Holographic Algorithms With Unsymmetric Signatures *

Jin-Yi Cai †
University of Wisconsin-Madison

Pinyan Lu‡
Tsinghua University

Abstract

Holographic algorithms were introduced by Valiant as a new methodology to derive polynomial time algorithms. Here information and computation are represented by exponential sums using the so-called *signatures*. These signatures express superpositions of perfect matchings, and are used to achieve exponential sized cancellations, and thereby exponential speedups. Most holographic algorithms so far used *symmetric signatures*. In this paper we use *unsymmetric signatures* to give some new holographic algorithms. We also prove a characterization theorem for a class of realizable *unsymmetric signatures*, each of which may be used to design new holographic algorithms.

1 Introduction

A central problem in the Theory of Computing is to design polynomial time algorithms for combinatorial problems. What makes a problem solvable or not solvable in polynomial time is not well understood. It is generally conjectured that many combinatorial problems in the class NP or #P are not solvable in polynomial time, presumably it requires the accounting or processing of exponentially many possibilities representing potential solution fragments to the problem. The accepted methodology consists of a two-pronged approach. On the one hand, we have certain widely applicable algorithm design principles to derive efficient algorithms, such as divide and conquer, greedy algorithms, linear programming, SDP programming, dynamic programming, network flow, etc. On the other hand, when such attempts fail, we try to prove the problem NP-hard or #P-hard.

The theory of holographic algorithms was initiated by Valiant [25]. It is an algorithmic methodology for some seemingly exponential time computations. It does that by evaluating certain exponential sums in polynomial time [25, 1, 28, 5]. Somewhat analogous to quantum computing, information in these algorithms is represented and processed through a choice of linear basis vectors in an exponential "holographic" mix. The algorithm is designed to create huge cancellations on these exponential sums. Ultimately the computation is reduced to the Fisher-Kasteleyn-Temperley (FKT) method on planar perfect matchings [15, 16, 22] via the Holant Theorem. Unlike quantum algorithms, these give classical polynomial time algorithms.

To get a feel for holographic algorithms, we first note that for most combinatorial problems, it is quite natural to express the solution as a suitable exponential sum. Take for instance the canonical NP-complete problem SAT. Its counting version is #P-complete. Moreover the problem remains complete for many restricted classes. If we define #Pl-Rtw-Mon-3CNF to be the counting problem which counts the number of satisfying assignments to a planar read-twice monotone 3CNF formula Φ, it remains #P-complete. The syntactic restriction facilitates the formulation of the problem in the theory of holographic algorithms which has an algebraic framework, while at the same time retains its structural complexity. The number of satisfying assignments to Φ can be expressed as an exponential sum as follows. For each clause C in Φ with 3 variables we define a vector $R_C = (0, 1, 1, 1, 1, 1, 1, 1)$, where the entries are indexed by 3 bits $b_1b_2b_3 \in \{0, 1\}^3$. Here $b_1b_2b_3$ corresponds to a truth assignment to the 3 variables, and R_C corresponds to a Boolean OR gate. Suppose in the formula Φ a Boolean variable x appears in two clauses C and C'. Then we use $G_x = (1, 0, 0, 1)^{\mathrm{T}}$, indexed by $b_1b_2 \in \{0, 1\}^2$, to indicate that the fan-out value from x to C and C' must be consistent, i.e., they must be either 00 or 11. In the language of holographic algorithms these R_C and G_x are called *signatures*. Now we can form the tensor products $\mathbf{R} = \bigotimes_C R_C$ and $\mathbf{G} = \bigotimes_x G_x$. Suppose in the planar formula Φ there are exactly e edges connecting various x's to various C's, then both $\mathbf{R}$ and $\mathbf{G}$ have e indicies, each taking values in $\{0, 1\}$, and both tensors have 2^e entries. The indices of $\mathbf{R} = (R_{i_1 i_2 \ldots i_e})$ and $\mathbf{G} = (G^{i_1 i_2 \ldots i_e})$ match up one-to-one according to which x appears in which C. Then the exponential sum $\langle \mathbf{R}, \mathbf{G} \rangle = \sum_{i_1, i_2, \ldots, i_e \in \{0,1\}} R_{i_1 i_2 \ldots i_e} G^{i_1 i_2 \ldots i_e}$ counts exactly the number of satisfying assignments to Φ. This

*Supported by NSF CCR-0511679 and by the National Natural Science Foundation of China Grant 60553001 and the National Basic Research Program of China Grant 2007CB807900, 2007CB807901.

†jyc@cs.wisc.edu
‡lpy@mails.tsinghua.edu.cn

is because each tuple $(i_1, i_2, \ldots, i_e) \in \{0,1\}^e$ assigns a value 0 or 1 to each connecting edge, and the product $R_{i_1 i_2 \ldots i_e} G^{i_1 i_2 \ldots i_e}$ is 1 when this is a consistent assignment of truth values to each variable and the truth assignment satisfies each clause; the product value is 0 otherwise. (See more details in Section 2.)

Of course, it is not surprising that we can express the answer to the problem (which is something that can be computed in exponential time) as an exponential sum. What is perhaps surprising is that for a variety of combinatorial problems, holographic algorithms can evaluate such an exponential sum in *polynomial time*. This happens when suitable signatures are *realizable*. In particular, for #Pl-Rtw-Mon-3CNF this theory can evaluate the sum over the field $\mathbf{Z}_7$ [28]. This counts the number of satisfying assignments mod 7 for Φ. In addition to the #P-hardness of #Pl-Rtw-Mon-3CNF (without the modulus), it is also known that counting mod 2 for #Pl-Rtw-Mon-3CNF is NP-hard. Put in this context, this success with counting mod 7 is rather extraordinary (or "accidental" [28]).

