Electronic Colloquium on Computational Complexity, Report No. 3 (2007)

Bases Collapse in Holographic Algorithms

Jin-Yi Cai[1] and Pinyan Lu[2]
[1] Computer Sciences Department, University of Wisconsin
Madison, WI 53706, USA
jyc@cs.wisc.edu
[2] Department of Computer Science and Technology, Tsinghua University
Beijing, 100084, P. R. China
lpy@mails.tsinghua.edu.cn

Abstract

Holographic algorithms are a novel approach to design polynomial time computations using linear superpositions. Most holographic algorithms are designed with basis vectors of dimension 2. Recently Valiant showed that a basis of dimension 4 can be used to solve in P an interesting (restrictive SAT) counting problem mod 7. This problem without modulo 7 is #P-complete, and counting mod 2 is NP-hard.

We give a general collapse theorem for bases of dimension 4 to dimension 2 in the holographic algorithms framework. We also define an extension of holographic algorithms to allow more general support vectors. Finally we give a bases folding theorem showing that in a natural setting the support vectors can be simulated by basis of dimension 2.

1 Introduction

The most fundamental dichotomy in computational complexity is polynomial time versus exponential time computation. Various methods have been devised to achieve exponential speed-ups for a specific problem or a class of problems. This includes the methods of dynamic programming, linear programming, semidefinite programming, randomization, quantum algorithms etc. The theory of holographic algorithms introduced recently by Valiant [16] is another attempt at exponential speed-ups for certain computations.

In this methodology it is possible to give polynomial time algorithms for some problems which seem to require exponential time. At the heart of a holographic algorithm, one tries to devise a custom made process of exponential cancellations. This process is carried out by representing meaningful computational information in a superposition of linear vectors, somewhat analogous to quantum computing. Here these superpositions of vectors are processed in a classical way. Ultimately they are transformed by the Holant Theorem [16] to an evaluation of the perfect matching polynomial PerfMatch for planar graphs, which is then computed by the elegant FKT method [9, 10, 13]. This remarkable algorithm counts the number of perfect matchings in a planar graph in polynomial time.

There are two main ingredients in the design of a holographic algorithm. First, a collection of planar matchgates. Second, a choice of a linear basis vectors, through which the computation is expressed and interpreted. In this framework, Valiant obtained polynomial time algorithms for a number of combinatorial problems which were not known to be in P and minor variations are known to be NP-hard. In [2, 1] several other problems were shown to be solvable in this framework.

Because the underlying basic computation is ultimately reduced to perfect matchings, the set of linear basis vectors which express the computation are necessarily of dimension 2^k, where k is called

ISSN 1433-8092

the size of the basis. In almost all cases [16, 2, 1], the successful design of a holographic algorithm was accomplished by a basis of size 1. Typically there are two basis vectors $\mathbf{n}$ and $\mathbf{p}$ in dimension 2, which represent the truth values True and False, and their tensor product will represent a combination of 0-1 bits. It is the superpositions of these vectors in the tensor product space that are manipulated by a holographic algorithm in the computation.

However, utilizing bases of a higher dimension is always a theoretical possibility which may allow us to devise more holographic algorithms that are not feasible with bases of size 1. Indeed in [19], Valiant used a basis of size 2 to show $\#_7$Pl-Rtw-Mon-3CNF $\in$ P. This problem is a very restrictive Satisfiability counting problem. It counts the number of satisfying assignments of a planar read-twice monotone 3CNF formula, modulo 7. Even though the form of the Boolean formulae is severely restricted, it is known that the counting problem for these formulae without the modulo 7 is #P-complete. Also, the counting problem modulo 2, i.e., to decide whether there are an even or an odd number of satisfying assignments for these formulae is $\oplus$P-complete (thus NP-hard by randomized reductions). Put in this context, the solvability in P of the counting problem modulo 7 is very surprising. This opens up the realistic possibility that bases of size 2 may be in fact more powerful.

In a forthcoming paper [4] we have shown, among other things, that for the particular problem $\#_7$Pl-Rtw-Mon-3CNF, this use of bases of size 2 is unnecessary. There is another basis of size 1, for which one can devise a holographic algorithm which also solves $\#_7$Pl-Rtw-Mon-3CNF. The main result in [4] is a characterization of all the realizable *symmetric signatures* over all bases of size 1. The holographic algorithm for $\#_7$Pl-Rtw-Mon-3CNF using bases of size 1 follows as a consequence.

This leaves open whether bases of size 2 can always be replaced by bases of size 1. We settle this problem affirmatively in this paper. It turns out that technically this collapse is subtle. To explain this we need some more terminologies.

A (planar) matchgate is a planar undirected weighted graph $\Gamma = (G, X)$, where $G = (V, E, W)$, and $X \subseteq V$ is a subset of m external nodes, considered as inputs/outputs. If all vertices in X are output nodes then Γ is called a *generator*. If all vertices in X are input nodes then Γ is a *recognizer*. To each matchgate Γ we assign a *standard signature* which has 2^m entries $G^{i_1 i_2 \dots i_m} = \text{PerfMatch}(G - Z)$, where $Z \subseteq X$ has the characteristic sequence $\chi_Z = i_1 i_2 \dots i_m$. These signatures transform under various basis transformations, which make it possible to assume certain desired values. These matchgates are connected to form a *matchgrid* for which one can define a *Holant*. It is the Holant that expresses the desired computational value. Meanwhile by the remarkable Holant Theorem [16], Holant(Γ) is always computable in polynomial time by the FKT method. The idea is then to find appropriate matchgates and a basis, such that we can realize the desired signatures. (For more background, please see [16, 2, 1].)

Consider the problem #Pl-Rtw-Mon-3CNF, i.e., counting the number of satisfying assignments of a planar read-twice monotone 3CNF formula. Given a 3CNF formula φ as a planar graph G_φ where variables and clauses are represented by vertices. For each variable x we wish to find a generator G with signature $G^{00} = 1, G^{01} = 0, G^{10} = 0, G^{11} = 1$. or $(1, 0, 0, 1)$ for short. It is indeed possible to construct a matchgate which consists of a path of length 3 and all weights 1. Note that when we remove exactly one of the two external nodes we get 3 vertices left and therefore the value of PerfMatch is 0. If we remove both or none of the two external nodes we get the value 1. We can replace the vertex for x in the planar formula by this generator G. This signature $(1, 0, 0, 1)$ intuitively corresponds to a truth assignment: its outputs will be a consistent assignment of either 0 or 1. We also wish to find a recognizer R with 3 inputs having signature $(0, 1, 1, 1, 1, 1, 1, 1)$. This signature intuitively corresponds to a Boolean OR. The matchgrid is formed by connecting the generator outputs to the recognizer inputs as given in G_φ. If we could find this recognizer, we would have shown #Pl-Rtw-Mon-3CNF $\in$ P, and therefore $\text{P}^{\#\text{P}} = \text{P}$.

It can be shown by a simple parity argument that a recognizer with the *standard* signature $(0, 1, 1, 1, 1, 1, 1, 1)$ does not exist. However, under a suitable basis transformation this signature is in fact realizable by

some recognizer. Indeed this is simultaneously realizable together with a generator having the signature $(1, 0, 0, 1)$, *over the filed* $\mathbf{Z}_7$ (but not over $\mathbf{Q}$). This gives the surprising result that $\#_7$Pl-Rtw-Mon-3CNF $\in$ P.

Now we can explain the subtlety of whether it is possible to universally replace a basis of size 2 by a basis of size 1. It turns out that if we only focus on the recognizers, bases of size 2 are in fact provably more powerful than bases of size 1. It is only in the context of simultaneous realizability of both generators and recognizers that we are able to achieve this universal bases collapse. Due to this subtlety, the proofs are delicate.

Utilizing bases of higher dimensions is one way to extend the reach of holographic algorithms. There is another way in which the basic framework of holographic algorithms could be extended. With the additional dimension in the basis vectors, comes the extra freedom of having more than two linearly independent basis vectors. One can introduce a notion of a set of support vectors. If all the generators have one set of support vectors, while all the recognizers have another set of support vectors, then one can define the Holant of the matchgrid just as before, whose value will only depend on the intersection of the two sets of support vectors. In this case the Holant Theorem is still valid and we can still evaluate the Holant by the FKT method. This extension provides another degree of freedom in the design of holographic algorithms, and thus an opportunity to solve more problems this way. Holographic algorithms without this extension can be considered as a special case. This extension to more varied support vector sets is particularly interesting when we have basis size $k > 1$.

Regarding the extension with support vectors, for basis size $k = 2$ we prove a folding bases theorem in Section 5. This theorem says that in a natural and interesting case, this notion of support vectors can be simulated by holographic algorithms with bases of size 1.

The results in this paper have the general implication that a more extended version of holographic algorithms can be simulated by holographic algorithms on bases of size 1. However, the case with higher bases size ≥ 3 is still open. As well, the general case with arbitrary support vectors is also open. We also remark that, from an algorithm design point of view, even if everything collapses to bases of size 1, these extensions (of basis size $k > 1$ and with support vectors) might still be interesting as useful options in finding a holographic algorithm. However, from a strict complexity theory point of view, especially for proving lower bounds, these extensions no longer have any importance, and we should focus only on bases of size 1.

This paper is organized as follows. In Section 2, we give a brief summary of background information and a proof outline. In Section 3, we prove a general theorem about degenerate bases and degenerate signatures of (planar) matchgates. In Section 4, we give the proof of the main theorem, namely, every holographic algorithm on some basis of size 2 using at least one non-degenerate generator can be realized on some basis of size 1. In Section 5, we prove the folding bases theorem.

