choices to extend at v to a Vertex Cover, *or* has some of its k adjacent vertices not in S, in which case there is exactly one

choice to extend at v to a Vertex Cover. Thus, following the general recipe for holographic algorithms, we want to construct a generator with signature $[1, 0, 1]$ and a recognizer with signature $[2, 1, 1, \cdots, 1]$ (with k 1's) simultaneously.

From Lemma 4.5, where $A = 1, B = 1, \alpha = 1, \beta = 0$, we have:

$$B_{rec}([2, 1, 1, \cdots, 1]) = \left\{ \left[\begin{pmatrix} 1+\omega \\ 1-\omega \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right] \middle| \, \omega^k = \pm 1 \right\}.$$

This set is exactly the same as $B_{rec}([0, 1, 1, \cdots, 1])$. Then the proof in Section 5.1 gives us:

THEOREM 5.2. *There is a polynomial time algorithm for $\#_{2^k-1}$Pl-k/2Bip-VC. Furthermore, any modulus m for which the appropriate signatures exist must be a divisor of $2^k - 1$.*

Our general machinery not only can find the required signatures when they exist, but also can prove certain desired signatures do not exist or can not be simultaneously realized. As an example, one may wish to extend the previous two problems to allow variables to be read more than twice. This calls for a simultaneous realizability of $[1, 0, 0, \cdots, 0, 1]$ ($l - 1$ 0's, $l > 2$) and $[0, 1, 1, \cdots, 1]$ (k 1's). This can be shown to result in an empty intersection on $\mathcal{M}$.

6. SOME MORE EXAMPLES

In [29] Valiant gave a list of combinatorial problems all of which can be solved by holographic algorithms. In each case, a "magic" design of matchgates and signatures were presented to derive the algorithm. With our machinery, we can show all these problems can be systematically derived. In particular, we will see how the two somewhat mysterious bases **b1** and **b2** show up naturally. The framework here can handle all the problems from [29]. (But for PL-FO-2-COLOR, which uses a basis of three vectors, it is more naturally dealt with in the context of more general bases.)

6.1 Not-All-Equal Gate

In [29], four problems employ the NAE (Not-All-Equal) gate $[0, 1, 1, 0]$. They are #PL-3-NAE-SAT, #PL-3-NAE-ICE, #PL-3-(1,1)-CYCLECHAIN and
PL-NODE-BIPARTITION (this last one uses a generator with signature $[x, 1, 1, x]$.)

Notice that they have a common restriction of "maximum degree 3". This is necessary because if $k > 3$, then $[0, 1, 1, \cdots, 1, 0]$ ($k - 1$ 1's) is not realizable. This is a result of [5], but it's easy to see now.

For the case of degree 3, by Lemma 4.5, take α, β to be the two roots of $x^2 - x + 1 = 0$ and $A/B = -1$, we have $B_{rec}([0, 1, 1, 0]) = \left\{ \left[\begin{pmatrix} 1+\omega \\ 1-\omega \end{pmatrix}, \begin{pmatrix} \alpha+\beta\omega \\ \alpha-\beta\omega \end{pmatrix} \right] \middle| \, \omega^3 = \pm 1 \right\}$.

Notice that $\alpha^3 = -1$ and $\alpha\beta = 1$, let $\omega = \alpha$, we have (using $\sim$ on $\mathcal{M}$)

$$\left[\begin{pmatrix} 1+\omega \\ 1-\omega \end{pmatrix}, \begin{pmatrix} \alpha+\beta\omega \\ \alpha-\beta\omega \end{pmatrix} \right] =$$
$$\left[\begin{pmatrix} 1+\alpha \\ 1-\alpha \end{pmatrix}, \begin{pmatrix} \alpha+\beta\alpha \\ \alpha-\beta\alpha \end{pmatrix} \right] = \left[\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right].$$

This is **b2** in [29]. Actually for each of the four problems, in order to intersect with the subvarieties of other generators and recognizers, this is the only choice. Due to space limitation, we omit the details.

6.2 $\#_{k+1}2/k$-X-Matchings

Input: A planar bipartite graph $G = (V_1, V_2, E)$. Nodes in V_1 and V_2 have degrees 2 and k respectively.
Output: The number mod $(k + 1)$ of all (not necessarily perfect) matchings.

This problem is a slight variation on #X-Matchings [29], which has general weights on edges and uses an *unsymmetric* signature. (We will discuss unsymmetric signatures in Section 7.) The case $k = 4$ was explicitly stated in [29], but the proof there clearly also handles general k. Jerrum [17] showed that counting matchings for planar graphs is #P-complete. Vadhan [26] showed that this remains #P-complete for planar bipartite graphs of degree 6.