In the successes of holographic algorithms so far, mostly the signatures used have been *symmetric signatures*. In the above example, the signatures $R_C = (0,1,1,1,1,1,1,1)$ and $G_x = (1,0,0,1)^{\mathrm{T}}$ are both symmetric. A signature is called symmetric if its entries only depend on the Hamming weight of the index. For symmetric signatures we have achieved a fairly complete characterization [5].

In this paper we extend the reach of holographic algorithms further, by giving polynomial time algorithms to several problems using some newly discovered *unsymmetric signatures*. These particular unsymmetric signatures have been used for the first time. Moreover, in all previous holographic algorithms, the planarity condition is usually explicitly included in the problem statement. The problems solved in this paper are not stated with a planarity condition.

The success of finding a holographic algorithm for a particular combinatorial problem typically boils down to the existence of suitable signatures in a suitable tensor space. This is called the realizability problem for signatures. For the above problems we first prove this realizability. In general, realizability is specified by a family of algebraic equations. These families of equations are non-linear, exponential in size, and difficult to handle. But whenever we find a suitable solution, we get an exotic polynomial time algorithm.

Beyond the concrete problems, in this paper we also give a characterization theorem for an entire class of realizable unsymmetric signatures. These signatures can all be potentially used to design novel polynomial time algorithms. The crux of this theorem involves proving the orthogonality of a family of exponentially sized matrices. These matrices are given implicitly so that one does not even have an explicit formula for its dimensions. But we show that distinct columns of the matrix are mutually orthogonal by designing a suitable involution which cancels out all the terms pair-wise in the inner product of any two distinct columns.

2 Some Background

In this section we review some definitions and results. More details can be found in [23, 25, 24, 3, 2, 1].

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

Each matchgate is assigned a *signature* tensor. A generator Γ with n output nodes is assigned a contravariant tensor $\mathbf{G} \in V_0^n$ of type $\binom{n}{0}$. Under the standard basis $\mathbf{b} = [\mathbf{e}_1, \mathbf{e}_2]$ it has the form

$$\sum \underline{G}^{i_1 i_2 \ldots i_n} \mathbf{e}_{i_1} \otimes \mathbf{e}_{i_2} \otimes \cdots \otimes \mathbf{e}_{i_n},$$

where

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

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

$$\sum \underline{R}_{i_1 i_2 \ldots i_n} \mathbf{e}^{i_1} \otimes \mathbf{e}^{i_2} \otimes \cdots \otimes \mathbf{e}^{i_n},$$

where

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

where Z is the subset of the input nodes having $\chi_Z = i_1 i_2 \ldots i_n$. These values $(\underline{G}^{i_1 i_2 \ldots i_n})$ and $(\underline{R}_{i_1 i_2 \ldots i_n})$ form the standard signatures.

According to general principles [10], $\mathbf{G}$ and $\mathbf{R}$ transform contravariantly and covariantly under a basis transformation $\boldsymbol{\beta}_j = \sum_{i=1,2} \mathbf{e}_i t_j^i$, $j = 1, 2$,

$$G^{i_1 i_2 \ldots i_n} = \sum \underline{G}^{j_1 j_2 \ldots j_n} \tilde{t}_{j_1}^{i_1} \tilde{t}_{j_2}^{i_2} \ldots \tilde{t}_{j_n}^{i_n},$$

$$R_{i_1 i_2 \ldots i_n} = \sum \underline{R}_{j_1 j_2 \ldots j_n} t_{i_1}^{j_1} t_{i_2}^{j_2} \ldots t_{i_n}^{j_n},$$

where $(\tilde{t}_j^i)$ is the inverse matrix of (t_j^i).

A signature is called symmetric if its values only depend on the Hamming weight of its indices. This notion is invariant under a basis transformation.

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 edge C_i has weight 1 and joins an output node of a generator with a input node of a recognizer, so that every input and output node in every constituent matchgate has exactly one such incident connecting edge.

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

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

where $\boldsymbol{\beta}$ is any basis. The remarkable Holant Theorem is

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

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

This reduces the computation to the FKT algorithm, which can compute the perfect matching polynomial $\text{PerfMatch}(G)$ for a planar graph in polynomial time.

Let us look at the counting problem #Pl-Rtw-Mon-3CNF mod 7 and its holographic algorithm more closely. The claim is this: There exist (1) a suitable generator matchgate A with two external nodes; (2) a suitable recognizer matchgate B with three external nodes; and (3) a particular basis $\boldsymbol{\beta}$ over the field $\mathbf{Z}_7$, such that the following holds. Let the contravariant tensor $\mathbf{G}$ and the covariant tensor $\mathbf{R}$ assigned to A and B have the standard signatures $(\underline{G}^{i_1 i_2})$ and $(\underline{R}_{i_1 i_2 i_3})$ respectively. Under the basis transformation $\boldsymbol{\beta}_j = \sum_i \mathbf{e}_i t_j^i$, $\mathbf{G}$ and $\mathbf{R}$ take the forms

$$G^{i_1 i_2} = \sum_{j_1 j_2} \underline{G}^{j_1 j_2} \tilde{t}_{j_1}^{i_1} \tilde{t}_{j_2}^{i_2} = (1, 0, 0, 1)^{\mathrm{T}}, \tag{2.1}$$

$$R_{i_1 i_2 i_3} = \sum_{j_1 j_2 j_3} \underline{R}_{j_1 j_2 j_3} t_{i_1}^{j_1} t_{i_2}^{j_2} t_{i_3}^{j_3} = (0, 1, 1, 1, 1, 1, 1, 1). \tag{2.2}$$

To form our matchgrid Ω, we assign one generator A_i for each variable x_i and one recognizer B_j for each clause C_j, where $1 \le i \le n$ and $1 \le j \le m$, and connect the wires as in Φ. Then we form the tensor products $\mathbf{G} = \bigotimes_{i=1}^{n} \mathbf{G}(A_i)$ and $\mathbf{R} = \bigotimes_{j=1}^{m} \mathbf{R}(B_j)$. Note that if we evaluate the $\text{Holant}(\Omega) = \langle \mathbf{R}, \mathbf{G} \rangle$ under the particular basis $\boldsymbol{\beta}$, we accumulate 1 (this is done mod 7 since the underlying field has characteristic 7) for each valid Boolean assignment which satisfies the formula, and 0 otherwise.

