Signature Theory in Holographic Algorithms

Jin-Yi Cai · Pinyan Lu

Abstract In the theory of holographic algorithms proposed by Valiant, computation is expressed and processed in terms of signatures. We substantially develop the signature theory in holographic algorithms. This theory is developed in terms of d-realizability and d-admissibility. For the class of 2-realizable signatures we prove a Birkhoff-type theorem which determines this class. It gives a complete structural understanding of the relationship between 2-realizability and 2-admissibility. This is followed by characterization theorems for 1-realizability and 1-admissibility. Finally, using this theory of general (i.e., unsymmetric) signatures we give additional counting problems solvable in polynomial time by holographic algorithms.

1 Introduction

It is generally conjectured that many combinatorial problems in the class NP or #P are not computable in polynomial time. The prevailing opinion is that these problems seem to require the accounting or processing of exponentially many potential solution fragments to the problem. However it is rather natural, and it should not cause any

J.-Y. Cai
Computer Sciences Department, University of Wisconsin, Madison, WI 53706, USA
e-mail: jyc@cs.wisc.edu

P. Lu (✉)
Microsoft Research Asia, Beijing 100190, China
e-mail: pinyanl@microsoft.com

surprise, that the answer to such a problem can in general be expressed as a suitable exponential sum.

Take for instance the canonical Boolean Satisfiability problem SAT. It is NP-complete, and 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 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 $b_1 b_2 b_3 \in \{0, 1\}^3$. Here $b_1 b_2 b_3$ 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 $b_1 b_2 \in \{0, 1\}^2$, to indicate that the fan-out value from x to C and C' must be consistent. In the language of holographic algorithms these R_C and G_x are called *signatures*. Now we can form the tensor product $\mathbf{R} = \bigotimes_C R_C$ 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 indices, 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 a moment reflection shows that 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. Basically, each tuple $(i_1, i_2, \ldots, i_e) \in \{0, 1\}^e$ assigns a value 0 or 1 to each connecting edge. 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 as it fans out to its two connecting clauses, and the truth assignment satisfies each clause; the product value is 0 otherwise.

Of course, this is not a big deal, as we just expressed something that can be computed in exponential time as an expression involving exponentially many terms. The power of holographic algorithms is to evaluate such an exponential sum in *polynomial time*, for a variety of combinatorial problems. This happens when suitable signatures are *realizable*. In particular, for #Pl-Rtw-Mon-3CNF this theory can evaluate the sum over the field $\mathbf{Z}_7$. This counts the number of satisfying assignments mod 7 for Φ. (It is known that counting mod 2 for #Pl-Rtw-Mon-3CNF is NP-hard.) Exactly which sum is computable in polynomial time by holographic algorithms brings us to the subject of *signature theory*.

This paper develops the signature theory of holographic algorithms for general signatures.

The theory of holographic algorithms was initiated by Valiant [21]. It produces surprising algorithms by evaluating certain exponential sums in polynomial time [1, 4, 21, 22]. 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 [13, 14, 18] via the Holant Theorem. Unlike quantum algorithms, these give classical polynomial time algorithms. We give a brief review of definitions and background on holographic algorithms in Sect. 2. More details can be found in [1–3, 19–21].

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 the realizability problem. The requirements are specified by families 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.[1] Of course the big question is whether such "freak objects" exist for any of the NP-hard problems. If not, is there a coherent explanation? "Any proof of P ≠ NP may need to explain, and not only to imply, the unsolvability" [21] of NP-hard problems using this approach. Thus, the primary motivation for us is complexity theory.

In [4] we have developed an algebraic framework which gave a satisfactory theory of *symmetric signatures*. In this framework, we defined a basis manifold $\mathcal{M}$, and the signature theory is expressed in terms of d-admissibility and d-realizability, where d is the dimension of the algebraic variety of $\mathcal{M}$ corresponding to a desired signature. While *a priori* the tensor space can have basis vectors of arbitrary dimension, in [5] we have proved a general basis collapse theorem which effectively restricted the theory to the basis manifold $\mathcal{M}$ corresponding to $\mathbf{GL}_2$. Thus to Valiant's challenge what remains is the general (i.e., not necessarily symmetric) signature theory on $\mathcal{M}$.

We first prove a Birkhoff-type theorem which gives a complete and explicit characterization of the class of 2-realizable signatures (over char. 0). This turns out to be the vertices of a simplex, of which the linear span is precisely the class of 2-admissible signatures, whose dimension is the Catalan number. The 2-realizable signatures also have an explicit combinatorial interpretation in terms of planar tensor product of perfect matchings. In general the realizability of signatures is controlled by an exponential sized set of algebraic equations called Matchgate Identities (MGI), a.k.a. useful Grassmann-Plücker Identities [1, 3, 20]. The proof here uses MGI implicitly, in the form of explicit Pfaffian representations. Next we give characterization theorems concerning 1-realizability and 1-admissibility. The proof techniques are mainly algebraic. Finally we present some new algorithms using this general theory of signatures. The structural theory for general signatures developed here substantially move forward our understanding of the ultimate capabilities of holographic algorithms.

2 Some Background

In this section, for the convenience of readers, we review some definitions and results. More details can be found in [1–3, 19–21].

Let $G = (V, E, W)$, $G' = (V', E', W')$ be weighted undirected planar graphs. A *generator matchgate* Γ is a pair (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

---

[1]From [22]: "The objects enumerated are sets of polynomial systems such that the solvability of any one member would give a polynomial time algorithm for a specific problem. ... the situation with the P = NP question is not dissimilar to that of other unresolved enumerative conjectures in mathematics. The possibility that accidental or freak objects in the enumeration exist cannot be discounted, if the objects in the enumeration have not been systematically studied previously."

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 $\binom{n}{0}$. This tensor under the standard basis $\mathbf{b}$ has the form

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

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

where $\text{PerfMatch}(G - Z) = \sum_M \prod_{(i,j) \in M} w_{ij}$, is a sum over all perfect matchings M in $G - Z$, 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

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

where

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

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

According to general principle [10], $\mathbf{G}$ transforms contravariantly under a basis transformation $\boldsymbol{\beta}_j = \sum_i \mathbf{b}_i t_j^i$,

$$(G')^{i_1' i_2' \ldots i_n'} = \sum G^{i_1 i_2 \ldots i_n} \tilde{t}_{i_1}^{i_1'} \tilde{t}_{i_2}^{i_2'} \cdots \tilde{t}_{i_n}^{i_n'},$$

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

$$(R')_{i_1' i_2' \ldots i_n'} = \sum R_{i_1 i_2 \ldots i_n} t_{i_1'}^{i_1} t_{i_2'}^{i_2} \cdots t_{i_n'}^{i_n}.$$

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

Let $\mathbf{G} = \bigotimes_{i=1}^g \mathbf{G}(A_i)$ be the tensor product of all the generator signatures, and let $\mathbf{R} = \bigotimes_{j=1}^r \mathbf{R}(B_j)$ be the tensor product of all the recognizer signatures. Then $\text{Holant}(\Omega)$ is defined to be the contraction of the two product tensors, under some basis $\boldsymbol{\beta}$, where the corresponding indices match up according to the f connecting edges C_k.

The remarkable Holant Theorem is

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

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

The FKT algorithm can compute the perfect matching polynomial PerfMatch(G) for a planar graph in polynomial time.

We illustrate these concepts by the following example. The problem can be solved by a holographic algorithm in polynomial time [21].

#PL-3-NAE-ICE
INPUT: A planar regular graph $G = (V, E)$ of degree 3.
OUTPUT: The number of orientations such that no node has all the edges directed towards it or all the edges directed away from it.

To solve this problem by a holographic algorithm, we design a matchgrid as follows: We represent each node of degree 3 in V by a recognizer matchgate with signature $(G^{b_1 b_2 b_3}) = (0, 1, 1, 1, 1, 1, 1, 0)$. This represents a NOT-ALL-EQUAL or NAE gate on 3 bits. For each edge in E we use a generator matchgate with signature $(0, 1, 1, 0)^{\mathrm{T}}$, which stands for an orientation from either one of the two nodes to the other one. Note that $(G^{b_1 b_2 b_3}) = (0, 1, 1, 1, 1, 1, 1, 0)$ has non-zero entries G^{001} as well as G^{011}, where the index bit patterns 001 and 011 are odd and even respectively. This implies that there is no matchgate that has this G as its standard signature. This is a property implied by perfect matching. However, under the basis transformation by $\left[\left(\begin{smallmatrix}1\\1\end{smallmatrix}\right), \left(\begin{smallmatrix}1\\-1\end{smallmatrix}\right)\right]$, both generator and recognizer signatures can be transformed to standard signatures realizable by suitable planar matchgates.

To complete the construction of the matchgrid, we connect the external nodes of these matchgates by an edge of weight 1, in a one-to-one fashion according to the given planar graph G.

Now consider the exponential sum evaluated in the definition of Holant under this basis. Each term in the sum is a product of 0's and 1's which are appropriate entries of the signatures of the matchgates in the matchgrid. Each term is indexed by a 0-1 assignment on all connecting edges between external nodes of these matchgates. Then it is not hard to see, when this exponential sum is evaluated, each term is 0 or 1, and it is 1 iff it corresponds to an orientation of every edge such that at each vertex the local NOT-ALL-EQUAL constraint is satisfied. Thus, the value of Holant is precisely the number of valid orientations required by #PL-3-NAE-ICE. While Holant expresses the solution for #PL-3-NAE-ICE, by the Holant Theorem, we compute this sum by the FKT algorithm in polynomial time.

The following simple Proposition 4.3 of [21] is due to Valiant.

Proposition 2.1 (Valiant [21]) *If there is a generator (recognizer) with certain signature for size one basis $\{(n_0, n_1), (p_0, p_1)\}$ then there is a generator (recognizer) with the same signature for size one basis $\{(xn_0, yn_1), (xp_0, yp_1)\}$ or $\{(xn_1, yn_0), (xp_1, yp_0)\}$ for any $x, y \in \mathbf{F}$ and $xy \neq 0$.*

This leads to the following definition of an equivalence relation:

Definition 2.1 Two bases $\boldsymbol{\beta} = [n, p] = \left[\binom{n_0}{n_1}, \binom{p_0}{p_1}\right]$ and $\boldsymbol{\beta}' = [n', p'] = \left[\binom{n'_0}{n'_1}, \binom{p'_0}{p'_1}\right]$ are equivalent, denoted by $\boldsymbol{\beta} \sim \boldsymbol{\beta}'$, iff there exist $x, y \in \mathbf{F}^*$ such that $n'_0 = xn_0, p'_0 = xp_0, n'_1 = yn_1, p'_1 = yp_1$ or $n'_0 = xn_1, p'_0 = xp_1, n'_1 = yn_0, p'_1 = yp_0$.

Theorem 2.2 $\mathrm{GL}_2(\mathbf{F})/\sim$ *is a two dimensional manifold* (*for* $\mathbf{F} = \mathbf{C}$ *or* $\mathbf{R}$).

We call this the *basis manifold* $\mathcal{M}$. For $\mathbf{F} = \mathbf{R}$, it can be shown that topologically $\mathcal{M}$ is a Möbius strip. From now on we identify a basis $\boldsymbol{\beta}$ with its equivalence class containing it. When it is permissible, we use the dehomogenized coordinates $\left(\begin{smallmatrix} 1 & x \\ 1 & y \end{smallmatrix}\right)$ to represent a point (i.e., a basis class) in $\mathcal{M}$.

Under a basis transformation $G' = \left(\begin{smallmatrix} 1 & x \\ 1 & y \end{smallmatrix}\right)^{\otimes n} G$, the entry indexed by T

$$G'^T = \left\langle \bigotimes_{\sigma=1}^{n} [1, x_{[\sigma \in T]}], G \right\rangle = \sum_{\substack{0 \le i \le n - |T| \\ 0 \le j \le |T|}} x^i y^j \sum_{\substack{A \subset T^c, |A| = i \\ B \subset T, |B| = j}} G^{A \cup B}, \tag{1}$$

where T is a subset of $[n]$, and used as an index in G'^T, i.e., T is identified with a 0-1 bit pattern of length n, and where we write $x_0 = x$ and $x_1 = y$.