2 Background and Proof Outline

2.1 Background

We give a brief recap of definitions.

Let $G = (V, E, W)$ be a weighted undirected planar graph. 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 (or 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 $\mathbf{G}$ of type $\binom{m}{0}$. Under the standard basis, it takes the form $\underline{G}$ with 2^m entries,

where

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

and where Z is the subset of the output nodes having the characteristic sequence $\chi_Z = i_1 i_2 \ldots i_m$. $\underline{G}$ is called the standard signature of the generator Γ. We can view $\underline{G}$ as a column vector.

Similarly a recognizer $\Gamma' = (G', Y)$ with m input nodes is assigned a covariant tensor $\mathbf{R}$ of type $\binom{0}{m}$. Under the standard basis, it takes the form $\underline{R}$ with 2^m entries, where

$$\underline{R}_{i_1 i_2 \ldots i_m} = \text{PerfMatch}(G' - Z),$$

where Z is the subset of the input nodes having $\chi_Z = i_1 i_2 \ldots i_m$. $\underline{R}$ is called the standard signature of the recognizer Γ'. We can view $\underline{R}$ as a row vector.

A basis T contains 2 vectors $(\boldsymbol{t_0}, \boldsymbol{t_1})$ (also denoted as $\boldsymbol{n}, \boldsymbol{p}$), each of them has dimension 2^k (size k). We use the following notation:

$$T = (t_i^\alpha), \text{ where } i \in \{0,1\} \text{ and } \alpha \in \{0,1\}^k.$$

(Also denoted as $[n_\alpha, p_\alpha]$ where $\alpha \in \{0,1\}^k$. We follow the convention that upper index i is for row and lower index j is for column [6].) We assume $\text{rank}(T) = 2$ in the following discussion because a basis of $\text{rank}(T) = 1$ is useless.

Under a basis T, we can talk about non-standard signatures (or general signatures, or simply signatures).

Definition 2.1. *The contravariant tensor* $\mathbf{G}$ *of a generator* Γ *has signature* G *under basis* T *iff* $\underline{G} = T^{\otimes m} G$ *is the standard signature of the generator* Γ.

We have

$$\underline{G}^{\alpha_1 \alpha_2 \cdots \alpha_n} = \sum_{i_1, i_2, \cdots, i_n \in \{0,1\}} G^{i_1 i_2 \cdots i_n} t_{i_1}^{\alpha_1} t_{i_2}^{\alpha_2} \cdots t_{i_n}^{\alpha_n} \text{ (where } \alpha_j \in \{0,1\}^k). \tag{1}$$

Definition 2.2. *The covariant tensor* $\mathbf{R}$ *of a recognizer* Γ' *has signature* R *under basis* T *iff* $R = \underline{R} T^{\otimes m}$, *where* $\underline{R}$ *is the standard signature of the recognizer* Γ'.

We have

$$R_{i_1 i_2 \cdots i_n} = \sum_{\alpha_1, \alpha_2, \cdots, \alpha_n \in \{0,1\}^k} \underline{R}_{\alpha_1 \alpha_2 \cdots \alpha_n} t_{i_1}^{\alpha_1} t_{i_2}^{\alpha_2} \cdots t_{i_n}^{\alpha_n} \text{ (where } i_j \in \{0,1\} \text{ for } j = 1, 2, \cdots, n). \tag{2}$$

Remark: Under a basis of size k, if a general signature is of arity n, then the standard signature is of arity nk. nk is also the number of external nodes in the matchgate. So a standard generator signature $\underline{G}$ (resp. a standard recognizer signature $\underline{R}$) can also be viewed as a contravariant (resp. covariant) tensor in $\underline{V}_0^n$ (resp. $\underline{V}_n^0$) where $\underline{V}$ is a vector space of $\dim(\underline{V}) = 2^k$ (here we use standard notations V_k^ℓ for tensor spaces [6]). It is convenient to view it blockwise when we discuss its transformation or symmetry, and to view it bitwise when we discuss its parity or realizability.

Definition 2.3. *A contravariant tensor* $\mathbf{G} \in V_0^n$ *(resp. covariant tensor* $\mathbf{R} \in V_n^0$*) is realizable on a basis* T *iff there exists a generator* Γ *(resp. a recognizer* Γ'*) such that* G *(resp.* R*) is the signature of* Γ *(resp.* Γ'*) under basis* T.

For a string $\alpha \in \{0,1\}^n$, we use the notation $\text{wt}(\alpha)$ to denote its Hamming weight. A signature G or R on index $\alpha = \alpha_1 \alpha_2 \ldots \alpha_n$, where each $\alpha_i \in \{0,1\}^k$, is symmetric iff the value of G^α or R_α only depends on the number of k-bit patterns of α_i. For $k = 1$ it only depends on the Hamming weight of

its index $\mathrm{wt}(\alpha)$. For $k = 1$, we can denote a symmetric signature by the notation $[z_0, z_1, \ldots, z_n]$, where i is the Hamming weight.

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 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 $G(A_i, T)$ be the signature of generator A_i under the basis T and $R(B_j, T)$ be the signature of recognizer B_j under the basis T. And Let $G = \bigotimes_{i=1}^{g} G(A_i, T)$ and $R = \bigotimes_{j=1}^{r} R(B_j, T)$. Then $\mathrm{Holant}(\Omega)$ is defined to be the contraction of these two product tensors, where the corresponding indices match up according to the f connecting edges C_k.

Valiant's Holant Theorem is

Theorem 2.1 (Valiant). *For any matchgrid Ω over any basis T, let G be its underlying weighted graph, then*

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

Standard signatures (of either generators or recognizers) are characterized by the following two sets of conditions. (1) The parity requirements: either all even weight entries are 0 or all odd weight entries are 0. This is due to perfect matchings. (2) A set of Matchgate Identities (MGI) [1, 3]: Let $\underline{G}$ be a realizable standard signature of arity n (we use $\underline{G}$ here, it is the same for $\underline{R}$). A pattern α is an n-bit string, i.e., $\alpha \in \{0,1\}^n$. A position vector $P = \{p_i\}, i \in [l]$, is a subsequence of $\{1, 2, \ldots, n\}$, i.e., $p_i \in [n]$ and $p_1 < p_2 < \cdots < p_l$. We also use p to denote the pattern, whose $(p_1, p_2, \ldots, p_l)$-th bits are 1 and others are 0. Let $e_i \in \{0,1\}^n$ be the pattern with 1 in the i-th bit and 0 elsewhere. Let $\alpha + \beta$ be the pattern obtained from bitwise XOR the patterns α and β. Then for any pattern $\alpha \in \{0,1\}^n$ and any position vector $P = \{p_i\}, i \in [l]$, we have the following identity:

$$\sum_{i=1}^{l} (-1)^i \underline{G}^{\alpha + e_{p_i}} \underline{G}^{\alpha + p + e_{p_i}} = 0. \tag{3}$$

The following simple Proposition 4.3 of [16] is due to Valiant and gives an equivalence relation on basis of size 1. Let $\mathbf{F}$ be a field.

Proposition 2.1 (Valiant). *[16] If there is a generator (recognizer) with certain signature for size one basis $\{(n_0, n_1)^{\mathtt{T}}, (p_0, p_1)^{\mathtt{T}}\}$ then there is a generator (recognizer) with the same signature for size one basis $\{(xn_0, yn_1)^{\mathtt{T}}, (xp_0, yp_1)^{\mathtt{T}}\}$ or $\{(xn_1, yn_0)^{\mathtt{T}}, (xp_1, yp_0)^{\mathtt{T}}\}$ for any $x, y \in \mathbf{F}$ and $xy \neq 0$.*

2.2 An Outline

In [19], Valiant employed a basis of size 2: $n = (1, 1, 2, 1)^{\mathtt{T}}, p = (2, 3, 6, 2)^{\mathtt{T}}$, and showed that $\#_7$Pl-Rtw-Mon-3CNF is in P. He found that, in the notation for symmetric signatures, a generator for $[1, 0, 1]$ and a recognizer for $[0, 1, 1, 1]$ over $\mathbf{Z}_7$ are simultaneously realizable on this basis of size 2. In [4], we showed that a generator for $[1, 0, 1]$ and a recognizer for $[0, 1, 1, 1]$ over $\mathbf{Z}_7$ can also be simultaneously realized on the following basis of size 1: $\left[\binom{1}{6}, \binom{3}{5}\right]$. The natural question is whether this is luck or this is universally true.

