Some Results on Matchgates and Holographic Algorithms

Jin-Yi Cai [1]   Vinay Choudhary [2]
Computer Sciences Department
University of Wisconsin
Madison, WI 53706. USA.
Email: {jyc, vinchr}@cs.wisc.edu

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

Abstract

We establish a 1-1 correspondence between Valiant's *character* theory of matchgate/matchcircuit [14] and his *signature* theory of planar-matchgate/matchgrid [16], thus unifying the two theories in expressibility. In [5], we had established a complete characterization of general matchgates, in terms of a set of *useful* Grassmann-Plücker identities. With this correspondence, we give a corresponding set of identities which completely characterizes planar-matchgates and their signatures. Applying this characterization we prove some negative results for *holographic algorithms*. On the positive side, we also give a polynomial time algorithm for a simultaneous node-edge deletion problem, using holographic algorithms. Finally we give characterizations of symmetric signatures realizable in the Hadamard basis.

1 Introduction

Recently Valiant has introduced a novel methodology in algorithm design. In a ground breaking paper [14], Valiant initiated a new theory of matchgate/matchcircuit computations. Subsequently, in [16], he further proposed the theory of holographic algorithms, based on planar matchgates and matchgrids. Underlying both theories are the beautiful ideas of (a) using perfect matchings to encode and organize computations, and (b) applying the algebraic construct called the Pfaffian.

A basic component in both theories is a matchgate. A matchgate is essentially a finite graph with certain nodes designated as inputs or outputs. In the matchcircuit theory, each matchgate defines a *character matrix*, with entries defined in terms of the Pfaffian. In the theory of holographic algorithms, only planar matchgates are considered, and each planar matchgate defines a *signature matrix*, which directly captures the properties of the matchgate under the consideration of (perfect) matchings when certain input and/or output nodes are retained or removed.

These matchgates are combined to form matchcircuits or matchgrids. For a matchcircuit, some of its global properties can be interpreted as realizing certain computations which would seem to take exponential time in the size of the circuit. However, due to the way the matchcircuits are constructed and the algebraic properties of Pfaffians defining the character matrices of the constituent matchgates, these properties can in fact be computed in polynomial time. For holographic algorithms, a new crucial ingredient was added—a choice of a set of linear basis vectors, in terms of which the computation can be expressed and interpreted. They are called holographic, because the algorithm introduces an exponential number of solution fragments in a pattern of interference, analogous to quantum computing. However, because of the planarity condition, the computation by matchgrids can be expressed via the elegant Fisher-Kasteleyn-Temperley (FKT) method [9, 10, 12] for planar perfect matchings, and therefore computable in P. Valiant [14] used matchcircuits to show that a non-trivial fragment of quantum circuits can be simulated classically in polynomial time. With holographic algorithms, he was able to devise polynomial time algorithms for several problems, which were not known to be in P, and certain minor variations of which are NP-hard (or even #P-hard). It is not clear what are the ultimate computational capabilities of either theories.

In a paper currently in submission [5], the present authors investigated a number of interesting properties of matchgate computations. In particular, we gave a necessary and sufficient condition, in terms of a set of *useful* Grassmann-Plücker identities, which completely captures the realizability of matchgates with given characters. The study of matchgate identities was already initiated by Valiant in [15]. It was shown in [5] that the matchgates form an algebraic variety, and a certain group action underlies the symmetry present in the character matrices.

In this paper, we first unite the two theories: matchcircuit computation on the one hand and matchgrid computation on the other. We show that, the planarity restriction not withstanding, any matchcircuit computation can be simulated by a matchgrid, and vice versa. In fact we will give an interpretation between the characters and signatures in a one-to-one fashion. Thus, all important theorems in [14] (e.g., its Matchcircuit Theorem and its Main Theorem) can be stated in terms of planar matchgrids. Conversely, to design holographic algorithms, one can ignore the planar restriction on the matchgates. For the proof of this equivalence theorem, in one direction we use a cross-over gadget designed by Valiant [16]; in the other direction we use the FKT method [9, 10, 12].

As part of this proof, we also define a notion of a *naked character*. Based on our previous work reported in [5], we can derive a corresponding set of matchgate identities, which are necessary and sufficient for naked characters. Then we prove that a matrix is a naked character matrix iff it is a signature matrix. This gives us a complete characterization on the realizability of planar matchgates in terms of their signatures.

Such a characterization provides for the first time the possibility of proving negative results for holographic algorithms. We note that, by definition, even with a fixed number of input and output nodes, a matchgate may consist of an arbitrarily large number of internal nodes. Thus one can prove the existence of a matchgate fulfilling certain computational requirements by construction. But one cannot prove in this way the non-existence of such a matchgate. Our characterization makes this possible. Indeed, we define *holographic templates* to capture a restricted but natural subclass of holographic algorithms, and prove certain non-existence theorems. In particular, we prove that certain natural generalizations of some of the problems solved by P-time algorithms in [16] do not have P-time algorithms by holographic templates by linearly independent basis. In many of the problems in [16], a particular basis **b2** (which can be called the Hadamard basis) was particularly useful. We characterize the representable matchgate signatures that are based on cardinality alone over this basis. This uses the properties of Krawtchouk polynomials. We also give a positive result by deriving a polynomial time algorithm for a problem using holographic templates. It is a simultaneous node-edge deletion problem for a graph to become bipartite, for planar graphs with maximal degree 3. This generalizes both the edge deletion problem, and the node deletion problem which was considered in [16] for such graphs. We note that the edge deletion problem is the same as the MAX-CUT problem. [1]

The most intriguing question is whether this new theory leads to any collapse of complexity classes. The kinds of algorithms that are obtained by this theory are quite unlike anything before and almost exotic. If our belief in NP $\neq$ P is based on the sense and experience that the usual algorithmic paradigms are insufficient for NP-hard problems (certainly it is not due to strong lower bounds), then we feel our erstwhile experience does not apply to these new algorithms. Of course it is quite possible that the theory of matchcircuit and holographic algorithms do not in the end lead to any collapse of complexity classes. But even in this eventuality, as Valiant suggested in [16], "any proof of P $\neq$ NP may need to explain, and not only to imply, the unsolvability" of NP-hard problems using this approach. Regardless of its final outcome, this paper is an attempt towards such a fundamental understanding.

The rest of the paper is organized as follows: In Section 2, we give a brief account of the background. Due to space limitations, most details are left out. The readers are referred to [14, 15, 16, 4, 5]. In Section 3, we give the equivalence theorem of the two theories. We also discuss matchgate identities for naked characters and signatures. In Section 4, we give a positive result on the simultaneous node-edge deletion problem. In Section 5 we define holographic templates, and give some impossibility results. In Section 6, we characterize symmetric signatures for basis **b2**.

2 Background

2.1 Graph and Pfaffian

Let $G = (V, E, W)$ be a weighted undirected graph, where V is the set of vertices represented by integers, E is the set of edges and W are the weights of the edges. In general, $V = \{k_1, \ldots, k_n\}$ where $k_1 < \ldots < k_n$. We represent the graph by the *skew-symmetric adjacency* matrix M, where $M(i,j) = w(k_i, k_j)$ if $i < j$, $M(i,j) = -w(k_i, k_j)$ if $i > j$, and $M(i,i) = 0$. We speak of G and M interchangeably.

The Pfaffian of an $n \times n$ skew-symmetric matrix M is defined to be 0 if n is odd, 1 if n is 0, and if $n = 2k$ where $k > 0$ then it is defined as

$$\mathrm{Pf}(M) = \sum_{\pi} \epsilon_\pi w(i_1, i_2) w(i_3, i_4) \ldots w(i_{2k-1}, i_{2k}),$$

where

[1] MAX-CUT for planar graphs is known to be in P [6].