In this paper we will assume the field $\mathbf{F} = \mathbf{C}$ and develop the theory exclusively on the complex numbers.

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, 20]: 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 of 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:

$$\sum_{i=1}^{l} (-1)^i \underline{G}^{\alpha + e_{p_i}} \underline{G}^{\alpha + p + e_{p_i}} = 0. \tag{2}$$

More symmetrically, let $\alpha, \beta \in \{0, 1\}^m$ be any patterns, and let $P = \{p_i\} = \alpha + \beta$, $i \in [l]$, be their bitwise XOR as a position vector. Then

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

We note that for each MGI, the sum of the weights of indices for every term in $\underline{G}^{\alpha + e_{p_i}} \underline{G}^{\beta + e_{p_i}}$ is the same.

By the FKT algorithm, perfect matchings for a planar graph (and its subgraphs with some external nodes removed) can be expressed as the Pfaffian (and sub-Pfaffians) of a skew symmetric matrix. The MGI being necessary conditions for the

standard signatures is due to the algebraic identities called Grassmann-Plücker Identities that the sub-Pfaffians of any skew symmetric matrix must satisfy. The fact that together with the parity requirements they are also sufficient is derived from a non-trivial sequence of steps and constructions. See [1, 3, 20] for more details.

In view of these conditions, we have the following definitions:

Definition 2.2 A tensor G is *admissible* as a generator on a basis $\boldsymbol{\beta}$ iff $G' = \boldsymbol{\beta}^{\otimes n} G$ satisfies the *parity requirements*. It is called *realizable* as a generator on a basis $\boldsymbol{\beta}$ iff $G' = \boldsymbol{\beta}^{\otimes n} G$ satisfies both the *parity requirements* and all the *MGI*. This is equivalent to G' being the standard signature of some planar matchgate (see [1, 3] for this equivalence).

Definition 2.3 Let $B_{gen}(G)$ (resp. $B_{gen}^p(G)$) be the set of all possible bases in $\mathcal{M}$ for which a generator G is realizable (resp. admissible).

Definition 2.4 A generator G is called d-realizable (resp. d-admissible) for an integer $d \geq 0$ iff $B_{gen}(G) \subset \mathcal{M}$ (resp. $B_{gen}^p(G) \subset \mathcal{M}$) is a (non-empty) algebraic subset of dimension at least d.

To be d-admissible is to have a d-dimensional solution subvariety in $\mathcal{M}$, satisfying all the parity requirements. This is part of the requirements in order to be realizable. To be d-realizable is to have a d-dimensional solution subvariety in $\mathcal{M}$ for all realizability requirements, which include the parity requirements as well as the requirements of MGI. To have 0-realizability is a necessary condition. But to get holographic algorithms one needs simultaneous realizability of both generators and recognizers. This is accomplished by having a non-empty intersection of the respective subvarieties for the realizability of generators and recognizers. And this tends to be accomplished by having d-realizability (which implies d-admissibility), for $d \geq 1$, on at least one side. Therefore it is important to investigate d-realizability and d-admissibility for $d \geq 1$.

3 Preliminary Results on Realizability

We recall and state some preliminary results on realizability and admissibility. In our STOC 07 paper [4], only Theorem 3.1 was proved in the proceedings. Some other results were briefly stated without proof. Here we include some other proofs.

The first theorem is a complete characterization of 2-admissibility.

Theorem 3.1 *G is 2-admissible iff* (1) *$n = 2k$ is even;* (2) *all $G^S = 0$ except for* $|S| = k$; *and* (3) *for all $T \subset [n]$ with $|T| = k + 1$,*

$$\sum_{S \subset T, |S| = k} G^S = 0. \qquad (4)$$

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

The theorem still holds when we replace condition (3) with the following condition:

$(3)'$ for all $T \subset [n]$ with $|T| = k - 1$,

$$\sum_{S \supset T, |S| = k} G^S = 0. \tag{5}$$

We will use both versions in this paper.

We have some more results on 2-admissibility. Most of the proofs and some theorem statements were not included in [4] due to space limit. So we include both theorems and proofs here.

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

Theorem 3.2 *If G is 2-admissible with arity $2k$, then $\forall \beta = \begin{pmatrix} n_0 & p_0 \\ n_1 & p_1 \end{pmatrix} \in \mathcal{M}, \beta^{\otimes 2k} G = (n_0 p_1 - n_1 p_0)^k G$.*

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

Lemma 3.1 *Let G be 2-admissible with arity $2k$, $S \subset [2k]$ with $|S| = k$, and $A \subset S^c$. Then*

$$\sum_{B \subset S \text{ and } |B| = k - |A|} G^{A \cup B} = (-1)^{|A|} G^S$$

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

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

Inductively we assume the lemma has been proved for all $|A| \leq i - 1$, for some $i \geq 1$. Let $|A| = i > 0$. Since G is 2-admissible, we have

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

Then

$$0 = \sum_{C \subset A \cup S \text{ and } |C| = k} G^C$$

$$= \sum_{B \subset S \text{ and } |B| = k - |A|} G^{A \cup B} + \sum_{t=0}^{|A|-1} \sum_{A_1 \subset A, |A_1| = t} \sum_{B \subset S, |B| = k - |A_1|} G^{A_1 \cup B},$$

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

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

So

$$0 = \sum_{B \subset S \text{ and } |B|=k-|A|} G^{A \cup B} + G^S \sum_{t=0}^{|A|-1} (-1)^t \binom{|A|}{t}$$

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

From the last equation, we have

$$\sum_{B \subset S \text{ and } |B|=k-|A|} G^{A \cup B} = (-1)^{|A|} G^S$$

This completes the proof.   □

From this lemma, we have the following corollary which is also useful.

Corollary 3.1 *If G is any 2-admissible signature, then $\forall S \subset [2k]$, $G^S = (-1)^k G^{S^c}$.*

Now we can prove Theorem 3.2.

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

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

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

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

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

By Lemma 3.1 and for $A \subset S^c, |A| = i$, we have

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

So

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

$$= G^S \sum_{0 \leq i \leq k} x^i y^{k-i} (-1)^i \binom{k}{i} = (y - x)^k G^S.$$

This completes the proof. □

Since a scaling preserves realizability, the theorem gives:

Corollary 3.2 *If a 2-admissible G is realizable on some basis (e.g., on the standard basis), then it is realizable on any basis, which means it is 2-realizable.*

We also have the following operator, which is a useful language in the characterization of 2-realizability.

Definition 3.1 Let $\text{Rot}_r(G)$ be the tensor obtained by circularly rotating clockwise the coordinates of G by r bit positions, i.e., $[\text{Rot}_r(G)]^{i_1,i_2,...,i_n} = G^{i_{r+1},i_{r+2},...,i_n,i_1,...,i_r}$, where n is the arity of G. Let $G \otimes G'$ be the tensor product with all indices of G before all indices of G'. A planar tensor product is a finite sequence of operations of $\text{Rot}_r(G)$ and $G \otimes G'$.

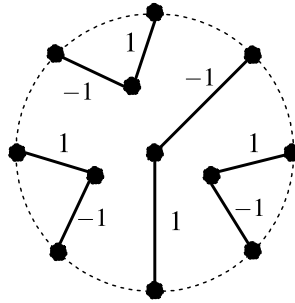This operator has the following nice property.

Theorem 3.3 $B_{gen}(\text{Rot}_r(G)) = B_{gen}(G)$ *and, for G_1 and G_2 not identically zero,* $B_{gen}(G_1 \otimes G_2) = B_{gen}(G_1) \cap B_{gen}(G_2)$. *Thus a planar tensor product preserves* B_{gen}. *In particular, any planar tensor product of 2-realizable signatures is also 2-realizable.*

Proof We first prove $B_{gen}(\text{Rot}_r(G)) = B_{gen}(G)$. Let G be a signature of arity n and let $T \in B_{gen}(G)$, then $\underline{G} = T^{\otimes n}G$ is realized as the standard signature of a matchgate Γ. $\text{Rot}_r(\underline{G})$ is realized by the same matchgate, but with the labels of its external nodes circularly rotated by r bit positions from Γ. By definition, $T^{\otimes n}\text{Rot}_r(G) = \text{Rot}_r(T^{\otimes n}G)$, since cyclically rotating the n copies of T in the tensor product $T^{\otimes n}$ keeps it invariant. Hence $B_{gen}(G) \subseteq B_{gen}(\text{Rot}_r(G))$. The reverse direction also follows since $\text{Rot}_r(\cdot)$ has an inverse $\text{Rot}_{-r}(\cdot)$.

Next we prove $B_{gen}(G_1 \otimes G_2) = B_{gen}(G_1) \cap B_{gen}(G_2)$. Suppose $T \in B_{gen}(G_1) \cap B_{gen}(G_2)$, where G_1 and G_2 have arities n_1 and n_2 respectively. Then both $T^{\otimes n_1}G_1$ and $T^{\otimes n_2}G_2$ are realizable by matchgates Γ_1 and Γ_2 respectively. It follows that $T^{\otimes(n_1+n_2)}(G_1 \otimes G_2) = T^{\otimes n_1}G_1 \otimes T^{\otimes n_2}G_2$ is realizable by a matchgate which is just putting Γ_1 and Γ_2 together as a disjoint union. Therefore $T \in B_{gen}(G_1 \otimes G_2)$.

For the other direction, let $T \in B_{gen}(G_1 \otimes G_2)$. Then $T^{\otimes(n_1+n_2)}(G_1 \otimes G_2) = T^{\otimes n_1}G_1 \otimes T^{\otimes n_2}G_2$ is realizable by some matchgate Γ of arity $n_1 + n_2$. Since G_2 is not identically zero, and T is invertible, there exists a bit pattern $i_1 i_2 \ldots i_{n_2}$ such that $c = (T^{\otimes n_2}G_2)^{i_1 i_2 \ldots i_{n_2}} \neq 0$. Now we modify Γ to Γ' as follows: We view the first n_1 external nodes of Γ as external nodes in Γ'. All other nodes of Γ are now considered internal nodes of Γ'. For any $1 \leq j \leq n_2$, if $i_j = 1$ in the bit pattern, then append an extra new edge to the $(n_1 + j)$-th external node of Γ. This new edge has weight 1 and the newly added vertex is also considered an internal node of Γ'. Finally add an isolated extra new edge with weight $1/c$. Then clearly the standard signature of Γ' is $\Gamma'^{j_1 j_2 \ldots j_{n_1}} = \frac{1}{c}\Gamma^{j_1 j_2 \ldots j_{n_1} i_1 i_2 \ldots i_{n_2}} = (T^{\otimes n_1}G_1)^{j_1 j_2 \ldots j_{n_1}}$. Therefore $T \in B_{gen}(G_1)$. Similarly we can prove $T \in B_{gen}(G_2)$ as well. So $T \in B_{gen}(G_1) \cap B_{gen}(G_2)$. □

4 Characterization of 2-Realizability

In [4] we have developed an algebraic framework for the signature theory. In Sect. 3 we give a summary of these results. The theory is developed in terms of d-admissibility and d-realizability. The key to the success of a holographic algorithm is to find generators and recognizers whose signatures we desire and whose realizability varieties intersect. This typically happens with at least one side having a d-realizability for $d \geq 1$. Of course 2-realizability is the most desirable. The central results from [4] in this regard are characterizations of 2-admissible signatures. The arity of any 2-admissible signature must be an even number $n = 2k$. The 2-admissible signatures are the solutions to a homogeneous linear equation system. The dimension of the solution space is $\frac{1}{k+1}\binom{2k}{k}$, the Catalan number. In this section, $n = 2k$ will always refer to the arity.

It turns out that there is a particular set of solutions with a clear combinatorial meaning. These are signatures of planar matchgates with k pairs of points on the circumference of a unit disk D, constructed by planar tensor product.