Now this exponential sum $\text{Holant}(\Omega)$ is actually evaluated as the equivalent PerfMatch on the planar graph of the matchgrid. Look closely how this exponential sum is evaluated: Each term in the exponential sum $\text{Holant}(\Omega)$ is itself replaced by an exponential sum of perfect matchings (via standard signatures) by the tensor product form of (2.1) and (2.2). Conversely, we can consider the evaluation of PerfMatch, where each perfect matching term in PerfMatch corresponds to an exponential sum (a "holographic" mix) of the combinatorial configurations of the satisfiability problem #Pl-Rtw-Mon-3CNF (mod 7).

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 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:

$$\sum_{i=1}^{l} (-1)^i \underline{G}^{\alpha + e_{p_i}} \underline{G}^{\alpha + p + e_{p_i}} = 0. \tag{2.3}$$

If $\underline{G} = \boldsymbol{\beta}^{\otimes n} G$ satisfies the parity conditions, then G is *admissible* on $\boldsymbol{\beta}$. If $\underline{G}$ further satisfies all the MGIs (then $\underline{G}$ is realizable as the standard signature of some matchgate), then G is *realizable* on $\boldsymbol{\beta}$.

3 A Family of Unsymmetric Signatures in b2 Basis

The basis $\mathbf{b2} = \left[\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right]$ is probably the most successful basis in the design of holographical algorithms. Most problems in Valiant's first paper [25] used the basis **b2**. However, all the signatures based on **b2** which have been used are symmetric. A complete characterization of all the symmetric signatures using **b2** was given in [1]. In [4], we further extended the characterization theorem for symmetric signatures on all bases. Followed from these characterization theorems, we have achieved a satisfactory theory for holographic algorithms using symmetric signatures [5].

Although symmetric signatures have a clear combinatorial meaning and therefore are very useful, some combinatorial problems require unsymmetric signatures. In this section, we introduce a family of unsymmetric signatures, which is realizable on **b2**.

THEOREM 3.1. *For any a and $b \in \mathbf{C}$, the following signature for a generator with arity 4 is realizable on* **b2**.

$$G^{\alpha} = \begin{cases} a, & \alpha \in \{0101, 1010\}, \\ b, & \alpha \in \{0011, 1100\}, \\ 0, & \textit{otherwise}. \end{cases} \tag{3.4}$$

Proof:

$$\underline{G} = (\mathbf{b2})^{\otimes 4} G = (2a{+}2b, 0, 0, -2a{+}2b, 0, 2a{-}2b, -2a{-}2b, 0, 0, -2a-2b, 2a-2b, 0, -2a+2b, 0, 0, 2a+2b)^{T}.$$

This 16-dimensional vector, indexed by $\{0,1\}^4$, has all entries of odd Hamming weight equal to 0. So it satisfies the parity condition. We can also verify that $\underline{G}$ satisfies the unique (non-trivial) MGI for matchgates of arity 4 as follows:

$$\underline{G}^{0000}\underline{G}^{1111} - \underline{G}^{1100}\underline{G}^{0011} + \underline{G}^{1010}\underline{G}^{0101} - \underline{G}^{1001}\underline{G}^{0110}$$

$$= (2a+2b)^2 - (2b-2a)^2 + (2a-2b)^2 - (-2a-2b)^2 = 0.$$

A planar matchgate explicitly realizing this signature is given in the Appendix (see Figure 1). ∎

In the next section, we will show that this family of signatures have very interesting special cases when we choose suitable a and b. In Section 5, we will show that this family of signatures are not only realizable on the basis **b2**, but also realizable on an infinite family of bases **B2**. This makes it potentially more useful because they can be simultaneously realizable with other signatures on some basis in **B2**. Furthermore, Section 5 gives a characterization theorem for all the signatures which are realizable on **B2**. From this, we obtain a vast generalization as higher dimensional extensions of this family. Since the size of signatures and the number of MGIs will increase exponentially with arity, the proof is much more involved than here (we only have one non-trivial MGI for signatures of arity 4.)

4 Some Holographic Algorithms

Problem 1

INPUT: Given a set S of n points on a plane, where no three points are colinear. Also given a set of edges (straight line segments) between some pairs of points in S. We assume no 3 edges intersect at a point ($\notin S$). Every point of S is incident to either 2 or 3 edges.

OUTPUT: The number of 2-colorings for the edges which satisfy the following conditions: (1) for every point in S, the incident edges are not monochromatic; (2) when two edges cross over each other, they have different colors.

SOLUTION: For every point in S with 2 incident edges, we use a generator for $(0,1,1,0)^{\mathsf{T}}$ (for Not-Equal); for every point with 3 incident edges, we use a generator for $(0,1,1,1,1,1,1,0)^{\mathsf{T}}$ (for Not-All-Equal); for every point ($\notin S$) where two edges intersect, we use a generator with arity 4 by setting $a = 1$ and $b = 0$ in (3.4); and finally for every segment of an edge separated by points which are either the end points of the edge (i.e., from S) or the intersection points of edges, we use a recognizer for $(1,0,0,1)^{\mathsf{T}}$ (for Equality). Then it can be seen that the Holant is exactly the number of valid colorings. The unsymmetric generator of arity 4 makes sure that the color of the edge is transmitted at intersection points while only allowing different colored edges to meet at these intersection points. Because all the signatures involved are realizable on **b2**, we have a polynomial time algorithm for this problem. A formal description of the holographic algorithm for this problem can be found in the Appendix. Planar matchgates explicitly realizing all the signatures involved here are also given in the Appendix.