For this problem we are looking for a generator with signature $[1, 1, 0]$ and a recognizer with signature $[1, 1, 0, \cdots, 0]$ ($k-1$ 0's) simultaneously. From Lemma 4.6, with $A = B = 1, \alpha = 0$, we have: $[B_{rec}([1, 1, 0, \cdots, 0]) = \left\{ \left[\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ k \end{pmatrix} \right] \right\}$.
We hope that $\left[\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ k \end{pmatrix} \right] \in B_{gen}([1, 1, 0])$.

From Lemma 4.8, we must have $k+1 = 0$. So we can only work inside the ring $\mathbf{Z}_{k+1}$.

Remark: In $\mathbf{Z}_{k+1}$, this basis $\left[\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ k \end{pmatrix} \right]$ in $\mathcal{M}$ under the equivalence relation $\sim$ is exactly **b1** in [29].

THEOREM 6.1. *There is a polynomial time algorithms for $\#_{k+1}2/k$-X-Matchings. Any modulus m for which the appropriate signatures exist must be a divisor of $k + 1$.*

Note that being able to compute mod $k + 1$ implies being able to compute mod m for any divisor $m|k + 1$. Thus the above characterization is exact.

We omit the discussion of $\oplus$PL-EVEN-LIN2, the last problem from [29]. It can also be treated naturally in our framework.

7. BEYOND SYMMETRIC SIGNATURES

The theory of symmetric signatures has been satisfactorily developed. Symmetric signatures are particularly useful because they have clear combinatorial meanings. However general (i.e. unsymmetric) signatures have also been used before. To understand completely the power of holographic algorithms, we must study unsymmetric signatures as well. (In the following, we discuss generators only; the situation for recognizers is similar.)

Following the framework in [4], a generator is a contravariant tensor of the form $G = (g^{i_1 i_2 \cdots i_n})$ where $i_1 i_2 \ldots i_n \in \{0, 1\}$. We also denote $G = (g^S)$ where $S \subset [n]$, and $g^S = g^{\chi_S(1)\chi_S(2)\cdots\chi_S(n)}$. A generator signature G is realizable on a basis $\boldsymbol{\beta}$ iff the standard signature $G' = \boldsymbol{\beta}^{\otimes n} G$ can be realized by some planar matchgate. There are two conditions for a standard signature to be realizable:

Parity Constraint: Either $g'^S = 0$ for all $|S|$ even, or $g'^S = 0$ for all $|S|$ odd.
Matchgate Identities: G' satisfies all the *useful Grassmann-Plücker identities* (see [3, 5, 28]).

DEFINITION 7.1. *A tensor G is* admissible *as a generator on a basis $\boldsymbol{\beta}$ iff $G' = \boldsymbol{\beta}^{\otimes n} G$ satisfies the* Parity Constraint. *Let $B^p_{gen}(G)$ denote the subset of $\mathcal{M}$ for which G is admissible as a generator.*

By definition we have $B_{gen}(G) \subseteq B^p_{gen}(G)$ for all G.

For symmetric signatures, we already observed that there are some different levels of realizability. Some signatures are realizable on isolated points, while others are realizable on lines or curves. Success at getting a holographic algorithm typically results from either a generator or a recognizer having more than isolated points of realizability. In terms of $\mathcal{M}$, this refers to the dimension of the subvariety $B_{gen}(G)$. More precisely,

DEFINITION 7.2. *A generator G is called d-realizable (resp. d-admissible) for an integer $d \geq 0$ iff $B_{gen}(G) \subset \mathcal{M}$ (resp. $B^p_{gen}(G) \subset \mathcal{M}$) is a (non-empty) algebraic subset of dimension at least d. (The notation $\subset$ allows equality.)*

By definition, if a generator G is d-realizable, then it is d-admissible.

Remark: Since $\mathcal{M}$ has dimension two, 2-realizability is universal realizability which means that G is realizable on any basis. This is because the conditions defining realizability are polynomial equations (with coefficients from (g^S), and variables on $\mathcal{M}$). If there is at least one polynomial which is not identically 0, the algebraic set has dimension ≤ 1. Therefore using any 2-realizable signature is a freebie in the design of holographic algorithms; it places no restriction on the rest of the design. Therefore they are particularly desirable.