Let P be the basic matchgate consisting of a path of length 2, where we place the two end points on the circumference of D, and the two edges are weighted $+1$ and -1 respectively. This gives a planar matchgate of arity 2 with the (standard) signature $(0, +1, -1, 0)$. It is easy to verify that this signature is indeed 2-realizable. Now we can form planar tensor product recursively using disjoint copies of P as the basic building block. Theorem 3.3 tells us that the planar matchgate formed is also 2-realizable. Combinatorially this process is very simple: We end up with $2k$ vertices on the circumference of D, which are pair-wise matched up by k disjoint paths each with weights $+1$ and -1 on its two edges, respectively. The union of these k disjoint paths form a planar graph with a total of $3k$ vertices (planar tensor product preserves planarity, and these k paths do not cross each other). This family of matchgates with $2k$ external nodes is denoted by $\mathcal{D}_{2k}$. See Fig. 1.

Let $G \in \mathcal{D}_{2k}$, and let $(G^S)_{S \subset [2k]}$ be its signature. We show that (G^S) satisfies Theorem 3.1 to be 2-admissible. First note that each entry G^S is 0, except when S contains exactly one end point from each P. This follows from the definition of perfect matching. In particular $G^S \neq 0$ only for $|S| = k$. Now we show that $\sum_{S \subset T} G^S = 0$, for any subset $T \subset [2k]$ of cardinality $k + 1$. Since $|T| = k + 1$, there must be at least one pair $\{i, j\} \subset T$, where i and j are connected by some P of length 3 in G. Then the only *possible* non-zero terms in $\sum_{S \subset T} G^S$ come from $S = T - \{i\}$ and $S = T - \{j\}$.

In order to be actually non-zero, the set $T - \{i, j\}$ must contain exactly one vertex from each pair of the other $k - 1$ pairs of external nodes connected by length-3 paths. Thus either every term in $\sum_{S \subset T} G^S$ is zero, or there are exactly two non-zero terms of opposite values ± 1. Thus, $\sum_{S \subset T} G^S = 0$ for all $|T| = k + 1$.

This proof gives an explicit set of solutions to the system in Theorem 3.1. The cardinality of this set is the Catalan number $\frac{1}{k+1}\binom{2k}{k}$, which is the dimension of the solution subspace, a fact we know separately from the exact knowledge of the rank of the system (rank estimates related to the *Kneser Graph* $KG_{2k+1,k}$ [8, 9, 11, 12, 15–17]). If we order the entries of the signature G^S lexicographically by its index $S \subset [2k]$, the first non-zero entry (with value $+1$) occurs at the location where for each matched pair $i < j$ by a path P we assign 0 to the i-th bit and 1 to the j-th bit. This corresponds to a balanced parenthesized expression (BPE), i.e., a sequence of length $2k$ consisting of k 0's and k 1's, and any prefix has at least as many 0's as 1's (write 0 for "(" and 1 for ")"). This mapping from $\mathcal{D}_{2k}$ to BPE of length $2k$ is also reversible. By considering the submatrix whose rows are these $\frac{1}{k+1}\binom{2k}{k}$ signatures from $\mathcal{D}_{2k}$ and whose columns are indexed by BPE, it follows that these signatures are linearly independent. At this point the class of 2-admissible signatures is completely understood. They form the linear span of the signatures from $\mathcal{D}_{2k}$.

Theorem 4.1 *The set of $\frac{1}{k+1}\binom{2k}{k}$ signatures from $\mathcal{D}_{2k}$ are 2-realizable, and forms a basis of the solution space of the set of all 2-admissible signatures of arity $2k$.*
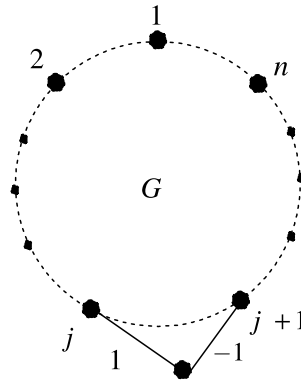
Our main theorem in this section is to prove that the signatures from $\mathcal{D}_{2k}$ are precisely the class of 2-realizable signatures of arity $2k$ (over char. 0), after a scaling factor.

Theorem 4.2 *Up to a scalar factor, every 2-realizable signature is obtainable as a planar tensor product from $(0, 1, -1, 0)$. For arity $2k$, this is precisely the set of $\frac{1}{k+1}\binom{2k}{k}$ signatures from $\mathcal{D}_{2k}$.*

Proof Outline: Since the proof of Theorem 4.2 is quite involved, we first give an outline. At the top level, the theorem is proved by an induction on the arity. Given a 2-realizable signature, we show that in a certain planar matchgate of this signature, there exist two contiguous nodes $(i, i + 1)$, which are isolated from the rest. The part on $(i, i + 1)$ makes one copy of $(0, 1, -1, 0)$. Then we can apply induction on the remaining part.

However the proof for the existence of such two contiguous nodes is complicated. We first prove this under the condition that $G^{0101\cdots 01} \neq 0$. If this is true, by flipping all odd bits, we can define a new signature G_A which has the property that $G_A^{1111\cdots 11} \neq 0$. Then, from the general theory [1, 3], we know that G_A can be realized by Pfaffians of a (weighted, but not necessarily planar) graph Γ *without* internal nodes. This transformation is a key idea of this proof and through which we bypass the difficulty of having to deal with exponentially many MGI explicitly. After that we deal with edge weights of the graph Γ rather than the entries of G. This reduces the number of variables from 2^n to $\binom{n}{2}$, and the explicit form of Pfaffian satisfies all MGI implicitly. We translate the conditions of G being 2-admissible to conditions on G_A. Then we apply

these conditions on the edge weights in Γ and prove that there is one isolated edge connecting two contiguous nodes. These are proved in Lemmas 4.4 and 4.5.

Then all we need to prove is that $G^{0101\cdots01} \neq 0$ (Lemma 4.3). This turns out to be at least as difficult as Lemmas 4.4 and 4.5. We prove Lemma 4.3 by an induction (a nested induction on k and then on i). First we introduce *derivative operators* ∂_j which construct 2-realizable signatures of arity $n-2$ from a 2-realizable signature of arity n. After a normalization, we use the operator and the inductive hypothesis (of the outer induction on k) to prove that at least one of the two values $G^{0101\cdots01}$, $G^{1001\cdots01}$ is non-zero. Then we prove (by the inner induction on i) that the case $G^{0101\cdots01} = 0$, $G^{1001\cdots01} \neq 0$ leads to a contradiction. This proof also uses the method of explicit Pfaffian representation.

Now we proceed to the proof, which is presented in the reverse order of the above outline.

Lemma 4.1 *Let G be a 2-realizable signature with arity $n = 2k$ and $j \in [n]$. We define a tensor $\partial_j G$ with arity $n-2$ as follows*:

$$(\partial_j G)^{i_1 i_2 \cdots i_{n-2}} = G^{i_1 i_2 \cdots i_{j-1} 01 i_j i_{j+1} \cdots i_{n-2}} - G^{i_1 i_2 \cdots i_{j-1} 10 i_j i_{j+1} \cdots i_{n-2}}. \tag{6}$$

Then $\partial_j G$ is also 2-realizable.

The above expression technically assumes $1 \leq j \leq n-1$. For $j = n$, the two bits with 01 and 10 should occur at bit positions n and 1 respectively. In general realizable signatures should be viewed as having been realized by a planar matchgate whose indices are viewed cyclically.

Proof If G is 2-realizable, then it is realizable as a standard signature. By Fig. 2, it is clear that $\partial_j G$ is also realizable as a standard signature, for all $j \in [n]$. Then, according to Corollary 3.2, we only need to prove that $\partial_j G$ is 2-admissible.

For notational convenience, we assume $j = n - 1$. If $\mathrm{wt}(i_1 i_2 \cdots i_{n-2}) \neq k - 1$, then $\mathrm{wt}(i_1 i_2 \cdots i_{n-2} 01) = \mathrm{wt}(i_1 i_2 \cdots i_{n-2} 10) \neq k$. So by (6), we have $(\partial_{n-1} G)^{i_1 i_2 \cdots i_{n-2}} = 0$.

Now for any $T \subset [n-2]$ and $|T| = k$, we have

$$\sum_{S \subset T, |S|=k-1} (\partial_{n-1} G)^S = \sum_{S \subset T, |S|=k-1} (G^{S \cup \{n\}} - G^{S \cup \{n-1\}})$$

$$= \left(G^T + \sum_{S \subset T, |S|=k-1} G^{S \cup \{n\}} \right)$$

$$- \left(G^T + \sum_{S \subset T, |S|=k-1} G^{S \cup \{n-1\}} \right)$$

$$= \sum_{S' \subset T \cup \{n\}, |S'|=k} G^{S'} - \sum_{S' \subset T \cup \{n-1\}, |S'|=k} G^{S'}$$

$$= 0 - 0 = 0.$$

Therefore we know that $\partial_{n-1} G$ is 2-admissible by Theorem 3.1. The same proof works for all $\partial_j G$.   □

Let G be a non-trivial 2-realizable signature. Consider any $A \subset [n]$ where $|A| = n/2$. We can define a new signature G_A by $G_A^S = G^{A \oplus S}$, for all $S \subset [n]$, where $A \oplus S$ denotes the symmetric difference. The conditions in Theorem 3.1 for G to be 2-admissible translate to the following conditions for G_A:

Lemma 4.2 *G is* 2-*admissible if and only if the following conditions are satisfied*: (1) *All* $G_A^S = 0$ *except for those S which satisfy* $|S \cap A| = |S \cap A^c|$. (2) *For all* $T_1 \subset A^c$, $T_2 \subset A$ *with* $|T_1| = |T_2| + 1$,

$$\sum_{S \subset T_1, |S|=|T_1|-1} G_A^{S \cup T_2} + \sum_{T_2 \subset S \subset A, |S|=|T_2|+1} G_A^{T_1 \cup S} = 0. \tag{7}$$

The second condition, as stated in (7), *but for all* $T_1 \subset A$, $T_2 \subset A^c$ *with* $|T_1| = |T_2| + 1$, *together with the first condition, also remain necessary and sufficient for G being* 2-*admissible.*

This equation (7) should be remembered as follows: Start with any two sets $T_1 \subset A^c$ and $T_2 \subset A$, (or respectively any two sets $T_1 \subset A$ and $T_2 \subset A^c$) where the cardinality differs by exactly one, $|T_1| = |T_2| + 1$. Then the sum of G_A^X in (7) is over all subsets X, where X is obtained from $T_1 \cup T_2$ by either "shrinking" from T_1 or "growing" from T_2 within A (or respectively within A^c) by one point.

To see that Theorem 3.1 and Lemma 4.2 are equivalent, we observe the following: as $|A| = n/2$ and $|A| = |A \cap S| + |A \cap S^c|$, it follows that $|A \oplus S| = |A^c \cap S| + |A \cap S^c| = n/2$ iff $|A \cap S| = |A^c \cap S|$. For (7), write a general T of cardinality $|T| = k + 1$ as $T = (T \cap A^c) \cup (T \cap A)$, and let $T_1 = T \cap A^c$, $T_2 = T^c \cap A = A - (T \cap A)$. Then $|T_1| = |T_2| + 1$. So the sum $\sum_{S \subset T, |S|=k} G^S$ in Theorem 3.1 is precisely over those S obtained from T by taking one point off from T_1 or from $T \cap A$. In terms of $\sum_S G_A^S$,

this is precisely over those obtained from T by taking one point off from T_1 or adding one point of A to T_2.

The statement when A is exchanged with A^c, i.e., $T_1 \subset A$ and $T_2 \subset A^c$, $|T_1| = |T_2| + 1$, is proved equivalent to 2-admissibility of G by invoking Theorem 3.1 with (5) in its condition (3)′.