It turns out that if we only focus on realizable signatures for recognizers, there do exist some signatures which are realizable on a basis of size 2, but not realizable on any basis of size 1. The following basis of size 2 is such an example: $n = (1, 2, 3, 4)^{\mathtt{T}}, p = (5, 6, 7, 8)^{\mathtt{T}}$. (We omit the particular

matchgate and signature that witness this, since it is not particularly illuminating for the rest.) The next key insight is that when we have a holographic algorithm, given by a matchgrid consisting of a set of generators and recognizers, we need to have a basis on which their signatures are simultaneously realizable. For some bases such as $n = (1, 2, 3, 4)^{\mathtt{T}}, p = (5, 6, 7, 8)^{\mathtt{T}}$, no generator is realizable on them. This is a new phenomenon. In the case of bases of size 1, any $\left[\begin{pmatrix} n_0 \\ n_1 \end{pmatrix}, \begin{pmatrix} p_0 \\ p_1 \end{pmatrix}\right] \in \mathrm{GL}_2(\mathbf{F})$ can be a potential basis (for which some generator can be realized). But this is not true for an arbitrary $n = (n_{00}, n_{01}, n_{10}, n_{11})^{\mathtt{T}}, p = (p_{00}, p_{01}, p_{10}, p_{11})^{\mathtt{T}}$. Informally speaking, the underlying reason for this is the following fact. If a generator G is realizable on $n = (n_{00}, n_{01}, n_{10}, n_{11})^{\mathtt{T}}, p = (p_{00}, p_{01}, p_{10}, p_{11})^{\mathtt{T}}$, then G is also realizable on the following 4 bases of size 1: $\left[\begin{pmatrix} n_{00} \\ n_{01} \end{pmatrix}, \begin{pmatrix} p_{00} \\ p_{01} \end{pmatrix}\right]$, $\left[\begin{pmatrix} n_{00} \\ n_{10} \end{pmatrix}, \begin{pmatrix} p_{00} \\ p_{10} \end{pmatrix}\right]$, $\left[\begin{pmatrix} n_{01} \\ n_{11} \end{pmatrix}, \begin{pmatrix} p_{01} \\ p_{11} \end{pmatrix}\right]$, $\left[\begin{pmatrix} n_{10} \\ n_{11} \end{pmatrix}, \begin{pmatrix} p_{10} \\ p_{11} \end{pmatrix}\right]$. This constraint forces that the values $n_{00}, n_{01}, n_{10}, n_{11}, p_{00}, p_{01}, p_{10}$ and p_{11} can not be arbitrary. After ruling out a degenerate case, we can prove that this requires the above 4 bases of size 1 to be equivalent in the sense of Proposition 2.1. Up to this equivalence we can define it to be the embedded basis of size 1. Such bases of size 2 are called valid bases. It implies that $n_{00}p_{11} - n_{11}p_{00} = 0$ and $n_{01}p_{10} - n_{10}p_{01} = 0$.

Now one can expect some kind of collapse property focusing only for valid bases. Then on a valid basis of size 2, are there any more realizable recognizers which are not realizable on bases of size 1? This we answer in the negative. We prove that any recognizer which is realizable on a size 2 valid basis can also be realized on a size 1 basis. More precisely, it can be realized on its embedded size 1 basis. For the above example, we notice that $n = (1, 1, 2, 1)^{\mathtt{T}}, p = (2, 3, 6, 2)^{\mathtt{T}}$ is valid. Furthermore its 4 embedded bases of size 1: $\left[\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 3 \end{pmatrix}\right]$, $\left[\begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 2 \\ 6 \end{pmatrix}\right]$, $\left[\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 3 \\ 2 \end{pmatrix}\right]$, $\left[\begin{pmatrix} 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 6 \\ 2 \end{pmatrix}\right]$ and our basis $\left[\begin{pmatrix} 1 \\ 6 \end{pmatrix}, \begin{pmatrix} 3 \\ 5 \end{pmatrix}\right]$ are all equivalent in the sense of Proposition 2.1, over $\mathbf{Z}_7$.

The above result is proved by ruling out a degenerate case, which happens when the size 2 basis are of the form $n = (n_{00}, 0, 0, n_{11})^{\mathtt{T}}, p = (p_{00}, 0, 0, p_{11})^{\mathtt{T}}$, or $n = (0, n_{01}, n_{10}, 0)^{\mathtt{T}}, p = (0, p_{01}, p_{10}, 0)^{\mathtt{T}}$. We call such bases degenerate. It turns out that degenerate cases are tricky technically. In fact, on a degenerate basis, there is no general collapse for recognizers, i.e., there do exist some recognizers which are realizable on a degenerate basis of size 2, but not realizable on any basis of size 1. Furthermore, there are some generators realizable on some degenerate bases. But we can show that the only generators realizable on a degenerate basis are trivial. They are essentially only tensors of arity 1 (technically they can only be a tensor product of some arity 1 generators; we call such generators degenerate). We will argue that holographic algorithms which only use degenerate generators are not interesting. They essentially degenerate into ordinary algorithms, without any holographic superpositions.

In the next section we start with degenerate bases.

3 Degenerate Bases

Definition 3.1. *A basis T is* degenerate *iff $t^{\alpha} = 0$ for all $\mathrm{wt}(\alpha)$ even (or for all $\mathrm{wt}(\alpha)$ odd).*

Definition 3.2. *A generator tensor $G \in V_0^n$ (where $\dim(V) = 2$) is* degenerate *iff it has the following form:*

$$G = G_1 \otimes G_2 \otimes \cdots \otimes G_n, \tag{4}$$

where $G_i \in V$.

Remark: Every generator with arity 1 is trivially degenerate. G is degenerate iff G completely factors into a tensor product of arity 1 tensors. This means that there is no interaction or interference between

the output bits of the generator. Such generators should really be considered as n separate one-bit generators.

Now we prove a general theorem showing that a degenerate basis can only accommodate degenerate generators. The proof uses Matchgate Identities in an essential way. Therefore it depends crucially on the fact that we are dealing with planar matchgates (or for readers who are familiar with the character theory of general matchgates, it ultimately depends on the properties of Pfaffians and the equivalence of the signature theory of planar matchgates and the character theory of general matchgates [14, 16, 1, 3]).

Theorem 3.1. *If a basis T is degenerate and* $\mathrm{rank}(T) = 2$*, then every generator $G \in V_0^n$ realizable on the basis T is degenerate.*

Proof: Since T is degenerate, we assume $t^\alpha = 0$ for all $\mathrm{wt}(\alpha)$ odd. The other case is similar. Let $\underline{G} = T^{\otimes n}G$. Then $\underline{G}$ can be realized as the standard signature of a planar matchgate and from (1) we know that it has the following property: for every non-zero entry $\underline{G}^{\alpha_1\alpha_2\cdots\alpha_n}$, $\mathrm{wt}(\alpha_j)$ is even for $j = 1, 2, \cdots, n$.

If $\underline{G} \equiv 0$, i.e., G is identically 0, then the Theorem is obviously true. Otherwise there exists some $\beta \in \{0,1\}^{nk}$ such that $\underline{G}^\beta \neq 0$. We can assume $\beta = 00\cdots0$, and further assume $\underline{G}^{00\cdots0} = 1$. This is because we may let $\underline{G'}^\alpha = \underline{G}^{\alpha\oplus\beta}/\underline{G}^\beta$, then $\underline{G'}^{00\cdots0} = 1$. Then the proof works for $\underline{G'}$. In terms of $\underline{G} = T^{\otimes n}G$, this becomes $\underline{G'} = (T_1 \otimes T_2 \otimes \cdots \otimes T_n)G$, where each T_i is obtained from T by a permutation of its rows determined by α_i. In the following we assume $\underline{G}^{00\cdots0} = 1$.

Since $\underline{G}$ is realizable, it can be realized as some matchgate Γ with nk external nodes. View its k external nodes in the i-th block still as external nodes and other nodes as internal, we have a matchgate Γ_i with k external nodes. This is our $\underline{G_i}$. By definition we have

$$\underline{G_i}^\alpha = \underline{G}^{00\cdots0\alpha00\cdots0} \quad \text{where the position of } \alpha \text{ in the RHS is the } i\text{-th block of } \underline{G}.$$

We want to prove that

$$\underline{G}^{\alpha_1\alpha_2\cdots\alpha_n} = \underline{G_1}^{\alpha_1}\underline{G_2}^{\alpha_2}\cdots\underline{G_n}^{\alpha_n}. \tag{5}$$

If any $\mathrm{wt}(\alpha_i)$ is odd, then both sides are 0 and this equation is satisfied.

Now we prove (5) by induction on $\mathrm{wt}(\alpha_1\alpha_2\cdots\alpha_n) \geq 0$ and all $\mathrm{wt}(\alpha_i)$ are even.

If $\mathrm{wt}(\alpha_1\alpha_2\cdots\alpha_n) = 0$, we have the only case that $\alpha_1\alpha_2\cdots\alpha_n = 00\cdots0$. In this case (5) is obvious.

If $\mathrm{wt}(\alpha_1\alpha_2\cdots\alpha_n) = 2$, since we require that all $\mathrm{wt}(\alpha_j)$ are even, the two 1's must be in the same block. Then (5) is obvious too.

Inductively we assume (5) has been proved for all $\mathrm{wt}(\alpha_1\alpha_2\cdots\alpha_n) \leq 2(i-1)$, for some $i \geq 2$. Now $\mathrm{wt}(\alpha_1\alpha_2\cdots\alpha_n) = 2i > 0$. W.l.o.g, we can assume $\alpha_1 \neq 00\cdots0$, a block a k 0's. Let t be the position of the first 1 in α_1. Using the pattern $\alpha_1\alpha_2\cdots\alpha_n + e_t$ and positions $\alpha_1\alpha_2\cdots\alpha_n$ (we denote it as $P = \{p_j\}$ where $j = 1, 2, \ldots, 2i$), we have the following matchgate identity:

$$\underline{G}^{\alpha_1\alpha_2\cdots\alpha_n} = \sum_{j=2}^{2i}(-1)^j \underline{G}^{\alpha_1\alpha_2\cdots\alpha_n + e_t + e_{p_j}}\underline{G}^{e_t+e_{p_j}}.$$

Let $w = \mathrm{wt}(\alpha_1)$. Then when $j \geq w+1$, $\underline{G}^{e_t+e_{p_j}} = 0$ because the weight of its first block is 1, which is odd. Therefore, we have

$$\underline{G}^{\alpha_1\alpha_2\cdots\alpha_n} = \sum_{j=2}^{w}(-1)^j \underline{G}^{(\alpha_1+e_t+e_{p_j})\alpha_2\cdots\alpha_n}\underline{G}^{(e_t+e_{p_j})00\cdots0}.$$

Here for convenience we consider $e_t, e_{p_j} \in \{0,1\}^k$.