- $\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$, is a permutation,

- summation is over all permutations π where $i_1 < i_2, i_3 < i_4, \dots, i_{2k-1} < i_{2k}$ and $i_1 < i_3 < \dots < i_{2k-1}$, and

- $\epsilon_\pi \in \{-1, 1\}$ is the sign of the permutation π. Another equivalent definition of ϵ_π is that it is the sign or parity of the number of *overlapping* pairs where a pair of edges $(i_{2r-1}, i_{2r}), (i_{2s-1}, i_{2s})$ is overlapping iff $i_{2r-1} < i_{2s-1} < i_{2r} < i_{2s}$ or $i_{2s-1} < i_{2r-1} < i_{2s} < i_{2r}$.

The Pfaffian is computable in polynomial time. In particular $(\mathrm{Pf}(M))^2 = \det(M)$.

There is a graph-theoretic interpretation of the Pfaffian. If M is the matrix of a graph G, then there is a one-to-one correspondence between monomials in the Pfaffian and perfect matchings in G. The monomial $w(i_1, i_2) \dots w(i_{2k-1}, i_{2k})$ in $\mathrm{Pf}(M)$ corresponds to the perfect matching $\{(i_1, i_2), \dots, (i_{2k-1}, i_{2k})\}$ in G. The condition on the permutation implies that every perfect matching corresponds to exactly one monomial. The coefficient ϵ_π of this monomial is the parity of the number of overlapping pairs of edges, in the sense defined earlier.

If M is an $n \times n$ matrix and $A = \{i_1, \dots, i_r\} \subseteq \{1, \dots, n\}$, then $M[A]$ denotes the matrix obtained after deleting from M, the rows and columns indexed by elements of A. We also denote by $M(A) = M[\overline{A}]$, where $\overline{A}$ is the complement of A. The Pfaffian Sum of M is a polynomial over indeterminates $\lambda_1, \lambda_2, \dots, \lambda_n$ defined as

$$\mathrm{PfS}(M) = \sum_A \left(\prod_{i \in A} \lambda_i \right) \mathrm{Pf}(M[A])$$

where the summation is over the 2^n submatrices obtained from M by deleting some subset A of indices. The Pfaffian Sum of M is also computable in polynomial time for any values of λ_i. We will only need instances where each λ_i is fixed to be 0 or 1. If $S = \{i \mid \lambda_i = 1\}$, then S is called the *omittable* vertices of the graph, as $\mathrm{PfS}(M)$ in this case sums over all matchings which can only omit vertices in S.

2.2 Grassmann-Plücker Identities

Let M be a skew-symmetric matrix, and $A = \{i_1, \dots, i_r\}$ where $i_1 < \dots < i_r$. $\mathrm{Pf}_M(i_1, \dots, i_r)$, or simply $\mathrm{Pf}(i_1, \dots, i_r)$ or $\mathrm{Pf}(A)$, is defined as the Pfaffian of the matrix obtained by restricting M to rows and columns present in A, namely $i_1, \dots, i_r$. When $i_1, \dots, i_r$ are not in increasing order, the sign will vary, e.g., $\mathrm{Pf}_M(i_2, i_1, \dots, i_r) = -\mathrm{Pf}_M(i_1, i_2, \dots, i_r)$ and so on.

The following theorem states the Grassmann-Plücker identities [2, 3].

Theorem 2.1. *For any $n \times n$ skew-symmetric matrix M, and any $I = \{i_1, \dots, i_K\} \subseteq [n]$ and $J = \{j_1, \dots, j_L\} \subseteq [n]$,*

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

2.3 Matchgates and Matchcircuits

A *matchgate* Γ is a quadruple (G, X, Y, T) where $G = (V, E, W)$ is a graph, $X \subseteq V$ is a set of *input* nodes, $Y \subseteq V$ is a set of *output* nodes, and $T \subseteq V$ is a set of *omittable* nodes such that X, Y and T are pairwise disjoint, and are ordered such that $\forall i \in T$, if $j \in X$ then $j < i$ and if $j \in Y$ then $j > i$. We call the set $X \cup Y$ the *external* nodes. Furthermore, each external node is assumed to have exactly one incident *external edge*. For nodes in X, the other end point of the external edge is assumed to have index less than any node in V and for nodes in Y, the other end point has index more than any node in V. The allowed matchings will be those that match all the unomittable nodes and also an arbitrary (possibly empty) subset of T. Whenever we refer to the Pfaffian Sum of a matchgate fragment, we assume that $\lambda_i = 1$, if $i \in T$, and 0 otherwise. We say that a matchgate Γ has *normal numbering* if the numbers of nodes in V are consecutive from 1 to $|V|$ and X, Y have minimal and maximal numbers, respectively.

For $Z \subseteq X \cup Y$, the *character* $\chi(\Gamma, Z)$ of Γ with respect to Z is defined to be the value $\mu(\Gamma, Z)\mathrm{PfS}(G - Z)$, where $G - Z$ denotes the graph obtained after deleting the vertices in Z together with their incident edges from G and the *modifier* $\mu(\Gamma, Z) \in \{-1, 1\}$ counts the parity of the number of overlaps between matched edges in $G - Z$ and matched external edges. Here, the nodes in Z are assumed to be matched externally. Since the index numbers of input nodes are always less than any omittable node and those of output nodes always greater, it can be shown that the modifier is well-defined as it depends only on Z and not on the actual matchings in $G - Z$.

The *character matrix* $\chi(\Gamma)$ is defined to be the $2^{|X|} \times 2^{|Y|}$ matrix where rows are indexed by subsets $X' \subseteq X$ and columns by subsets $Y' \subseteq Y$ and the entries are $\chi(\Gamma, Z)$ for various $Z = X' \cup Y'$. To define the ordering of the rows and columns of this matrix precisely, we need to define a 1-1 correspondence between subsets of X (and respectively subsets of Y) and the rows (and respectively columns) of the matrix. Here, we assume that the character matrices are *normally ordered* i.e. rows and columns are indexed by binary bit strings of length $|X|$ and $|Y|$ respectively, and they correspond to subsets in lexicographic order. Consider an entry (i, j) of $\chi(\Gamma)$, where $0 \leq i < 2^{|X|}$ and $0 \leq j < 2^{|Y|}$. The subset $X' \subseteq X$ corresponding to i is obtained as follows. If $v \in X$ is the m^{th} smallest input vertex, then $v \in X'$ iff the m^{th} bit from the right in the binary expansion of i is 1. Similarly, the m^{th} largest output vertex is in Y' iff the m^{th} bit from the right in j is 1. And $Z = X' \cup Y'$.

A *matchcircuit* is a way of combining matchgates using what are called connecting edges. Informally, all inputs/outputs of constituent matchgates have an external edge. The external edges are connected to each other with an odd number of connecting edges. The matchgates are arranged in a layered fashion from left to right where the connecting edges separate these layers. Figure 3 shows a typical matchcircuit. We refer the reader to [14] for a more formal definition. The character of a matchcircuit is defined in the same way as the character of a matchgate except that there is no modifier μ as we do not consider the matchcircuit itself to have any external edges. Another difference is that 1 and 0 have opposite meanings with respect to deletion of external nodes in matchgates and matchcircuits.

2.4 Matchgate Identities

Character matrices of matchgates satisfy a rich set of algebraic constraints called *matchgate identities*. Valiant already derived a number of these identities in [15]. In our paper [5] we derived a complete set of algebraic identities using the so-called useful Grassmann-Plücker identities. Due to space limitation we will only describe these for 4×4 character matrices B.

