Journal of Computer and System Sciences 77 (2011) 41–61

Contents lists available at ScienceDirect

Journal of Computer and System Sciences

www.elsevier.com/locate/jcss

Holographic algorithms: From art to science ☆

Jin-Yi Cai [a,*,1], Pinyan Lu [b,2]

[a] Computer Sciences Department, University of Wisconsin, Madison, WI 53706, USA
[b] Microsoft Research Asia, Beijing, 100190, PR China

ARTICLE INFO

Article history:
Received 23 June 2009
Received in revised form 22 December 2009
Accepted 7 June 2010
Available online 11 June 2010

Keywords:
Holographic algorithm
Matchgate
Matchgate realizability

ABSTRACT

We develop the theory of holographic algorithms initiated by Leslie Valiant. First we define a basis manifold. Then we characterize algebraic varieties of realizable symmetric generators and recognizers on the basis manifold, and give a polynomial time decision algorithm for the simultaneous realizability problem. These results enable one to decide whether suitable signatures for a holographic algorithm are realizable, and if so, to find a suitable linear basis to realize these signatures by an efficient algorithm. 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 and some general constructions of admissible and realizable families.

1. Introduction

It is a testament to the enormous impact of NP-completeness theory [2,18] that the *conjecture* $P \neq NP$ has become a leading hypothesis in all computer science and mathematics. We consider it a great honor and privilege to dedicate this paper to the 2009 Kyoto Prize Laureate Prof. Richard M. Karp, a founder of this theory.

The NP-completeness theory is so well established that most computer scientists consider it a proof of computational intractability in terms of worst-case complexity if a problem is proved to be NP-complete. Expressed in terms of complexity classes, it has become more or less an article of faith among theoretical computer scientists that the *conjecture* $P \neq NP$ holds. The theory of holographic algorithms, however, provides a cautionary coda, that our understanding of the ultimate capability of polynomial time algorithms is far from well understood.

Certainly there are good reasons to believe the *conjecture* $P \neq NP$, 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. On the other hand, 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) [19,20,25]. In [27,29] L. Valiant introduced an algorithmic design technique of breathtaking originality, called *holographic algorithms*. 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 re-

☆ A preliminary version of this paper appeared in the 39th ACM Symposium on Theory of Computing (STOC 2007) (J.-Y. Cai and P. Lu (2007) [7]).

* Corresponding author.
E-mail addresses: jyc@cs.wisc.edu (J.-Y. Cai), pinyanl@microsoft.com (P. Lu).

[1] Supported by NSF CCR-0208013 and CCR-0511679.

[2] Work performed while the author was a graduate student at Tsinghua University.

0022-0000/$ – see front matter
doi:10.1016/j.jcss.2010.06.005

strictive 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 [30] 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, a result due to Xia et al. [31]; the problem mod 2, $\#_2$Pl-Rtw-Mon-3CNF, is known to be $\oplus$P-complete (thus NP-hard), a result due to Valiant [30]. The surprising tractability mod 7 is due to the unexpected existence of suitable generators and recognizers over $\mathbf{Z}_7$.

These signatures are specified by families of algebraic equations. These families of equations are typically exponential in size. Searching for their solutions is what Valiant called "the enumeration" of "freak objects" in his "Accidental algorithm" paper [30].[3] Dealing with such algebraic equations can be difficult due to the exponential size. So far the successes have been an expression of *artistic* inspiration.

To sustain a belief in $\mathrm{P} \neq \mathrm{NP}$, we must develop a systematic understanding of the capabilities of holographic algorithms. One might take the view that the problems such as $\#_7$Pl-Rtw-Mon-3CNF that have been solved in this framework are 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 $\mathrm{P} \neq \mathrm{NP}$ would have applied equally to $\#_7$Pl-Rtw-Mon-3CNF and to $\#_2$Pl-Rtw-Mon-3CNF. Thus, Valiant suggested in [29], "any proof of $\mathrm{P} \neq \mathrm{NP}$ 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.

In this paper we have achieved a complete account for all 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 $k \geqslant 3$ (the problem is trivial for $k \leqslant 2$). 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 linear basis for which certain signatures of both generators and recognizers can be simultaneously realized (we give a quick review of terminologies in Section 2. See [29,27,4,5] for more details). 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 polynomial in n. With this structural understanding we can give (i) a complete account of all the previous successes of holographic algorithms using symmetric signatures [29,5,30]; (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. We think this is 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. This is a part of the requirements 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 $d \geqslant 1$, on at least one side. Therefore it is important to investigate d-realizability and d-admissibility for $d \geqslant 1$. We give a complete characterization of 2-admissibility. We also give some non-trivial 1-admissible families, and 1- or 2-realizable families.

This paper is organized as follows. In Section 2 we give a review of terminologies. 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

[3] From [30]: "The objects enumerated are sets of polynomial systems such that the solvability of any one member would give a polynomial time algorithm for a specific problem. ... 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, if the objects in the enumeration have not been systematically studied previously."

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, for the convenience of readers, we review some definitions and results. More details can be found in [27,29,28,5,4,3].

Let $G = (V, E, W)$ and $G' = (V', E', W')$ be weighted undirected planar graphs, where V and V' are vertices, E and E' are edges, and W and W' are edge weights. A *generator matchgate* Γ is a tuple (G, X) where $X \subseteq V$ is a set of external *output* nodes. A *recognizer matchgate* Γ' is a tuple (G', Y) where $Y \subseteq V'$ 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 $\binom{m}{0}$, where V_0^m is the tensor space spanned by the m-fold tensor products of the standard basis $\mathbf{b} = [\mathbf{b}_0, \mathbf{b}_1] = \left[\binom{1}{0}, \binom{0}{1}\right]$. The tensor $\mathbf{G}$ under the standard basis $\mathbf{b}$ has the form

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

where

$$G^{i_1 i_2 \ldots i_m} = \text{PerfMatch}(G - Z),$$

where $\text{PerfMatch}(G - Z) = \sum_M \prod_{(i,j)\in M} w_{ij}$, is a sum over all perfect matchings M in $G - Z$, w_{ij} is the weight of the edge (i, j), and where Z is the subset of the output nodes of Γ having the characteristic sequence $\chi_Z = i_1 i_2 \ldots i_m$. 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

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

where

$$R_{i_1 i_2 \ldots i_m} = \text{PerfMatch}\big(G' - Z\big),$$

where Z is the subset of the input nodes of Γ' having the characteristic sequence $\chi_Z = i_1 i_2 \ldots i_m$.

In particular, $\mathbf{G}$ transforms as a contravariant tensor under a basis transformation $\boldsymbol{\beta}_j = \sum_i \mathbf{b}_i t_j^i$,

$$\big(G'\big)^{j_1 j_2 \ldots j_m} = \sum G^{i_1 i_2 \ldots i_m} \tilde{t}_{i_1}^{j_1} \tilde{t}_{i_2}^{j_2} \cdots \tilde{t}_{i_m}^{j_m},$$

where $(\tilde{t}_i^j)$ is the inverse matrix of (t_j^i). Similarly, $\mathbf{R}$ transforms as a covariant tensor, namely

$$\big(R'\big)_{j_1 j_2 \ldots j_m} = \sum R_{i_1 i_2 \ldots i_m} t_{j_1}^{i_1} t_{j_2}^{i_2} \cdots t_{j_m}^{i_m}.$$

A signature is *symmetric* if each entry only depends on the Hamming weight of the index $i_1 i_2 \ldots i_m$. This notion is invariant under a basis transformation. A symmetric signature is denoted by $[\sigma_0, \sigma_1, \ldots, \sigma_m]$, where σ_i denotes the value of a signature entry whose Hamming weight of its index is i.

A *matchgrid* $\Omega = (A, B, C)$ is a weighted planar graph consisting of a disjoint union of: a set of g generators $A = (A_1, \ldots, A_g)$, a set of r recognizers $B = (B_1, \ldots, B_r)$, and a set of f connecting edges $C = (C_1, \ldots, C_f)$, where each C_i edge has weight 1 and joins an output node of a generator with an 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 $\text{Holant}(\Omega)$ 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 C_k:

$$\text{Holant}(\Omega) = \langle \mathbf{R}, \mathbf{G} \rangle = \sum_{x \in \boldsymbol{\beta}^{\otimes f}} \left\{ \left[\prod_{1 \leqslant i \leqslant g} \mathbf{G}(A_i, x|_{A_i}) \right] \cdot \left[\prod_{1 \leqslant j \leqslant r} \mathbf{R}\big(B_j, x^*\big|_{B_j}\big) \right] \right\}.$$

(If we write the tensor product for the covariant tensor $\mathbf{R}$ as a row vector of dimension 2^f, and write the contravariant tensor $\mathbf{G}$ as a column vector of dimension 2^f, then $\text{Holant}(\Omega)$ is just the inner product of these two vectors.)