Problem 2

We extend Problem 1 by allowing curves (not necessarily line segments) between two points of S. We assume that every such curve between two points of S does not go through additional points of S. Also any two curves can share at most $n^{O(1)}$ points not in S, and no three curves share such a point. Here "sharing a point" means that they may cross each other or be tangent at the point.

SOLUTION: We use the same signatures as in Problem 1. The additional situation is that two curves may be tangent with each other rather than cross over at a point. (Note that just pulling the tangent curves apart does not guarantee that they are of different colors.) At such a point, we use a generator with arity 4 by setting $a = 0$ and $b = 1$ in (3.4). Since this signature is also realizable on **b2**, we have a polynomial time algorithms for this problem.

Problem 3

Some graphs may not have any valid colorings satisfying

all the requirements. Now we allow edges to change colors on different segments. More precisely, at any point where two curves meet (either transversal or tangent to each other), we still require them to have different colors, but now we allow them to either both keep their colors or both change their colors. Other requirements are the same as above. However, we still want as few such changes as possible, and the problem is to find the minimal number of changes such that at least one valid coloring exists.
SOLUTION: Signatures for original points and segments of curves remain the same. For every cross point, we use a generator with arity 4 by setting $a = 1$ and $b = x$ in (3.4). And for every tangent point, we use a generator with arity 4 by setting $a = x$ and $b = 1$ in (3.4).

Since they are all realizable on **b2**, we have a polynomial time algorithm to compute the Holant. This time the Holant is a polynomial of x. The degree of this polynomial is bounded by $n^{O(1)}$, and the coefficients all have at most $n^{O(1)}$ bits. The coefficient of x^k is the number of valid colorings with exactly k changes of color. By the interpolation method, we can evaluate the Holant a polynomial number of times with different values of x, and compute the polynomial, and therefore get the degree of the non-zero term of the smallest degree.

We note that these problems are not *a priori* about planar graphs due to intersecting edges. The unsymmetric signatures (and their planar matchgates) created the necessary planarity.

5 The Bases Set B2

In this section, we extend the basis **b2** to a bases set **B2** defined as follows (note that we have $\mathbf{b2} \in \mathbf{B2}$):

$$\mathbf{B2} = \left\{ \left[\begin{pmatrix} n_0 \\ n_1 \end{pmatrix}, \begin{pmatrix} p_0 \\ p_1 \end{pmatrix} \right] \in \mathbf{GL}_2(\mathbf{C}) \middle| n_0 p_1 + n_1 p_0 = 0 \right\}.$$

Based on the equivalence relation in the *basis manifold* $\mathcal{M}$ (see [5]), we will use dehomogenized coordinates $\begin{pmatrix} 1 & x \\ 1 & -x \end{pmatrix}$ for notational simplicity. (If there are exceptional cases ("at infinity"), they can be verified directly; or one can invoke general theorems in algebraic geometry.)

We will give a complete characterization theorem of all the signatures which are realizable on **B2**. The plan is to first give a characterization of all the signatures which are admissible on **B2**. Then we apply the set of all MGIs to them to get the characterization theorem.

For the parity constraint, we assume they are admissible as odd matchgate signatures (the case of even matchgates is similar). Consider an arbitrary $\begin{pmatrix} 1 & x \\ 1 & -x \end{pmatrix} \in \mathbf{B2}$, where non-singularity implies that $x \neq 0$. Under a basis transformation $\underline{G} = \begin{pmatrix} 1 & x \\ 1 & -x \end{pmatrix}^{\otimes n} G$, the entry

$$\underline{G}^T = \left\langle \bigotimes_{\sigma=1}^{n} [1, (-1)^{\chi_{[\sigma \in T]}} x], G \right\rangle \tag{5.5}$$

$$= \sum_{\substack{0 \le i \le n-|T| \\ 0 \le j \le |T|}} x^i (-x)^j \sum_{\substack{A \subset T^c,\, |A| = i \\ B \subset T,\, |B| = j}} G^{A \cup B},$$

The polynomials should be identically zero when $|T|$ is even. This is the necessary and sufficient condition for G to be admissible on **B2**. Thus for any T with $|T|$ even, the coefficient of x^i in the polynomial of (5.5) is

$$\sum_{|S|=i} (-1)^{|S \cap T|} G^S = 0. \tag{5.6}$$

When T ranges over all even subsets, we have a linear system for G^S. Thus we get $n + 1$ linear equation systems according to the weight of S; the i-th linear system, $0 \le i \le n$, is over the set of variables G^S with $|S| = i$, where the equations are indexed by subsets T with even cardinality. We define the coefficient matrix of the system as M, which is indexed by T and S. Then we have the following calculation of $M^{\mathtt{T}} M$:

$$(M^{\mathtt{T}} M)_{S_1, S_2} = \sum_{|T| \text{ is even}} (-1)^{|S_1 \cap T|} (-1)^{|S_2 \cap T|} \tag{5.7}$$

$$= \sum_{|T| \text{ is even}} (-1)^{|(S_1 \oplus S_2) \cap T|}.$$

There are three cases: If $S_1 \oplus S_2 = \emptyset$, or if $S_1 \oplus S_2 = [n]$, we have $\sum_{|T| \text{ is even}} (-1)^{|(S_1 \oplus S_2) \cap T|} = 2^{n-1}$.

The third case is $S_1 \oplus S_2 \neq \emptyset$ and $S_1 \oplus S_2 \neq [n]$. We can take two elements a and b such that $a \in S_1 \oplus S_2$ and $b \notin S_1 \oplus S_2$. Then we can give a perfect matching of all the even subsets T by matching T and $T \oplus \{a, b\}$ together. For each pair of T and $T \oplus \{a, b\}$, one contributes a $+1$ and the other contributes a -1 in (5.7). They cancel out by each other, so overall we have $\sum_{|T| \text{ is even}} (-1)^{|(S_1 \oplus S_2) \cap T|} = 0$.