Denote by $D(ij, kl) = \begin{vmatrix} B_{ik} & B_{il} \\ B_{jk} & B_{jl} \end{vmatrix}$, the 2×2 minor of B consisting of rows i and j, and columns k and l. Let S denote the set of $\binom{4}{2}$ unordered pairs of $\{1, 2, 3, 4\}$, $S = \{\{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}\}$. Define an involution σ on S which exchanges the pair $\{1, 4\}$ and $\{2, 3\}$, and leaves everything else fixed. Then it is proved in [5] that B is a character matrix iff the following set of identities hold:

$$D(p, q) = D(\sigma(p), \sigma(q)),$$

for any $(p, q) \in S \times S$. E.g., $B_{11}B_{44} - B_{14}B_{41} = B_{22}B_{33} - B_{23}B_{32}$ and $B_{12}B_{43} - B_{13}B_{42} = B_{21}B_{34} - B_{24}B_{31}$, etc.

Theorem 2.2. *[5] Let B be a 4×4 matrix over a field F. It satisfies the above set of matchgate identities (there are ten non-trivial identities) iff there exists a matchgate Γ such that $\chi(\Gamma) = B$.*

Theorem 2.3. *[5] There is an effectively constructible set of matchgate identities which completely characterizes any k input l output matchgate.*

The matchgate identities have far reaching implications. On the positive side, the proof in [5] indicates that whenever B is a $2^k \times 2^l$ character matrix there is a matchgate Γ of size $O(k+l)$ realizing it, thus it can be found in a bounded search. On the negative side, the complete characterization provides us with the tools to prove non-existence for general parameters k and l.

2.5 Planar matchgates and matchgrids

When the weighted graph $G = (V, E, W)$ is planar, we have a *planar matchgate* $\Gamma = (G, X, Y)$. We assume a planar embedding of G is given, where counter-clock wise one encounters vertices of the input nodes X, labeled $1, \ldots, |X|$ and then the output nodes Y, labeled $|Y|, \ldots, 1$.

In contrast to characters, a planar matchgate is assigned a *signature* matrix. Let $\text{PerfMatch}(G) = \sum_M \prod_{(i,j) \in M} w_{ij}$, where the sum is over all perfect matchings M. The *standard signature*, $u = u(\Gamma)$, is defined to be a $2^{|X|} \times 2^{|Y|}$ matrix whose entries are indexed by subsets $X' \subseteq X$ and $Y' \subseteq Y$, and the entry indexed by (X', Y') is $\text{PerfMatch}(G - Z)$, where $Z = X' \cup Y'$. Here $G - Z$ denotes the subgraph of G obtained by removing the subset of nodes in Z (and all their incident edges). We also permit omittable nodes on the outer face of a matchgate, and use $\text{MatchSum}(G)$ to define signature entries. Here $\text{MatchSum}(G) = \sum_{M'} \prod_{i \notin M'} \lambda_i \prod_{(i,j) \in M'} w_{ij}$, where the sum is over all (not necessarily perfect) matchings M', and $\lambda_i = 1$ for omittable i, and 0 otherwise. When all omittable nodes are on the outer face, $\text{MatchSum}(G)$ can be evaluated in P, using the FKT method [10].

Matchgates with only output nodes are called *generators*. Matchgates with only input nodes are called *recognizers*. More generally, with both input and output nodes a matchgate is called a *transducer*. We note that the standard signature of a generator is a row vector and the standard signature of a recognizer is a column vector.

Let $\mathbf{b}$ denote the standard basis for two dimensional space, $\mathbf{b} = [e_0, e_1] = [(1, 0), (0, 1)]$. Consider another basis $\boldsymbol{\beta} = [n, p] = [(n_0, n_1), (p_0, p_1)]$. Let $T = \begin{bmatrix} n_0 & n_1 \\ p_0 & p_1 \end{bmatrix}$.

Let Γ be a generator with m output nodes. Then by definition its standard signature $u = u(\Gamma)$ is a 2^m-vector. The *signature of this generator with respect to the basis* $\boldsymbol{\beta}$ is a row vector of dimension 2^m, denoted as $\text{valG}(\Gamma)$, or u_β, such that

$$u = u_\beta T^{\otimes m},$$

where $T^{\otimes m}$ denotes the m-fold tensor product of T.

Similarly let Γ' be a recognizer with m input nodes. The *signature of this recognizer with respect to the basis* $\boldsymbol{\beta}$ is a column vector of dimension 2^m, denoted as $\text{valR}(\Gamma')$, or u_β, such that (cf. [4])

$$u_\beta = T^{\otimes m} u,$$

If a signature has the same value at entries indexed by subsets of equal cardinality, then we abbreviate the 2^m-vector by a *symmetric signature* $[\sigma_0, \sigma_1, \ldots, \sigma_m]$.

Next, a *matchgrid* $\Omega = (A, B, C)$ is defined to be a weighted planar graph consisting of a disjoint union of: a set of g generators $A = (A_1, \ldots, A_g)$, a set of r recognizers $B = (B_1, \ldots, B_r)$, and a set of f connecting edges $C = (C_1, \ldots, C_f)$, where each C_i edge has weight 1 and joins an output node of a generator with a input node of a recognizer, so that every input and output node in every constituent matchgate has exactly one such incident connecting edge. (If omittable nodes are present they must be on the outer face.)

Now we come to the central definition of the theory of holographic algorithms —the Holant.

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

The following Holant Theorem says that the Holant can be efficiently computed.

Theorem 2.4 (Valiant)**.** *For any matchgrid Ω over any basis $\boldsymbol{\beta}$, let G be its underlying weighted graph, then*

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

3 An Equivalence Between Matchcircuits and Planar Matchgrids

3.1 Naked characters

In [5], we showed that the set of *useful* Grassmann-Plücker identities gives a complete characterization of matchgate characters, i.e., every character matrix satisfies these equations and any matrix satisfying these is the character of some matchgate. A *useful* Grassmann-Plücker identity is derived from a Grassmann-Plücker identity on (I, J), where I and $J \subseteq V$ are subsets of nodes of the matchgate containing all internal nodes. We refer to [5] for details. For convenience of proof, we also define a *naked character* as a character without the modifiers. Thus, the entries of the *naked character* of a k-input, l-output matchgate is simply $\text{PfS}(G - Z)$ where Z varies over subsets of $X \cup Y$ (see 2.3). Since the modifier $\mu(Z)$ does not depend on the internal nodes, the useful Grassmann-Plücker identities can be considered as identities over the entries of the naked character matrix. These identities completely characterize the naked character matrices of matchgates.

3.2 Equivalence of matchgates and planar matchgates

In this subsection, we prove a surprising equivalence between matchgates (which are generally not planar) and planar matchgates. Specifically, we can show that the set of naked character matrices of k-input, l-output matchgates is the same as the set of signature matrices of k-input, l-output planar matchgates. This theorem has remarkable implications. In particular, it implies that the set of matchgate identities (for naked characters) also characterize all signature matrices. With this we obtain a complete algebraic characterization of planar matchgates. This will enable us to prove some impossibility results.

Lemma 3.1. *Given a matchgate Γ with naked character matrix B, there exists a planar matchgate Γ' with signature B.*

Proof. Recall that the vertices of Γ are numbered 1 through n with the first k being inputs and the last l being outputs. Now arrange the vertices (with their edges) on a *strictly convex* curve, e.g., a upper semicircle, such that as we move clockwise from vertex 1, we encounter all the vertices in increasing order (see Figure 1). By doing this, we have achieved the following: Any two edges (i, j) and (k, l) overlap (i.e. $i < k < j < l$ or $k < i < l < j$) *iff* they physically cross each other as two straight line segments. If any such pair of overlapping edges is present in a matching, it introduces a negative sign to the Pfaffian. Now we can convert this graph into a planar graph by using the gadget given in Figure 2. We will replace any physical crossing by a *local* copy of the gadget. We then use the properties of this gadget proved in Proposition 6.3 of [16]. We omit the details, but it can be shown that the MatchSum polynomial of the new graph is the same as the Pfaffian Sum of the original graph. It follows that the signature of this planar graph is the same as the character of Γ except that the signature doesn't consider any external edges and hence, it doesn't have any modifiers. This means that the signature is actually equal to the naked character B. Note that, in this construction, if omittable nodes are present, they are now all on the outer face (in fact all the original nodes of Γ are now on the outer face). $\square$

Lemma 3.2. *Given a planar matchgate Γ with signature u, there is a matchgate Γ' with naked character equal to u.*

Proof. The underlying graph of Γ' is the same as that of Γ but we'll change the weights suitably. For that, we have to consider the orientation given to edges by the FKT algorithm to count the number of perfect matchings as described in [10]. For any edge (i, j) where $i < j$, if the direction assigned to it is i to j, then we keep the weight as is, otherwise we multiply the weight by a -1. The matrix whose Pfaffian we evaluate to count the number of perfect matchings in Γ is exactly the same as the (skew-symmetric) adjacency matrix of the new graph. That means that its character, after dropping the modifiers μ, is the same as the signature of Γ.