Valiant's beautiful Holant Theorem is

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

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

The FKT algorithm can compute the perfect matching polynomial $\mathrm{PerfMatch}(G)$ 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].

Theorem 2.2. *For any $n \times n$ skew-symmetric matrix M, and any $I = \{i_1, \ldots, i_K\} \subseteq [n]$ and $J = \{j_1, \ldots, j_L\} \subseteq [n]$,*

$$\sum_{l=1}^{L} (-1)^l \mathrm{Pf}(j_l, i_1, \ldots, i_K)\mathrm{Pf}(j_1, \ldots, \widehat{j_l}, \ldots, j_L) + \sum_{k=1}^{K} (-1)^k \mathrm{Pf}(i_1, \ldots, \widehat{i_k}, \ldots, i_K)\mathrm{Pf}(i_k, j_1, \ldots, j_L) = 0,$$

where the notation $\hat{\imath}$ indicates that the entry i is omitted.

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

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

Theorem 2.3. *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, $0 \leqslant i \leqslant n$,*

$$x_i = \lambda\big[(sn_0 + tn_1)^{n-i}(sp_0 + tp_1)^i + \epsilon(sn_0 - tn_1)^{n-i}(sp_0 - tp_1)^i\big]. \tag{1}$$

- *Form* 2: *there exists an* (*arbitrary*) *constant λ, such that for all i, $0 \leqslant i \leqslant n$,*

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

- *Form* 3: *there exists an* (*arbitrary*) *constant λ, such that for all i, $0 \leqslant i \leqslant n$,*

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

We take the convention that $\alpha^0 = 1$ and $0 \cdot \alpha^{0-1} = 0$.

Theorem 2.4. *A symmetric signature $[x_0, x_1, \ldots, x_n]$ for a generator is realizable under the basis $\boldsymbol{\beta} = [n, p] = \left[\binom{n_0}{n_1}, \binom{p_0}{p_1}\right]$ (more precisely in the dual basis)* 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, $0 \leqslant i \leqslant n$,*

$$x_i = \lambda\big[(sp_1 - tp_0)^{n-i}(-sn_1 + tn_0)^i + \epsilon(sp_1 + tp_0)^{n-i}(-sn_1 - tn_0)^i\big]. \tag{4}$$

- *Form* 2: *there exists an* (*arbitrary*) *constant λ, such that for all i, $0 \leqslant i \leqslant n$,*

$$x_i = \lambda\big[(n-i)p_1(n_0)^i(-p_0)^{n-1-i} - in_1(n_0)^{i-1}(-p_0)^{n-i}\big]. \tag{5}$$

- *Form* 3: *there exists an* (*arbitrary*) *constant λ, such that for all i, $0 \leqslant i \leqslant n$,*

$$x_i = \lambda\big[-(n-i)p_0(-n_1)^i(p_1)^{n-1-i} + in_0(-n_1)^{i-1}(p_1)^{n-i}\big]. \tag{6}$$

Theorem 2.5. *A symmetric signature $[x_0, x_1, \ldots, x_n]$ is realizable on some basis iff there exist three constants a, b, c (not all zero), such that for all k, $0 \leqslant k \leqslant n-2$,*

$$ax_k + bx_{k+1} + cx_{k+2} = 0. \tag{7}$$

The following two simple lemmas are used in the proof of Lemmas 4.5 and 4.6.

Lemma 2.1. *Suppose a sequence* $(x_i)_{i=0,1,\ldots,n}$, *where* $n \geqslant 3$, *has the following form*: $x_i = A\alpha^i + B\beta^i$ $(AB \neq 0,\ \alpha \neq \beta)$, *then the representation is unique. That is, if* $x_i = A'(\alpha')^i + B'(\beta')^i$ $(i = 0, 1, \ldots, n,\ n \geqslant 3)$, *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* $n \geqslant 3$, *has the following form*: $x_i = Ai\alpha^{i-1} + B\alpha^i$ $(A \neq 0)$, *then the representation is unique. That is, if* $x_i = A'i(\alpha')^{i-1} + B'(\alpha')^i$ $(i = 0, 1, \ldots, n,\ n \geqslant 3)$, *then* $A' = A$, $B' = B$, $\alpha' = \alpha$.

These follow from the fact that second order homogeneous linear recurrence sequence has a unique representation.

3. The basis manifold $\mathcal{M}$

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 [30], 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. In [8] and [9], we show that this is generally true, i.e., higher dimensional bases *do not* extend the reach of holographic algorithms. Therefore, in this paper we will develop our theory exclusively with bases of size 1; but our results are universally applicable.

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

Proposition 3.1 *(Valiant). (See [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* $xy \neq 0$.

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 $x, y \in \mathbf{F}^*$, the non-zero elements in $\mathbf{F}$, such that $n'_0 = xn_0$, $p'_0 = xp_0$, $n'_1 = yn_1$, $p'_1 = yp_1$ or $n'_0 = xn_1$, $p'_0 = xp_1$, $n'_1 = yn_0$, $p'_1 = yp_0$.

In other words, to obtain $\boldsymbol{\beta'}$ from $\boldsymbol{\beta}$, viewed as a 2×2 matrix, we can multiply each row by a non-zero constant, or exchange the two rows.

Theorem 3.1. $\mathrm{GL}_2(\mathbf{F})/\sim$ *is a 2-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 $\left(\begin{smallmatrix} 1 & x \\ 1 & y \end{smallmatrix}\right)$ 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 (Theorems 2.3–2.5). 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. The simultaneous realizability is equivalent to a non-empty intersection of these subvarieties. Thus we have to go beyond Theorems 2.3–2.5. For every signature which is realizable according to Theorem 2.5, we need to determine the subvariety where it is realizable.

Definition 4.1. Let $B_{rec}([x_0, x_1, \ldots, x_n])$ (resp. $B_{gen}([x_0, x_1, \ldots, x_n])$) be the set of all possible bases in $\mathcal{M}$ for which a symmetric signature $[x_0, x_1, \ldots, x_n]$ for a recognizer (resp. a generator) is realizable. We also use $B_{rec}(R)$ and $B_{gen}(G)$ to denote the realizability subvarieties for general (unsymmetric) signatures R and G.

Since the identically zero signature is realizable in every basis, we will assume the signature is not identically 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.

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

Remark. Every signature with arity 1 is trivially of this form. We will omit the scalar factor λ below as it is trivial. Since we will exclude the identically 0 signature, a and b are not both 0.

Proof of Lemma 4.1. If $n = 1$, the standard signature can and can only be $(\lambda, 0)$ or $(0, \lambda)$ (where λ is arbitrary). One entry of the signature must be zero due to the parity requirement, as matchgates are defined in terms of perfect matchings. So the signature over the basis $\left[\binom{n_0}{n_1}, \binom{p_0}{p_1}\right]$ is $(\lambda n_0, \lambda p_0)$ or $(\lambda n_1, \lambda p_1)$. Since we require the signature to be (a, b), all possible bases as expressed in $\mathcal{M}$ are $\left[\binom{a}{n_1}, \binom{b}{p_1}\right]$, taking into account the equivalence relation $\sim$, where n_1, p_1 are arbitrary, except $ap_1 - bn_1 \neq 0$.

Now we assume $n > 1$. First suppose this signature is expressed as Form 1 of Theorem 2.3.

In Form 1, denote by $u_0 = sn_0 + tn_1$, $u_1 = sp_0 + tp_1$, $v_0 = sn_0 - tn_1$, and $v_1 = sp_0 - tp_1$. Then up to a constant factor λ, for each $0 \leqslant i \leqslant n$, we have $u_0^{n-i}u_1^i + \epsilon v_0^{n-i}v_1^i = a^{n-i}b^i$.

We first assume $u_0 v_0 \neq 0$. Then by multiplying the equations for $i = 0$ and $i = 2$, and multiplying the equation for $i = 1$ by itself, we get an equation on u_0, u_1, v_0 and v_1. After some simplifications we get $u_1/u_0 = v_1/v_0$. Denote this common ratio by ρ.

We claim in this case $a \neq 0$, and $\rho = b/a$. Assume for a contradiction that $a = 0$, then all entries of the signature are 0 for $i = 0, \ldots, n-1$. However the entry at $i = n$ is obtained from the entry at $i = n-1$ by multiplying with the ratio ρ, and thus it is also 0. Then it follows that $b = 0$ as well, contrary to assumption. Therefore $a \neq 0$ and b/a is defined. Now consider the signature entry at $i = 0$ and $i = 1$. The entry at $i = 0$ is $a^n \neq 0$, and the entry at $i = 1$ is obtained by multiplying the non-zero entry at $i = 0$ by the ratio b/a, as well as by the common ratio ρ. It follows that $\rho = b/a$.