The following theorem is a complete characterization of 2-admissibility (over fields of characteristic 0. The treatment of fields of positive characteristic will be reported in the future.) The proof uses rank estimates related to the *Kneser Graph* $\mathrm{KG}_{2k+1,k}$ [20, 22, 23, 11, 12, 14, 15].

THEOREM 7.1. *G is 2-admissible iff (1) $n = 2k$ is even; (2) all $g^S = 0$ except for $|S| = k$; and (3) for all $T \subset [n]$ with $|T| = k+1$,*

$$\sum_{S \subset T, |S|=k} g^S = 0. \tag{6}$$

The solution space is a linear subspace of dimension $\frac{1}{2k}\binom{2k}{k}$ (the Catalan number).

Consider all subsets of $[n]$ of a certain cardinality. Let $0 \leq k \leq \ell \leq n$, and let $A_{k,\ell,n}$ denote the $\binom{n}{k} \times \binom{n}{\ell}$ Boolean matrix indexed by (A, B), where $A, B \subset [n]$ and $|A| = k, |B| = \ell$, and the entry at (A, B) is $\chi_{[A \subset B]}$. It is known that over the rationals $\mathbf{Q}$, the rank $\mathrm{rk}(A_{k,\ell,n}) = \min\{\binom{n}{k}, \binom{n}{\ell}\}$ [11, 12, 14, 15]. (The situation with finite characteristic p is interesting and is more involved. For example, Linial and Rothschild [15] gave exact rank formulae for characteristic 2 and 3. The rank "defect" compared to the characteristic 0 case provides more admissible signatures. This will be discussed in future work.) We restate the definition of d-admissibility in more detail.

DEFINITION 7.3. *$G = (g^S)_{S \subset [n]}$ is called d-admissible if the following algebraic variety V has dimension at least d, where $V = V_0 \cup V_1 \subset \mathcal{M}$, and V_0 (resp. V_1) is defined by the set of all parity requirements for the generator signature of an odd (resp. even) matchgate.*

Consider V_0. We take a point (in dehomogenized coordinates) $\begin{pmatrix} 1 & x \\ 1 & y \end{pmatrix} \in \mathcal{M}$. Also denote $x_0 = x, x_1 = y$. Let $T \subset [n]$ with $|T|$ even. Then we require

$$\left\langle \bigotimes_{\sigma=1}^{n} [1, x_{[\sigma \in T]}], G \right\rangle = 0.$$

Similarly we define V_1, where we require that all $|T|$ odd. Note that

$$\left\langle \bigotimes_{\sigma=1}^{n} [1, x_{[\sigma \in T]}], G \right\rangle = \sum_{\substack{0 \leq i \leq n-|T| \\ 0 \leq j \leq |T|}} x^i y^j \sum_{\substack{A \subset T^c, |A| = i \\ B \subset T, |B| = j}} g^{A \cup B}. \tag{7}$$

If $\dim(V) = 2$, then either $\dim(V_0) = 2$ or $\dim(V_1) = 2$. For $\dim(V_0) = 2$, we have the following: For all $T \subset [n]$ with $|T|$ even, and for all $0 \leq i \leq n - |T|$ and $0 \leq j \leq |T|$,

$$\sum_{A \subset T^c, B \subset T, |A|=i, |B|=j} g^{A \cup B} = 0. \tag{8}$$

(If there is one equation not satisfied, then there is at least one non-trivial polynomial among the parity requirements, which implies $\dim(V_0) \leq 1$.) For $\dim(V_1) = 2$, the above holds for all $|T|$ odd. Continuing with $\dim(V_0) = 2$, by taking $i = 0$, we get for all $T \subset [n]$ with $|T|$ even, $j \leq |T|$,

$$\sum_{S \subset T, |S|=j} g^S = 0. \tag{9}$$

Also by taking $j = 0$, we get for all $i \leq n - |T|$,

$$\sum_{S \subset T^c, |S|=i} g^S = 0.$$

If $S \subset [n]$ with $|S|$ even, then we may take $T = S$ and $j = |T|$, and it follows that

$$g^S = 0.$$

If n is odd, then T is even and T^c is odd, and together they range over all possible subsets of $[n]$. It follows that

$$g^S = 0,$$

for all $S \subset [n]$. That is, G is trivial.

An identical argument also shows that for $\dim(V_1) = 2$ and n odd, the trivial $G \equiv 0$ is the only possibility.