If omittable nodes are present, we need to evaluate MatchSum. Since the omittable nodes are all on the outer face, one single consistent orientation can be chosen for all edges, as the result of FKT algorithm, simultaneously for all terms of MatchSum. This reduces to a Pfaffian Sum. $\square$

Lemmas 3.1 and 3.2 prove the following theorem.

Theorem 3.1. *The set of signature matrices of planar matchgates is the same as the set of naked character matrices of matchgates.*

3.3 Equivalence of matchcircuits and planar matchgrids

We can now prove that matchcircuits and planar matchgrids are computationally equivalent. To make this meaningful, matchgrids must be generalized to have inputs and outputs. Previously every input/output node of a matchgate is required to be incident to exactly one connecting edge (to another matchgate). Now for some input/output nodes of some matchgates, we allow them to be *free*, i.e. not incident to any connecting edge, if that input/output is on the outer face of the matchgrid. These are the input/output nodes of the matchgrid. We also require that if we move in clockwise direction from some vertex on the outer face of a planar matchgrid, we first encounter all the free input nodes, perhaps interspersed with some internal nodes, then the free output nodes. Now we can define the *signature* matrix of a matchgrid where each entry is the PerfMatch polynomial (or MatchSum, if omittable nodes are present) of the graph obtained by deleting a subset of the free inputs and outputs (see 2.5).

Every theorem in [14] on matchcircuits has a formulation in the theory of planar matchgrids with signatures. For instance, the Matchcircuit Theorem can be stated as

Theorem 3.2. *For any matchcircuit Γ, there is a polynomial time computable transformation to a planar matchgrid Ω with graph G, where each matchgate Γ_i in Γ is replaced by a planar matchgate Γ_i' whose signature is equal to the naked character of Γ_i. In addition, there are a polynomial number of cross-over planar matchgates.*

$$\mathrm{MatchSum}(G) = \sum_S \epsilon_S \prod_i \mathrm{MatchSum}(\Gamma_i' - S_i),$$

where S runs through all choices of assigning every input/output node of all Γ_i' to be matched by an edge internal or external to the matchgate, S_i is the set of externally matched nodes of Γ_i' by S, and $\epsilon_S = \pm 1$ depending only on S and not on the internal matchings of each matchgate.

Proof. Recall that the Matchcircuit theorem in [14] states that

$$\mathrm{PfS}(\Gamma) = \sum_S \epsilon_S \prod_i \mathrm{PfS}(\Gamma_i - S_i).$$

The construction of Ω from Γ is similar to the one in the proof of Lemma 3.1. We arrange the vertices (with their edges) on a *strictly convex* curve, e.g., an upper semicircle, such that as we move clockwise from vertex 1, we encounter all the vertices in increasing order (see Figure 4). Again, we replace any physical crossing by a *local* copy of the gadget in Figure 2. Following the same argument as before, it can be shown that the MatchSum polynomial of the new graph is the same as the Pfaffian Sum of the original graph: $\mathrm{MatchSum}(G) = \mathrm{PfS}(\Gamma)$.

Now we analyze what happens to any matchgate Γ_i which was part of the matchcircuit Γ. Note that, by definition, the vertices of Γ are numbered in such a way that the numbers of the vertices of Γ_i are contiguous. Therefore, these vertices are (physically) contiguous in G, in the sense that as we move in clockwise direction from the first vertex of Γ_i to its last vertex, we encounter only the vertices of Γ_i. These vertices and any new ones introduced with the gadgets used to replace crossings between edges among them (vertices of Γ_i) now form a planar graph, say H_i. The planar matchgate Γ_i' formed by H_i is the same as what we would have obtained by applying the construction in Lemma 3.1 to Γ_i. In particular, the naked character of Γ_i is the same as the signature of Γ_i'. Hence, $\forall S, \mathrm{MatchSum}(\Gamma_i' - S_i) = \mathrm{PfS}(\Gamma_i - S_i)$. The theorem now follows from the Matchcircuit theorem of [14]. ☐

If the matchgates Γ_i are of the restriction stipulated in the Main Theorem in [14], then all $\epsilon_S = 1$ and we obtain a classical simulation of the same fragment of quantum computation by planar matchgrids.

Theorem 3.3. *The same fragment of quantum computation that was simulated by matchcircuits in [14] can be simulated by matchgrids.*

Conversely,

Theorem 3.4. *Given a planar matchgrid Ω, there is a matchcircuit Γ such that the signature of Ω is equal to the character of Γ.*

Proof. Here is the process to convert from a matchgrid to a matchcircuit. First, number the vertices of this graph in some arbitrary way. For every free input/output, we add a set of two new vertices with an edge between them. We connect one of these new vertices to the free input/output and the other new vertex is the new input/output as shown in Figure 5. All the newly added vertices are such that they lie on the outer face. All the newly added edges have weight 1. Let's call this new graph G'. We number the newly added vertices in such a way that they are ordered from left to right as shown in Figure 5. In particular, the new inputs and their adjacent nodes have numbers lower than any node of Ω whereas the new outputs and their adjacent nodes have higher numbers. The signature of G' is the same as the signature of Ω. Now we use FKT to change the weights of the edges of G' suitably, as in Lemma 3.2 to obtain a graph G'' such that the signature of G' is the same as the naked character of G''. G'' has the structure of a matchcircuit composed of only one matchgate. The naked character of a matchcircuit is the same as its character since a matchcircuit has no external edges and its character has no modifiers. Therefore, G'' is our matchcircuit Γ with the same character as the signature of the planar matchgrid Ω. ☐

4 Simultaneous Node-Edge Deletion

In this section we give a holographic algorithm for a simultaneous node-edge deletion problem. This is the first poly-time algorithm for this problem. The problem is a generalization of the PL-NODE-BIPARTITION problem for which the first polynomial time algorithm was given by Valiant [16]. It also generalizes the planar edge deletion problem, which is the same as MAX-CUT. Planar MAX-CUT is known to be in P [6]. We note that the closely related problem of Planar-Max-Bisection (where a bisection is a cut with two equal parts) was a long standing open problem till Jerrum proved it NP-hard (see [7]). There has also been important progress on its approximability [7]. We also note that the status of Planar-Min-Bisection remains open.

PL-NODE-EDGE-BIPARTITION

Input: A planar graph $G = (V, E)$ of maximum degree 3. A non-negative integer $k \leq |V|$. **Output:** The minimal l such that deletion of at most k nodes (including all of their incident edges) and l more edges results in a bipartite graph.