Since every $\underline{G}^{\alpha}$ in the RHS has weight $\mathrm{wt}(\alpha) \leq 2i-2$, we can apply (5) to them, and get:

$$\underline{G}^{\alpha_1\alpha_2\cdots\alpha_n} = \underline{G_2}^{\alpha_2}\cdots\underline{G_n}^{\alpha_n}\sum_{j=2}^{w}(-1)^j\underline{G_1}^{\alpha_1+e_t+e_{p_j}}\underline{G_1}^{e_t+e_{p_j}}.$$

The matchgate identity for $\underline{G_1}$ using pattern α_1+e_t and positions α_1 gives us

$$\underline{G_1}^{\alpha_1} = \sum_{j=2}^{w}(-1)^j\underline{G_1}^{\alpha_1+e_t+e_{p_j}}\underline{G_1}^{e_t+e_{p_j}}.$$

It follows that

$$\underline{G}^{\alpha_1\alpha_2\cdots\alpha_n} = \underline{G_1}^{\alpha_1}\underline{G_2}^{\alpha_2}\cdots\underline{G_n}^{\alpha_n}.$$

We can rewrite it as

$$\underline{G} = \underline{G_1}\otimes\underline{G_2}\otimes\cdots\otimes\underline{G_n}. \tag{6}$$

To prove (4), we apply a transformation. Since $\mathrm{rank}(T)=2$, there exists a 2×2^k matrix $\tilde{T}$ such that $\tilde{T}T = I_2$. Therefore

$$G = (\tilde{T}T)^{\otimes n}G = \tilde{T}^{\otimes n}T^{\otimes n}G = \tilde{T}^{\otimes n}\underline{G}.$$

Substituting (6) in this, we have

$$G = \tilde{T}^{\otimes n}(\underline{G_1}\otimes\underline{G_2}\otimes\cdots\otimes\underline{G_n}) = (\tilde{T}\underline{G_1})\otimes(\tilde{T}\underline{G_2})\otimes\cdots\otimes(\tilde{T}\underline{G_n}).$$

Let $G_j = \tilde{T}\underline{G_j}$, we have

$$G = G_1\otimes G_2\otimes\cdots\otimes G_n.$$

If we take into account the transformation from $\underline{G}$ to $\underline{G'}$, then we must use a permuted $\tilde{T_i}$ for each T_i separately. This completes the proof. □

Definition 3.3. *A basis T is* valid *iff there exists some non-degenerate generator realizable on T.*

Corollary 3.1. *A valid basis is non-degenerate.*

In the main collapse theorem, we will rule out the case that a holographic algorithm only employs degenerate generators. This is justified as follows.

Let there be given a matchgrid Ω in a holographic algorithm consisting of a number of generators $G_1, G_2, \ldots, G_s$ and recognizers $R_1, R_2, \ldots, R_t$. If all the generators $G_1, G_2, \ldots, G_s$ are degenerate then we can decompose every generator as in Theorem 3.1 without changing the value for the Holant of the matchgrid. After that every generator has arity 1. So every generator connects to a unique recognizer. Suppose the arity of R_i is n_i, we rename the generator (after decomposition) which connects to the j-th node of R_i as $G_{i,j}$, where $i\in[t], j\in[n_i]$. Then the Holant can be evaluated for each recognizer separately and then multiplied:

$$\mathrm{Holant}(\Omega) = \prod_{i=1}^{t}\left[\sum_{x_1,x_2,\ldots,x_{n_i}\in\{0,1\}}(R_i)_{x_1,x_2,\ldots,x_{n_i}}G_{i,1}^{x_1}G_{i,2}^{x_2}\cdots G_{i,n_i}^{x_{n_i}}\right].$$

This means that the value of $\mathrm{Holant}(\Omega)$ can be completely decomposed into the local components of the individual recognizer matchgate R_i, without any interation between these matchgates. For example, if this is a Satisfiability problem and the recognizers correspond to clauses. Then the sum for a single recognizer corresponding to a clause is to count all the satisfying assignments to that clause. This is trivial if all its input variables do not have any interaction with any other clauses. In general we assume the combinatorial problem is defined in such a way that the notion that corresponds to a *local* component is sufficiently simple, so that the sum for the matchgate signature for that local component alone is computable in polynomial time. This is in particular true if the size of the local component is at most $O(\log N)$, where N is the input size to the problem.

4 Collapse Bases of Size 2

In this section, we develop a general collapse result for bases of size 2. Some of the lemmas are generally true for any size k, in such cases, we state the results for arbitrary k.

First we give the following simple lemmas:

Lemma 4.1. *If a generator G is realizable on a basis $T = [n, p]$ of size k, then for all $\alpha \in \{0,1\}^k$ and $i \in [k]$, G is also realizable on the following size 1 basis: $\left[\binom{n_\alpha}{n_{\alpha+e_i}}, \binom{p_\alpha}{p_{\alpha+e_i}}\right]$.*

Proof: The fact that G is realizable on the basis $T = [n, p]$ means that there exists a matchgate Γ with kn external nodes with a standard signature $\underline{G} = T^{\otimes n}G$. We construct a new matchgate as follows:

First, for every block and every $j \in [k]$, if the j-th bit of α is 1, add an additional edge of weight 1 between j and an additional nodes j'. Then viewing nodes i (if the i-th bit of α is 0) or i' (if the i-th bit of α is 1) in every block as external nodes and all the other nodes as internal nodes, we have a new matchgate Γ' with n external nodes.

From (1), we know that the standard signature of Γ' is exactly $\left[\binom{n_\alpha}{n_{\alpha+e_i}}, \binom{p_\alpha}{p_{\alpha+e_i}}\right]^{\otimes n} G$.

It follows that G is also realizable on the size 1 basis: $\left[\binom{n_\alpha}{n_{\alpha+e_i}}, \binom{p_\alpha}{p_{\alpha+e_i}}\right]$. □

Lemma 4.2. *If a non-degenerate symmetric generator is realizable on two linearly independent bases of size 1: $\left[\binom{n}{n_1}, \binom{p}{p_1}\right]$ and $\left[\binom{n}{n_2}, \binom{p}{p_2}\right]$, then $n_1p_2 - n_2p_1 = 0$.*

Proof: In the paper [5] we have obtained a complete characterization of symmetric realizable generators and recognizers on bases of size 1. The purpose of Lemma 4.1 is precisely to be able to apply this information. Being non-degenerate means that G is not of the form of Lemma 8.1 in [5]. And we can check with Lemma 8.2–Lemma 8.6 in [5] to verify that in every other case the statement of this Lemma is true. (For reader's convenience, we include the relevant Lemmas from [5] in an Appendix.) □

Lemma 4.3. *Let $T = [n, p]$ be a non-degenerate basis of size k, (and as usual assume $\mathrm{Rank}(T) = 2$.) Then there exist i and j, such that $\mathrm{wt}(i)$ is even, $\mathrm{wt}(j)$ is odd and $n_ip_j - n_jp_i \neq 0$.*

We denote by $\mathbf{v}_\alpha = (n_\alpha, p_\alpha)$ in the following.

Proof: We assume for a contradiction that for every i and j, with $\mathrm{wt}(i)$ even and $\mathrm{wt}(j)$ odd, $n_ip_j - n_jp_i = 0$.

Since T is non-degenerate, there exist i_0 and j_0 such that $\mathrm{wt}(i_0)$ is even, $\mathrm{wt}(j_0)$ is odd, $\mathbf{v}_{i_0} \neq (0,0)$, and $\mathbf{v}_{j_0} \neq (0,0)$. From the assumption, we know that there exists a λ, such that $\mathbf{v}_{j_0} = \lambda\mathbf{v}(i_0)$. Now for any $r \in \{0,1\}^k$, if $\mathrm{wt}(r)$ is odd, by assumption there exists some λ_r such that $\mathbf{v}_r = \lambda_r\mathbf{v}_{i_0}$; if $\mathrm{wt}(r)$ is even, there exists some λ'_r such that $\mathbf{v}_r = \lambda'_r\mathbf{v}_{j_0} = \lambda'_r\lambda\mathbf{v}_{j_0}$.

Therefore, every two vectors $\mathbf{v}_i, \mathbf{v}_j$ are linearly dependent. As a result $\mathrm{Rank}(T) = 1$. This contradiction completes the proof. □

Lemma 4.4. *Suppose a generator G is realizable on the basis $T = [n, p]$ of size k. Let $\underline{G} = T^{\otimes n}G$ be the standard signature of G. If $\mathrm{wt}(\alpha)$ is even, $\mathrm{wt}(\beta)$ is odd and the two non-zero vectors (n_α, p_α), (n_β, p_β) are linearly dependent, then whenever α or β occurs as some α_i in $\alpha_1\alpha_2\cdots\alpha_n$, we have $\underline{G}^{\alpha_1\alpha_2\cdots\alpha_n} = 0$.*

Proof: Suppose α or β occurs as some α_i in $\alpha_1\alpha_2\cdots\alpha_n$. From (1), when we replace either α with β or β with α at one place, the value of $\underline{G}$ is changed by a non-zero factor, because $\mathbf{v}_\alpha$ and $\mathbf{v}_\beta$ are linearly dependent and non-zero. But their parities are different. By the parity requirements of standard signatures, one of them is 0. So the only possibility is $\underline{G}^{\alpha_1\alpha_2\cdots\alpha_n} = 0$. □

Lemma 4.5. *If a non-degenerate symmetric generator G is realizable on a basis $T = [n, p]$ of size 2, then $n_i p_j - n_j p_i = 0$ for all $\mathrm{wt}(i), \mathrm{wt}(j)$ having the same parity.*

Proof: First, notice that every even pattern differs from every odd pattern of $\{00, 01, 10, 11\}$ by exactly one bit. From Lemma 4.1, we have for every even $\mathrm{wt}(i)$ and odd $\mathrm{wt}(j)$, the standard signature $\left[\binom{n_i}{n_j}, \binom{p_i}{p_j}\right]^{\otimes n} G$, is realizable.