Hence $bu_0 = au_1$ and $bv_0 = av_1$. Then by the definitions of u_i and v_j, it follows that $bsn_0 = asp_0$ and $btn_1 = atp_1$. Because at least one of a, b is non-zero, we claim that this implies either $s = 0$ or $t = 0$. Otherwise, $st \neq 0$, we have $n_0p_1 - n_1p_0 = 0$. This is impossible. So we must have $s = 0$ or $t = 0$ (and not both zero since otherwise the signature is identically zero). Now in either cases, it is easy to verify that all the possible bases are $\left[\binom{a}{n_1}, \binom{b}{p_1}\right] \in \mathcal{M}$, taking into account the equivalence relation $\sim$, where n_1, p_1 are arbitrary, except $ap_1 - bn_1 \neq 0$.

The same conclusion holds if we assume $u_1 v_1 \neq 0$. To complete the proof, assume both $u_0 v_0 = 0$ and $u_1 v_1 = 0$. By symmetry, suppose $u_0 = 0$ (the other cases are symmetric). In this case if $u_1 = 0$ as well, then $s = t = 0$ since the determinant $n_0p_1 - n_1p_0 \neq 0$. Then $v_0 = v_1 = 0$ and the signature is identically zero. Hence $u_1 \neq 0$. Then $v_1 = 0$. It follows that the signature has the form $\lambda[\epsilon v_0^n, 0, \ldots, 0, u_1^n]$, where there are a non-empty segment of zeros corresponding to $0 < i < n$. These are of the form $a^{n-i}b^i$, and thus $ab = 0$. But then the signature entry is zero at either $i = 0$ or at $i = n$. Since $u_1 \neq 0$, we get $v_0 = 0$. The statement of the lemma clearly holds when $u_0 = v_0 = 0$.

Now suppose the signature is expressed as Form 2 of Theorem 2.3. (The case with Form 3 is symmetric, exchanging subscript 0 for 1 in the basis.)

In that expression, if $n_1 = 0$, then $a = 0$ since $x_0 = a^n = nn_0n_1^{n-1} = 0$. At $i = n-1$, $x_{n-1} = n_0p_1^{n-1} = a^{n-1}b = 0$. This gives $n_0 = 0$ or $p_1 = 0$, together with $n_1 = 0$, we get a singular basis.

So we have $n_1 \neq 0$. Then we claim $a \neq 0$. Otherwise at $i = 0$, $x_0 = nn_0n_1^{n-1} = a^n = 0$, which implies that $n_0 = 0$. At $i = 1$, $x_1 = p_0n_1^{n-1} = a^{n-1}b = 0$, we get $p_0 = 0$. This gives a singular basis. So $a \neq 0$, and from the above we also get $n_0 \neq 0$. Then up to a scalar factor $a^n = 1$, $a^{n-1}b = c + \rho$, and $a^{n-2}b^2 = 2c\rho + \rho^2$, for $c = (n_1p_0 - n_0p_1)n_1/nn_0$ and $\rho = p_1/n_1$. It follows that $2c\rho + \rho^2 = (c + \rho)^2$, which implies that $c = 0$. As the determinant $n_1p_0 - n_0p_1 \neq 0$, and $n_1 \neq 0$, we get a contradiction.

This completes the proof. □

Definition 4.2. A symmetric signature $[x_0, x_1, \ldots, x_n]$, where $n \geqslant 2$, is called non-degenerate iff $\operatorname{rank}\left[\begin{smallmatrix} x_0 & \cdots & x_{n-1} \\ x_1 & \cdots & x_n \end{smallmatrix}\right] = 2$. Otherwise it is degenerate.

The signature is identically 0 iff $\operatorname{rank}\left[\begin{smallmatrix} x_0 & \cdots & x_{n-1} \\ x_1 & \cdots & x_n \end{smallmatrix}\right] = 0$. It has rank 1 iff it can be expressed as $\lambda[a^n, a^{n-1}b, \ldots, b^n]$, for $\lambda \neq 0$, and a, b not both 0. In the following we assume the signature is non-degenerate. We directly handle the case for arity $n = 2$ next.

Lemma 4.2.

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

Proof. Under the equivalence relation, we can assume $n_0 p_1 - n_1 p_0 = 1$.

Then $\left[\binom{n_0}{n_1}, \binom{p_0}{p_1}\right]^{-1} = \left[\binom{p_1}{-n_1}, \binom{-p_0}{n_0}\right]$. So the standard signature of $[x_0, x_1, x_2]$ is

$$\left[x_0 p_1^2 - 2x_1 p_1 n_1 + x_2 n_1^2, x_0 p_0 p_1 - x_1(n_0 p_1 + n_1 p_0) + x_2 n_0 n_1, x_0 p_0^2 - 2x_1 p_0 n_0 + x_2 n_0^2\right].$$

The fact that the only constraint of a standard signature of arity 2 is the parity constraint completes the proof. □

In the following we assume the signature has arity $n \geqslant 3$, and non-degenerate. In this case, we note that the constants a, b, c in Theorem 2.5 are unique up to a scalar factor. In fact if there are two linearly independent triples (a, b, c), then the following matrix

$$\begin{bmatrix} x_0 & x_1 & \dots & x_{n-2} \\ x_1 & x_2 & \dots & x_{n-1} \\ x_2 & x_3 & \dots & x_n \end{bmatrix}$$

has rank $\leqslant 1$. The first row and the last row are not both zero, otherwise the signature is identically zero (by $n \geqslant 3$). It follows that the matrix

$$\begin{bmatrix} x_0 & x_1 & \dots & x_{n-1} \\ x_1 & x_2 & \dots & x_n \end{bmatrix}$$

also has rank 1, hence the signature is degenerate.

Lemma 4.3. *Let $\lambda_1 \neq 0$. Let $p = \mathrm{char}.\mathbf{F}$. Suppose $p = 0$, or $p \nmid n$,*

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

For $p \mid n$ and $\lambda_2 = 0$, $B_{rec}([0, 0, \dots, 0, \lambda_1, 0]) = \left\{\left[\binom{0}{n_1}, \binom{1}{p_1}\right] \in \mathcal{M} \mid n_1, p_1 \in \mathbf{F}\right\}$. For $p \mid n$ and $\lambda_2 \neq 0$, the signature $[0, 0, \dots, 0, \lambda_1, \lambda_2]$ is not realizable.

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

Lemma 4.4. *For $AB \neq 0$,*

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

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

In the following we use the fact that the triple (a, b, c) in the statement of Theorem 2.5 is unique up to a scalar factor. Also in the remaining cases we may assume $c \neq 0$. So we have a unique characteristic equation $cx^2 + bx + a = 0$, which has two roots α and β. In particular Forms 1, 2 and 3 from Theorem 2.3 are mutually exclusive. If $\alpha \neq \beta$, we have the following lemma:

Lemma 4.5. *For $AB \neq 0$ and $\alpha \neq \beta$,*

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

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

Proof of Lemma 4.5. From $A + B = x_0$, $A\alpha + B\beta = x_1$, we can solve uniquely for A, B. We have $AB \neq 0$; otherwise $\{x_i\}$ has the form $\{a^{n-i}b^i\}$, which has been dealt with in Lemma 4.1. Having two distinct eigenvalues $\alpha \neq \beta$, this signature must be expressed as Form 1 of Theorem 2.3. Let $u_0 = sn_0 + tn_1$, $u_1 = sp_0 + tp_1$, $v_0 = sn_0 - tn_1$, and $v_1 = sp_0 - tp_1$. Then $A\alpha^i + B\beta^i = u_0^{n-i}u_1^i + \epsilon v_0^{n-i}v_1^i$.

We claim $u_0 \neq 0$. Otherwise, for $i = 0, 1, \dots, n-1$, the signature entry at i is $\epsilon v_0^{n-i}v_1^i$. It follows that $(A + B)(A\alpha^2 + B\beta^2) = (A\alpha + B\beta)^2$, and since $AB \neq 0$, we get $\alpha = \beta$, a contradiction. Similarly we have $v_0 \neq 0$.