Theorem 4.1. *There is a polynomial time algorithm for PL-NODE-EDGE-BIPARTITION.*

Proof. We will use the method of holographic algorithms [16]. Let the given input graph be G. First, note that we can simply delete any node of degree 1. We will replace each remaining nodes by recognizers with symmetric signature $[1, x, x, 1]$ or $[1, x, 1]$ depending on their degree. The edges will be replaced by generators with symmetric signature $[y, 1, y]$. This forms a matchgrid Ω. It is known that the above symmetric signatures are realizable in the Hadamard basis $\mathbf{b2} = [n, p] = [(1, 1), (1, -1)]$. (See [16] and also Section 6.) Every term in the Holant corresponds to an assignment of n or p to each end of every connecting edge in Ω. This induces an assignment on the vertices of G. We consider vertices in G that get nnn or nn (depending on the degree) are colored white and those that get ppp or pp are colored black. The remaining vertices are not colored. Now, every colored node contributes 1 to the Holant and every uncolored node contributes x. Any edge that is assigned nn or pp contributes y and any edge that is assigned np or pn contributes 1. It is clear that we can obtain a bipartite graph by deleting the uncolored vertices and the edges that are assigned nn or pp. We define

$$\begin{aligned} \ell(k) &= \min\{\ l' \mid \text{The coefficient of } x^k y^{l'} \text{ in Holant is non-zero.}\} \\ l(k) &= \min\{\ l' \mid \exists \text{ a subset } S \subseteq V \text{ of size } k \text{ and some } l' \text{ edges in } G - S \text{ such that} \\ &\qquad \text{removal of the } l' \text{ edges from } G - S \text{ gives a bipartite graph.}\} \end{aligned}$$

Claim 1. $l(k) \leq \ell(k)$.

This follows from our discussion earlier.

Claim 2. $l(k)$ *is a strictly monotonic decreasing in* k*, until* $l(k) = 0$.

Proof. Let $k' < k$. We show that if $l(k') > 0$, then $l(k') > l(k)$. Let $S \subseteq V$ be a subset of size k', such that the deletion of S and some $l(k')$ edges from $G - S$ results in a bipartite graph. Then, if we are allowed to delete $k > k'$ vertices, we can choose to delete S and some of the vertices to which the other $l(k')$ edges are incident. Then, clearly, $l(k) < l(k')$. ☐

Claim 3. $\ell(k) \leq l(k)$

Proof. Let $S \subseteq V$ be a subset of size k such that the deletion of S and some $l(k)$ other edges results in a bipartite graph. Assign nnn or nn to the vertices on the left and ppp or pp to those on the right. This means that for a connecting edge incident to a recognizer for a node on the left, we assign n to its end which is incident to it. Similarly for a connecting edge incident to a recognizer for a node on the right we assign p there. The generator corresponding to any edge present in the bipartite graph gets np or pn and the $l(k)$ deleted edges get nn or pp, due to the minimality of $l(k)$. The remaining edges can be of three types: having one end point on the left side and one in S, having one end point on the right and one in S, or having both end points in S. The generators corresponding to all these edges are given *np* or *pn* in such a way that any output adjacent to a recognizer on the left gets n and any output adjacent to a recognizer on the right gets p. This can be done, since the remaining edges have at least on end point in S, we have at least one *free* output.

It is easy to see that the degree of y in this term of the Holant is exactly $l(k)$. Note that all the vertices not in S are assigned *nnn* or *ppp* (or *nn* or *pp*) and contribute 1 to the Holant. We further claim that no vertex in S gets *nnn* or *ppp* (or *nn* or *pp*). Hence the coefficient of $x^k y^{l(k)}$ is positive, and therefore $\ell(k) \leq l(k)$. If some vertex in S were to get *nnn* or *ppp* (or *nn* or *pp*), we can add those vertices and their incident edges to the bipartite graph, and we will still have a bipartite graph, since all the edges incident to any vertex in S are assigned either *np* or *pn*. This means that for some $k' < k$, $l(k') \leq l(k)$ which is impossible, by Claim 2. □

The proof of the theorem is now easy. The required value is $l = l(k)$. As $l(k) = \ell(k)$, we can find this by computing the Holant, which is a polynomial in x and y of degree at most $|V| + |E|$. This is done by evaluating Holant at several values of x and y, and then by polynomial interpolation. Note that, since every term in the Holant contributes either a one or a zero to the coefficient of at most one term in the polynomial, the coefficients are bounded by $2^{2|E|}$, i.e., $O(|E|)$ bits. □

Valiant's PL-NODE-BIPARTITION [16] asks for the minimal k such that $l(k) = 0$, while PL-EDGE-BIPARTITION (Planar MAX-CUT for degree ≤ 3) [6] asks for $l(0)$. This problem generalizes both.

5 Limitations of Holographic Algorithms

There is not yet any formal definition of what is computable by holographic algorithms. In this section, we try to define the most basic kinds of holographic algorithms and call these *holographic templates*. The aim is to capture essentially what is computable by using only the Holant and nearly no other meaningful polynomial time computation. Then we look at some generalizations of two of the problems solved by Valiant using holographic algorithms in [16]. We show that there are no holographic templates for these generalizations. To make the impossibility results more meaningful, we will also need a formal definition of the types of problems to which holographic templates can possibly be applied. The formal definition of such problems and of holographic templates is presented in the Appendix. The definition captures the notion that local solution fragments of a counting problem are mapped to the non-zero entries in the signature of planar matchgates in such a way that the Holant of the matchcircuit is equal to the answer of the counting problem. All of the holographic algorithms presented by Valiant can essentially be realized in this notion of holographic templates.

By our definition, if there is holographic template for a problem then the answer produced by it, i.e. the Holant of the holographic template, is the answer of the counting problem. Below we will show the non-existence of holographic template algorithms for some problems. We will only consider holographic templates using planar matchgates and matchgrids without omittable nodes. The impossibility results will be achieved by showing that there are no bases in which there are recognizers and generators having some required signatures. Suppose we need to find a basis and some generators/recognizers with given signatures w.r.t. the basis. We first translate the signature into standard signatures. The entries of the standard signature will be in terms of the basis vectors. We will then use our algebraic equations that completely characterize the signature matrices of planar matchgates. These include the parity constraints and the matchgate identities. By parity constraints, we mean the constraint that for any standard signature, either all terms corresponding to deletion of an odd number of nodes are zero or all terms corresponding to deletion of even number of nodes are zero. This is a consequence of perfect matchings. For a number of problems, we will be able to show that there are no bases for which the standard signature satisfies all these constraints, thus concluding that these problems cannot be solved by this method.

Before moving on, we note that if a basis $\boldsymbol{\beta}$ consists of only two linearly dependent two-dimensional vectors, then the span of any higher tensor $\boldsymbol{\beta}^{\otimes \boldsymbol{f}}$ will also be one-dimensional and thus ruling out any interesting signatures from being in its span. So for the problems we consider, we will only look for linearly independent bases without explicitly proving that any linearly dependent basis of two vectors doesn't work.

#X-Matchings

One problem solved by Valiant by a holographic algorithm [16] is called #X-Matchings. This is motivated by its proximity to counting the number of (not necessarily perfect) matchings in a planar graph, which was proved to be #P-complete by Jerrum [8]. Vadhan [13] subsequently proved that it remains #P-complete for planar bipartite graphs of degree 6. For degree two the problem can be easily solved. For Valiant's #X-Matchings, a planar bipartite graphs $G = (V, E, W)$ is given with bipartition $V = V_1 \cup V_2$, where nodes in V_1 have degree 2 and nodes in V_2 have arbitrary degrees. The problem is to compute $\sum_M m(M)$, where M runs through all (not necessarily perfect) matchings, and the mass $m(M)$ is the product of (1) weights of $e \in M$ and (2) the quantity $-(w_1 + \ldots + w_k)$ for each unmatched node in V_2, where w_i are the weights of edges incident to that node. One can use this to compute the total number of matchings mod 5, if all vertices in V_2 have degree 4.