Now suppose we have some A, where $|A| = n/2$, and $G_A^{11\cdots1} = 1$. From (a) the equivalence theorem between planar matchgate signatures and general matchgate characters and (b) the realizability theorem of general matchgate characters [1, 3], a planar matchgate signature can be realized by the Pfaffians of various submatrices of the skew-symmetric matrix of a weighted graph Γ. This graph Γ is not necessarily planar, but under the condition that $G_A^{11\cdots1} = 1$, the graph Γ can be chosen to contain no internal nodes, and for every $S \subset [n]$, the entry G_A^S is equal to the Pfaffian of the skew-symmetric matrix of Γ after removing all rows and columns corresponding to S. In our case, Γ has $2k$ nodes $\{1, 2, \ldots, 2k\}$, and we use $x_{i,j}$ to denote the weight of the edge $\{i, j\}$ for all $i, j \in [2k]$. We also write $x_{j,i} = x_{i,j}$. (In the skew-symmetric matrix, for $i < j$, the entry at (i, j) is $x_{i,j}$ and at (j, i) is $-x_{i,j}$.)

Assuming $G_A^{11\cdots1} = 1$, from Lemma 4.2 we have $x_{i,j} = 0$ when i, j are both in A or both in A^c. Now we use (7) to obtain more conditions on $x_{i,j}$'s.

For any $i \in A$, using $T_1 = A^c$ and $T_2 = A - \{i\}$ in Lemma 4.2 we get,

$$\sum_{j \in A^c} x_{i,j} = -1. \tag{8}$$

Here the term -1 comes from $-G_A^{11\cdots1}$, obtained from "growing" T_2 at i, and the term $x_{i,j} = G_A^{[n]-\{i,j\}}$ is obtained from "shrinking" T_1 at j.

Similarly, by taking $T_1 = A$ and $T_2 = A^c - \{i\}$, we have for any $i \in A^c$,

$$\sum_{j \in A} x_{i,j} = -1. \tag{9}$$

Lemma 4.3 *Let G be a non-trivial 2-realizable signature. Then $G^{0101\cdots01} \neq 0$.*

Proof Let $n = 2k$ be the arity of a non-trivial 2-realizable signature. We will prove this lemma by a double induction. The outer induction is on k.

The case $k = 1$ is easy: we have $G^{01} + G^{10} = \sum_{S \subset \{1,2\}, |S|=1} G^S = 0$. Being non-trivial, and the only non-zero entries are at half weight, we must have both $G^{01}, G^{10} \neq 0$.

Inductively we assume the lemma has been proved for all $n' \leq 2(k-1)$, for some $k \geq 2$. Let G be a 2-realizable signature with arity $2k$. From Lemma 4.1, we know that for all $i \in [n]$, $\partial_i G$ is a 2-realizable signature with arity $2(k-1)$. If all $\partial_i G$ are trivial, for $i \in [n]$, then G is symmetric. It follows that for any $|S| = k$, if we pick any $t \notin S$, and let $T = S \cup \{t\}$, then $G^S = \frac{1}{k+1} \sum_{S' \subset T, |S'|=k} G^{S'} = 0$. Thus G is trivial as well. Since we assumed G is non-trivial, we have some $j \in [n]$, such that $\partial_j G$ is non-trivial. For notational simplicity we assume $j = 1$, after a cyclic permutation of the indices. By induction, we have $(\partial_1 G)^{0101\cdots01} \neq 0$. By definition, we have $(\partial_1 G)^{0101\cdots01} = G^{0101\cdots01} - G^{1001\cdots01}$. We assume for a contradiction that $G^{0101\cdots01} = 0$, then $G^{1001\cdots01} = -(\partial_1 G)^{0101\cdots01} \neq 0$.

Let $A = \{2, 3, 5, \ldots, 2k-1\}$, we have $G_A^{1111\cdots1} = G^{1001\cdots01} \neq 0$. By a scaling we can assume $G_A^{1111\cdots1} = 1$. Then we can define $x_{i,j}$ to give a Pfaffian representation to G_A^S as above. Note that $G_A^{[n]-\{i,j\}} = x_{i,j}$. The assumption $G^{0101\cdots01} = 0$ means that $x_{1,2} = G_A^{0011\cdots11} = 0$. Now we inductively prove (the inner induction on i):

Claim (Assume $G^{0101\cdots01} = 0$ and $G^{1001\cdots01} = 1$.) *For all* $i \geq 3$, $x_{1,i} = x_{2,i} = 0$.

The base case is $i = 3$. The case $x_{2,3} = 0$ is obvious, since both $2, 3 \in A$. Using $T_1 = A^c - \{1\}$ and $T_2 = A - \{2, 3\}$ in Lemma 4.2, we have

$$0 = x_{1,2} + x_{1,3} + \sum_{t \in A^c, t \neq 1} (x_{1,2}x_{t,3} - x_{1,3}x_{t,2} + x_{1,t}x_{2,3}) \tag{10}$$

$$= x_{1,3} - \sum_{t \in A^c, t \neq 1} x_{1,3}x_{2,t} \tag{11}$$

$$= x_{1,3} - x_{1,3}(-1 - x_{1,2}) \tag{12}$$

$$= 2x_{1,3}. \tag{13}$$

Here in (10) the first two terms stem from "growing" T_2 with 3 and 2 respectively, and the t-th term in the summation stems from "shrinking" t from T_1. This term is a 4×4 Pfaffian, where the signs record the parity of crossovers. In (11) we make use of $x_{1,2} = 0$ and $x_{2,3} = 0$. In (12) we use (8). It follows that $x_{1,3} = 0$.

Inductively (on i) we assume the **Claim** has been proved for all $[3, i-1]$ for some $i \geq 4$. There are two cases: i is even or odd.

If i is even, then $x_{1,i} = 0$ is obvious, since both $1, i \in A^c$. We assume for a contradiction that $x_{2,i} \neq 0$. Let $B = \{3, 5, \ldots, i-1\}$ and $C = \{4, 6, \ldots, i-2\}$ (note that $|B| = |C| + 1$). For any $j \in B$, using $T_1 = A^c - \{i\}$ and $T_2 = A - \{2, j\}$ in Lemma 4.2, we have

$$0 = x_{2,i} + x_{i,j} + \sum_{t \in C}(+x_{2,i}x_{j,t}) + \sum_{t \in A^c - (C \cup \{1, i\})}(-x_{2,i}x_{j,t})$$
$$+ \sum_{t \in A^c - (C \cup \{1, i\})}(+x_{2,t}x_{j,i}) \tag{14}$$

$$= x_{2,i} + x_{i,j} + x_{2,i}\left(1 + x_{i,j} + 2\sum_{t \in C}x_{j,t}\right) + x_{i,j}(-1 - x_{2,i}) \tag{15}$$

$$= 2x_{2,i}\left(1 + \sum_{t \in C}x_{j,t}\right). \tag{16}$$

Here in line (14) the first two terms come from growing T_2 with j and 2 respectively. The first sum comes from shrinking T_1 at $t \in C$; here we made use of $x_{t,i} = 0$ (since both $t, i \in A^c$), and inductively $x_{2,t} = 0$. The second and third sums in (14) come from shrinking T_1 at $t \in A^c$ where $t > i$. The signs take into account of crossovers. Note also that in (14) the Pfaffian term corresponding to shrinking T_1 at 1 does not

appear, because all product terms in this Pfaffian are 0 by inductive hypothesis. From (14) to (15) we combine the first two sums using (8), and also $x_{1,j} = 0$ for this $j \in B$ by induction. The third sum of (14) is also handled by (8), and also $x_{2,t} = 0$ for all $t \in C \cup \{1\}$, by induction.

As $x_{2,i} \neq 0$ by our assumption, we have for any $j \in B$, $\sum_{t \in C} x_{j,t} = -1$. Sum over all $j \in B$, we have

$$\sum_{j \in B} \sum_{t \in C} x_{j,t} = -|B|. \tag{17}$$

Now we fix any $j \in C$. Using $T_1 = A - \{2\}$ and $T_2 = A^c - \{i, j\}$ in Lemma 4.2, we have (with similar justifications, such as $x_{2,j} = 0$ by induction)

$$0 = x_{2,i} + x_{2,j} + \sum_{t \in B} x_{2,i} x_{t,j} - \sum_{t \in A - (B \cup \{2\})} x_{2,i} x_{t,j}$$

$$= x_{2,i} + x_{2,i} \left(1 + x_{j,2} + 2 \sum_{t \in B} x_{j,t} \right)$$

$$= 2x_{2,i} \left(1 + \sum_{t \in B} x_{j,t} \right).$$

Since $x_{2,i} \neq 0$ by assumption, we have for any $j \in C$, $\sum_{t \in B} x_{j,t} = -1$. Sum over all $j \in C$, we have

$$\sum_{j \in C} \sum_{t \in B} x_{j,t} = -|C|. \tag{18}$$

Together with (17) and (18), we have $|B| = |C|$. This is a contradiction. As a result, $x_{2,i} = 0$, completing the inner induction on i for i even.

If i is odd, then $x_{2,i} = 0$ is obvious, since both $2, i \in A$. Using $T_1 = A^c - \{1\}$ and $T_2 = A - \{2, i\}$ in Lemma 4.2, we have

$$0 = x_{1,i} + \sum_{t \in [4, i-1] \cap A^c} x_{1,i} x_{2,t} - \sum_{t \in A^c - [1, i-1]} x_{1,i} x_{2,t} \tag{19}$$

$$= x_{1,i} + 0 - x_{1,i}(-1) \tag{20}$$

$$= 2x_{1,i}. \tag{21}$$

Here the term 0 in (20) refers to the first summation in (19), since $x_{2,t} = 0$ for all $t \in [4, i - 1] \cap A^c$ by induction. This fact together with $x_{2,1} = 0$ are also used to "complete" the second sum in (19), and then we use (8) to get to (20).

So it follows that $x_{1,i} = 0$. This completes the induction on i and proves the **Claim**.

However, then the **Claim** gives $-1 = \sum_{j \in A} x_{1,j} = 0$. This contradiction completes the proof of the induction on k, except the remark about the cyclic permutation on the index.

To address the cyclic permutation on the index (when we assumed $\partial_1 G$ is nontrivial), we use Corollary 3.1 in the Appendix. Note that a cyclic permutation on the

bit pattern $0101\cdots 01$ is either itself or $1010\cdots 10$. Thus we have either $G^{0101\cdots 01} \neq 0$ or $G^{1010\cdots 10} \neq 0$. Corollary 3.1 says $G^{0101\cdots 01} = (-1)^k G^{1010\cdots 10}$. This completes the proof of Lemma 4.3.   □

From Lemma 4.3, we know $G^{0101\cdots 01} \neq 0$. Now for the remainder of this section we define $A = \{1, 3, 5, \ldots, 2k - 1\}$, we have $G_A^{11\cdots 1} \neq 0$. By a scaling factor we can assume $G_A^{11\cdots 1} = 1$. Similarly based on this A we can define a set of weights $x_{i,j}$ in a graph Γ, the Pfaffian minors of its skew-symmetric matrix define G_A, as explained earlier.

From Lemma 4.2, we have $x_{i,j} = G_A^{[n]-\{i,j\}} = 0$ when i, j have the same parity. Now we use (7) to obtain more information on $x_{i,j}$.

For any odd $i \in [2k]$, we can take $T_1 = A^c$ and $T_2 = A - \{i\}$ in Lemma 4.2 and get,

$$\sum_{j \in A^c} x_{i,j} = -1. \tag{22}$$

Similarly we have for any even $i \in [2k]$,

$$\sum_{j \in A} x_{i,j} = -1. \tag{23}$$

Lemma 4.4 *If G is non-trivial, then there exists $i \in [n - 1]$ such that $x_{i,i+1} \neq 0$.*

Proof We assume for a contradiction that for all $i \in [n - 1]$, $x_{i,i+1} = 0$. Under this assumption we prove that for all $i, j \in [n], i \neq j, x_{i,j} = 0$. (This would imply that G_A, and therefore G, is trivial, arriving at a contradiction.) If i, j have the same parity, we already know that this is true. Now we prove $x_{i,j} = 0$ by induction on $|i - j|$ and $|i - j|$ is odd.

The case $|i - j| = 1$ is the assumption.