Now we assume $n = 2k$ is even, and continuing with $\dim(V_0) = 2$. Both T and T^c are even. Pick any T even and $i = n - |T|$, we get

$$\sum_{A \subset T^c, B \subset T, |A|=i, |B|=j} g^{A \cup B} = \sum_{S \supset T^c, |S|=i+j} g^S = 0.$$

i.e. for all even $T' \subset [n]$ and all $i \geq |T'|$,

$$\sum_{S \supset T', |S|=i} g^S = 0. \tag{10}$$

If $|S| = i < k$, we form the following system of equations from (9),

$$\sum_{S \subset T, |S|=i} g^S = 0,$$

where T ranges over all subsets of $[n]$ with $|T| = t$, and $t = i$ or $i+1$, whichever is even. This linear system has rank $\binom{n}{i}$. It follows that $g^S = 0$ for all $|S| < k$.

Similarly if $|S| = i > k$, we can use (10) with $|T| = i$ or $i - 1$, whichever is even, and summing over all subsets

S containing T. This linear system also has rank $\binom{n}{i}$. It follows that $g^S = 0$ for all $|S| > k$.

Therefore the only non-zero entries of G are among g^S with half weight $|S| = k$. Also with $\dim(V_0) = 2$, we may assume k is odd. Otherwise, we already know $g^S = 0$ for all $|S|$ even.

A similar argument for V_1 shows that, in order for $\dim(V_1) = 2$, we must have $n = 2k$ even, all $g^S = 0$ except for $|S| = k$ and k is even. Summarizing, we have

LEMMA 7.1. *If G is 2-admissible, then $n = 2k$ is even, all $g^S = 0$ except for $|S| = k$. If k is odd (resp. even) then the only possibility is $\dim(V_0) = 2$ (resp. $\dim(V_1) = 2$). Moreover, for all $T \subset [n]$ with $|T| = k + 1$,*

$$\sum_{S \subset T, |S| = k} g^S = 0. \tag{11}$$

Next we prove that the conditions in Lemma 7.1 are also sufficient for G being 2-admissible, i.e., we prove (8), thus all the polynomials in (7) are identically zero.

Suppose k odd. We prove $\dim(V_0) = 2$. A similar argument does for k even and $\dim(V_1) = 2$. We only need to verify (8) for all $i + j = k$, namely for all $T \subset [n]$ with $|T|$ even, and for all $0 \le i \le n - |T|$, and $0 \le j = k - i \le |T|$,

$$\sum_{A \subset T^c, B \subset T, |A| = i, |B| = k - i} g^{A \cup B} = 0. \tag{12}$$

Denote by $t = |T|$ and $s = n - |T|$. By symmetry of T and T^c (both being even subsets of $[n]$) we may assume $s \le t$. Since k is odd, we have the strict $s < t$, for otherwise $s = t = k$ would be odd.

We prove (12) by induction on $i \ge 0$. For the base case $i = 0$, $j = k$, we consider all $U \subset T$ with $|U| = k + 1$. Note that as $t \ge k + 1$, such U exists. By (11) we have

$$\sum_{S \subset U, |S| = k} g^S = 0.$$

Summing over all such U, and consider how many times each $S \subset [n]$ with $|S| = k$ appears in the sum, we get

$$\sum_{\substack{A \subset T^c, |A| = 0 \\ B \subset T, |B| = k}} g^{A \cup B} = \sum_{S \subset T, |S| = k} g^S = \frac{1}{\binom{t-k}{1}} \sum_{\substack{U \subset T \\ |U| = k+1}} \sum_{S \subset U, |S| = k} g^S \tag{13}$$

which is 0.

Inductively we assume (12) has been proved for $i - 1$, for some $i \ge 1$. Consider i and $j = k - i$. We may assume $i \le s$; otherwise we are done. Also $k - i + 1 \le t$. Consider all subsets $U = U_1 \cup U_2 \subset [n]$, where $U_1 \subset T^c$, $U_2 \subset T$, with $|U_1| = i$ and $|U_2| = k - i + 1$. Note that $|U| = k + 1$. We have

$$0 = \sum_{S \subset U, |S| = k} g^S = \sum_{A \subset U_1, |A| = i-1} g^{A \cup U_2} + \sum_{B \subset U_2, |B| = k-i} g^{U_1 \cup B},$$

as all sets $S \subset U$ with $|S| = k$ are classified into two classes according to whether $|S \cap U_1| = i - 1$ or i. Then summing over all such U,

$$\begin{aligned} 0 = \sum_U \sum_{S \subset U, |S| = k} g^S &= \binom{s - (i-1)}{1} \sum_{\substack{A \subset T^c, |A| = i-1 \\ B \subset T, |B| = k-i+1}} g^{A \cup B} \\ &+ \binom{t - (k-i)}{1} \sum_{\substack{A \subset T^c, |A| = i \\ B \subset T, |B| = k-i}} g^{A \cup B}, \end{aligned}$$

by considering how many times each S of the two classes appears in the sum $\sum_U \sum_S$. Since the first sum is 0 by inductive hypothesis, and $t - k + i \ge 1$, the second sum is also zero. Thus

$$\sum_{A \subset T^c, B \subset T, |A| = i, |B| = k-i} g^{A \cup B} = 0.$$

This proves Theorem 7.1.