From Lemma 4.3, w.l.o.g, we assume $\mathbf{v}_{00}$ and $\mathbf{v}_{01}$ are linearly independent, i.e., $n_{00}p_{01} - n_{01}p_{00} \neq 0$. (If it is the pair $(\mathbf{v}_{00}, \mathbf{v}_{10})$ we can just exchange the first with the second bit. It is similar with the case where it is the vector $\mathbf{v}_{11}$ instead of $\mathbf{v}_{00}$ (for the even weight i from Lemma 4.3).) We use the notation $D(\mathbf{u}, \mathbf{v})$ to say the vectors $\mathbf{u}$ and $\mathbf{v}$ are linearly dependent. Then from Lemma 4.2, if $\neg D(\mathbf{v}_{00}, \mathbf{v}_{10})$ then $D(\mathbf{v}_{01}, \mathbf{v}_{10})$, and if $\neg D(\mathbf{v}_{11}, \mathbf{v}_{01})$ then $D(\mathbf{v}_{00}, \mathbf{v}_{11})$. As a result, both $\mathbf{v}_{10}$ and $\mathbf{v}_{11}$ are in the following three cases: (1) a non-zero multiple of $\mathbf{v}_{00}$, (2) a non-zero multiple of $\mathbf{v}_{01}$, or (3) the zero vector $(0, 0)$.

In order to prove Lemma 4.5 we only need to rule out the following cases:

- Case 1: $\mathbf{v}_{11} = (0, 0)$, and $\mathbf{v}_{10}$ is a non-zero multiple of $\mathbf{v}_{00}$.

  In this case, from Lemma 4.4, any occurrence of 00 or 10 will make $\underline{G}^{\alpha_1\alpha_2\cdots\alpha_n} = 0$. Since $\mathbf{v}_{11} = (0, 0)$, from eqn. (1) any occurrence of 11 will also make $\underline{G}^{\alpha_1\alpha_2\cdots\alpha_n} = 0$. So the only possible non-zero entry of $\underline{G}$ is $\underline{G}^{01,01,\cdots,01}$. Then $\underline{G}$ is degenerate, and so is G. A contradiction.

- Case 2: $\mathbf{v}_{10}$ is $(0, 0)$, and $\mathbf{v}_{11}$ is a non-zero multiple of $\mathbf{v}_{01}$. This case is similar with Case 1.

- Case 3: $\mathbf{v}_{10}$ is a non-zero multiple of $\mathbf{v}_{00}$, and $\mathbf{v}_{11}$ is a non-zero multiple of $\mathbf{v}_{01}$.

  As in Case 1, any occurrence of 00 or 10 will make $\underline{G}^{\alpha_1\alpha_2\cdots\alpha_n} = 0$. And also any occurrence of 11 or 01 will make $\underline{G}^{\alpha_1\alpha_2\cdots\alpha_n} = 0$. Therefore $\underline{G}$ is trivial. It follows that G is also trivial, a contradiction.

- Case 4: $\mathbf{v}_{10}$ and $\mathbf{v}_{11}$ are both non-zero multiples of $\mathbf{v}_{00}$.

  In this case, from Lemma 4.4, any occurs of 00, 10 or 11 will make $\underline{G}^{\alpha_1\alpha_2\cdots\alpha_n} = 0$. So the only possible non-zero entry of $\underline{G}$ is $\underline{G}^{01,01,\cdots 01}$. Then $\underline{G}$ is degenerate, so is G. A contradiction.

- Case 5: $\mathbf{v}_{10}$ and $\mathbf{v}_{11}$ are both non-zero multiples of $\mathbf{v}_{01}$.

  This case is similar to Case 4. We can show that the only possible non-zero entry of $\underline{G}$ is $\underline{G}^{00,00,\cdots 00}$.

This completes the proof. □

Remark: It seems that the "degeneracy" of having some identically 0 vectors in the basis does present additional technical difficulty in the proof. The main contour of the proof of the Collapse Theorem is simpler in spirit, when one does not have to deal with these zero vectors. In a way, all the preceding lemmas are handling some "border line cases". However we can not dismiss these bases of "border line cases" from the theory, for in fact most successes of holographic algorithms have utilized these "accidental" bases.

Now we can prove the following theorem.

Theorem 4.1. *For every valid basis $T = [n, p]$ of size 2, we have $D(\mathbf{v}_i, \mathbf{v}_j)$, i.e., $\mathbf{v}_i$ and $\mathbf{v}_j$ are linearly dependent, for all $\mathrm{wt}(i), \mathrm{wt}(j)$ having the same parity.*

Proof: Since $T = [n, p]$ is valid, by definition, there exists a non-degenerate generator G which is realizable on T. From Corollary 3.1, we know $T = [n, p]$ is non-degenerate.

Let $T_0 = \left[\begin{pmatrix} n_{00} \\ n_{11} \end{pmatrix}, \begin{pmatrix} p_{00} \\ p_{11} \end{pmatrix}\right]$ and $T_1 = \left[\begin{pmatrix} n_{01} \\ n_{10} \end{pmatrix}, \begin{pmatrix} p_{01} \\ p_{10} \end{pmatrix}\right]$.

Then all we need to prove is $\det(T_0) = \det(T_1) = 0$.

According to the parity of the arity n and the parity of the matchgate realizing G, we have four cases:

Case 1: even n and odd matchgate

From the parity constraint, we have $T_0^{\otimes n}G = 0$ and $T_1^{\otimes n}G = 0$. Since $G \not\equiv 0$ (i.e., G is not identically 0), we have $\det(T_0) = \det(T_1) = 0$.

Case 2: odd n and odd matchgate

From the parity constraint, we have $T_0^{\otimes n}G = 0$. Since $G \not\equiv 0$, we have $\det(T_0) = 0$. Since the basis is not degenerate, from Lemma 4.3, we know that there exist i and j, such that $\mathrm{wt}(i)$ is even, $\mathrm{wt}(j)$ is odd and $\neg D(\mathbf{v}_i, \mathbf{v}_j)$.

From the parity constraint, for all $t \in [n-2]$, we also have

$$(T_1^{\otimes t} \otimes [n_i, p_i] \otimes [n_j, p_j] \otimes T_1^{\otimes n-2-t})G = 0,$$

$$(T_1^{\otimes t} \otimes [n_j, p_j] \otimes [n_i, p_i] \otimes T_1^{\otimes n-2-t})G = 0.$$

Subtract these two equations we get:

$$(n_i p_j - n_j p_i)(T_1^{\otimes t} \otimes [0, 1, -1, 0] \otimes T_1^{\otimes n-2-t})G = 0.$$

Since $n_i p_j - n_j p_i \neq 0$, we have

$$(T_1^{\otimes t} \otimes [0, 1, -1, 0] \otimes T_1^{\otimes n-2-t})G = 0.$$

Let G_t be a tensor of V_0^{n-2} such that

$$G_t^{i_1 i_2 \ldots i_{n-2}} = G^{i_1 i_2 \ldots i_{t-1} 01 i_t i_{t+1} \ldots i_{n-2}} - G^{i_1 i_2 \ldots i_{t-1} 10 i_t i_{t+1} \ldots i_{n-2}}.$$

Then we have $T_1^{\otimes (n-2)} G_t = 0$.

If there exists any $t \in [n-2]$ such that $G_t \not\equiv 0$, we have $\det(T_1) = 0$.

Otherwise $\forall t \in [n-2]$ we have $G_t \equiv 0$. This implies that G is symmetric. Then from Lemma 4.5, we have $\det(T_1) = 0$.

Case 3: odd n and even matchgate

This case is similar to Case 2. We apply the argument for T_0 to T_1, and apply the argument for T_1 to T_0.

Case 4: even n and even matchgate

This case is also similar to Case 2 and Case 3. We simply apply the same argument for T_1 as in Case 2 and the same argument for T_0 as in Case 3. □

From this theorem, we know that for any valid basis $T = \left[\begin{pmatrix} n_{00} \\ n_{01} \\ n_{10} \\ n_{11} \end{pmatrix}, \begin{pmatrix} p_{00} \\ p_{01} \\ p_{10} \\ p_{11} \end{pmatrix}\right]$, there exist (n_0, p_0), (n_1, p_1), $\lambda_{00}, \lambda_{01}, \lambda_{10}$ and λ_{11}, such that $\mathbf{v}_{ij} = \lambda_{ij}(n_b, p_b)$, where $i, j = 0, 1$ and $b = i + j \bmod 2$.

From Lemma 4.3, we know that (n_0, p_0), (n_1, p_1) are linearly independent, and each is determined up to a scalar multiplier.

Definition 4.1. *We call* $\hat{T} = \left[\begin{pmatrix} n_0 \\ n_1 \end{pmatrix}, \begin{pmatrix} p_0 \\ p_1 \end{pmatrix}\right]$ *an embedded size 1 basis of* T.