Now for the i-th system, for $i = |S| \neq n/2$, the case $S_1 \oplus S_2 = [n]$ does not occur. So the matrix $M^{\mathtt{T}} M$ is $2^{n-1} I$, which means that $G^S = 0$, for all $|S| \neq n/2$. (In particular, only trivial $G \equiv 0$ exists for n odd.)

If $|S| = n/2$, the $n/2$-th linear system gives $G^S = -G^{S^c}$. For the even matchgate case ($|T|$ is odd), it gives $G^S = G^{S^c}$. This is also sufficient. So we have the following theorem, which completely solves the problem of admissibility for **B2**:

THEOREM 5.1. *For a signature G with arity n, G is admissible on* **B2** *iff there exists $\epsilon = \pm 1$ such that $G^S = 0$ for all $|S| \neq n/2$ and $G^S = \epsilon G^{S^c}$ for all $|S| = n/2$.*

Now we move on to the more difficult question of realizability. Realizability is more difficult than admissibility because it is controlled by the set of Matchgate Identities (MGI). These MGI are not only exponential in size, but also non-linear. We will apply all the MGIs to the signatures in the above theorem to get our characterization theorem over **B2**.

For a $\boldsymbol{\beta} = \begin{pmatrix} 1 & x \\ 1 & -x \end{pmatrix} \in$ **B2**, let $\underline{G} = \boldsymbol{\beta}^{\otimes n} G$. The problem is to characterize when $\underline{G}$ is realizable by an even matchgate as a standard signature. (The case for odd matchgate is similar.) From Theorem 5.1, we know that $G^S = 0$ for all $|S| \neq n/2$, and $G^S = G^{S^c}$ for all $|S| = n/2$. (For odd matchgates it would be $G^S = -G^{S^c}$; we omit it here.) By the basis transformation $\underline{G} = \boldsymbol{\beta}^{\otimes n} G$, we have ($T$ is even):

$$\underline{G}^T = x^{n/2} \sum_{|S|=n/2} (-1)^{|T \cap S|} G^S.$$

In the above equation, when substituted in any MGI, $x^{n/2}$ is just a global scaling factor. So we can just let $x = 1$, without changing its realizability.

We consider an arbitrary MGI of $\underline{G}$: for a pattern set A ($|A|$ is odd), position set P ($|P|$ is even), we have

$$\begin{aligned} 0 &= \sum_{i=1}^{|P|} (-1)^i \underline{G}^{A \oplus \{p_i\}} \underline{G}^{A \oplus P \oplus \{p_i\}} \\ &= \sum_{i=1}^{|P|} (-1)^i \sum_{|S_1|=n/2} (-1)^{|(A \oplus \{p_i\}) \cap S_1|} G^{S_1} \\ &\quad \sum_{|S_2|=n/2} (-1)^{|(A \oplus P \oplus \{p_i\}) \cap S_2|} G^{S_2} \\ &= \sum_{|S_1|=|S_2|=n/2} G^{S_1} G^{S_2} \\ &\quad \sum_{i=1}^{|P|} (-1)^i (-1)^{|(A \oplus \{p_i\}) \cap S_1|} (-1)^{|(A \oplus P \oplus \{p_i\}) \cap S_2|}. \end{aligned}$$

Over all odd A and even P these are also sufficient conditions. Note that for even matchgates, both A and $A \oplus P$ must be odd (so that the single bit flips $A \oplus \{p_i\}$ and $A \oplus P \oplus \{p_i\}$ are even).

Because the sets $A \oplus \{p_i\}$ and $A \oplus P \oplus \{p_i\}$ are both even, the coefficients of the four terms $G^{S_1} G^{S_2}$, $G^{S_1} G^{S_2^c}$, $G^{S_1^c} G^{S_2}$ and $G^{S_1^c} G^{S_2^c}$ are all equal. Therefore we can combine these four terms (and divide by 4) and have

$$\begin{aligned} 0 &= \sum_{|S_1|=|S_2|=n/2,\ 1 \in S_1 \cap S_2} G^{S_1} G^{S_2} \\ &\quad \sum_{i=1}^{|P|} (-1)^i (-1)^{|(A \oplus \{p_i\}) \cap S_1|} (-1)^{|(A \oplus P \oplus \{p_i\}) \cap S_2|} \\ &= \sum_{|S_1|=|S_2|=n/2,\ 1 \in S_1 \cap S_2} G^{S_1} G^{S_2} (-1)^{|A \cap (S_1 \oplus S_2)|} \\ &\quad (-1)^{|P \cap S_2|} \sum_{i=1}^{|P|} (-1)^i (-1)^{|\{p_i\} \cap (S_1 \oplus S_2)|}. \end{aligned}$$

We identify a set $X \subset [n]$ with its characteristic vector in our notations. We call an X a *single run* iff it is $\emptyset$, or $[n]$, or as a 0-1 characteristic vector it consists of a contiguous segment of 0's and then 1's, in a circular fashion. We have the following theorem.

THEOREM 5.2. *For a signature G with arity n, G is realizable on* **B2** *iff there exists $\epsilon = \pm 1$ such that*

1. *$G^S = 0$ for all $|S| \neq n/2$;*
2. *$G^S = \epsilon G^{S^c}$ for all $|S| = n/2$; and*
3. *for any pair (S_1, S_2), if $G^{S_1} G^{S_2} \neq 0$, then $S_1 \oplus S_2$ is a single run.*

Proof: First we denote $X = S_1 \oplus S_2$ and use S instead of S_2 in the above MGI (we note that X is an even set and $1 \notin X$):

(5.8)

$$\sum_{|X| \text{ is even},\ 1 \notin X} (-1)^{|A \cap X|} \sum_{|S|=|S \oplus X|=n/2,\ 1 \in S} G^S G^{S \oplus X}$$

$$(-1)^{|P \cap S|} \sum_{i=1}^{|P|} (-1)^i (-1)^{|\{p_i\} \cap X|} = 0.$$

The above equation is valid for all odd sets A and even sets P. We define a set of valuables $Y(X, P)$ as

$$Y(X, P) =$$

$$\sum_{\substack{|S| = |S \oplus X| = n/2 \\ 1 \in S}} G^S G^{S \oplus X} (-1)^{|P \cap S|} \sum_{i=1}^{|P|} (-1)^{i + |\{p_i\} \cap X|}.$$

We fix an arbitrary even P. Then let A go through all the odd sets, we have a linear system for the valuables $Y(X, P)$ from (5.8), where the variables are indexed by even X not containing 1, and the equations are indexed by odd A. The coefficient matrix of this system is $((-1)^{|A \cap X|})$. This matrix has full rank, which can be proved similarly as in the two out of three cases for (5.7).