The next theorem shows that any basis transformation on a 2-admissible G is just a scaling. The proof is omitted here.

THEOREM 7.2. *If G is 2-admissible with arity $2k$, then $\forall \boldsymbol{\beta} = \begin{pmatrix} n_0 & p_0 \\ n_1 & p_1 \end{pmatrix} \in \mathcal{M}$, $\boldsymbol{\beta}^{\otimes 2k} G = (n_0 p_1 - n_1 p_0)^k G$.*

COROLLARY 7.1. *If G is 2-admissible and realizable on some basis (e.g. on the standard basis), then it is 2-realizable.*

For $n = 6$, all 2-admissible G's form a 5 dimensional linear space. Applying the Matchgate Identities, we find that there are 5 different 2-realizable signatures (up to scaling). Let G_1 and G_2 be the following

$$g_1^\alpha = \begin{cases} 1, & \alpha \in \{000111, 011001, 101010, 110100\}, \\ -1, & \alpha \in \{111000, 100110, 010101, 001011\}, \\ 0, & \text{otherwise}, \end{cases}$$

$$g_2^\alpha = \begin{cases} 1, & \alpha \in \{010101, 011010, 100110, 101001\}, \\ -1, & \alpha \in \{101010, 100101, 011001, 010110\}, \\ 0, & \text{otherwise}. \end{cases}$$

Then all the 2-realizable signatures are obtained by cyclically rotating the indices of G_1 or G_2. (Rotating 3 bits on G_1 is G_1 itself up to a scaling factor -1; rotating 2 bits on G_2 gives G_2 back. So there are 3 different 2-realizable signatures from rotating G_1 and 2 different ones from rotating G_2.)

It turns out that all of these can be obtained from a *planar tensor product* operation.

DEFINITION 7.4. *Let $\mathrm{Rot}_r(G)$ be the tensor obtained by circularly rotating clockwise the coordinates of G by r bits. Let $G \otimes G'$ be the tensor product with all indices of G before all indices of G'. A planar tensor product is a finite sequence of operations of $\mathrm{Rot}_r(G)$ and $G \otimes G'$.*

THEOREM 7.3.

$$B_{gen}(\mathrm{Rot}_r(G)) = B_{gen}(G),$$

and

$$B_{gen}(G_1 \otimes G_2) = B_{gen}(G_1) \cap B_{gen}(G_2).$$

Thus a planar tensor product preserves B_{gen}.

The proof uses direct constructions and Matchgate Identities, and is omitted here.

THEOREM 7.4. *Each of the five 2-realizable signatures for $n = 6$ is obtainable as a planar tensor product from $(0, 1, -1, 0)$.*

From $(0, 1, -1, 0)$, we can construct a family of 2-realizable signatures for any arity $2k$ by planar tensor product.

In subsequent work we will report further developments along this direction.

DEFINITION 7.5. *A signature G is called prime iff it cannot be decomposed as a tensor product of two signatures of positive arity.*

In particular $(0, 1, -1, 0)$ is a prime 2-realizable signature.

Some results on prime signatures will be reported in forthcoming papers.

We can also prove that 1-admissibility (resp. 1-realizability) is strictly weaker than 2-admissibility (resp. 2-realizability). We have some constructions of 1-admissible and 1-realizable families which are not in general 2-admissible or 2-realizable. These are in fact prime signatures. These results are omitted here.

Acknowledgments

We would like to thank L. Valiant for many comments and discussions. We also thank E. Bach, S. Cook, J. Kleinberg, E. Hemaspaandra, L Hemaspaandra, S. Vadhan and A. Wigderson for their comments. Finally we wish to thank the anonymous referees for very insightful and helpful comments.

8. REFERENCES

[1] S. Aaronson and D. Gottesman. Improved simulation of stabilizer circuits. Phys. Rev. A 70, 052328 (2004).