Hence we have two expressions

$$x_i = A\alpha^i + B\beta^i = u_0^n\left(\frac{u_1}{u_0}\right)^i + \epsilon v_0^n\left(\frac{v_1}{v_0}\right)^i.$$

From Lemma 2.1, we know that the representation is unique. So $u_0^n = A$, $\epsilon v_0^n = B$, $\frac{u_1}{u_0} = \alpha$ and $\frac{v_1}{v_0} = \beta$ (exchanging notations A with B, and α with β if necessary). It follows that $\left[\binom{2sn_0}{2tn_1}, \binom{2sp_0}{2tp_1}\right] = \left[\binom{u_0+v_0}{u_0-v_0}, \binom{u_1+v_1}{u_1-v_1}\right]$. Since $\alpha \neq \beta$, we can show $st \neq 0$, by the same proof showing $u_0 \neq 0$ and $v_0 \neq 0$. Now let $\omega = v_0/u_0$, then $\omega^n = \pm B/A$, and

$$\left[\binom{n_0}{n_1}, \binom{p_0}{p_1}\right] \sim \left[\binom{2sn_0}{2tn_1}, \binom{2sp_0}{2tp_1}\right] \sim \left[\binom{1+\omega}{1-\omega}, \binom{\alpha+\beta\omega}{\alpha-\beta\omega}\right].$$

This completes the proof. □

If the characteristic roots $\alpha = \beta$, we have the following lemma:

Lemma 4.6. *Let $p = \mathrm{char}.\mathbf{F}$ and let $A \neq 0$.*

Case 1: *$p = 0$ or $p \nmid n$.*

$$B_{rec}\left(\left[Ai\alpha^{i-1} + B\alpha^i \mid i = 0, 1, \ldots, n\right]\right) = \left\{\left[\binom{1}{B}, \binom{\alpha}{nA + B\alpha}\right]\right\}.$$

Case 2: *$p \mid n$ and $x_0 = 0$. In this case, the signature has entries $x_i = Ai\alpha^{i-1}$, with $B = 0$ in the above form.*

$$B_{rec}\left(\left[Ai\alpha^{i-1} \mid i = 0, 1, \ldots, n\right]\right) = \left\{\left[\binom{1}{n_1}, \binom{\alpha}{p_1}\right] \in \mathcal{M} \;\middle|\; n_1, p_1 \in \mathbf{F}\right\}.$$

Case 3: *$p \mid n$ and $x_0 \neq 0$. In this case the signature $[Ai\alpha^{i-1} + B\alpha^i \mid i = 0, 1, \ldots, n]$ is not realizable.*

Remark. If $\alpha = 0$, and $i = 0$, we take the convention that $i\alpha^{i-1} = 0$, and also $\alpha^i = 1$.

Proof of Lemma 4.6. 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 2.3 we claim $n_1 \neq 0$. Otherwise, all signature entries $x_i = 0$ for $i = 0, \ldots, n-2$. Since $n \geqslant 3$, we have $x_0 = x_1 = 0$, which implies that $A = 0$, contrary to assumption. In the following we assume Form 2 of Theorem 2.3, Form 3 will give an equivalent basis. Then we have $x_i = i(n_1 p_0 - n_0 p_1) n_1^n (\frac{p_1}{n_1})^{i-1} + n n_0 n_1^{n-1} (\frac{p_1}{n_1})^i$. So by uniqueness $(n_1 p_0 - n_0 p_1) n_1^n = A$, $\frac{p_1}{n_1} = \alpha$, $n n_0 n_1^{n-1} = B$. 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 Cases 2 and 3. □

The above list of realizable symmetric signatures for recognizers is complete and mutually exclusive. To see that, by Theorem 2.5, we have a recurrence relation for any realizable signature. The case for any degenerate signature, including the case $n = 1$, is handled in Lemma 4.1. Now assume the signature is non-degenerate. The case $n = 2$ is handled in Lemma 4.2. Next we assume the signature is non-degenerate and arity $n \geqslant 3$. Then Theorem 2.5 provides a tuple $(a, b, c) \neq 0$, unique up to a non-zero constant multiple. If $c \neq 0$ this defines a unique second order recurrence relation. If $a \neq 0$ this defines a unique second order recurrence relation for the reversal. (If both $a = 0$ and $c = 0$, this defines the signature $[A, 0, \ldots, 0, B]$ where $AB \neq 0$, due to non-degeneracy. This is included in Lemma 4.4, with $\alpha = 0$.) Assume $c \neq 0$ then the recurrence relation is second order and has eigenvalues α and β. Depending on whether it has a pair of distinct eigenvalues or a double eigenvalue, we have Lemmas 4.5 and 4.6. The case when the recurrence relation is for the reversal signature results in the same expression, except in the case when one of the eigenvalue is 0. And these special cases are handled in Lemmas 4.4 and 4.3 respectively.

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.

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

Lemma 4.8.

$$B_{gen}\left([x_0, x_1, x_2]\right) = \left\{\left[\binom{n_0}{n_1}, \binom{p_0}{p_1}\right] \in \mathcal{M} \;\middle|\; \begin{array}{c} x_0 n_0^2 + 2x_1 n_0 p_0 + x_2 p_0^2 = 0, x_0 n_1^2 + 2x_1 n_1 p_1 + x_2 p_1^2 = 0 \\ \text{or } x_0 n_0 n_1 + x_1(n_0 p_1 + n_1 p_0) + x_2 p_0 p_1 = 0 \end{array}\right\}.$$

Lemma 4.9. *Let $\lambda_1 \neq 0$. Let $p = \text{char.}\mathbf{F}$. Suppose $p = 0$, or $p \nmid n$,*

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

For $p \mid n$ and $\lambda_2 = 0$, $B_{gen}([0, 0, \ldots, 0, \lambda_1, 0]) = \left\{ \left[\binom{1}{n_1}, \binom{0}{p_1} \right] \in \mathcal{M} \mid n_1, p_1 \in \mathbf{F} \right\}$. For $p \mid n$ and $\lambda_2 \neq 0$, then $[0, 0, \ldots, 0, \lambda_1, \lambda_2]$ is not realizable.

Lemma 4.10. *For $AB \neq 0$,*

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

Lemma 4.11. *For $AB \neq 0$ and $\alpha \neq \beta$,*

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

Lemma 4.12. *Let $p = \text{char.}\mathbf{F}$ and let $A \neq 0$.*

Case 1: *$p = 0$ or $p \nmid n$.*

$$B_{gen}(\{Ai\alpha^{i-1} + B\alpha^i \mid i = 0, 1, \ldots, n\}) = \left\{ \left[\begin{pmatrix} nA + B\alpha \\ -\alpha \end{pmatrix}, \begin{pmatrix} -B \\ 1 \end{pmatrix} \right] \right\}.$$

Case 2: *$p \mid n$ and $x_0 = 0$. In this case, the signature has entries $x_i = Ai\alpha^{i-1}$, with $B = 0$ in the above form*:

$$B_{gen}([Ai\alpha^{i-1} \mid i = 0, 1, \ldots, n]) = \left\{ \left[\begin{pmatrix} -\alpha \\ n_1 \end{pmatrix}, \begin{pmatrix} 1 \\ p_1 \end{pmatrix} \right] \in \mathcal{M} \,\middle|\, n_1, p_1 \in \mathbf{F} \right\}.$$

Case 3: *$p \mid n$ and $x_0 \neq 0$. In this case the signature $[Ai\alpha^{i-1} + B\alpha^i \mid i = 0, 1, \ldots, n]$ is not realizable.*

4.3. Simultaneous realizability

Definition 4.3. 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 exists; "NO" if they are not simultaneously realizable.

Algorithm.

For every signature $[x_0, x_1, \ldots x_n]$, check if it satisfies Theorem 2.5.
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 one of the lemmas.
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 2.5 can obviously be done in polynomial time. To find the right form and then the right lemma for a signature which satisfies Theorem 2.5 can also be done in polynomial time as they are mutually exclusive.

Every subvariety of bases from Lemmas 4.1 to 4.6 and from Lemmas 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. Expressing things in terms of the manifold $\mathcal{M}$ shows that: For Lemma 4.1 we get a line with $x = \text{const.}$ (in the notation defining $\mathcal{M}$). 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. (Solving quadratic equations over large finite field may require randomized polynomial time.)

For Lemma 4.3 we have either a single point for $p \mid n$ 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 **Q** or an algebraic extension field of **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 (i.e., in randomized polynomial time). We need to be able to solve equations such as $X^n = \text{const}$. These can be done in randomized polynomial time; see [1] for more details. □

5. Some not-so-accidental algorithms

In [30], 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 $k = 3$.

To solve the problem by a holographic algorithm, we wish to replace each variable by a generator with the signature $[1, 0, 1]$, and each clause by a recognizer with the signature $[0, 1, 1, \ldots, 1]$ (with k 1's). The symmetric signature $[1, 0, 1]$ corresponds to a consistent truth assignment on two edges leading to clauses (i.e. the equality function $=_2$ on two Boolean inputs), and $[0, 1, 1, \ldots, 1]$ corresponds to a Boolean OR function 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 **Q**).