Note that for two X_1 and X_2, we have $X_1 \oplus X_2 \neq [n]$, because $1 \notin X_1 \oplus X_2$.

Therefore we have for any even P and any even X with $1 \notin X$,

(5.9)
$$\sum_{\substack{|S| = |S \oplus X| = \frac{n}{2} \\ 1 \in S}} G^S G^{S \oplus X} (-1)^{|P \cap S|} \sum_{i=1}^{|P|} (-1)^{i + |\{p_i\} \cap X|} = 0.$$

Now we will fix an even X with $1 \notin X$, and view (5.9) as a linear system on the variables $G^S G^{S \oplus X}$, where the equations are indexed by all even P.

First we show that if X is a single run, then (5.9) always holds. If $P \cap X$ is even, since X is a single run and is even, and P is even, it follows that there are an even number of elements in both $P \cap X$ and $P \cap X^c$. A moment reflection shows that $\sum_{i=1}^{|P|}(-1)^i(-1)^{|\{p_i\} \cap X|} = 0$.

If $P \cap X$ is odd, then by symmetry of S to $S \oplus X$, the combined coefficient of $G^S G^{S \oplus X} = G^{S \oplus X} G^S$ is $(-1)^{|P \cap S|} + (-1)^{|P \cap (S \oplus X)|} = (-1)^{|P \cap S|}[1 + (-1)^{|P \cap X|}]$. When $P \cap X$ is odd, this is 0. So we proved the "if" part of this theorem.

Now we prove that the conditions in Theorem 5.2 are also necessary. We will show that in order to satisfy all the MGI, for any even X with $1 \notin X$, if X is not a single run, then for all S, $G^S G^{S \oplus X} = 0$. This is more difficult. The crux of the proof is to show that a certain exponential sized matrix has mutually orthogonal columns, a matrix which we don't even have an explicit formula for its dimension.

Fix an even X with $1 \notin X$. We assume X is not a single run. Then we can pick a particular P with 4 elements, such that $p_1 < p_2 < p_3 < p_4$, and $p_2, p_4 \in X$ and $p_1, p_3 \notin X$. This can be done greedily, e.g., pick $p_1 = 1$ (we know that $1 \notin X$). Then run from $1, 2, 3, \ldots$ till the first $i \in X$. That is our p_2. Since X is not a single run, by our definition $X \neq \emptyset$ in particular. So p_2 exists. Then the first one after that which is not in X is p_3. Being not a single run, such a p_3 must exist. Then there must be another one after p_3, which belongs to X, again by X being not a single run. This is our $p_4 \in X$. Now for this particular P, we can see that $\sum_{i=1}^{|P|}(-1)^i(-1)^{|\{p_i\} \cap X|} \neq 0$.

For a fixed even X with $1 \notin X$, and X is not a single run, consider the linear equation system:

For all even P such that $\sum_{i=1}^{|P|}(-1)^i(-1)^{|\{p_i\} \cap X|} \neq 0$, and $P \cap X$ is also even,

(5.10)
$$\sum_{|S| = |S \oplus X| = n/2,\ 1 \in S} (-1)^{|P \cap S|} G^S G^{S \oplus X} = 0.$$

Here the variables are all "$G^S G^{S \oplus X}$", where $|S| = |S \oplus X| = n/2,\ 1 \in S$. Note that, as shown above, if $P \cap X$ is odd, then the combined coefficients of $G^S G^{S \oplus X} = G^{S \oplus X} G^S$ is zero in (5.9). (That proof does not depend on X being a single run or not.) For $P \cap X$ is even, the coefficients of $G^S G^{S \oplus X} = G^{S \oplus X} G^S$ are the same, which can be combined. Consequently in (5.10) we combine the coefficients of $G^S G^{S \oplus X} = G^{S \oplus X} G^S$, but only consider for $P \cap X$ even. After this identification, the equation system in (5.10) (for a fixed X satisfying the conditions) has equations indexed by the P's satisfying its stated conditions, has variables $G^S G^{S \oplus X}$ after the identification S with $S \oplus X$. They range over unordered pairs $\{S, S \oplus X\}$ obtained by taking 1, and exactly half the elements of X and exactly $\frac{n}{2} - \frac{|X|}{2} - 1$ elements of $[n] - \{1\} - X$. We will not give a closed-form formula for the number of equations indexed by the P's; nevertheless, we will show that columns of the matrix of the linear system (5.10) are mutually orthogonal!

In the following, when we say, consider two "distinct" S and S' in this equation system, we have the following property: $S \oplus S'$ is not any of the four sets: $\emptyset, [n], X, X^c$. (Not equal to $\emptyset$ because they are distinct; not equal to $[n]$ because both contain 1; not equal to X because of the above identification; and finally not equal to X^c because $1 \notin S \oplus S'$ and yet $1 \in X^c$.)

Our goal is to show, for the linear equation system (5.10), the columns of "distinct" S and S' are orthogonal. First some comments. We will not use explicitly below the fact that X is not a single run to show orthogonality. Not being a single run was used to show that the column coefficient vectors in (5.9) are non-zero (for these vectors the entries are indexed by P as P runs through all the appropriate sets, the set of vectors is indexed by various S). In going from (5.9) to (5.10), we have already taken that into account.