Inductively we assume $x_{i,j} = 0$ has been proved for all $|i - j| \leq 2h - 1$, for some $h \geq 1$. Now $|i - j| = 2h + 1$. We assume $i < j$, i is odd and j is even, (so in fact $j \geq i + 3$). Other cases can be proved similarly. Using $T_1 = A - \{i\}$ and $T_2 = A^c - \{i + 1, j\}$ in Lemma 4.2, we have

$$0 = x_{i,i+1} + x_{i,j} + \sum_{t \in A, t \neq i} x_{i,i+1} x_{t,j} + \sum_{t \in [i+2, j-1] \cap A} x_{i,j} x_{t,i+1} - \sum_{t \in A-[i, j-1]} x_{i,j} x_{t,i+1}. \tag{24}$$

In this expression, the first two terms come from growing A^c at j and $i + 1$. The other three sums account for the Pfaffian term by shrinking t from A. The signs take into account of the parity of crossovers.

By assumption $x_{i,i+1} = 0$, the first sum is zero.

When $t \in [i + 2, j - 1]$, we have $|t - (i + 1)| \leq j - 1 - (i + 1) = 2h - 1$. So by induction the second sum is also zero.

We can use these two observations to "complete" the third sum, and then from (23) we get

$$\sum_{t \in A-[i, j-1]} x_{i,j} x_{i+1,t} = x_{i,j} \sum_{t \in A-[i, j-1]} x_{i+1,t} = x_{i,j} \sum_{t \in A} x_{i+1,t} = -x_{i,j}.$$

Back to (24), we have

$$0 = x_{i,j} - (-x_{i,j}) = 2x_{i,j}.$$

This completes the induction and also completes the proof.   □

By this Lemma 4.4, after a cyclic permutation, we may assume $x_{1,2} \neq 0$, for notational simplicity. Under this notation, we have the statements Lemma 4.5.

Lemma 4.5 *After a cyclic permutation, we may assume* $x_{1,2} \neq 0$. *Then, for all* $i \geq 3$, $x_{1,i} = x_{2,i} = 0$.

Proof We prove this by induction on i. For the case $i = 3$, $x_{1,3} = 0$ is obvious since they both belong to A. Using $T_1 = A^c - \{2\}$ and $T_2 = A - \{1, 3\}$ in Lemma 4.2, we have

$$0 = x_{1,2} + x_{2,3} + \sum_{t \in A^c, t \neq 2} x_{1,2}x_{3,t} + \sum_{t \in A^c, t \neq 2} x_{1,t}x_{3,2}$$

$$= x_{1,2} + x_{2,3} + x_{1,2}(-1 - x_{3,2}) + x_{3,2}(-1 - x_{1,2})$$

$$= -2x_{1,2}x_{3,2}.$$

Since $x_{1,2} \neq 0$, we have $x_{2,3} = 0$.

Inductively we assume the lemma has been proved for all $j \in [3, i-1]$ for some $i \geq 4$, i.e., $x_{1,j} = x_{2,j} = 0$. There are two cases: i is even or odd.

If i is even, then $x_{2,i} = 0$ is obvious. Using $T_1 = A - \{1\}$ and $T_2 = A^c - \{2, i\}$ in Lemma 4.2, we have

$$0 = x_{1,2} + x_{1,i} + \sum_{t \in A, t \neq 1} x_{1,2}x_{t,i} + \sum_{t \in [3,i-1] \cap A} x_{1,i}x_{t,2} - \sum_{t \in A - [1,i-1]} x_{1,i}x_{t,2}$$

$$= x_{1,2} + x_{1,i} + x_{1,2}(-1 - x_{1,i}) + 0 - x_{1,i}(-1 - x_{1,2})$$

$$= 2x_{1,i},$$

where we used inductive hypothesis $x_{2,t} = 0$ for all $t \in [3, i-1] \cap A$ to handle both the second and third sum. It follows that $x_{1,i} = 0$.

If i is odd, then $x_{1,i} = 0$ is obvious. Using $T_1 = A^c - \{2\}$ and $T_2 = A - \{1, i\}$ in Lemma 4.2, by a similar argument we have

$$0 = x_{1,2} + x_{2,i} + \sum_{t \in A^c, t \neq 2} x_{1,2}x_{i,t} - \sum_{t \in [4,i-1] \cap A^c} x_{2,i}x_{1,t} + \sum_{t \in A^c - [2,i-1]} x_{2,i}x_{1,t}$$

$$= x_{1,2} + x_{2,i} + x_{1,2}(-1 - x_{2,i}) - 0 + x_{2,i}(-1 - x_{1,2})$$

$$= -2x_{1,2}x_{2,i}.$$

Since $x_{1,2} \neq 0$, we have $x_{2,i} = 0$.

This completes the proof.   □

Proof of Theorem 4.2 We prove this theorem by induction on k.

The case $k = 1$ is obvious.

Inductively we assume the theorem has been proved for signatures with arity $2k - 2$ for some $k \geq 2$. Now G is a non-trivial 2-realizable signature with arity $2k$; by Lemma 4.3 we can define G_A as above, where $A = \{1, 3, \ldots, 2k - 1\}$. After a cyclic permutation we may assume the statement of Lemma 4.5 holds. Then by (22), we know $x_{1,2} = -1$. The edge $(1, 2)$ has no crossover with any other edge. We may apply the general method to transform characters (Pfaffians) to signatures of planar matchgates [1, 3]; but in this case, the two vertices 1 and 2 are isolated from the rest. We can then extend every odd node by a new edge of weight 1 to come from G_A back to G. The part of the two vertices 1 and 2, now consists of a path P of length three, remains isolated. P has three nodes $1', 1, 2$, and two edges $(1', 1), (1, 2)$, with weights $+1$ and -1 respectively. This part is exactly one copy of $(0, 1, -1, 0)$, and has no crossovers with the rest. It follows that G is a tensor product of $(0, 1, -1, 0)$ with some G' of arity $n - 2$ which is also 2-realizable. Induction now completes the proof.   □

5 1-Realizability

Section 4 gives a complete characterization of 2-realizable signatures. In this section, we study 1-realizable signatures. As discussed in Sect. 2, d-realizability for $d > 0$ is key to finding interesting holographic algorithms, since they result from a non-empty intersection of the signature varieties of both recognizers and generators. We present a structural characterization theorem for 1-realizable signatures. They are also restrictive, but they are much richer than 2-realizable signatures, and we will use them in the Sect. 7 to give polynomial time algorithms for some interesting new problems.

First we prove the following key lemma. This lemma plays an important role in the proof of Theorem 5.1. Moreover, this lemma reveals a key property of the set $B^p_{gen}(G)$, which is useful not only for the study of 1-realizable signatures, but also for the study of signatures in general.

Lemma 5.1 *For any G, if $T_1 = \begin{pmatrix} 1 & \alpha \\ 1 & y_1 \end{pmatrix} \in B^p_{gen}(G)$ and $T_2 = \begin{pmatrix} 1 & \alpha \\ 1 & y_2 \end{pmatrix} \in B^p_{gen}(G)$ (for $y_1 \neq y_2$), then for all $y \in \mathbf{C} - \{\alpha\}$, $\begin{pmatrix} 1 & \alpha \\ 1 & y \end{pmatrix} \in B^p_{gen}(G)$.*

Proof If G is trivial, then the lemma is obvious. Now we assume G is non-trivial.

Let $B^p_{gen}(G) = V_0 \cup V_1 \subset \mathcal{M}$, and V_0 (resp. V_1) be the set defined by all the parity requirements for being an odd (resp. even) matchgate. Since G is non-trivial, we have $V_0 \cap V_1 = \emptyset$. Then there are four cases, depending on whether T_1 and T_2 are in V_0 or V_1. Here we will present the proof for the case where both $T_1, T_2 \in V_0$ and the case for $T_1 \in V_0$ and $T_2 \in V_1$. The other two cases are similar to these two cases.

Let $T_1, T_2 \in V_0$. We recall the parity polynomial equation (1) for V_0 (for $|T|$ even):

$$\left\langle \bigotimes_{\sigma=1}^{n} [1, x_{[\sigma \in T]}], G \right\rangle = \sum_{\substack{0 \leq i \leq n-|T| \\ 0 \leq j \leq |T|}} x^i y^j \sum_{\substack{A \subset T^c, |A|=i \\ B \subset T, |B|=j}} G^{A \cup B} = 0. \tag{25}$$

For any $T \subset [n]$ and $|T|$ even, let

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

Then for all even T, $\deg(f_T) \le |T|$ and $f_T(y_1) = f_T(y_2) = 0$. We note that $y_1 \ne \alpha$ and $y_2 \ne \alpha$. We want to prove that f_T is identically 0 for all even T.

We prove this by induction on $|T| \ge 0$ and $|T|$ is even. The case $|T| = 0$ is obvious.

Inductively we assume this has been proved for all $|T| \le 2(k - 1)$, for some $k \ge 1$. Now $|T| = 2k$. First we prove that α is a root of $f_T(y)$ with multiplicity at least $2k - 1$. We prove this by showing that $f_T^{[r]}(\alpha) = 0$ for $0 \le r \le 2(k - 1)$, where $f^{[0]} = f_T$ and $f_T^{[r]} = \frac{d}{dy}(f_T^{[r-1]})$ is the r-th derivative. We have

$$f_T^{[r]}(\alpha) = \sum_{\substack{0 \le i \le n - |T| \\ r \le j \le |T|}} r! \binom{j}{r} \alpha^i \alpha^{j-r} \sum_{\substack{A \subset T^c, |A| = i \\ B \subset T, |B| = j}} G^{A \cup B} = r! \sum_{\ell=0}^{n-r} \alpha^\ell \sum_{|S| = \ell + r} \binom{|T \cap S|}{r} G^S.$$
(26)

Note that the second equality follows from considering each G^S, where $|S \cap T| = j \ge r$ and $|S \cap T^c| = i$.

If r is even, we consider any T' where $|T'| = r$. Since $r \le 2(k - 1)$, by induction, we have $f_{T'} \equiv 0$. Then $f_{T'}^{[r]} \equiv 0$ and $f_{T'}^{[r]}(\alpha) = 0$. On the other hand, just as in (26), we have

$$f_{T'}^{[r]}(\alpha) = r! \sum_{i=0}^{n-r} \alpha^i \sum_{|S| = i + r} \binom{|T' \cap S|}{r} G^S = r! \sum_{i=0}^{n-r} \alpha^i \sum_{|S| = i + r, S \supset T'} G^S,$$

where the second equality is due to $|T'| = r$, which implies that in the inner sum over S, the only non-zero terms are those $S \supset T'$.

Summing over all $T' \subset T$ where $|T'| = r$, we get:

$$0 = \sum_{T' \subset T, |T'| = r} f_{T'}^{[r]}(\alpha)$$

$$= r! \sum_{i=0}^{n-r} \alpha^i \sum_{T' \subset T, |T'| = r} \sum_{|S| = i + r, S \supset T'} G^S$$

$$= r! \sum_{i=0}^{n-r} \alpha^i \sum_{|S| = i + r} \binom{|T \cap S|}{r} G^S = f_T^{[r]}(\alpha).$$

The third equality is by considering how many times each G^S appears, where $|S \cap T| \ge r$ and $|S| = i + r$.