Then the question boils down to whether there is a basis in $\mathcal{M}$ where $[1, 0, 1]$ for a generator and $[0, 1, 1, \ldots, 1]$ (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

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

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

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 $p \mid 2^k - 1$, #$_p$Pl-Rtw-Mon-kCNF is computable in polynomial time. In particular this is true for every Mersenne prime $2^q - 1$. (Note that $\omega^2 = 2$ means that 2 is a quadratic residue.) 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 **C**, from Lemmas 4.8 and 4.4, we can see that a generator for $[1, 0, 1]$ and a recognizer for $[1 + \epsilon 2^{k/2}, 1, 1, \ldots, 1]$ (where there are k 1's, and $\epsilon = \pm 1$) are simultaneously realizable in the basis $\boldsymbol{\beta} = \left[\binom{1+\sqrt{2}}{1-\sqrt{2}}, \binom{1}{1}\right]$.

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

$$\text{Holant}(\Omega) = \text{PerfMatch}(G). \tag{8}$$

We will denote this value by X.

From the left-hand side of (8) 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 (8) 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 $\mathbf{Z}_{2^k-1}$. (Formally we could develop the theory over such a ring, and consider invertible elements and matrices for the basis manifold. But we will omit this formality; everything we need can be easily done by a slight modification of the proofs given before.) 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 $\boldsymbol{\beta} = \left[\binom{1+\sqrt{2}}{1-\sqrt{2}}, \binom{1}{1}\right] = \left[\binom{1+2^{(k+1)/2}}{1-2^{(k+1)/2}}, \binom{1}{1}\right]$, we have a generator for $[1,0,1]$ and a recognizer for $[0,1,1,\ldots,1]$ (with k 1's) according to Lemmas 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 $p \mid 2^k - 1$, 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. These are called regular $(k,2)$-bipartite graphs. 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 [30]. 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 $[2,1,1,\ldots,1]$ (with k 1's), to be simultaneously realized over some basis.

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

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

We realize that this set is exactly the same as $B_{rec}([0,1,1,\ldots,1])$. 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 cannot be simultaneously realized. As an example, one may wish to extend the previous two problems to allow more than Read-twice as in #Pl-R_l-Mon-kCNF, where $l > 2$. This calls for a simultaneous realizability of $[1,0,0,\ldots,0,1]$ (where there are $(l-1)$ 0's) and $[0,1,1,\ldots,1]$ (where there are k 1's). This can be shown to result in an empty intersection on $\mathcal{M}$.

5.3. An edge-vertex cover problem

Another way to think of a regular $(k,2)$-bipartite graph is to identify every degree 2 vertex on the right together with its two incident edges as a new edge. Then we obtain precisely the class of k-regular graphs. We say a subset of edges *and* vertices is an *edge-vertex cover* if every vertex is either in the subset or all of its k incident edges are in the subset. We consider the following edge-vertex cover problem $\#_{2^k-1}$Pl-k-Reg-EVC: Given a planar k-regular graph G, count the number of edge-vertex covers of G mod $2^k - 1$.

It is clear that this problem is really the same problem as the one in Section 5.2 and thus the same algorithm also gives a polynomial time algorithm for this problem.

Theorem 5.3. *There is a polynomial time algorithm for $\#_{2^k-1}$Pl-k-Reg-EVC. Furthermore, any modulus m for which the appropriate signatures exist must be a divisor of $2^k - 1$.*

5.4. A problem from neural networks

Consider the following planar two-level neural network N: The input nodes are Boolean variables $x_1, \ldots, x_n$. Each x_i has fan-out 2. The intermediate level nodes v all have fan-in k from the x_i's. The output of v feeds into the top node and can have $c+1$ different values $0, 1, \ldots, c$. If all k inputs of v are 0 then the output of v is 0 (unexcited state). Otherwise, the output of v can be any of the $c+1$ values (excited state). The problem is to count the total number of output (firing) patterns as received at the top node. (In the following, for simplicity we state the result for an odd c. We have a parallel set of results for c even, but the statement has some number theoretic complications.)

$\#_{2^k-c^2}$NN$k/c$-Firing-Pattern.
Input: A two-level neural network with parameters k and c as above.
Output: The number mod $(2^k - c^2)$ of all possible firing patterns.

First we suppose k is even. Then we do it over $\mathbf{C}$ by taking $\omega = \sqrt{2}$. We can use the same basis in Section 5.1 to realize the signature $[1 + 2^{k/2}, 1, 1, \ldots, 1]$ (with k 1's) for a recognizer and the signature $[1, 0, 1]$ for a generator simultaneously. This is verified by $\omega^2 = 2$ and $\omega^k = 2^{k/2}$.

Let X be the value of the Holant. With mod $2^{k/2} - c$, the recognizer signature is the same as $[1 + c, 1, 1, \ldots, 1]$. Thus

$$X \equiv \#\text{NN}k/c\text{-Firing-Pattern} \pmod{2^{k/2} - c}.$$

Similarly we can also achieve the signature $[1 - 2^{k/2}, 1, 1, \ldots, 1]$ (with k 1's) for a recognizer and the signature $[1, 0, 1]$ for a generator simultaneously. This is verified by $\omega^2 = 2$ and $\omega^k = -(-2^{k/2})$. This recognizer signature is congruent to $[1 + c, 1, 1, \ldots, 1]$ mod $2^{k/2} + c$. Thus we can compute in polynomial time some value X' for a Holant, where

$$X' \equiv \#\text{NN}k/c\text{-Firing-Pattern} \pmod{2^{k/2} + c}.$$

Then by Chinese remaindering, we can compute the value #NN$k/c$-Firing-Pattern modulo the l.c.m. of $2^{k/2} - c$ and $2^{k/2} + c$. Since c is odd, this is $2^k - c^2$.

Now we suppose k is odd. As c is relatively prime to $N = 2^k - c^2$, there exists a c' such that $cc' \equiv 1 \bmod N$. Take $\omega = 2^{(k+1)/2}c'$. Then $\omega^2 = 2^{k+1}c'^2 \equiv 2 \bmod N$. Also $\omega^k = (2^k)^{(k+1)/2}c'^k \equiv c^{k+1}c'^k \equiv c \bmod N$. Thus we can construct $[1 + c, 1, 1, \ldots, 1]$ (with k 1's) for a recognizer and the signature $[1, 0, 1]$ for a generator simultaneously in the ring $\mathbf{Z}_N$ directly.

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 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 $[0, 1, 1, \ldots, 1, 0]$ ($(k-1)$ 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, taking α, β to be the two roots of $x^2 - x + 1 = 0$ and $A/B = -1$, we have $B_{rec}([0, 1, 1, 0]) = \left\{\left[\binom{1+\omega}{1-\omega}, \binom{\alpha+\beta\omega}{\alpha-\beta\omega}\right] \mid \omega^3 = \pm 1\right\}$.

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

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

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. 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 from [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 $[1, 1, 0, \ldots, 0]$ ($(k-1)$ 0's) simultaneously. From Lemma 4.6, with $A = B = 1$, $\alpha = 0$, we have: $B_{rec}([1, 1, 0, \ldots, 0]) = \left\{\left[\binom{1}{1}, \binom{0}{k}\right]\right\}$. We hope that $\left[\binom{1}{1}, \binom{0}{k}\right] \in B_{gen}([1, 1, 0])$.

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 $\left[\binom{1}{1}, \binom{0}{k}\right]$ 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 $k + 1$.*

6.3. ⊕PL-EVEN-LIN2

In this problem, we wish to construct generators for $[1, x, 1]$, $[x, 1, x]$, $[1, 0, 1]$, $[0, 1, 0]$, $[1, 0, 0, \ldots, 0, 1]$ and recognizers for $[1, 0, -1, 0, 1]$, $[0, 1, 0, -1, 0]$, $[1, 0, 1]$, $[0, 1, 0]$.

By Lemma 4.5, for $A = B = 1/2$, $\alpha = i$, $\beta = -i$ (here $i = \sqrt{-1}$), we have

$$B_{rec}\big([1, 0, -1, 0, 1]\big) = \left\{\left[\binom{1+\omega}{1-\omega}, \binom{i-i\omega}{i+i\omega}\right] \,\middle|\, \omega^4 = \pm 1\right\}.$$

We hope that $\left[\binom{1+\omega}{1-\omega}, \binom{i-i\omega}{i+i\omega}\right]$ is also a basis for the recognizer $[0, 1, 0]$.

By Lemma 4.2, we require that $(1 + \omega)(i + i\omega) + (1 - \omega)(i - i\omega) = 0$. That is, $\omega = i$, and

$$\left[\binom{1+\omega}{1-\omega}, \binom{i-i\omega}{i+i\omega}\right] = \left[\binom{1+i}{1-i}, \binom{i+1}{i-1}\right] = \left[\binom{1}{1}, \binom{1}{-1}\right].$$

We can easily verify that this is also a basis for the other recognizers and generators and we remark that this basis is precisely **b2** in [29]. One can also prove 2 is the only modulus for this problem.