By Lemma 4.3 for at least one pair of indices ij and $i'j'$, one is of odd weight and the other of even weight, such that both $\lambda_{ij}, \lambda_{i'j'} \neq 0$. Then by Lemma 4.1 and apply Proposition 2.1, we have

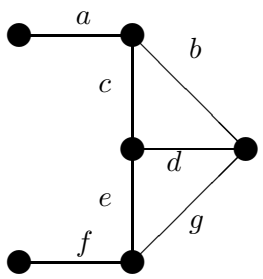
Theorem 4.2. *If a generator G is realizable on a valid basis T of size 2, then it is also realizable on its embedded size 1 basis $\hat{T}$.*

Now we address recognizers.

Theorem 4.3. *If a recognizer R is realizable on a valid basis T of size 2, then it is also realizable on its embedded size 1 basis $\hat{T}$.*

Proof: Suppose $\hat{T} = \left[\begin{pmatrix} n_0 \\ n_1 \end{pmatrix}, \begin{pmatrix} p_0 \\ p_1 \end{pmatrix}\right]$, and we have $\mathbf{v}_{ij} = \lambda_{ij}(n_b, p_b)$, where $i, j = 0, 1$ and $b = i + j \bmod 2$.

Let Γ be a matchgate realizing $\underline{R}$, where $R = \underline{R}T^{\otimes n}$. Γ has $2n$ external nodes. For every block of two nodes in Γ, we use the following gadget to extend Γ to get a new matchgate Γ' of arity n. The



parameters a, b, c, d, e, f, g satisfy $daf = \lambda_{11}, cf = \lambda_{01}, ae = \lambda_{10}, be + cg = \lambda_{00}$.

These equations are satisfiable as follows. If $\lambda_{10} = 0$, we set $e = 0, c = 1, f = \lambda_{01}$, and $g = \lambda_{00}$. Note importantly, when $\lambda_{10} = 0$, we have $\lambda_{01} \neq 0$. This follows from Lemma 4.3. So then we can let $a = 1$ and $d = f^{-1}\lambda_{11}$. If $\lambda_{10} \neq 0$, we set $e = f = 1$, and $g = 0$. Then $c = \lambda_{01}$, $a = \lambda_{10}$ and $d = a^{-1}\lambda_{11}$.

Note the following: If the right most vertex of this gadget is removed, then there are exactly two perfect matching fragments of Γ', with weight cf and ae respectively, which correspond to the bit patterns 01 and 10 respectively in the original matchgate Γ. If the right most vertex is kept, then there are exactly three perfect matching fragments of Γ', the first with weight daf which corresponds to the bit pattern 11 in Γ, and the second and third with weight be and cg, both correspond to the bit pattern 00 in Γ.

Let $\underline{R'}$ be the standard signature of Γ'. Then we have the exponential sum for all $i_1, i_2, \ldots, i_n = 0, 1$:

$$\underline{R'}_{i_1 i_2 \ldots i_n} = \sum_{j_r + j'_r = i_r} \underline{R}_{j_1 j'_1, j_2 j'_2, \cdots, j_n j'_n} \lambda_{j_1 j'_1} \lambda_{j_2 j'_2} \cdots \lambda_{j_n j'_n}.$$

(The summation $j_r + j'_r = i_r$ in the index is done in $\mathbf{Z}_2$.)

We want to prove that $\underline{R'}$ in the basis $\left[\begin{pmatrix} n_0 \\ n_1 \end{pmatrix}, \begin{pmatrix} p_0 \\ p_1 \end{pmatrix}\right]$ and $\underline{R}$ in the basis $\left[\begin{pmatrix} n_{00} \\ n_{01} \\ n_{10} \\ n_{11} \end{pmatrix}, \begin{pmatrix} p_{00} \\ p_{01} \\ p_{10} \\ p_{11} \end{pmatrix}\right]$ give the same recognizer R.

For the summation notation below, we use (t_l^i) and $(\bar{t}_l^{jj'})$ to represent the above two bases, where $l, i, j, j' \in \{0, 1\}$. Here $l = 0$ is for the $n_{\bullet}$ vectors and $l = 1$ is for the $p_{\bullet}$ vectors. Then $\bar{t}_l^{jj'}$ is the product of $\lambda_{jj'}$ and $t_l^{j+j'}$.

Now from (2) we have

$$\begin{aligned}
R_{l_1 l_2 \cdots l_n} &= \sum_{j_r, j'_r \in \{0,1\}} \underline{R}_{j_1 j'_1, j_2 j'_2, \cdots, j_n j'_n} \bar{t}^{j_1 j'_1}_{l_1} \bar{t}^{j_2 j'_2}_{l_2} \cdots \bar{t}^{j_n j'_n}_{l_n} \\
&= \sum_{i_r \in \{0,1\}} \sum_{j_r + j'_r = i_r} \underline{R}_{j_1 j'_1, j_2 j'_2, \cdots, j_n j'_n} \bar{t}^{j_1 j'_1}_{l_1} \bar{t}^{j_2 j'_2}_{l_2} \cdots \bar{t}^{j_n j'_n}_{l_n} \\
&= \sum_{i_r \in \{0,1\}} \sum_{j_r + j'_r = i_r} \underline{R}_{j_1 j'_1, j_2 j'_2, \cdots, j_n j'_n} \lambda_{j_1 j'_1} t^{j_1 + j'_1}_{l_1} \lambda_{j_2 j'_2} t^{j_2 + j'_2}_{l_2} \cdots \lambda_{j_n j'_n} t^{j_n + j'_n}_{l_n} \\
&= \sum_{i_r \in \{0,1\}} t^{i_1}_{l_1} t^{i_2}_{l_2} \cdots t^{i_n}_{l_n} \sum_{j_r + j'_r = i_r} \underline{R}_{j_1 j'_1, j_2 j'_2, \cdots, j_n j'_n} \lambda_{j_1 j'_1} \lambda_{j_2 j'_2} \cdots \lambda_{j_n j'_n} \\
&= \sum_{i_r \in \{0,1\}} t^{i_1}_{l_1} t^{i_2}_{l_2} \cdots t^{i_n}_{l_n} \underline{R'}_{i_1 i_2 \cdots i_n} \\
&= R'_{l_1 l_2 \cdots l_n}.
\end{aligned}$$

This completes the proof. □

Together from Theorems 4.1 to 4.3, we have the following main theorem:

Theorem 4.4. *(Bases Collapse Theorem) Any holographic algorithm on basis of size 2 which employs at least one non-degenerate generator can be done in basis of size 1. More precisely, if generators $G_1, G_2, \ldots, G_s$ and recognizers $R_1, R_2, \ldots, R_t$ are simultaneously realizable on a size 2 basis, and not all generators are degenerate, then all the generators and recognizers are simultaneously realizable on a basis of size 1.*

Proof: Suppose generators $G_1, G_2, \ldots, G_s$ and recognizer $R_1, R_2, \ldots, R_t$ are simultaneously realizable on the size 2 basis $T = \left[\begin{pmatrix} n_{00} \\ n_{01} \\ n_{10} \\ n_{11} \end{pmatrix}, \begin{pmatrix} p_{00} \\ p_{01} \\ p_{10} \\ p_{11} \end{pmatrix} \right]$. Since some G_i is not degenerate, we know that T is valid. Let $\hat{T} = \left[\begin{pmatrix} n_0 \\ n_1 \end{pmatrix}, \begin{pmatrix} p_0 \\ p_1 \end{pmatrix} \right]$ be the embedded size 1 basis of $\hat{T}$. From Theorem 4.2, we know that all the generators $G_1, G_2, \ldots, G_s$ are realizable on $\hat{T}$. From Theorem 4.3, we know that all the recognizers $R_1, R_2, \ldots, R_t$ are also realizable on $\hat{T}$. This completes the proof.

□

5 More General Support Vectors

In this section we consider an extension to the basic model of holographic algorithms. The present set-up at a technical level–where the rubber meets the road–can be described as follows. We have a collection of planar matchgates which are endowed with their standard signatures $\underline{G}$. These are defined by the PerfMatch polynomial. Then we look for a suitable linear basis $[\mathbf{n}, \mathbf{p}]$ on which we can express the standard signatures of the matchgates (superpositions). More precisely for a generator of arity n we have a contravariant tensor $\mathbf{G}$, when viewed as a column vector G, it satisfies the relation $\underline{G} = [\mathbf{n}, \mathbf{p}]^{\otimes n} G$. Similarly we have recognizers as covariant tensors, and they satisfy $R = \underline{R}[\mathbf{n}, \mathbf{p}]^{\otimes n}$, where $\underline{R}$ is the standard signature of the recognizer and R is the signature under this basis. (We view $\underline{G}$ and G as column vectors and view $\underline{R}$ and R as row vectors.) We then form tensor products of the

signatures in the order specified by the matchgrid. With an abuse of notation we still denote by G and R the signatures for the matchgrid.

The Holant is the contraction of $\mathbf{R}$ on $\mathbf{G}$. This is also, when viewed as an inner product of row/column vectors, equal to $\langle R, G\rangle$. Abstractly the Holant Theorem is just

$$\langle R, G\rangle = \langle \underline{R}, \underline{G}\rangle.$$

To solve a combinatorial problem we design matchgates and find a basis so that the entries of R and G have the desired combinatorial meanings. Then the Holant $\langle R, G\rangle$ expresses the computational value one wishes to compute, which is usually an exponential sum. And the Holant Theorem tells us that this is the same as $\langle \underline{R}, \underline{G}\rangle$, which can then be computed by the FKT method in polynomial time.