If r is odd, we consider any T' where $|T'| = r + 1$. Since $r + 1 \le 2(k - 1)$, by induction, we have $f_{T'} \equiv 0$. Then $f_{T'}^{[r]}(\alpha) = 0$. On the other hand, similarly with (26),

we have

$$f_{T'}^{[r]}(\alpha) = r! \sum_{i=0}^{n-r} \alpha^i \sum_{|S|=i+r} \binom{|T' \cap S|}{r} G^S$$

$$= r! \sum_{i=0}^{n-r} \alpha^S \left(\sum_{|S|=i+r, T' \subset S} (r+1) G^S + \sum_{t \in T'} \sum_{|S|=i+r, T' \setminus S=\{t\}} G^S \right).$$

Summing over all $T' \subset T$ where $|T'| = r + 1$, we can show that the following quadruple sum, which is 0 to start with, finally simplifies to $(|T| - r) f_T^{[r]}(\alpha)$.

$$0 = \sum_{T' \subset T, |T'|=r+1} f_{T'}^{[r]}(\alpha)$$

$$= r! \sum_{T' \subset T, |T'|=r+1} \sum_{i=0}^{n-r} \alpha^i \left(\sum_{|S|=i+r, T' \subset S} (r+1) G^S + \sum_{t \in T'} \sum_{|S|=i+r, T' \setminus S=\{t\}} G^S \right)$$

$$= r! \sum_{i=0}^{n-r} \alpha^i \sum_{T' \subset T, |T'|=r+1} \left(\sum_{|S|=i+r, T' \subset S} (r+1) G^S + \sum_{t \in T'} \sum_{|S|=i+r, T' \setminus S=\{t\}} G^S \right)$$

$$= r! \sum_{i=0}^{n-r} \alpha^i \sum_{|S|=i+r} G^S \left(\binom{|T \cap S|}{r+1}(r+1) + \binom{|T \cap S|}{r}\binom{|T \setminus S|}{1} \right)$$

$$= r! \sum_{i=0}^{n-r} \alpha^i \sum_{|S|=i+r} G^S \binom{|T \cap S|}{r}(|T \cap S| - r + |T \setminus S|)$$

$$= (|T| - r) f_T^{[r]}(\alpha).$$

Since $|T| - r > 0$, we have $f_T^{[r]}(\alpha) = 0$.

To sum up, we proved that $f_T^{[r]}(\alpha) = 0$ for $r = 0, 1, \ldots, 2(k-1)$. So α is a root of multiplicity at least $2k - 1$. The degree of f_T is at most $2k$, and we know f_T has at least two more roots y_1 and y_2. Therefore f_T must be identically 0. This completes the proof of case 1.

For case 2, we can extend our definition of $f_T(y)$ for odd T. Then $f_T(y_1) = 0$ for even T; $f_T(y_2) = 0$ for odd T. Similarly we prove all the $f_T(y)$ are trivial. We also prove this by induction on $|T|$ but for all $|T|$. The case $|T| = 0$ is obvious. Inductively we assume this has been proved for all $|T| \leq k - 1$, for some $k \geq 1$. Now $|T| = k$. First we prove that α is at least a k-th order multiple root of $f_T(y)$. We prove this by showing that $f_T^{[r]}(\alpha) = 0$ for $r = 0, 1, \ldots, k - 1$. The proof is similar with the above proof when r is even. On the other hand, $\deg(f_T(y)) = k$, so $f_T(y)$ can not have any other root if it is non-trivial. But we know $f_T(y)$ has at least one more root y_1 or y_2 depending on the parity of $|T|$. This contradiction completes the proof. □

This lemma says that, for any fixed $x \in \mathbf{C}$, either for all y or for at most one $y \in \mathbf{C} - \{x\}$, we have $\left(\begin{smallmatrix} 1 & x \\ 1 & y \end{smallmatrix}\right) \in B_{gen}^p(G)$.

In the following we give some characterization theorems for 1-admissibility and 1-realizability of signatures. It turns out that, for a general 1-admissible signature, after omitting isolated points in $B_{gen}^p(G)$, one can show that $B_{gen}^p(G)$ is the solution for a single polynomial $F(x, y)$ on $\mathcal{M}$. Using Lemma 5.1, we can show that this $F(x, y)$ must be multilinear. More precisely we have the following characterization theorem of 1-admissibility. (Since we are talking about 1-admissibility or 1-realizability, in this section we will omit isolated points for both $B_{gen}^p(G)$ or $B_{gen}(G)$.)

Theorem 5.1 *If G is 1-admissible, then there exist three constants a, b, c such that*

$$B_{gen}^p(G) = \left\{ \left[\binom{n_0}{n_1}, \binom{p_0}{p_1} \right] \in \mathcal{M} \,\middle|\, an_0n_1 + b(n_0p_1 + n_1p_0) + cp_0p_1 = 0 \right\}.$$

Also for any three constants a, b, c, there exists a signature G such that the above equation holds.

Proof We first note that for any given a, b, c, the existence of G can be fulfilled by the symmetric signature $(G^{00}, G^{01}, G^{10}, G^{11})^{\mathrm{T}} = (a, b, b, c)^{\mathrm{T}}$ of arity 2. This is called a symmetric signature since the entries only depend on the Hamming weight of the index. In symmetric signature notation the signature is written as $[a, b, c]$, which is the form they are stated in [4].

If $a = b = c = 0$, then clearly the signature $[a, b, c]$ is 2-admissible, and $B_{gen}^p(G) = \mathcal{M}$. Suppose the given a, b, c are not all 0. In the paper [4] the following lemma was proved

Lemma

$B_{gen}([x_0, x_1, x_2])$

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

The equations simply express the following: After the basis transformation the signature is the standard signature $\Gamma^{b_1b_2}$ of a planar matchgate, and thus either its even-indexed entries $\Gamma^{00} = \Gamma^{11} = 0$, or its odd-indexed entries $\Gamma^{01} = \Gamma^{10} = 0$. This is exactly the parity requirement; for standard signatures of arity 2, the matchgate identities are trivially satisfied. Note that the equation $x_0n_0n_1 + x_1(n_0p_1 + n_1p_0) + x_2p_0p_1 = 0$ is exactly the one given here for $[a, b, c]$. The other alternative is a pair of non-trivial equations on (n_0, p_0) and on (n_1, p_1) separately. They are non-trivial because a, b, c are not all 0. Considering the equivalence relation defining $\mathcal{M}$ this alternative gives only isolated points, and thus can be omitted. The displayed equation for $B_{gen}([x_0, x_1, x_2])$ indicates that the signature is 1-admissible.

Now assume we are given a 1-admissible signature G. If G is in fact 2-admissible, we take $a = b = c = 0$, then there is no constraint on the bases. Now we assume G is not 2-admissible. In the following proof, we use the dehomogenized coordinates

$\left(\begin{smallmatrix} 1 & x \\ 1 & y \end{smallmatrix}\right) \in \mathcal{M}$. The exceptional cases are similar. If there are two bases $\left(\begin{smallmatrix} 1 & \alpha \\ 1 & y_1 \end{smallmatrix}\right) \in B_{gen}^p(G)$ and $\left(\begin{smallmatrix} 1 & \alpha \\ 1 & y_2 \end{smallmatrix}\right) \in B_{gen}^p(G)$ $(y_1 \neq y_2)$, by Lemma 5.1, we have

$$\left\{ \begin{pmatrix} 1 & \alpha \\ 1 & y \end{pmatrix} \in \mathcal{M} \,\middle|\, y \in \mathbf{C} - \{\alpha\} \right\} \subset B_{gen}^p(G). \tag{27}$$

Now we prove that

$$B_{gen}^p(G) = \left\{ \begin{pmatrix} 1 & \alpha \\ 1 & y \end{pmatrix} \in \mathcal{M} \,\middle|\, y \in \mathbf{C} - \{\alpha\} \right\}.$$

If not, we assume for a contradiction that $\left(\begin{smallmatrix} 1 & u \\ 1 & v \end{smallmatrix}\right) \in B_{gen}^p(G)$ and $u, v \neq \alpha$ (recall the equivalence relation on $\mathcal{M}$). Under this assumption, we prove that G is 2-admissible. For any basis $T = \left(\begin{smallmatrix} 1 & x_0 \\ 1 & y_0 \end{smallmatrix}\right) \in \mathcal{M}$, if $x_0 = \alpha$ or $y_0 = \alpha$ then we know $T \in B_{gen}^p(G)$. Now we assume $x_0, y_0 \neq \alpha$. Since $\left(\begin{smallmatrix} 1 & u \\ 1 & v \end{smallmatrix}\right) \in B_{gen}^p(G)$ and $\left(\begin{smallmatrix} 1 & u \\ 1 & \alpha \end{smallmatrix}\right) \in B_{gen}^p(G)$ by (27), it follows from Lemma 5.1 that for any $t \neq u$, we have

$$\begin{pmatrix} 1 & u \\ 1 & t \end{pmatrix} \in B_{gen}^p(G). \tag{28}$$

So if $x_0 = u$ or $y_0 = u$, we have $T \in B_{gen}^p(G)$. Similarly if $x_0 = v$ or $y_0 = v$, we also have $T \in B_{gen}^p(G)$. Now we further assume $x_0, y_0 \notin \{u, v\}$. Then we have $\left(\begin{smallmatrix} 1 & u \\ 1 & y_0 \end{smallmatrix}\right) \in B_{gen}^p(G)$ by (28) and $\left(\begin{smallmatrix} 1 & \alpha \\ 1 & y_0 \end{smallmatrix}\right) \in B_{gen}^p(G)$ by (27). By Lemma 5.1, we have $\left(\begin{smallmatrix} 1 & x_0 \\ 1 & y_0 \end{smallmatrix}\right) \in B_{gen}^p(G)$. Since this is true for any $T = \left(\begin{smallmatrix} 1 & x_0 \\ 1 & y_0 \end{smallmatrix}\right) \in \mathcal{M}$, we conclude that G is 2-admissible, which we assumed not to be. Therefore if G is not 2-admissible and if $\left(\begin{smallmatrix} 1 & \alpha \\ 1 & y_1 \end{smallmatrix}\right) \in B_{gen}^p(G)$ and $\left(\begin{smallmatrix} 1 & \alpha \\ 1 & y_2 \end{smallmatrix}\right) \in B_{gen}^p(G)$ (for $y_1 \neq y_2$), then

$$B_{gen}^p(G) = \left\{ \begin{pmatrix} 1 & \alpha \\ 1 & y \end{pmatrix} \in \mathcal{M} \,\middle|\, y \in \mathbf{C} - \{\alpha\} \right\}.$$

We can set $a = \alpha^2, b = -\alpha, c = 1$ in the theorem.

Now we can assume $B_{gen}^p(G)$ does not contain two bases of the above form. More precisely, for a basis $\left(\begin{smallmatrix} 1 & x \\ 1 & y \end{smallmatrix}\right) \in \mathcal{M}$, whenever we fix an x, there exists at most one y, such that $\left(\begin{smallmatrix} 1 & x \\ 1 & y \end{smallmatrix}\right) \in B_{gen}^p(G)$. This is also true for any fixed y. On the other hand, if we disregard at most finitely many points, it can be shown that, to be 1-admissible, there exists a single polynomial $F(x, y) \in \mathbf{C}[x, y]$ such that

$$B_{gen}^p = \left\{ \begin{pmatrix} 1 & x \\ 1 & y \end{pmatrix} \in \mathcal{M} \,\middle|\, F(x, y) = 0 \right\}.$$

Furthermore we will assume $F(x, y)$ is of minimal degree. In particular, we may assume $F(x, y)$ is square-free.

W.o.l.o.g., assume $d = \deg_y F \geq \deg_x F$. Clearly $d \geq 1$. Otherwise, $F(x, y)$ is a constant, which is absurd. Write

$$F(x, y) = f_d(x)y^d + f_{d-1}(x)y^{d-1} + \cdots + f_0(x), \tag{29}$$

where $f_i(x) \in \mathbf{C}[x]$, $\deg f_i \leq d$, for all $0 \leq i \leq d$, and f_d is not identically zero.

For any x_0 such that $f_d(x_0) \neq 0$, we can write

$$F(x_0, y) = f_d(x_0) \left(y^d + \frac{f_{d-1}(x_0)}{f_d(x_0)} y^{d-1} + \cdots + \frac{f_0(x_0)}{f_d(x_0)} \right). \tag{30}$$

This polynomial in y has d roots in $\mathbf{C}$ counting multiplicity, but does not have two distinct roots. Therefore, there exists $\alpha \in \mathbf{C}$ such that

$$F(x_0, y) = f_d(x_0)(y + \alpha)^d. \tag{31}$$

If we compare the expressions in (30) and (31), we get for all $1 \leq k \leq d$,

$$\binom{d}{k} \alpha^k = \frac{f_{d-k}(x_0)}{f_d(x_0)}.$$

It follows that

$$\binom{d}{k} \left(\frac{f_{d-1}(x_0)}{\binom{d}{1} f_d(x_0)} \right)^k = \frac{f_{d-k}(x_0)}{f_d(x_0)},$$

for $1 \leq k \leq d$.