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 $G = (g^{i_1 i_2 \ldots i_n})$ where the index $i_1 i_2 \ldots i_n \in \{0, 1\}^n$. We also denote $G = (g^S)$ where $S \subseteq [n]$, and $g^S = g^{\chi_S(1)\chi_S(2)\ldots\chi_S(n)}$. 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 (g'^S) to be realizable:

Parity constraints: 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*.

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 constraints*. 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. Any success of 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 $B_{gen}(G)$ (and the corresponding subvarieties for recognizers). More precisely,

Definition 7.2. A generator G is called d-realizable (resp. d-admissible) for an integer $d \geqslant 0$ iff $B_{gen}(G) \subseteq \mathcal{M}$ (resp. $B^p_{gen}(G) \subseteq \mathcal{M}$) is a (non-empty) algebraic subset of dimension at least d.

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 $\leqslant 1$. 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.

7.1. Characterization of 2-admissibility

The following theorem is a complete characterization of 2-admissibility over fields of characteristic 0. It uses rank estimates related to the *Kneser Graph* $\mathrm{KG}_{2k+1,k}$ [21–23,12–15].

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 $T \subseteq [n]$ with $|T| = k+1$,*

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

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

Consider all subsets of $[n]$ of a certain cardinality. Let $0 \leqslant k \leqslant \ell \leqslant n$, and let $A_{k,\ell,n}$ denote the $\binom{n}{k} \times \binom{n}{\ell}$ Boolean matrix indexed by (A, B), where $A, B \subseteq [n]$ and $|A| = k, |B| = \ell$, and the entry at (A, B) is $\chi_{[A \subseteq B]}$, i.e., it is 1 if $A \subseteq B$ and 0 otherwise. It is known that over the rationals $\mathbf{Q}$, the rank $\mathrm{rk}(A_{k,\ell,n}) = \min\{\binom{n}{k}, \binom{n}{\ell}\}$ [12–15]. We will not deal with finite characteristics here. The situation with finite characteristic p is interesting and is more involved. For example, Linial and Rothschild [15] proved exact rank formula 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. $G = (g^S)_{S \subseteq [n]}$ is called d-admissible if the following algebraic variety V has dimension at least d, where $V = V_0 \cup V_1 \subseteq \mathcal{M}$, 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.

More precisely, consider V_0. We take a point (in dehomogenized coordinates) $\left(\begin{smallmatrix} 1 & x \\ 1 & y \end{smallmatrix}\right) \in \mathcal{M}$. We also denote $x_0 = x$, $x_1 = y$. Let $T \subseteq [n]$ with $|T|$ even. Then we require

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

Note that the left-hand side is precise the entry of the standard signature indexed at T, under the (contravariant) basis transformation. Similarly we define V_1, where the equations are over all T with an odd cardinality.

We note that

$$\left\langle \bigotimes_{\sigma=1}^{n} [1, x_{[\sigma \in T]}], G \right\rangle = \sum_{\substack{0 \leqslant i \leqslant n-|T| \\ 0 \leqslant j \leqslant |T|}} x^i y^j \sum_{\substack{A \subseteq T^c,\, |A|=i \\ B \subseteq T,\, |B|=j}} g^{A \cup B}. \tag{10}$$

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 $T \subseteq [n]$ with $|T|$ even, and for all $0 \leqslant i \leqslant n - |T|$ and $0 \leqslant j \leqslant |T|$,

$$\sum_{A \subseteq T^c,\, B \subseteq T,\, |A|=i,\, |B|=j} g^{A \cup B} = 0. \tag{11}$$

(If there is one equation not satisfied, then there is at least one non-trivial polynomial among the parity requirements, which implies $\dim(V_0) \leqslant 1$.) 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 $T \subseteq [n]$ with $|T|$ even, and $j \leqslant |T|$,

$$\sum_{S \subseteq T,\, |S|=j} g^S = 0. \tag{12}$$

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

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

If $S \subseteq [n]$ 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 $S \subseteq [n]$. That is, G is trivial.

An identical argument also shows that for n odd and $\dim(V_1) = 2$, 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

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

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

$$\sum_{S \supseteq T',\, |S|=i} g^S = 0. \tag{13}$$

If $|S| = i < k$, we form the following system of equations from (12),

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

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 (13) 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 $T \subseteq [n]$ with $|T| = k + 1$,*

$$\sum_{S \subseteq T,\, |S|=k} g^S = 0. \tag{14}$$

Next we prove that the conditions in Lemma 7.1 are also sufficient for G being 2-admissible, i.e., we prove (11), thus all the polynomials in (10) 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 (11) for all $i + j = k$, namely for all $T \subseteq [n]$ with $|T|$ even, and for all $0 \leqslant i \leqslant n - |T|$, and $0 \leqslant j = k - i \leqslant |T|$,

$$\sum_{A \subseteq T^c,\, B \subseteq T,\, |A|=i,\, |B|=k-i} g^{A \cup B} = 0. \tag{15}$$

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

We prove (15) by induction on $i \geqslant 0$. The base case is $i = 0$ and $j = k$. Let's consider all $U \subseteq T$ with $|U| = k + 1$. Note that as $t \geqslant k + 1$, this is not vacuous. By (14) we have

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

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

$$\sum_{\substack{A \subseteq T^c,\, |A|=0 \\ B \subseteq T,\, |B|=k}} g^{A \cup B} = \sum_{S \subseteq T,\, |S|=k} g^S = \frac{1}{\binom{t-k}{1}} \sum_{\substack{U \subseteq T \\ |U|=k+1}} \sum_{S \subseteq U,\, |S|=k} g^S = 0. \tag{16}$$

Inductively we assume (15) has been proved for $i-1$, for some $i \geqslant 1$. Consider i and $j = k-i$. We may assume $i \leqslant s$; otherwise we are done. Also $k-i+1 \leqslant k+1 \leqslant t$. Consider all subsets $U = U_1 \cup U_2 \subseteq [n]$, where $U_1 \subseteq T^c$, $U_2 \subseteq T$, with $|U_1| = i$ and $|U_2| = k-i+1$. Note that $|U| = k+1$. We have

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

as all sets $S \subseteq U$ 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,

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

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 $t-k+i \geqslant 1$, the second sum is also zero. Thus

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

This proves Theorem 7.1.

We can further prove:

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

In order to prove this theorem, we first prove the following lemma:

Lemma 7.2. *Let G be 2-admissible with arity $2k$, $S \subseteq [2k]$ with $|S| = k$, and $A \subseteq S^c$. Then*

$$\sum_{B \subseteq S \text{ and } |B|=k-|A|} g^{A \cup B} = (-1)^{|A|} g^S.$$

Proof. We prove it by induction on $|A| \geqslant 0$.

The case $|A| = 0$ is obvious.

Inductively we assume the lemma has been proved for all $|A| \leqslant i-1$, for some $i \geqslant 1$. Letting $|A| = i > 0$ and letting G be 2-admissible, it follows from Lemma 7.1 that we have

$$\sum_{C \subseteq A \cup S \text{ and } |C|=k} g^C = 0.$$

Then

$$\begin{aligned} 0 &= \sum_{C \subseteq A \cup S \text{ and } |C|=k} g^C \\ &= \sum_{B \subseteq S \text{ and } |B|=k-|A|} g^{A \cup B} + \sum_{t=0}^{|A|-1} \sum_{A_1 \subseteq A,\, |A_1|=t} \sum_{B \subseteq S,\, |B|=k-|A_1|} g^{A_1 \cup B}, \end{aligned}$$

according to $t = |A \cap C| = 0, 1, \ldots, |A|$. Since $|A_1| = t \leqslant |A|-1$, by induction we have:

$$\sum_{B \subseteq S,\, |B|=k-|A_1|} g^{A_1 \cup B} = (-1)^{|A_1|} g^S = (-1)^t g^S.$$

So

$$\begin{aligned} 0 &= \sum_{B \subseteq S \text{ and } |B|=k-|A|} g^{A \cup B} + g^S \sum_{t=0}^{|A|-1} (-1)^t \binom{|A|}{t} \\ &= \sum_{B \subseteq S \text{ and } |B|=k-|A|} g^{A \cup B} - (-1)^{|A|} g^S. \end{aligned}$$

From the last equation, we have

$$\sum_{B \subseteq S \text{ and } |B|=k-|A|} g^{A \cup B} = (-1)^{|A|} g^S.$$

This completes the proof. □

Corollary 7.1. *If G is any 2-admissible signature, then $\forall S \subseteq [2k]$, $g^S = (-1)^k g^{S^c}$.*

Now we can prove Theorem 7.2.