Still, the quantity $-(w_1+\ldots+w_k)$ seems artificial. If one were to be able to replace $-(w_1+\ldots+w_k)$ by 1, then one would be able to count all (not necessarily perfect) matchings in such planar bipartite graphs. However, we prove that this is impossible using holographic templates.

Theorem 5.1. *There is no holographic template using any basis of two linearly independent vectors to solve the counting problem for all (not necessarily perfect) matchings for such graphs, which is the same as the above problem with $-(w_1 + \ldots + w_k)$ replaced by 1.*

The proof uses our characterizations of realizability of matchgates and the equivalence theorems on characters and signatures. Due to space limitations the details are in the Appendix.

Several other problems solved by Valiant in [16] use a matchgate with a symmetric signature which is logically a Not-All-Equal gate. This is typified by the following problem:

#PL-3-NAE-ICE

Input: A planar graph $G = (V, E)$ of maximum degree 3.
Output: The number of orientations such that no node has all edges directed towards it or away from it.

If one were to relax the degree bound $k = 3$, some of his problems [16] are known to be NP-hard. We prove that for any $k > 3$, one can not realize a Not-All-Equal by a symmetric signature.

Theorem 5.2. *There is no holographic template using any basis of two linearly independent vectors to solve the above ICE problem if we replace the degree bound by any $k > 3$.*

Again the proof uses our characterizations including matchgate identities, and is in the Appendix. As the proof deals with the non-existence of certain matchgates of prescribed signatures, this is applicable to other problems in addition to #PL-3-NAE-ICE.

6 Symmetric Signatures in b2

The most versatile basis in the design of holographic algorithms so far has been the Hadamard basis **b2**, namely $[n, p] = [(1, 1), (1, -1)]$. In [16], most often, it is used to realize a symmetric signature that has a clear Boolean logical meaning, such as the Not-All-Equal function. In this section, we give a complete characterization of all the symmetric signatures that can be realized by some generators or recognizers (having no omittable nodes) in this basis.

Let T denote the matrix $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. T is symmetric and non-singular, and therefore $T^{\otimes n}$ is a symmetric non-singular $2^n \times 2^n$ matrix. It follows that for **b2**, realizability for a recognizer is the same as for a generator.

The Hamming weight of a row or column index to $T^{\otimes n}$, which is a 0-1 vector in binary representation, is the number of 1's in it. Suppose we have a generator having standard signature u and signature u_{b2} under **b2**. We claim that u_{b2} is a symmetric signature iff u is. Since $T^{-1} = \frac{1}{2}T$, we only need to show this in one direction.

Row vectors u and u_{b2} are related by $u = u_{b2}T^{\otimes n}$ (see 2.5). Suppose u_{b2} is a symmetric signature. We sum the rows of equal Hamming weight in $T^{\otimes n}$ to obtain an $(n + 1) \times 2^n$ matrix M. It is clear that M has a full row rank because any linear combination of rows of M is a linear combination of rows of $T^{\otimes n}$, which is non-singular. It can be seen that any two columns of M having indices of the same Hamming weight are equal. So M has at most $n + 1$ distinct columns. Thus u is also symmetric. And since the rank of M is $n + 1$, there must be exactly $n + 1$ distinct columns, and they are linearly independent. Consider the $(n + 1) \times (n + 1)$ matrix $A = [a_{ij}]$ obtained by taking the distinct columns from M. A is non-singular.

In fact, these a_{ij} can be expressed by the Krawtchouk polynomials [11].

Lemma 6.1. $a_{ij} = \sum_{k=0}^{i}(-1)^k \binom{j}{k}\binom{n-j}{i-k}$. *In particular,* $a_{ij} = (-1)^i a_{i,n-j} = (-1)^j a_{n-i,j}$.

Theorem 6.1. *A symmetric signature* $[x_0, x_1, \ldots, x_n]$ *is realizable under the Hadamard basis b2 iff it takes the following form: There exist (arbitrary) constants* λ, s, t *and* ϵ *where* $\epsilon = \pm 1$*, such that for all* $0 \le i \le n/2$,

$$x_i = \lambda\left((s + t)^{n-i}(s - t)^i + \epsilon(s - t)^{n-i}(s + t)^i\right).$$

and $x_{n-i} = \epsilon x_i$.

The proof uses the properties of the Krawtchouk polynomials and matchgate identities. It is in the Appendix.

7 Conclusions and Future Work

In this paper, we have substantially developed the theory of matchcircuit and matchgrid computations, uniting the two in expressibility. Building on the structural theory, we also derived some results on holographic algorithms, some positive and some negative. We have also defined the notion of holographic templates to capture a substantial part of holographic algorithms. It is still premature to speculate on the ultimate capability of all the holographic algorithms. It seems more tractable to prove this for holographic templates. Linear bases with more than two basis vectors or linearly dependent bases have not been investigated. They have proved to be useful in some problems solved by holographic algorithms in polynomial time. We have achieved a complete understanding of symmetric signatures under the Hadamard basis. However this is only restricted to the Hadamard basis. It is plausible that we can characterize this for other bases. A systematic exploration of non-symmetric signatures seems still out of reach.

Acknowledgments

We would like to thank Leslie Valiant for very encouraging comments and discussions, especially while both he and the first author visited Beijing. We want to thank Eric Bach for his many insightful comments. We also thank Andrew Yao, and his group of students in Tsinghua University, for listening to the lectures by the first author on some of this material. We also thank in particular Rakesh Kumar and Anand Kumar Sinha for many interesting discussions on this and related topics.

References

[1] A. C. Aitken. Determinants and Matrices, Oliver and Boyd, London, 1951.

[2] R. A. Brualdi, H. J. Ryser. Combinatorial Matrix Theory, Cambridge University Press, Cambridge, 1991.

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

[4] Jin-Yi Cai, V. Choudhary. Valiant's Holant Theorem and Matchgate Tensors. To appear in the Proceedings of *Theory and Applications of Models of Computation*, TAMC 2006. Lecture Notes in Computer Science. Springer. Also available at Electronic Colloquium on Computational Complexity, Report TR05-118.

[5] Jin-Yi Cai, V. Choudhary. On the Theory of Matchgate Computations. *Submitted*. Also available at Electronic Colloquium on Computational Complexity, Report TR06-018.

[6] F. Hadlock. Finding a Maximum Cut of a Planar Graph in Polynomial Time. *SIAM Journal on Computing*, 4 (1975): 221-225.

[7] K. Jansen, M. Karpinski, A. Lingas, and E. Seidel. Polynomial Time Approximation Schemes for MAX-BISECTION on Planar and Geometric Graphs. *Proceedings of 18th Symposium on Theoretical Aspects in Computer Science (STACS) 2001*, LNCS 2010: 365-375, Springer (2001).

[8] M. R. Jerrum. Two-dimensional Monomer-Dimer Systems are Computationally Intractable. *Journal of Statistical Physics*, 48, 1/2: 121-134 (1987). (Also 59, 3/4: 1087-1088 (1990)).

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

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

[11] F. MacWilliams and N. Sloane, The Theory of Error-Correcting Codes, NorthHolland, Amsterdam, p. 309, 1977.

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

[13] S. P. Vadhan. The Complexity of Counting in Sparse, Regular and Planar Graphs. *SIAM Journal on Computing*, 8(1): 398-427 (2001).

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

[15] L. G. Valiant. Expressiveness of Matchgates. *Theoretical Computer Science*, 281(1): 457-471 (2002). See also 299: 795 (2003).

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

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

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

Appendix

Definition of Holographic Templates

Here we try to define formally the most basic kinds of holographic algorithms. We call these holographic templates. First we define the type of counting problems to which these algorithms can be applied. These include essentially all the problems discussed by Valiant [16], and therefore we call them *Valiant Counting Problems*. Some of his problems, such as planar Boolean formula problems, may not be directly presented as such; but they can all be easily and isomorphically expressed in this way by an obvious transformation.