Writing in terms of polynomials, for all $1 \leq k \leq d$,

$$\binom{d}{k} \frac{f_{d-1}^k(x)}{d^k} = f_{d-k}(x) f_d^{k-1}(x), \tag{32}$$

holds for infinitely many $x \in \mathbf{C}$, and therefore holds identically, as polynomials in $\mathbf{C}[x]$.

It follows that

$$f_d^{d-1}(x) \cdot F(x, y) = \left(f_d(x)y + \frac{f_{d-1}(x)}{d} \right)^d, \tag{33}$$

in $\mathbf{C}[x, y]$.

Assume for a contradiction that $d \geq 2$. Take $k = 2$ in (32), we get $f_d(x) | f_{d-1}(x)$ in $\mathbf{C}[x]$. Also for all $k \geq 1$, $f_{d-k}(x) = \frac{\binom{d}{k}}{d^k} f_{d-1}(x) \left(\frac{f_{d-1}(x)}{f_d(x)} \right)^{k-1}$, and therefore $f_{d-1}(x) | f_{d-k}(x)$ in $\mathbf{C}[x]$. In particular $f_d(x) | f_{d-k}(x)$ for all $k \geq 1$, which implies that $f_d(x) | F(x, y)$ in $\mathbf{C}[x, y]$. If $\deg f_d(x) \geq 1$, then for a root x of f_d, there would have been infinitely many zero of $F(x, y)$. Since this is not the case, we must have $\deg f_d(x) = 0$, i.e., $f_d(x)$ is a non-zero constant $c \in \mathbf{C}$.

It follows that

$$F(x, y) = c \left(y + \frac{f_{d-1}(x)}{cd} \right)^d.$$

But $F(x, y)$ is square-free in $\mathbf{C}[x, y]$, it follows that $d = 1$ after all.

So back to (33) we obtain

$$F(x, y) = f_1(x)y + f_0(x),$$

and deg f_1, deg $f_0 \leq 1$. Therefore $F(x, y)$ is of the form $a + bx + b'y + cxy$. By symmetry on x and y in $\mathcal{M}$, we get $b = b'$. □

Now we can prove the characterization theorem for 1-realizability.

Theorem 5.2 *If G is 1-realizable, then there exist three constants a, b, c such that*

$$B_{gen}(G) = \left\{ \left[\binom{n_0}{n_1}, \binom{p_0}{p_1} \right] \in \mathcal{M} \,\middle|\, an_0 n_1 + b(n_0 p_1 + n_1 p_0) + cp_0 p_1 = 0 \right\}.$$

Also for any three constants a, b, c, there exists a signature G such that the above equation holds.

Proof Again, we first remark that for a given a, b, c, the existence of G can be fulfilled by symmetric signatures, by the same proof in Theorem 5.1.

Since G is 1-realizable, G is also 1-admissible. There are two cases: if G is in fact 2-admissible, then as a 1-realizable signature, G is at least realizable on some bases. It follows from Corollary 3.2, G is indeed a 2-realizable signature. In this case we take $a = b = c = 0$.

If G is 1-admissible but not 2-admissible, then in Theorem 5.1 we must have a non-zero triple (a, b, c), defining $B_{gen}^p(G)$ as a 1-dimensional variety. We claim that, for any $T \in B_{gen}^p(G)$, all the MGI of $T^{\otimes n}G$ must vanish. Otherwise $B_{gen}(G)$ cannot have dimension 1. Since all MGI are satisfied for any $T \in B_{gen}^p(G)$, we get $B_{gen}(G) = B_{gen}^p(G)$. Theorem 5.2 now follows from Theorem 5.1. □

6 Some Families of 1-Realizable Signatures

We have now developed the theory sufficiently to the point where we can say the main problem of 1-realizability is that given a, b, c, find all the signatures G such that

$$B_{gen}(G) = \left\{ \left[\binom{n_0}{n_1}, \binom{p_0}{p_1} \right] \in \mathcal{M} \,\middle|\, an_0 n_1 + b(n_0 p_1 + n_1 p_0) + cp_0 p_1 = 0 \right\}.$$

For convenience, we introduce a new notation:

Definition 6.1 For a set of bases $B \subset \mathcal{M}$, we define Gen(B) (resp. Gen$^p(B)$) as the set of generators, which are realizable (resp. admissible) on the set of bases in B.

If $a = b = c = 0$, then this is Gen($\mathcal{M}$), which means that G is 2-realizable. In Sect. 4, we have given a complete characterization in this case.

In this section, we study this problem for some other families of a, b and c. We define sets of bases $B2$ and $B1$ corresponding to the basis $b2$ and $b1$ in Valiant's paper [21]. It's not only because $b2 \in B2$ and $b1 \in B1(0)$, but they are also similar in spirit.

6.1 The Bases Set B2

First we consider the case $a = c = 0$ and $b \neq 0$. In terms of homogenized coordinates, we consider

$$B2 = \left\{ \left[\binom{n_0}{n_1}, \binom{p_0}{p_1} \right] \in \mathcal{M} \middle| n_0 p_1 + n_1 p_0 = 0 \right\},$$

and try to characterize the set $\text{Gen}(B2)$. For an arbitrary basis in $B2$, we will use dehomogenized coordinates $\left(\begin{smallmatrix} 1 & x \\ 1 & -x \end{smallmatrix} \right)$ for notational simplicity. (If there are exceptional cases ("at infinity"), they can be verified directly; or one can invoke general theorems in algebraic geometry.)

The plan is to first give a characterization of $\text{Gen}^p(B2)$. Then we apply the set of all MGI to them to get $\text{Gen}(B2)$. The proof will be quite involved.

Consider an arbitrary $\left(\begin{smallmatrix} 1 & x \\ 1 & -x \end{smallmatrix} \right) \in B2$, where non-singularity implies that $x \neq 0$. When we replace y with $-x$ in (1), all the polynomials should be identically zero. This is the iff condition for $G \in \text{Gen}^p(B2)$. The coefficient of x^i is

$$\sum_{|S|=i} (-1)^{|S \cap T|} G^S = 0. \tag{34}$$

When T ranges over all even subsets or all odd subsets according to the parity of matchgate, we have a linear system for G^S. (The even (resp. odd) sets correspond to admissibility as odd (resp. even) matchgate signatures.) Thus we get $n+1$ linear equation systems according to the weight of S; the i-th linear system, $0 \leq i \leq n$, is over the set of variables G^S with $|S| = i$, where the equations are indexed by subsets T with even cardinality. (The alternative case with all odd subsets is similar.) We define the coefficient matrix of the system as M, which is indexed by T and S. Then we have the following calculation of $M^T M$:

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

There are three cases: If $S_1 \oplus S_2 = \emptyset$, we have

$$\sum_{|T| \text{ is even}} (-1)^{|(S_1 \oplus S_2) \cap T|} = 2^{n-1}. \tag{35}$$

If $S_1 \oplus S_2 = [n]$, we have also

$$\sum_{|T| \text{ is even}} (-1)^{|(S_1 \oplus S_2) \cap T|} = 2^{n-1}. \tag{36}$$

If $S_1 \oplus S_2 \neq \emptyset$ and $S_1 \oplus S_2 \neq [n]$, we can take two elements a, 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. They cancel out by each other, so overall we have

$$\sum_{|T| \text{ is even}} (-1)^{|(S_1 \oplus S_2) \cap T|} = 0. \tag{37}$$

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 $M^{\mathrm{T}} M$ is $2^{n-1} I$, which means that $G^S = 0$, for all $|S| \neq n/2$.

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 1-admissibility for $B2$:

Theorem 6.1 *For a signature G with arity n, $G \in \mathrm{Gen}^p(B2)$ 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 MGI to $\mathrm{Gen}^p(B2)$ to get a characterization for $\mathrm{Gen}(B2)$.

For a $\left(\begin{smallmatrix} 1 & x \\ 1 & -x \end{smallmatrix} \right) \in B_{gen}^p(G)$, let $\underline{G} = \beta^{\otimes n} G$. 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 6.1, 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 $\underline{G} = \beta^{\otimes n} G$, 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. This gives us

$$\underline{G}^T = \sum_{|S|=n/2} (-1)^{|T \cap S|} G^S. \tag{38}$$

(Note that this is just Valiant's basis $b2$; however the results we derive here hold for 1-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

$$0 = \sum_{i=1}^{|P|} (-1)^i \underline{G}^{A \oplus \{p_i\}} \underline{G}^{A \oplus P \oplus \{p_i\}}$$

$$= \sum_{i=1}^{|P|} (-1)^i \sum_{|S_1|=n/2} (-1)^{|(A \oplus \{p_i\}) \cap S_1|} G^{S_1} \sum_{|S_2|=n/2} (-1)^{(|A \oplus P \oplus \{p_i\}) \cap S_2|} G^{S_2}$$

$$= \sum_{|S_1|=|S_2|=n/2} G^{S_1} G^{S_2} \sum_{i=1}^{|P|} (-1)^i (-1)^{|(A \oplus \{p_i\}) \cap S_1|} (-1)^{(|A \oplus P \oplus \{p_i\}) \cap S_2|}.$$

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

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

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

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

Theorem 6.2 *For a signature G with arity n, $G \in \mathrm{Gen}(B2)$ 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 $1 \notin X$):

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

$$= 0. \tag{39}$$

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

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

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 (39), 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 (35) and (37). 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 $1 \notin X$,

$$\sum_{|S|=|S \oplus X|=n/2, 1 \in S} G^S G^{S \oplus X}(-1)^{|P \cap S|} \sum_{i=1}^{|P|}(-1)^i(-1)^{|\{p_i\} \cap X|} = 0. \tag{40}$$

Now we will fix an X with $1 \notin X$, and view (40) 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 (40) always holds. If $P \cap X$ is even, X being a single run and 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 "if" part of this theorem.

Now we prove that the conditions in Theorem 6.2 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. In the end we will show that a certain exponential sized matrix has mutually orthogonal columns, a matrix which we can't even give 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 X, which is an even subset not containing 1, and is not a single run, consider the following 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,

$$\sum_{|S|=|S \oplus X|=n/2, 1 \in S} (-1)^{|P \cap S|} G^S G^{S \oplus X} = 0. \tag{41}$$

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. (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 (41) 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 (41) (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 bother with 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 (41) 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 $1 \in X^c$.)

Now for the linear equation system (41), we want to show the columns of distinct S and S' are orthogonal.

Note: 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 (40) are non-zero (for these vectors the entries are indexed by P as P runs through all the appropriate sets, the set of vectors are indexed by various S). In going from (40) to (41), we have already taken that into account.

We had proved earlier that for X not a single run, there is some 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 (40) the above quantity 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 (40) where the above quantity is non-zero, and factor out this sum from each such equation. This gives us (41). Of course in (40) those equations (indexed by P) where the above sum is zero is trivially satisfied. This means that the orthogonality of the coefficient vectors in (41) implies that all $G^S G^{S \oplus X} = 0$ in (41) and therefore in (40).

(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 these "in" segments or "out" segments. 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. 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. Now the key observation is that: 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 -1 to the sum.

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.   □

When $n = 4$, the theorem gives Corollary 6.1, which is used in Sect. 7.

Corollary 6.1 *For any $a, b \in \mathbf{C}$, the following generator*

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

is realizable on bases $\begin{pmatrix} 1 & x \\ 1 & -x \end{pmatrix}$ for all $x \neq 0$.

6.2 The Bases Set B1

This time we consider the case $b^2 = ac$. In the dehomogenized coordinates, the equation

$$a + \sqrt{ac}(x + y) + cxy,$$

factors into $(\sqrt{a} + \sqrt{c}x)(\sqrt{a} + \sqrt{c}y)$. After taking into account of symmetry of the equivalence relation on $\mathcal{M}$, we have the following set:

$$B1(\alpha) = \left\{ \left[\begin{pmatrix} 1 \\ n_1 \end{pmatrix}, \begin{pmatrix} \alpha \\ p_1 \end{pmatrix} \right] \in \mathcal{M} \,\middle|\, n_1, p_1 \in \mathbf{F} \right\}.$$

We will try to characterize the set $\mathrm{Gen}(B1(\alpha))$.