Proof. To simplify notations, we use the dehomogenized coordinates $\boldsymbol{\beta} = \binom{1\ x}{1\ y} = \binom{1\ x_0}{1\ x_1}$. Some exceptional cases can be proved directly.

First it is obvious that $\boldsymbol{\beta}^{\otimes 2k} G$ is also 2-admissible. So for any $S \subseteq [2k]$ and $|S| \neq k$,

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

Now let $S \subseteq [2k]$ and $|S| = k$,

$$\left\langle \bigotimes_{\sigma=1}^{n} [1, x_{[\sigma \in S]}], G \right\rangle = \sum_{0 \leqslant i \leqslant k} x^i y^{k-i} \sum_{A \subseteq S^c,\, |A|=i} \sum_{B \subseteq S,\, |B|=k-i} g^{A \cup B}.$$

By Lemma 7.2 and for $A \subseteq S^c$, $|A| = i$, we have

$$\sum_{B \subseteq S,\, |B|=k-i} g^{A \cup B} = (-1)^i g^S.$$

So

$$\left\langle \bigotimes_{\sigma=1}^{n} [1, x_{[\sigma \in S]}], G \right\rangle = \sum_{0 \leqslant i \leqslant k} x^i y^{k-i} \sum_{A \subseteq S^c,\, |A|=i} (-1)^i g^S = g^S \sum_{0 \leqslant i \leqslant k} x^i y^{k-i} (-1)^i \binom{k}{i} = (y-x)^k g^S.$$

This completes the proof. □

Since a scaling preserves realizability, the theorem gives:

Corollary 7.2. *If a 2-admissible G is realizable on some basis (e.g., on the standard basis), then it is realizable on any basis, which means 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. See Figs. 1 and 2.)

It turns out that all of these can be obtained from the *planar tensor product* operation which we define next.

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 $G \otimes G'$.

By direct constructions and matchgate identities, we can prove the following theorem.

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}.*

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

Valiant [30] already noted that $(0, 1, -1, 0)$ is realizable under all bases, i.e., 2-realizable in our terminology. From $(0, 1, -1, 0)$, we can construct a family of 2-realizable signatures for any arity $2k$ by planar tensor product. It is an open question if this family (up to scaling) captures all the 2-realizable signatures. This is true for $n \leqslant 6$.

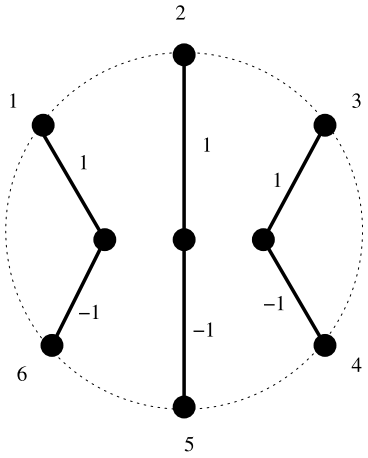

Fig. 1. One planar tensor product for arity 6.

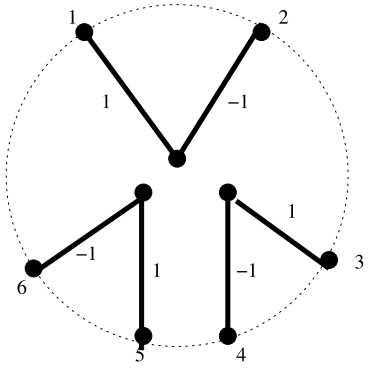

Fig. 2. Another planar tensor product for arity 6.

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

In particular $(0, 1, -1, 0)$ is a prime 2-realizable signature. The above open problem is essentially whether $(0, 1, -1, 0)$ is the unique prime 2-realizable signature (up to scaling).

7.2. 1*-admissibility and* 1*-realizability*

1-admissibility (resp. 1-realizability) is strictly weaker than 2-admissibility (resp. 2-realizability). In this section, we give 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. Planar tensor product can be applied to construct more 1-realizable families.

First we give a family of 1-admissible generators.

Theorem 7.5. *Letting $n = 2k$ be even, we have all $g^S = 0$ except for those $|S| = k$. Finally for all $S \subset [n]$ with $|S| = k$, $g^S = g^{S^c}$. Then G is* 1*-admissible.*

Proof. We prove this by showing that $\forall x$, $\left(\begin{smallmatrix} 1 & x \\ 1 & -x \end{smallmatrix}\right) \in V_1$, where V_1 is defined in Definition 7.3. Let $T \subset [n]$ with $|T|$ odd. Then we require the following polynomial to be identically zero:

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

where $x_0 = x$ and $x_1 = -x$. In the above setting, we have

$$\left\langle \bigotimes_{\sigma=1}^{n} [1, x_{[\sigma \in T]}], G \right\rangle = x^k \sum_{\max\{0,|T|-k\} \leqslant i \leqslant \min\{k,|T|\}} (-1)^i \sum_{\substack{A \subseteq T^c, |A|=k-i \\ B \subseteq T, |B|=i}} g^{A \cup B}.$$

We assume that $k \geqslant |T|$ (the case $k < |T|$ is similar). Then the outer sum is $\sum_{i=0}^{|T|}$. Since $|T|$ is odd, the first and the last term of the outer sum cancel out. Similarly the second and the second last term cancel out, and so on. There are altogether an even number $|T|+1$ of terms of this outer sum over i, and the term indexed by i and by $|T|-i$ cancel out. It follows that this summation is identically 0. This completes the proof. □

For $n = 4$, in order to be 1-realizable, the matchgate identities further require $g^{0011} g^{1001} = 0$. This gives the following two 1-realizable signatures (they are prime for $a^2 \neq b^2$):

$$g^\alpha = \begin{cases} a, & \alpha \in \{0101, 1010\}, \\ b, & \alpha \in \{0011, 1100\}, \\ 0, & \text{otherwise} \end{cases}$$

and

$$g^\alpha = \begin{cases} a, & \alpha \in \{0101, 1010\}, \\ b, & \alpha \in \{1001, 0110\}, \\ 0, & \text{otherwise.} \end{cases}$$

This family of 1-realizable signatures has been used in a subsequent paper [10] to obtain some surprising holographic algorithms.

Next, we present another family of 1-realizable signatures, which are not subsumed by any of the above. It also has some generalized symmetry. It can be viewed as a generalization of Case 2 in Lemma 4.12.

Theorem 7.6. *For any $g_1, g_2, \ldots, g_n, \alpha \in \mathbf{F}$, where $g_1 + g_2 + \cdots + g_n = 0$, let $G = (g^S)_{S \subseteq [n]}$ be defined as follows*

$$g^S = \alpha^{|S|-1} \sum_{i \in S} g_i.$$

Then G is 1-realizable and

$$B_{gen}(G) = \left\{ \left[\begin{pmatrix} -\alpha \\ n_1 \end{pmatrix}, \begin{pmatrix} 1 \\ p_1 \end{pmatrix} \right] \in \mathcal{M} \;\middle|\; n_1, p_1 \in \mathbf{F} \right\}.$$

Proof. For simplicity, we use the dehomogenized coordinates $\left(\begin{smallmatrix} 1 & x \\ 1 & y \end{smallmatrix}\right)$ where $x = -1/\alpha$. Some exceptional cases such as $\alpha = 0$ can be proved directly (we use the convention that $\alpha^0 = 1$ and $0 \cdot \alpha^{0-1} = 0$ even when $\alpha = 0$).

Let $T \subseteq [n]$. If $|T| = 0$ or $|T| = n$, by (10) and the definition of G, it follows easily that

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

Otherwise we have

$$\begin{aligned}
&\left\langle \bigotimes_{\sigma=1}^{n} [1, x_{[\sigma \in T]}], G \right\rangle \\
&= \sum_{\substack{0 \leqslant i \leqslant n-|T| \\ 0 \leqslant j \leqslant |T|}} x^i y^j \sum_{\substack{A \subseteq T^c, |A|=i \\ B \subseteq T, |B|=j}} g^{A \cup B} \\
&= \sum_{\substack{0 \leqslant i \leqslant n-|T| \\ 0 \leqslant j \leqslant |T|}} x^i y^j \sum_{\substack{A \subseteq T^c, |A|=i \\ B \subseteq T, |B|=j}} \alpha^{|A \cup B|-1} \sum_{k \in A \cup B} g_k \\
&= \sum_{\substack{0 \leqslant i \leqslant n-|T| \\ 0 \leqslant j \leqslant |T|}} x^i y^j \alpha^{i+j-1} \sum_{\substack{A \subseteq T^c, |A|=i \\ B \subseteq T, |B|=j}} \left(\sum_{k \in A} g_k + \sum_{l \in B} g_l \right) \\
&= \sum_{\substack{0 \leqslant i \leqslant n-|T| \\ 0 \leqslant j \leqslant |T|}} x^i y^j \alpha^{i+j-1} \left(\binom{|T|}{j} \binom{|T^c|-1}{i-1} \sum_{k \in T^c} g_k + \binom{|T^c|}{i} \binom{|T|-1}{j-1} \sum_{l \in T} g_l \right)
\end{aligned}$$