We had proved earlier that for X not a single run, there exists some position vector P which makes the sum $\sum_{i=1}^{|P|}(-1)^i(-1)^{|\{p_i\} \cap X|} \neq 0$. For a fixed X, in the linear equation system (5.9) the above quantity $\sum_{i=1}^{|P|}(-1)^i(-1)^{|\{p_i\} \cap X|}$ does not depend on variables $G^S G^{S \oplus X}$ indexed by S. We can collect those equations (a non-empty subset of equations indexed by P) in (5.9) where the above quantity is non-zero, and factor out this sum from each such equation. This gives us (5.10). Of course in (5.9) those equations (indexed by P) where the above sum is zero is trivially satisfied. This means that the orthogonality of the coefficient vectors in (5.10) implies that all $G^S G^{S \oplus X} = 0$ in (5.10) and therefore in (5.9).

(For notational simplicity, we may consider the equality $G^S G^{S \oplus X} = 0$ above really for all S, and not worry about S being half weight or $S \oplus X$ being half weight. As otherwise they are obvious.)

Now we wish to prove any two "distinct" column vectors for S and S' are orthogonal. Let's consider the condition $\sum_{i=1}^{|P|}(-1)^i(-1)^{|\{p_i\}\cap X|} \neq 0$ more carefully. Lay out the elements $1,2,3,\ldots,n$, and lay out the elements of X in that order from left to right. It breaks $[n]$ into runs. Say $1,2,\ldots,a \notin X$, $a+1,a+2,\ldots,b \in X$, $b+1,b+2,\ldots,c \notin X$, etc. We call $[1,2,\ldots,a]$ an "out" segment for X, $[a+1,a+2,\ldots,b]$ an "in" segment for X, etc. Now consider going through elements of P, also from 1 to n. Put down $-$ and $+$ alternately under each such element of P, from p_1 to the last P-element. These record the factor $(-1)^i$ in the sum. In each "in" and "out" segment of X, P will have either an even or an odd number of elements. Since $|P|$ is even, there must be an even number of segments ("in" or "out") which have an odd number of P-elements. A moment reflection will convince us that whenever we have a segment which contains an even number of P-elements, we can ignore that segment. It does not affect the subsequent $\pm$ labelling. And for either an "in" segment or an "out" segment of X, the contribution of these even number of P-elements to the sum $\sum_{i=1}^{|P|}(-1)^i(-1)^{|\{p_i\}\cap X|}$ is 0. So we can imagine a sequence of "even-segment removal" operations as follows: Whenever we see an "even segment" (either an "in" or an "out" segment of X which contains an even number of elements of P), we can remove it, and then merge the neighboring segments. This keeps the segments to be alternately "in" and "out" for X, and P is still even and therefore there remains an even number of segments with an odd number of P-elements. We can continue this process until no more "even segment" is left. When this process ends, we have an even number of "odd segments" left. They will still be alternately "in" and "out" for X. Now the key observation is this: There is nothing left (that even number $= 0$) iff that original sum $\sum_{i=1}^{|P|}(-1)^i(-1)^{|\{p_i\}\cap X|} = 0$. This is because every "odd segment" that is left at the end contributes exactly the same ± 1 to the sum. If the even number of "odd segments" left starts with an "in" segment for X, then each segment contributes a $+1$; if it starts with an "out" segment for X, then each segment contributes a -1.

Now consider two "distinct" S and S', and consider the inner product of their column vectors. Denote by $D = S \oplus S'$. Then $D \neq \emptyset, [n], X, X^c$. The inner product is

$$\sum_P (-1)^{|P\cap S|}(-1)^{|P\cap S'|} = \sum_P (-1)^{|P\cap D|},$$

where P runs over all even subsets of $[n]$ with $P \cap X$ even, and satisfying $\sum_{i=1}^{|P|}(-1)^i(-1)^{|\{p_i\}\cap X|} \neq 0$.

Now we design an involution (order 2 permutation) with no fixed point on the set of all such P's: Since $D \neq \emptyset, [n], X, X^c$, as we examine all elements from 1 to n, there must be two elements next to each other, both in X or both out of X, and one is in D and the other one is out of D. (This is because: as $D \neq \emptyset, [n]$, there must be "changes" in membership of D as we go from 1 to n. And if all such changes coincide with boundaries of "segments" (these are the change boundaries) of X, then either $D = X$ or $D = X^c$, but both are ruled out.) Thus there are i and $i+1$ which are in the same segment of X (either "in" segment or "out" segment) such that $|D \cap \{i, i+1\}| = 1$. We use this $\{i, i+1\}$ to define our involution on the set of P's: $P \mapsto P' = P \oplus \{i, i+1\}$.

Note that P is even iff P' is even, and also, $P \cap X$ is even iff $P' \cap X$ is even. Moreover, in the "eliminating the even segment" process described above both P and P' will yield the same answer as to 0 or non-zero. Thus the involution is an involution on the set of even P, with $P \cap X$ even, and such that $\sum_{i=1}^{|P|}(-1)^i(-1)^{|\{p_i\}\cap X|} \neq 0$.

Finally in the sum $\sum_P (-1)^{|P\cap D|}$, the term $(-1)^{|P\cap D|}$ and $(-1)^{|P'\cap D|}$ cancel, since

$$(-1)^{|P'\cap D|} = (-1)^{|P\cap D|}(-1)^{|\{i,i+1\}\cap D|} = -(-1)^{|P\cap D|}.$$

This completes the proof. ∎

Theorem 3.1 is a special case of Theorem 5.2 when $n = 4$. This is used in Section 4.

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. To appear in Theoretical Computer Science. A preliminary version in Proceedings of TAMC 2006: Lecture Notes in Computer Science vol. 3959, pp 248-261.