Definition 8.1. *A* **Valiant Counting Problem** *is a counting problem with the following structure.*

- *A planar graph $G(V, E)$.*
- *A set of states S_1 for the vertices and another set of states S_2 for the edges.*
- *Every vertex can be in one of the states in S_1, i.e., an assignment assigns for every vertex $v \in V$ a state $s_v \in S_1$.*
- *Every edge can be in one of the states in S_2, i.e., an assignment assigns for every edge $e \in E$ a state $s_e \in S_2$.*
- *A* local acceptance criterion *ϕ to decide whether a given assignment of states to the vertices and edges is valid. By* local, *we mean that we can decide whether the state given to a vertex/edge is acceptable, simply by looking at the states given to the neighboring vertices and incident edges: For a vertex of degree k, we have a map $\phi : S_1 \times S_2^k \to \{0, 1\}$.*
- *Any vertex or edge in a valid state contributes a factor $f(s_v)$ or $g(s_e)$ to the* mass *of the assignment. The mass of a valid assignment is the product of the factors of all the vertices and edges.*
- *The problem is to count the total mass of all valid assignments of states to the vertices and edges.*

Now we present the definition of holographic templates.

Definition 8.2. Holographic Template*: Given a Valiant counting problem, as defined above, any holographic template to solve the problem is required to have the following structure.*

- *We have a basis $\boldsymbol{\beta}$.*

- *Every vertex v is replaced by a generator (or a recognizer) depending upon the state set S_1 and its degree. The generator has the same number of outputs as the degree of v.*
- *Every edge $e = (v_1, v_2)$ is replaced by a recognizer (or a generator) depending upon the state set S_2. The recognizer has two inputs, one of which is connected to an output of the generator for v_1 and the other to an output of the generator for v_2.*
- *Every assignment of basis elements in $\boldsymbol{\beta}$ to the external nodes of the generators or recognizers corresponds to a state of the vertex or edge. Consider an assignment $x \in \boldsymbol{\beta}^{\otimes k}$ to the external nodes of a generator Γ with k inputs. Suppose x corresponds to a state s, then $valG(\Gamma, x) = f(s)$. The same holds for the recognizers.*
- *If x is an invalid assignment to the connecting edges, then the term in the Holant corresponding to x is zero.*

It is clear that, by this definition, the Holant of a holographic template is the solution to the corresponding Valiant counting problem, as every term of the Holant is simply equal to the mass of the appropriate assignment.

Proof of Theorem 5.1

We consider a variant of the #X-Matchings problem where we drop the factor $-(w_1 + \ldots + w_k)$ for any unmatched V_2 node from the mass of a matching. This becomes the counting problem for all (not necessarily perfect) matchings for such graphs. We'll show that this problem cannot be solved by any holographic template with any basis of two linearly independent vectors. Specifically, replace each node on the left by a generator (or recognizer) with two external nodes and replace each node on the right of degree k by a recognizer (or generator) with k external nodes. Furthermore, we have to find a basis $\boldsymbol{\beta} = [n, p]$ such that the signature of the generator w.r.t. $\boldsymbol{\beta}$ is $(1, 1, 1, 0)$ and the signature w.r.t. $\boldsymbol{\beta}$ of a recognizer with k external nodes takes value 1 at $n \otimes \ldots \otimes n$, takes value w_i at $x_1 \otimes \ldots \otimes x_k$ where it has exactly one p at the i th place, namely, $x_i = p$, and $\forall j \neq i, x_j = n$, and takes value 0 otherwise. Here $w_1, \ldots, w_k$ are the weights of the edges incident to the vertex which is to be replaced by that recognizer.

Theorem 8.1. *Given $k \geq 3$ and weights $w_1, \ldots, w_k$ where w_i's are not all zero. Then, for any linearly independent basis $\boldsymbol{\beta} = [n, p]$ such that there are generators and recognizers with the following properties,*

- *A generator having two external nodes whose signature w.r.t. $\boldsymbol{\beta}$ is $(1, 1, 1, 0)$.*
- *A recognizer Γ having k external nodes with $valR(\Gamma, x_1 \otimes \ldots \otimes x_k)$ equal to*

  a. 1, if $x_1 = \ldots = x_k = n$;

  b. w_i, if $x_i = p$ and for every $j \neq i$, $x_j = n$; and

  c. 0, otherwise.

we have, $w_1 + \ldots + w_k = -1$.

Thus, the quantity in (a.) has to be $-(w_1 + \ldots + w_k)$.

Proof. Let $\boldsymbol{\beta} = [n, p]$ be a linearly independent basis, where $n = (n_0, n_1), p = (p_0, p_1)$. Suppose that a generator Γ' and a recognizer Γ as stated in the theorem exist. The generator signature w.r.t. $\boldsymbol{\beta}$ is $(1, 1, 1, 0)$, i.e., its standard signature can be written as

$$n \otimes n + n \otimes p + p \otimes n = (n_0^2 + 2n_0p_0, n_0n_1 + n_0p_1 + n_1p_0, n_0n_1 + n_0p_1 + n_1p_0, n_1^2 + 2n_1p_1).$$

As the matchgate Γ' is either even or odd without omittable nodes, the parity requirements on the standard signature imply that either

$$n_0^2 + 2n_0p_0 = 0 \quad (1)$$
$$n_1^2 + 2n_1p_1 = 0 \quad (2)$$

or

$$n_0n_1 + n_0p_1 + n_1p_0 = 0 \quad (3)$$

In the first case, from (1), $n_0 = 0$ or $n_0 = -2p_0$. From (2), $n_1 = 0$ or $n_1 = -2p_1$. Since the basis $\boldsymbol{\beta}$ is linearly independent, either $n_0 = 0 \wedge n_1 = -2p_1$ or $n_1 = 0 \wedge n_0 = -2p_0$. By Proposition 4.3 in [16], we need to consider only one of these. So let's assume $n_0 = 0$ and $n_1 = -2p_1 \neq 0$. Let $Z = \{1, \dots, k\}$ denote the k external nodes of the recognizer Γ, and let u be its standard signature. As stated in Section 2.5, the signature entries in valR(Γ) are inner products of the standard signature u with various basis elements in the tensor product space $\boldsymbol{\beta}^{\otimes k}$. In particular, $\langle u, n^{\otimes k}\rangle = 1$ and $\langle u, p \otimes n^{\otimes(k-1)}\rangle = w_1$, etc. Therefore,

$$\begin{aligned} u_Z &= \frac{1}{n_1^k} \qquad \text{and} \\ \text{For every } i,\ 1 \leq i \leq k: \qquad u_{Z-\{i\}} &= \frac{w_i + 1/2}{p_0 n_1^{k-1}}, \end{aligned}$$

applying the last equation just obtained.

By parity requirements on the standard signature, since $u_Z \neq 0$, we get $u_{Z-\{i\}} = 0$, i.e. $w_i = -\frac{1}{2}$, for every i.

Now we look at the signature entries with two or three bits of the index zero. By parity requirements, for any $1 \leq i < j < l \leq k$, $u_{Z-\{i,j,l\}} = 0$.

$$\text{For every } i \text{ and } j,\ 1 \leq i < j \leq k: \qquad n_1^{k-2}(p_1^2 u_Z + 0 + p_0^2 u_{Z-\{i,j\}}) = 0$$

Here the zero term in the sum comes from $u_{Z-\{i\}} = 0$ for every i. This equation gives $u_{Z-\{i,j\}} = -\frac{p_1^2}{p_0^2 n_1^k}$. It shows that in particular it only depends on the cardinality of $Z - \{i,j\}$ being $k-2$, and not the particular i and j. Next,

$$\text{For every } i, j \text{ and } l,\ 1 \leq i < j < l \leq k: n_1^{k-3}(p_1^3 u_Z + 0 + p_0^2 p_1 (3u_{Z''}) + 0) = 0$$

where Z'' denotes a subset of cardinality $k-2$, and the zero terms in the sum come from parity requirement. These equations imply that $p_1 = 0$, which makes the basis $\boldsymbol{\beta}$ linearly dependent.