Consider a matchgrid using a basis $\mathbf{t_0}, \mathbf{t_1}$ of size 2. Let's extend the basis to a 4×4 invertible matrix $T = (t^i_j)$ where $i, j \in \{0, 1, 2, 3\}$. Here it would be convenient to use the convention that upper index i is for row and lower index j is for column. We will use this convention consistently [6]. We also denote by $\widetilde{T} = T^{-1} = (\tilde{t}^i_j)$.

To say a generator tensor G is realizable is to have $\underline{G} = [\mathbf{t_0}, \mathbf{t_1}]^{\otimes n} G$ being a standard signature of a planar matchgate, which are constrained by the PerfMatch polynomial. Viewed in terms of $\mathbf{t_0}, \mathbf{t_1}, \mathbf{t_2}, \mathbf{t_3}$, we say the generator tensor G is supported on the subset $\{\mathbf{t_0}, \mathbf{t_1}\}$. This is the same as to say G can be augmented to $\hat{G}$ with zero entries, whenever the index involves 2 and 3, and then $\underline{G} = [\mathbf{t_0}, \mathbf{t_1}, \mathbf{t_2}, \mathbf{t_3}]^{\otimes n} \hat{G}$.

Now suppose we don't know how to construct some desired signature G as above, and yet we find some $\hat{G} = (G^{i_1, \dots i_n})_{i_r = 0,1,3}$ which is supported on $\mathbf{t_0}, \mathbf{t_1}, \mathbf{t_3}$. This means that $[\mathbf{t_0}, \mathbf{t_1}, \mathbf{t_3}]^{\otimes n} \hat{G}$ is realizable as a standard signature of a planar matchgate. Furthermore suppose when we restrict to $\mathbf{t_0}, \mathbf{t_1}$, $\hat{G}$ restricts to G, i.e., if we restrict all entries of $\hat{G}$ whose indices are 0 or 1 (but not 3) we get G.

Let's also consider recognizers. Suppose we wish to construct some desired signature R. Yet we can only find some $\hat{R} = (R_{i_1, \dots i_{n'}})_{i_r = 0,1,2}$ which restricts to R on $\tilde{\mathbf{t}}^{\mathbf{0}}, \tilde{\mathbf{t}}^{\mathbf{1}}$, and which is supported on $\tilde{\mathbf{t}}^{\mathbf{0}}, \tilde{\mathbf{t}}^{\mathbf{1}}, \tilde{\mathbf{t}}^{\mathbf{2}}$. This means that $\underline{R} = \hat{R} \begin{pmatrix} \tilde{\mathbf{t}}^{\mathbf{0}} \\ \tilde{\mathbf{t}}^{\mathbf{1}} \\ \tilde{\mathbf{t}}^{\mathbf{2}} \end{pmatrix}^{\otimes n'}$ is realizable as a standard signature of a planar matchgate. Equivalently we can say that the inner product of $\underline{R}$ with any column in $T^{\otimes n'}$ having indices involving 3 is zero.

In this case, the Holant, as the contraction $\langle \hat{R}, \hat{G}\rangle$, is equal to the desired value $\langle R, G\rangle$. Also the Holand can still be computed in polynomial time via the same FKT algorithm. Therefore as an algorithmic tool, this provides more freedom in the design of holographic algorithms.

While this is an extension of the mechanism of holographic algorithm designs, the complexity theory question is whether this provides an inherent extension of the expressive power for holographic algorithms.

In this section, we show that, in the context we outlined above, this does not provide an inherent extension. We will show that every holographic algorithm on bases of size 2, where the generators are supported on $\mathbf{t_0}, \mathbf{t_1}, \mathbf{t_3}$ and recognizers are supported on $\tilde{\mathbf{t}}^{\mathbf{0}}, \tilde{\mathbf{t}}^{\mathbf{1}}, \tilde{\mathbf{t}}^{\mathbf{2}}$, can be simulated by another holographic algorithm using a basis of size 1.
(In the following for notational convenience in the proofs, we will exchange the notation of G and $\hat{G}$.)

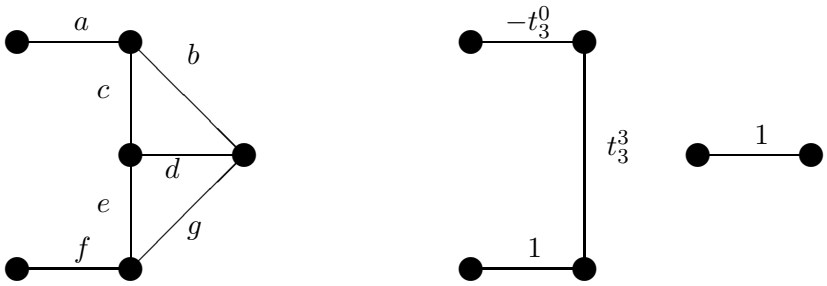
Theorem 5.1. *Suppose G is supported by $\{\mathbf{t}_0, \mathbf{t}_1, \mathbf{t}_3\}$ and is realizable. $\widehat{G}$ is G restricted on the first two basis vectors. Then $\widehat{G}$ is also realizable with the following basis of size 1:*

$$\tau^0_0 = t^0_0 t^3_3 - t^3_0 t^0_3,$$

$$\tau^1_0 = t^1_0 t^2_3 - t^2_0 t^1_3,$$

$$\tau_1^0 = t_1^0 t_3^3 - t_1^3 t_3^0,$$
$$\tau_1^1 = t_1^1 t_3^2 - t_1^2 t_3^1.$$

Proof: Let G be supported by $\{\mathbf{t_0}, \mathbf{t_1}, \mathbf{t_3}\}$ and realizable, where the basis has size 2. This means that $\underline{G} = [\mathbf{t_0}, \mathbf{t_1}, \mathbf{t_3}]^{\otimes n} G$ is realizable as the standard signature of some planar matchgate Γ with $2n$ external nodes. We design a new matchgate Γ' of n external nodes using either one of the following two gadgets. If t_3^1 and t_3^2 are not both 0, we use the gadget to the left. If both $t_3^1 = t_3^2 = 0$ we use the



gadget to the right. Each block of two output nodes of Γ are connected to the left hand side of a copy of this gadget and produces a single output node which is the right most vertex of the gadget. The parameters a, b, c, d, e, f and g satisfy $daf = -t_3^0, ae = -t_3^1, cf = t_3^2, be + cg = t_3^3$. These can be shown to be satisfiable as before. We omit the details.

For convenience, we will use two bits as superscript indices for t. Then the standard signature $\underline{G'}$ of Γ' is related to the standard signature $\underline{G}$ of Γ by the following exponential sum:

$$\underline{G'}^{l_1 l_2 \cdots l_n} = \sum_{j_r + j'_r = l_r} \underline{G}^{j_1 j'_1, j_2 j'_2, \cdots, j_n j'_n} (-1)^{j_1} t_3^{\bar{j_1}\bar{j'_1}} (-1)^{j_2} t_3^{\bar{j_2}\bar{j'_2}} \cdots (-1)^{j_n} t_3^{\bar{j_n}\bar{j'_n}}, \tag{7}$$

where $j_r + j'_r = l_r$ is done in $\mathbf{Z}_2$ and $\bar{j}$ denotes the complement bit of j.

By definition of support vectors,

$$\underline{G}^{j_1 j'_1, j_2 j'_2, \cdots, j_n j'_n} = \sum_{i_r \in \{0,1,3\}} G^{i_1 i_2 \cdots i_n} t_{i_1}^{j_1 j'_1} t_{i_2}^{j_2 j'_2} \cdots t_{i_2}^{j_2 j'_2}.$$

Substituting this in (7), we have

$$\begin{aligned}
\underline{G'}^{l_1 l_2 \cdots l_n} &= \sum_{j_r + j'_r = l_r} (-1)^{j_1} t_3^{\bar{j_1}\bar{j'_1}} (-1)^{j_2} t_3^{\bar{j_2}\bar{j'_2}} \cdots (-1)^{j_n} t_3^{\bar{j_n}\bar{j'_n}} \sum_{i_r \in \{0,1,3\}} G^{i_1 i_2 \cdots i_n} t_{i_1}^{j_1 j'_1} t_{i_2}^{j_2 j'_2} \cdots t_{i_2}^{j_2 j'_2} \\
&= \sum_{i_r \in \{0,1,3\}} G^{i_1 i_2 \cdots i_n} \sum_{j_r + j'_r = l_r} (-1)^{j_1} t_3^{\bar{j_1}\bar{j'_1}} t_{i_1}^{j_1 j'_1} (-1)^{j_2} t_3^{\bar{j_2}\bar{j'_2}} t_{i_2}^{j_2 j'_2} \cdots (-1)^{j_n} t_3^{\bar{j_n}\bar{j'_n}} t_{i_n}^{j_n j'_n} \\
&= \sum_{i_r \in \{0,1,3\}} G^{i_1 i_2 \cdots i_n} \prod_{r=1}^{n} \left(\sum_{j_r + j'_r = l_r} (-1)^{j_r} t_3^{\bar{j_r}\bar{j'_r}} t_{i_r}^{j_r j'_r} \right)
\end{aligned}$$

Let's look at the inner sum. If $i_r = 3$,

$$\sum_{j_r + j'_r = l_r} (-1)^{j_r} t_3^{\bar{j_r}\bar{j'_r}} t_{i_r}^{j_r j'_r} = t_3^{1\bar{l_r}} t_3^{0 l_r} - t_3^{0 l_r} t_3^{1\bar{l_r}} = 0.$$