[2] Bach, E. and Shallit, J. Algorithmic Number Theory, Vol. 1: Efficient Algorithms. MIT Press, 1996.

[3] J-Y. Cai and Vinay Choudhary. Some Results on Matchgates and Holographic Algorithms. In Proceedings of ICALP 2006, Part I. LNCS vol. 4051. pp 703-714. Also available at ECCC TR06-048, 2006.

[4] J-Y. Cai and Vinay Choudhary. Valiant's Holant Theorem and Matchgate Tensors. In Proceedings of TAMC 2006: LNCS vol. 3959, pp 248-261. Also available at ECCC Report TR05-118.

[5] J-Y. Cai, Vinay Choudhary and Pinyan Lu. On the Theory of Matchgate Computations. To appear in IEEE Conference on Computational Complexity 2007. Available at ECCC Report TR06-018.

[6] J-Y. Cai and Pinyan Lu. On Symmetric Signatures in Holographic Algorithms. In Proc. of STACS 2007. LNCS Vol. 4393, pp 429–440. Available at ECCC Report TR06-135.

[7] J-Y. Cai and Pinyan Lu. Bases Collapse in Holographic Algorithms. To appear in IEEE Conference on Computational Complexity 2007. Also at ECCC TR07-003.

[8] J-Y. Cai and Pinyan Lu. Holographic Algorithms: The Power of Dimensionality Resolved. Submitted. Also at ECCC TR07-020.

[9] J-Y. Cai and Pinyan Lu. On Block-wise Symmetric Signatures for Matchgates. Submitted. Also at ECCC TR07-019.

[10] E. Farhi, J. Goldstone, S. Gutmann and M. Sipser. Quantum Computation by Adiabatic Evolution. http://arxiv.org/abs/quant-ph/0001106 (January 2000)

[11] W. Foody and A. Hedayat. On theory and applications of BIB designs with repeated blocks, Annals Statist., 5 (1977), pp. 932-945.

[12] W. Foody and A. Hedayat. Note: Correction to "On Theory and Application of BIB Designs with Repeated Blocks". Annals of Statistics, Vol. 7, No. 4 (Jul., 1979), p. 925.

[13] D. Gottesman. The Heisenberg Representation of Quantum Computers. At http://arxiv.org/abs/quant-ph/9807006.

[14] R. L. Graham, S.-Y. R. Li, and W.-C. W. Li. On the Structure of t-Designs. SIAM. J. on Algebraic and Discrete Methods 1, 8 (1980).

[15] N. Linial and B. Rothschild. Incidence Matrices of Subsets–A Rank Formula. SIAM. J. on Algebraic and Discrete Methods 2, 333 (1981).

[16] D. Lichtenstein. Planar formulae and their uses. SIAM J. Comput. 11, 2:329-343.

[17] M. Jerrum. Two-dimensional monomer-dimer systems are computationally intractable. J. Stat. Phys. 48 (1987) 121-134; erratum, 59 (1990) 1087-1088

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

[19] P. W. Kasteleyn. Graph Theory and Crystal Physics. In *Graph Theory and Theoretical Physics*, Academic Press, 43-110 (1967).

[20] M. Kneser. "Aufgabe 360". Jahresbericht der Deutschen Mathematiker-Vereinigung, 2. Abteilung 58: 27. 1955.

[21] E. Knill. Fermionic Linear Optics and Matchgates. At http://arxiv.org/abs/quant-ph/0108033

[22] L. Lovász. "Kneser's conjecture, chromatic number, and homotopy". Journal of Combinatorial Theory, Series A 25: 319-324. 1978.

[23] J. Matoušek. "A combinatorial proof of Kneser's conjecture". Combinatorica 24 (1): 163-170. 2004.

[24] K. Murota. Matrices and Matroids for Systems Analysis, Springer, Berlin, 2000.

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

[26] S. P. Vadhan. The complexity of counting in sparse, regular, and planar graphs, SIAM J. on Computing 31 (2001) 398-427.

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

[28] L. G. Valiant. Expressiveness of Matchgates. *Theoretical Computer Science*, 281(1): 457-471 (2002).

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

[30] L. G. Valiant. Holographic circuits. In *Proc. 32nd International Colloquium on Automata, Languages and Programming*, 2005, 1–15.

[31] L. G. Valiant. Completeness for parity problems. In *Proc. 11th International Computing and Combinatorics Conference* (COCOON), LNCS, Vol. 3595, pp 1–8, (2005).

[32] L. G. Valiant. Accidental Algorithms. In *Proc.* of FOCS 2006, 509–517.