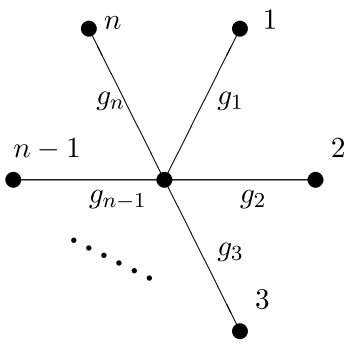

Fig. 3. 1-realizability.

$$= \sum_{k\in T^c} g_k\Bigg(\sum_{\substack{0\leqslant i\leqslant n-|T|\\ 0\leqslant j\leqslant |T|}} x^i y^j \alpha^{i+j-1} \binom{|T|}{j}\binom{n-|T|-1}{i-1} - \sum_{\substack{0\leqslant i\leqslant n-|T|\\ 0\leqslant j\leqslant |T|}} x^i y^j \alpha^{i+j-1} \binom{n-|T|}{i}\binom{|T|-1}{j-1}\Bigg)$$

$$= \sum_{k\in T^c} g_k\big(x(1+\alpha x)^{n-|T|-1}(1+\alpha y)^{|T|} - y(1+\alpha x)^{n-|T|}(1+\alpha y)^{|T|-1}\big).$$

If $|T| < n-1$, the above equation is identically 0 when $x = -1/\alpha$.

For $|T| = n-1$, suppose $T = [n] - \{t\}$, then at $x = -1/\alpha$, the value of the above equation is λg_t where $\lambda = -(1+\alpha y)^{n-1}/\alpha$. This standard signature is realizable by the star (see Fig. 3). □

Remark. When $n = 2$, this generator is the 2-realizable signature $(0, 1, -1, 0)$.

Addendum. In this paper we could only prove a characterization of 2-admissibility, some results on 2-realizability and constructed some families of 1-admissible and 1-realizable signatures. In a subsequent paper [11], we have proved a complete characterization of 2-realizability, which confirms the conjecture here. And the characterization of 2-admissibility in this paper serves as a good start point of that result. In [11], we also give some characterizations of 1-admissibility and 1-realizability.

Acknowledgments

We would like to thank Leslie Valiant for many comments and discussions. We also thank Eric Bach, Xi Chen, Steve Cook, Jon Kleinberg, Edith Hemaspaandra, Lane Hemaspaandra, Joseph Landsberg, Jason Morton, Salil Vadhan, Avi Wigderson and Mingji Xia for their comments and interests. We especially thank the anonymous referees for this paper, both for the conference version and for the journal version.

References

[1] E. Bach, J. Shallit, Algorithmic Number Theory, vol. 1: Efficient Algorithms, MIT Press, 1996.
[2] S. Cook, The complexity of theorem proving procedures, in: Proceedings of the Third Annual ACM Symposium on Theory of Computing, 1971, pp. 151–158.
[3] J.-Y. Cai, Vinay Choudhary, Some results on matchgates and holographic algorithms, in: Proceedings of ICALP 2006, Part I, in: Lecture Notes in Comput. Sci., vol. 4051, 2006, pp. 703–714; Int. J. Software Informatics 1 (1) (2007) 3–36; Also available at Electronic Colloquium on Computational Complexity TR06-048, 2006.
[4] J.-Y. Cai, Vinay Choudhary, Valiant's Holant Theorem and matchgate tensors, in: Proceedings of TAMC 2006, in: Lecture Notes in Comput. Sci., vol. 3959, 2006, pp. 248–261; Theoret. Comput. Sci. 384 (1) (2007) 22–32; Also available at Electronic Colloquium on Computational Complexity Report TR05-118.
[5] J.-Y. Cai, Vinay Choudhary, Pinyan Lu, On the theory of matchgate computations, in: IEEE Conference on Computational Complexity, 2007, pp. 305–318.
[6] J.-Y. Cai, Pinyan Lu, On symmetric signatures in holographic algorithms, in: Proceedings of STACS 2007, in: Lecture Notes in Comput. Sci., vol. 4393, 2007, pp. 429–440; Theory Comput. Syst. 46 (3) (2010) 398–415.
[7] J.-Y. Cai, Pinyan Lu, Holographic algorithms: From art to science, in: Proceedings of STOC, 2007, pp. 401–410.
[8] J.-Y. Cai, Pinyan Lu, Bases collapse in holographic algorithms, in: IEEE Conference on Computational Complexity, 2007, pp. 292–304, Comput. Complexity 17 (2) (2008) 254–281.
[9] J.-Y. Cai, Pinyan Lu, Holographic algorithms: The power of dimensionality resolved, in: Proceedings of ICALP, 2007, pp. 631–642, Theoret. Comput. Sci. 410 (18) (2009) 1618–1628.
[10] J.-Y. Cai, Pinyan Lu, Holographic algorithms with unsymmetric signatures, in: ACM–SIAM Symposium on Discrete Algorithms (SODA), 2008, pp. 54–63.
[11] J.-Y. Cai, Pinyan Lu, Signature theory in holographic algorithms, in: S.H. Hong, H. Nagamochi, T. Fukunaga (Eds.), Proceedings of ISAAC, in: Lecture Notes in Comput. Sci., vol. 5369, Springer, 2008, pp. 568–579.
[12] W. Foody, A. Hedayat, On theory and applications of BIB designs with repeated blocks, Ann. Statist. 5 (1977) 932–945.
[13] W. Foody, A. Hedayat, Note: Correction to "On theory and application of BIB designs with repeated blocks", Ann. Statist. 7 (4) (1979) 925.
[14] R.L. Graham, S.-Y.R. Li, W.-C.W. Li, On the structure of t-designs, SIAM. J. Algebraic Discrete Methods 1 (1980) 8.
[15] N. Linial, B. Rothschild, Incidence matrices of subsets—A rank formula, SIAM. J. Algebraic Discrete Methods 2 (1981) 333.

[16] D. Lichtenstein, Planar formulae and their uses, SIAM J. Comput. 11 (2) (1982) 329–343.
[17] M. Jerrum, Two-dimensional monomer-dimer systems are computationally intractable, J. Stat. Phys. 48 (1987) 121–134; J. Stat. Phys. 59 (1990) 1087–1088, Erratum.
[18] R.M. Karp, Reducibility among combinatorial problems, in: Raymond E. Miller, James W. Thatcher (Eds.), Complexity of Computer Computations, Plenum, New York, 1972, pp. 85–103.
[19] P.W. Kasteleyn, The statistics of dimers on a lattice, Physica 27 (1961) 1209–1225.
[20] P.W. Kasteleyn, Graph theory and crystal physics, in: F. Harary (Ed.), Graph Theory and Theoretical Physics, Academic Press, London, 1967, pp. 43–110.
[21] M. Kneser, Aufgabe 360, Jahresber. Deutsch. Math.-Verein. 2 (58) (1955) 27.
[22] L. Lovász, Kneser's conjecture, chromatic number, and homotopy, J. Combin. Theory Ser. A 25 (1978) 319–324.
[23] J. Matoušek, A combinatorial proof of Kneser's conjecture, Combinatorica 24 (1) (2004) 163–170.
[24] K. Murota, Matrices and Matroids for Systems Analysis, Springer, Berlin, 2000.
[25] H.N.V. Temperley, M.E. Fisher, Dimer problem in statistical mechanics – an exact result, Philos. Magazine 6 (1961) 1061–1063.
[26] S.P. Vadhan, The complexity of counting in sparse, regular, and planar graphs, SIAM J. Comput. 31 (2001) 398–427.
[27] L.G. Valiant, Quantum circuits that can be simulated classically in polynomial time, SIAM J. Comput. 31 (4) (2002) 1229–1254.
[28] L.G. Valiant, Expressiveness of matchgates, Theoret. Comput. Sci. 281 (1) (2002) 457–471.
[29] L.G. Valiant, Holographic algorithms (extended abstract), in: Proc. 45th IEEE Symposium on Foundations of Computer Science, 2004, pp. 306–315; A more detailed version appeared in Electronic Colloquium on Computational Complexity Report TR05-099.
[30] L.G. Valiant, Accidental algorithms, in: Proc. 47th Annual IEEE Symposium on Foundations of Computer Science, 2006, pp. 509–517.
[31] Mingji Xia, Peng Zhang, Wenbo Zhao, Computational complexity of counting problems on 3-regular planar graphs, Theoret. Comput. Sci. 384 (2007) 111–125.