If $i_r \in \{0,1\}$,

$$\sum_{j_r+j'_r=l_r} (-1)^{j_r} t_3^{\bar{j_r}\bar{j'_r}} t_{i_r}^{j_r j'_r} = t_3^{1\bar{l_r}} t_{i_r}^{0l_r} - t_3^{0l_r} t_{i_r}^{1\bar{l_r}} = \tau_{i_r}^{l_r}.$$

Substituting this in the above equation, we see that the outer sum is over $i_r \in \{0,1\}$, and we get

$$\underline{G'}^{l_1 l_2 \cdots l_n} = \sum_{i_r \in \{0,1\}} G^{i_1 i_2 \cdots i_n} \tau_{i_1}^{l_1} \tau_{i_2}^{l_2} \cdots \tau_{i_n}^{l_n}.$$

Notice that for $i_r \in \{0,1\}$, $G^{i_1 i_2 \cdots i_n} = \widehat{G}^{i_1 i_2 \cdots i_n}$, since G restricts to $\widehat{G}$. The above equation is exactly $\underline{G'} = \boldsymbol{\tau}^{\otimes n} \widehat{G}$. So $\widehat{G}$ is realizable on $\boldsymbol{\tau}$. This completes the proof. □

Similarly, we have:

Theorem 5.2. *(Folding Bases Theorem) Suppose R is supported by $\{\tilde{\mathbf{t}}^0, \tilde{\mathbf{t}}^1, \tilde{\mathbf{t}}^2\}$ and is realizable. R' is R restricted on the first two basis vectors. Then R' is also realizable at the following size 1 basis:*

$$\tilde{\tau'}_0^0 = \tilde{t}_0^0 \tilde{t}_3^2 - \tilde{t}_3^0 \tilde{t}_0^2,$$
$$\tilde{\tau'}_1^0 = \tilde{t}_1^0 \tilde{t}_2^2 - \tilde{t}_2^0 \tilde{t}_1^2,$$
$$\tilde{\tau'}_0^1 = \tilde{t}_0^1 \tilde{t}_3^2 - \tilde{t}_3^1 \tilde{t}_0^2,$$
$$\tilde{\tau'}_1^1 = \tilde{t}_1^1 \tilde{t}_2^2 - \tilde{t}_2^1 \tilde{t}_1^2.$$

Theorem 5.3. *If the basis $\left[\begin{pmatrix}\tau_0^0\\ \tau_0^1\end{pmatrix}, \begin{pmatrix}\tau_1^0\\ \tau_1^1\end{pmatrix}\right]$ in Theorem 5.1 is linearly independent, then the two bases of size 1 in Theorem 5.1 and 5.2 are inverses of each other, up to the equivalence relation in the sense of Proposition 2.1.*

Therefore the extended holographic algorithms using such support vectors can be simulated by holographic algorithms on bases of size 1 without such extension.

We remark that if $\widehat{G}$ is realizable on $\boldsymbol{\tau}$ and yet the basis τ is not linearly independent, then $\widehat{G}$ is trivial and uninteresting.

Proof: By Proposition 2.1, we only need to prove that $\tau_0^0 \tilde{\tau'}_1^0 + \tau_1^0 \tilde{\tau'}_1^1 = \tau_0^1 \tilde{\tau'}_0^0 + \tau_1^1 \tilde{\tau'}_0^1 = 0$. We show this by the following calculation.

$$\begin{aligned}
\tau_0^0 \tilde{\tau'}_1^0 + \tau_1^0 \tilde{\tau'}_1^1 &= (t_0^0 t_3^3 - t_0^3 t_3^0)(\tilde{t}_1^0 \tilde{t}_2^2 - \tilde{t}_2^0 \tilde{t}_1^2) + (t_1^0 t_3^3 - t_1^3 t_3^0)(\tilde{t}_1^1 \tilde{t}_2^2 - \tilde{t}_2^1 \tilde{t}_1^2) \\
&= t_3^3(t_0^0(\tilde{t}_1^0 \tilde{t}_2^2 - \tilde{t}_2^0 \tilde{t}_1^2) + t_1^0(\tilde{t}_1^1 \tilde{t}_2^2 - \tilde{t}_2^1 \tilde{t}_1^2)) - t_3^0(t_0^3(\tilde{t}_1^0 \tilde{t}_2^2 - \tilde{t}_2^0 \tilde{t}_1^2) + t_1^3(\tilde{t}_1^1 \tilde{t}_2^2 - \tilde{t}_2^1 \tilde{t}_1^2)) \\
&= t_3^3(\tilde{t}_2^2(t_0^0 \tilde{t}_1^0 + t_1^0 \tilde{t}_1^1) - \tilde{t}_1^2(t_0^0 \tilde{t}_2^0 + t_1^0 \tilde{t}_2^1)) - t_3^0(\tilde{t}_2^2(t_0^3 \tilde{t}_1^0 + t_1^3 \tilde{t}_1^1) - \tilde{t}_1^2(t_0^3 \tilde{t}_2^0 + t_1^3 \tilde{t}_2^1)) \\
&= -t_3^3(\tilde{t}_2^2(t_2^0 \tilde{t}_1^2 + t_3^0 \tilde{t}_1^3) - \tilde{t}_1^2(t_2^0 \tilde{t}_2^2 + t_3^0 \tilde{t}_2^3)) + t_3^0(\tilde{t}_2^2(t_2^3 \tilde{t}_1^2 + t_3^3 \tilde{t}_1^3) - \tilde{t}_1^2(t_2^3 \tilde{t}_2^2 + t_3^3 \tilde{t}_2^3)) \\
&= -t_3^3(\tilde{t}_2^2 t_3^0 \tilde{t}_1^3 - \tilde{t}_1^2 t_3^0 \tilde{t}_2^3) + t_3^0(\tilde{t}_2^2 t_3^3 \tilde{t}_1^3 - \tilde{t}_1^2 t_3^3 \tilde{t}_2^3) \\
&= 0.
\end{aligned}$$

Here the 4th equality uses the fact that $\tilde{T} = T^{-1}$.

Similarly, we have $\tau_0^1 \tilde{\tau'}_0^0 + \tau_1^1 \tilde{\tau'}_0^1 = 0$.

Even though we prove that in this natural setting, the use of more general support vectors can be simulated by holographic algorithms which do not use this extra freedom, we should not therefore conclude that this notion is useless. Logically this is not dissimilar to that of deterministic finite automata and non-deterministic finite automata. Moreover our proof here does not address the more general possibilities of two support vector sets intersecting at $[\mathbf{t_0}, \mathbf{t_1}]$. This situation is open.

References

[1] J-Y. Cai and Vinay Choudhary. Some Results on Matchgates and Holographic Algorithms. In Proceedings of ICALP 2006, Part I. Lecture Notes in Computer Science vol. 4051. pp 703-714. Also available at Electronic Colloquium on Computational Complexity TR06-048, 2006.

[2] J-Y. Cai and Vinay Choudhary. Valiant's Holant Theorem and Matchgate Tensors (Extended Abstract). In Proceedings of TAMC 2006: Lecture Notes in Computer Science vol. 3959, pp 248-261. Also available at Electronic Colloquium on Computational Complexity Report TR05-118.

[3] J-Y. Cai and Vinay Choudhary. On the Theory of Matchgate Computations . Submitted. Also available at Electronic Colloquium on Computational Complexity Report TR06-018.

[4] J-Y. Cai and Pinyan Lu. On Symmetric Signatures in Holographic Algorithms. To appear in STACS 2007. Also available at Electronic Colloquium on Computational Complexity Report TR06-135.

[5] J-Y. Cai and Pinyan Lu. Holographic Algorithms: From Art to Science. Submitted. Also available at Electronic Colloquium on Computational Complexity Report TR06-145.

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

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

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

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

[10] P. W. Kasteleyn. Graph Theory and Crystal Physics. In *Graph Theory and Theoretical Physics*, (F. Harary, ed.), Academic Press, London, 43-110 (1967).

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

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

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

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

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

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

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

[18] L. G. Valiant. Completeness for parity problems. In *Proc. 11th International Computing and Combinatorics Conference*, 2005, 1–8.

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

6 Appendix

In [4], we gave a characterization of all the realizable *symmetric signatures* over all bases of size 1.

Theorem 6.1. *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* $\forall k, 0 \leq k \leq n-2$,

$$ax_k + bx_{k+1} + cx_{k+2} = 0. \tag{8}$$

Based on this theorem, the following Lemmas in [5] gave a complete and mutually exclusive list of realizable symmetric signatures for generators, in terms of the exact set of bases of size 1 on which a signature is realized.

In the following, the *basis manifold* $\mathcal{M}$ is defined to be the set of all possible size 1 bases modulo the equivalence relation from Proposition 2.1. And the notation $B_{gen}([x_0, x_1, \ldots, x_n])$ is defined to be the set of all possible bases in $\mathcal{M}$ on which a symmetric signature $[x_0, x_1, \ldots, x_n]$ for a generator is realizable.

Lemma 6.1.

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

Lemma 6.2.

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

Lemma 6.3. *Let* $\lambda_1 \neq 0$. *Suppose* $p = \text{char.}\mathbf{F} \not| n$,

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

Lemma 6.4. *For* $AB \neq 0$,

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

Lemma 6.5. *For* $AB \neq 0$ *and* $\alpha \neq \beta$,

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

Lemma 6.6. *Let* $A \neq 0$ *and suppose* $p = \text{char.}\mathbf{F} \not| n$.

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

ECCC ISSN 1433-8092

http://eccc.hpi-web.de/