[3] J-Y. Cai, Vinay Choudhary and Pinyan Lu. On the Theory of Matchgate Computations. In the proceedings of IEEE Conference on Computational Complexity 2007, pp 305-318.

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

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

[6] J-Y. Cai and Pinyan Lu. Bases Collapse in Holographic Algorithms. In the proceedings of IEEE Conference on Computational Complexity 2007, pp 292-304.

[7] J-Y. Cai and Pinyan Lu. Holographic Algorithms: The Power of Dimensionality Resolved. To appear in ICALP 2007. Also available at Electronic Colloquium on Computational Complexity Report TR07-020.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[25] 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.

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

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

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

Appendix:

A Formal Description of the Holographic Algorithm for Problem 1

Algorithm:

STEP 1: Construct a bipartite graph $G(V_1, V_2)$ from the input as follows:

- V_1 contains all the points in S and all the points where two lines intersect;
- V_2 contains every segment of a line segment separated by points which are either the end points of the edge (i.e., from S) or the intersection points of line segments;
- there is an edge between a point in V_1 (either points from S or intersection points of lines) and a line segment in V_2 iff this point is one of the ends of the line segment.

(Note that G is a planar bipartite graph.)

STEP 2: Construct a graph G' by replacing each vertex in G by a corresponding matchgate as follows:

- each degree 2 vertex in V_1 is replaced by a generator matchgate G_2 with arity 2 (see Figure 4);
- each degree 3 vertex in V_1 is replaced by a generator matchgate G_3 with arity 3 (see Figure 2);
- each degree 4 vertex in V_1 (intersection point) is replaced by a generator matchgate G_4 with arity 4 (see Figure 3);
- each vertex in V_2 is replaced by a recognizer matchgate R with arity 2 (see Figure 5)

(Note that G' is a still a planar graph.)

STEP 3: Use the PKT algorithm to compute PerfMatch(G') and output the result.

Figures

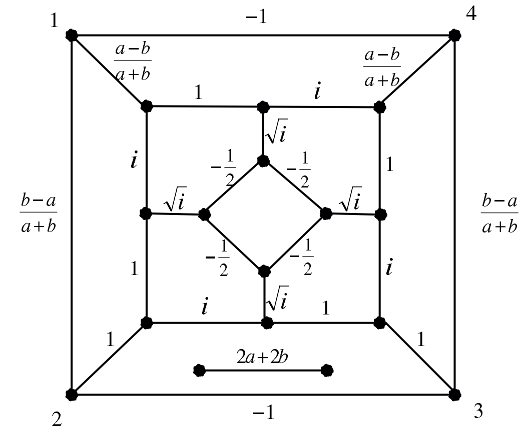

Figure 1: This planar matchgate has standard signature $(2a+2b, 0, 0, -2a+2b, 0, 2a-2b, -2a-2b, 0, 0, -2a-2b, 2a-2b, 0, -2a+2b, 0, 0, 2a+2b)^T$. Here $i = \sqrt{-1}$, and we assume $2a + 2b \neq 0$. (In case $2a + 2b = 0$, a similar matchgate will work.)

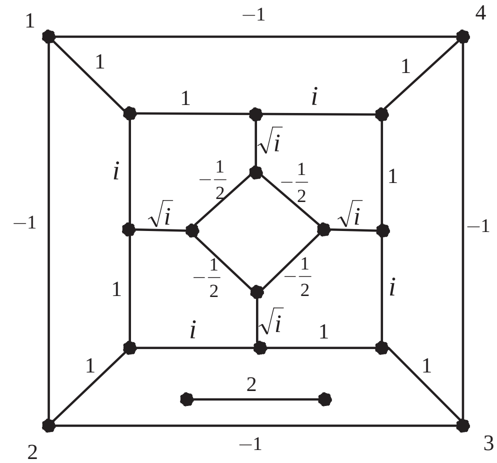

Figure 3: Under the basis **b2**, this generator matchgate has the signature G, where $G^{0101} = G^{1010} = 1$ and $G^{\alpha} = 0$ for other α. It makes sure that the color of the edge is transmitted at intersection points while only allowing different colored edges to meet at these intersection points.

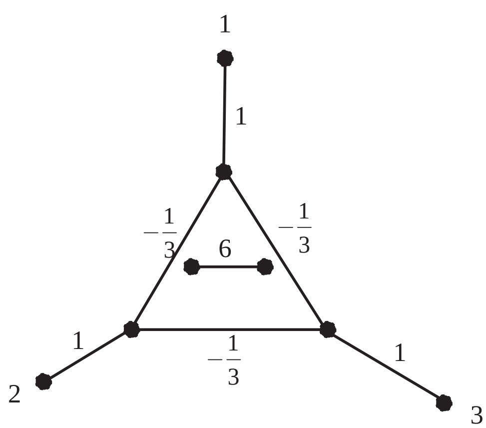

Figure 2: Under basis **b2**, this generator matchgate has the signature $(0, 1, 1, 1, 1, 1, 1, 0)^T$. It makes sure that the three incident edges of every degree 3 point in S are not monochromatic.

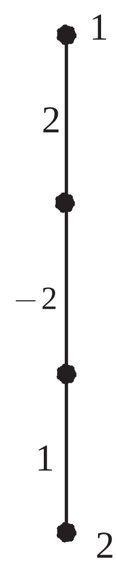

Figure 4: Under the basis **b2**, this generator matchgate has the signature $(0, 1, 1, 0)^T$. It makes sure that the two incident edges of every degree 2 point in S have different colors.

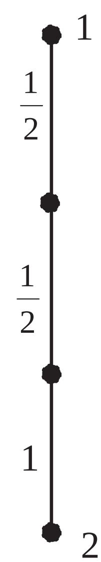

Figure 5: Under the basis **b2**, this recognizer matchgate has the signature $(1, 0, 0, 1)$. It makes sure that each segment has a consist coloring.