The treatment here is different from that of $B2$. We do not go through $\mathrm{Gen}^p(B1(\alpha))$ but deal with $\mathrm{Gen}(B1(\alpha))$ directly. Our presentation here will be sketchy; more results will be presented in the future. The main purpose here is to present an alternative family from $B2$.

We take $b1 = \begin{pmatrix} 1 & \alpha \\ 1 & \alpha+1 \end{pmatrix} \in B1(\alpha)$. If $G \in \mathrm{Gen}(B1(\alpha))$, then by definition $\underline{G} = b1^{\otimes n}G$ is realizable as a standard signature. Since $b1$ is invertible, this transformation is a bijection. Our characterization theorem will be described by $\underline{G}$ rather than G.

Take any basis $\beta = \begin{pmatrix} 1 & \alpha \\ n_1 & p_1 \end{pmatrix} \in B1(\alpha)$. By definition, $\beta^{\otimes n}G$ is realizable. If we replace G by $(b1^{-1})^{\otimes n}\underline{G}$, then we have

$$\beta^{\otimes n}G = \begin{pmatrix} 1 & \alpha \\ n_1 & p_1 \end{pmatrix}^{\otimes n} \begin{pmatrix} \alpha+1 & -\alpha \\ -1 & 1 \end{pmatrix}^{\otimes n} \underline{G} = \begin{pmatrix} 1 & 0 \\ n_1(1+\alpha)-p_1 & p_1 - \alpha n_1 \end{pmatrix}^{\otimes n} \underline{G}.$$

Note that the pair $(n_1(1+\alpha)-p_1, p_1 - \alpha n_1)$ can be arbitrary. The above calculation shows that $G \in \mathrm{Gen}(B1(\alpha))$ iff $\underline{G} \in \mathrm{Gen}(B1(0))$. As a result, we only need to study $\mathrm{Gen}(B1(0))$, and to simplify notations, we use G instead of $\underline{G}$.

Now take an arbitrary basis $\beta = \begin{pmatrix} 1 & 0 \\ 1 & y \end{pmatrix} \in B1(0)$. Substituting x by 0 in (1), we have

$$\sum_{S \subset T, |S|=j} G^S = 0, \tag{42}$$

where T ranges over all even sets or all odd sets depending on the parity of the matchgate. Similar to the proof of 2-admissible signatures [4], this implies that $G^S = 0$ for all $|S| < n/2$.

To sum up, we have the following theorem:

Theorem 6.3 *For a generator G with arity n, $G \in \mathrm{Gen}(B1(0))$ iff the following three conditions are satisfied*:

1. *G is realizable as a standard signature.*
2. *For all odd (or even) sets T, $\sum_{S \subset T, |S|=j} G^S = 0$.*
3. *$G^S = 0$ for all $|S| < n/2$.*

(Actually condition 3 is implied by condition 2. We list it here to be explicit.) In future work we plan to present explicit constructions of generators of this family.

7 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 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, the incident edges are not monochromatic; (2) when two edges cross over each other, they have different colors.

SOLUTION: For every point with 2 incident edges, we use a generator for $(0, 1, 1, 0)^{\mathrm{T}}$ (for Not-Equal); for every point with 3 incident edges, we use a generator for $(0, 1, 1, 1, 1, 1, 1, 0)^{\mathrm{T}}$ (for Not-All-Equal); for every point (not from S) where two edges intersect, we use a generator with arity 4 and the following signature

$$G^\alpha = \begin{cases} 1, & \alpha \in \{0101, 1010\}, \\ 0, & \text{otherwise}; \end{cases}$$

and 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 $(1, 0, 0, 1)^{\mathrm{T}}$ (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 $b2$ which belongs to $B2$ by setting $x = 1$ [21]; see Sect. 6 for details), we have a polynomial time algorithm for this problem. We give a formal description of the holographic algorithm here.

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 Fig. 5);
- each degree 3 vertex in V_1 is replaced by a generator matchgate G_3 with arity 3 (see Fig. 3);
- each degree 4 vertex in V_1 (intersection point) is replaced by a generator matchgate G_4 with arity 4 (see Fig. 4);
- each vertex in V_2 is replaced by a recognizer matchgate R with arity 2 (see Fig. 6)

Fig. 3 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
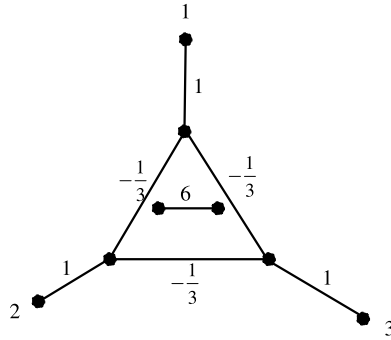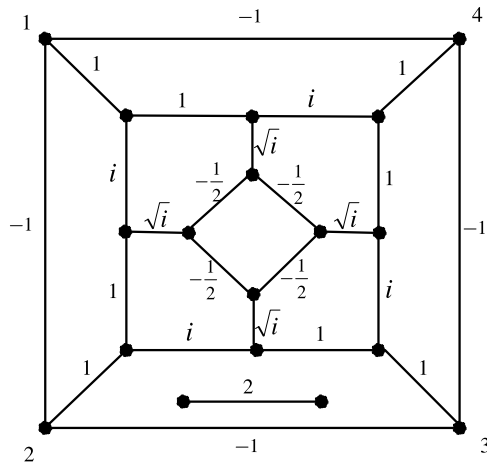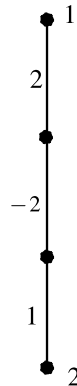
Fig. 4 Under the basis **b2**, this generator matchgate has the signature G, where $G^{0101} = G^{1010} = 1$ and $G^\alpha = 0$ for other α. It makes sure that the color of the edge is transmitted at intersection points while only allowing different colored edges to meet at these intersection points

Fig. 5 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
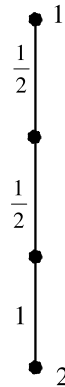
(Note that G' is a still a planar graph.)

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

Problem 2

We extend Problem 1 by allowing curves (not necessarily line segments) between two

Fig. 6 Under the basis **b2**, this recognizer matchgate has the signature $(1, 0, 0, 1)$. It makes sure that each segment has a consist coloring

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 a polynomial number (in n) of 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 and the following signature

$$G^\alpha = \begin{cases} 1, & \alpha \in \{0110, 1001\}, \\ 0, & \text{otherwise.} \end{cases}$$

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, for each curve, we have a orientation. And 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 and the following signature

$$G^\alpha = \begin{cases} 1, & \alpha \in \{0101, 1010\}, \\ x, & \alpha \in \{0110, 1001\}, \\ 0, & \text{otherwise.} \end{cases}$$

And for every tangent point, we use a generator with arity 4 and the following signature

$$G^\alpha = \begin{cases} x, & \alpha \in \{0101, 1010\}, \\ 1, & \alpha \in \{0110, 1001\}, \\ 0, & \text{otherwise.} \end{cases}$$

Since they are all realizable on $b2$, we have a polynomial time algorithm to compute the Holant. The Holant is a polynomial of x. The degree of this polynomial is bounded by $n^{O(1)}$, and the coefficients are 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 smallest non-zero term.

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.

References

1. Cai, J.-Y., Choudhary, V.: Some results on matchgates and holographic algorithms. In: Proceedings of ICALP 2006, Part I. Lecture Notes in Computer Science, vol. 4051, pp. 703–714. Springer, Berlin (2006). Also available at Electronic Colloquium on Computational Complexity TR06-048

2. Cai, J.-Y., Choudhary, V.: Valiant's Holant theorem and matchgate tensors (extended abstract). In: Proceedings of TAMC 2006. Lecture Notes in Computer Science, vol. 3959, pp. 248–261. Springer, Berlin (2006). Also available at Electronic Colloquium on Computational Complexity Report TR05-118

3. Cai, J.-Y., Choudhary, V., Lu, P.: On the theory of matchgate computations. In: Proceedings of CCC '07: Proceedings of the Twenty-Second Annual IEEE Conference on Computational Complexity, Washington, DC, USA, pp. 305–318. IEEE Computer Society, Los Alamitos (2007)

4. Cai, J.-Y., Lu, P.: Holographic algorithms: from art to science. In: Proceedings of STOC '07: Proceedings of the Thirty-Ninth Annual ACM Symposium on Theory of Computing, pp. 401–410. ACM, New York (2007). Also available at Electronic Colloquium on Computational Complexity Report TR06-145

5. Cai, J.-Y., Lu, P.: Holographic algorithms: The power of dimensionality resolved. In: Arge, L., Cachin, C., Jurdzinski, T., et al. (eds.) Proceedings of ICALP '07. Lecture Notes in Computer Science, vol. 4596, pp. 631–642. Springer, Berlin (2007)

6. Cai, J.-Y., Lu, P.: Holographic algorithms with unsymmetric signatures. In: Proceedings of SODA '08: Proceedings of the Nineteenth Annual ACM-SIAM Symposium on Discrete Algorithms, pp. 54–63. Society for Industrial and Applied Mathematics, Philadelphia (2008)

7. Cai, J.-Y., Lu, P.: Signature theory in holographic algorithms. In: Hong, S.H., Nagamochi, H., Fukunaga, T. (eds.) Proceedings of ISAAC. Lecture Notes in Computer Science, vol. 5369, pp. 568–579. Springer, Berlin (2008)

8. Foody, W., Hedayat, A.: On theory and applications of BIB designs with repeated blocks. Ann. Stat. **5**, 932–945 (1977)

9. Foody, W., Hedayat, A.: Note: Correction to "On Theory and Application of BIB Designs with Repeated Blocks". Ann. Stat. **7**(4), 925 (1979)

10. Dodson, C.T.J., Poston, T.: Tensor Geometry, 2nd edn. Graduate Texts in Mathematics, vol. 130. Springer, New York (1991)
11. Graham, R.L., Li, S.-Y.R., Li, W.-C.W.: On the structure of t-designs. SIAM. J. Algebraic Discrete Methods **1**, 8 (1980)
12. Linial, N., Rothschild, B.: Incidence matrices of subsets—a rank formula. SIAM. J. Algebraic Discrete Methods **2**, 333 (1981)
13. Kasteleyn, P.W.: The statistics of dimers on a lattice. Physica **27**, 1209–1225 (1961)
14. Kasteleyn, P.W.: Graph theory and crystal physics. In: Harary, F. (ed.) Graph Theory and Theoretical Physics, pp. 43–110. Academic Press, London (1967)
15. Kneser, M.: Aufgabe 360. Jahresber. Dtsch. Math.-Ver. **58**, 27 (1955) 2. Abteilung
16. Lovász, L.: Kneser's conjecture, chromatic number, and homotopy. J. Comb. Theory, Ser. A **25**, 319–324 (1978)
17. Matoušek, J.: A combinatorial proof of Kneser's conjecture. Combinatorica **24**(1), 163–170 (2004)
18. Temperley, H.N.V., Fisher, M.E.: Dimer problem in statistical mechanics—an exact result. Philos. Mag. **6**, 1061–1063 (1961)
19. Valiant, L.G.: Quantum circuits that can be simulated classically in polynomial time. SIAM J. Comput. **31**(4), 1229–1254 (2002)
20. Valiant, L.G.: Expressiveness of matchgates. Theor. Comput. Sci. **281**(1), 457–471 (2002)
21. Valiant, L.G.: Holographic algorithms (extended abstract). In: Proc. 45th IEEE Symposium on Foundations of Computer Science, pp. 306–315 (2004). A more detailed version appeared in Electronic Colloquium on Computational Complexity Report TR05-099
22. Valiant, L.G.: Accidental algorithms. In: Proc. 47th Annual IEEE Symposium on Foundations of Computer Science, pp. 509–517 (2006)