Now we are left with the other choice: (3) holds. First we consider what happens when some of the values n_0, n_1, p_0, p_1 are zero. Suppose $n_0 = 0$. This implies $n_1p_0 = 0$ which makes n and p linearly dependent. Similarly, $n_1 = 0$ implies $n_0p_1 = 0$ and again, n and p become linearly dependent. Therefore, we can assume that n_0 and n_1 are non-zero. Now suppose $p_1 = 0$. Then, $p_0 \neq 0$ and we get $n_0n_1 + n_1p_0 = 0$ and since $n_1 \neq 0$, it means $n_0 = -p_0 \neq 0$. By Proposition 4.3 in [16], we can do a simple change of scale, and assume $n = (-1, 1)$ and $p = (1, 0)$. (Note that this is Valiant's basis **b1** [16].) Let $u_{\boldsymbol{\beta}}$ be its signature of Γ w.r.t $\boldsymbol{\beta}$. Let M be the matrix $\begin{bmatrix} -1 & 1 \\ 1 & 0 \end{bmatrix}^{-1} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$. We have $u = M^{\otimes k} u_{\boldsymbol{\beta}}$ by Section 2.5. Note that $M^{\otimes k}$ expresses the function $\bigwedge_{i=1}^{k}(x_i \vee y_i)$ on 2 k-bit inputs x and y which index the rows and columns of $M^{\otimes k}$ respectively.

Consider u_Z and $u_{Z-\{i\}}$ for different values of i. Using this interpretation of $M^{\otimes k}$ as $\bigwedge_{i=1}^{k}(x_i \vee y_i)$, we have the following:

$$\begin{array}{rrcl} & u_Z & = & 1 + \sum_{i=1}^{k} w_i \\ \text{For every } i,\ 1 \le i \le k: & u_{Z-\{i\}} & = & w_i \end{array}$$

Since w_i's are not all zero, by the parity requirement, $u_Z = 0$. This forces $\sum_{i=1}^{k} w_i = -1$.

We next assume $p_1 \neq 0$. By Proposition 4.3 in [16], we may also assume $p_0 \neq 0$. Hence, from here on, we assume that all of n_0, n_1, p_0 and p_1 are non-zero. Now we'll need to change our notations slightly. Let M be the matrix $\begin{bmatrix} n_0 & n_1 \\ p_0 & p_1 \end{bmatrix}^{-1}$. Again by Proposition 4.3 from [16] we may assume the determinant of M is 1. Then $M = \begin{bmatrix} p_1 & -n_1 \\ -p_0 & n_0 \end{bmatrix}$. Denote by $a_0^0 = p_1$, $a_1^0 = -n_1$, $a_0^1 = -p_0$ and $a_1^1 = n_0$, then we can write M as simply $\begin{bmatrix} a_0^0 & a_1^0 \\ a_0^1 & a_1^1 \end{bmatrix}$. Eq. (3) translates to

$$a_0^0 a_1^1 + a_1^0 a_0^1 = a_1^0 a_1^1 \tag{4}$$

In the following, the tensor notation will be convenient (see [4] for details). We have $u = M^{\otimes k} u_\beta$. Then, for example, for the empty subset $\emptyset$, $u_\emptyset = \sum_{j_1 j_2 \ldots j_k} a^{0\,0\,\ldots\,0}_{j_1 j_2 \ldots j_k} u_{\boldsymbol{\beta}}^{j_1 j_2 \ldots j_k}$, where $a^{0\,0\,\ldots\,0}_{j_1 j_2 \ldots j_k} = a^0_{j_1} a^0_{j_2} \cdots a^0_{j_k}$. Of course, for the requisite $u_{\boldsymbol{\beta}}$, the only non-zero terms among $u_{\boldsymbol{\beta}}^{j_1 j_2 \ldots j_k}$ are for $j_1 j_2 \ldots j_k$ of Hamming weight ≤ 1.

We have two cases to consider.

Case 1. k is odd.

First assume that the recognizer Γ is an odd matchgate. So entries in the standard signature corresponding to even cardinality subsets of external nodes being deleted are all zero. Consider the empty subset $\emptyset$. By $u = M^{\otimes k} u_{\boldsymbol{\beta}}$ we have,

$$u_\emptyset = (a_0^0)^k \cdot 1 + (a_0^0)^{k-1} a_1^0 w_1 + (a_0^0)^{k-1} a_1^0 w_2 + \ldots + (a_0^0)^{k-1} a_1^0 w_k = 0 \tag{5}$$

Let $S = \sum_{i=1}^{k} w_i$. Since $a_0^0 \neq 0$, by (5), $a_0^0 = -S a_1^0$. Substituting this in (4), and canceling $a_1^0 \neq 0$, we get $a_0^1 = a_1^1(1+S)$. Note that this also forces $S \neq 0$ otherwise a_0^0 will be zero.

Now consider the subsets with $k-1$ elements. All the entries $u_{Z-\{i\}}$, $1 \le i \le k$, are zero, because $k-1$ is even. This gives us the following set of equations.

$$\text{For every } i,\ 1 \le i \le k: \qquad \sum_{j_1 j_2 \ldots j_k} a^{1 \ldots 0 \ldots 1}_{j_1 j_2 \ldots j_k} u_{\boldsymbol{\beta}}^{j_1 j_2 \ldots j_k} \;=\; 0$$

where the single 0 in the superscript is at the i^{th} place. This gives

$$\text{For every } i,\ 1 \le i \le k: \qquad a_0^0 (a_0^1)^{k-1} + w_i a_1^0 (a_0^1)^{k-1} + \sum_{j \neq i} w_j a_0^0 a_1^1 (a_0^1)^{k-2} \;=\; 0$$

Dividing throughout by $(a_0^1)^{k-2}$ and then adding up, we obtain

$$\begin{array}{rrcll} & k a_0^0 a_0^1 + S a_1^0 a_0^1 + (k-1) S a_0^0 a_1^1 & = & 0 & \\ \Rightarrow & -kS a_1^0 a_0^1 + S(a_1^0 a_0^1 + (k-1) a_0^0 a_1^1) & = & 0 & \qquad (\text{Using } a_0^0 = -S a_1^0) \end{array}$$

Since $S \neq 0$, then for $k > 1$, we have $a_0^0 a_1^1 = a_1^0 a_0^1$ which gives $\det M = 0$, a contradiction.

The other case is when Γ is an even matchgate. In that case, we get a complementary set of equations—we just interchange the roles of 0 and 1 in the above analysis and get the same result.

Case 2. k is even.

Our analysis again depends on whether Γ is odd or even. First assume that Γ is an odd matchgate. We consider the entries corresponding to the empty subset $\emptyset$ and the full set Z. We have,

$$u_\emptyset = (a_0^0)^k \cdot 1 + (a_0^0)^{k-1} a_1^0 w_1 + (a_0^0)^{k-1} a_1^0 w_2 + \ldots + (a_0^0)^{k-1} a_1^0 w_k \quad = \quad 0 \tag{6}$$

$$u_Z = (a_0^1)^k \cdot 1 + (a_0^1)^{k-1} a_1^1 w_1 + (a_0^1)^{k-1} a_1^1 w_2 + \ldots + (a_0^1)^{k-1} a_1^1 w_k \quad = \quad 0 \tag{7}$$

Again denote by $S = \sum_{i=1}^k w_i$. Since $a_0^0, a_0^1 \neq 0$, we may cancel a_0^0 and a_0^1, and get $a_0^0 = -S a_1^0$ and $a_0^1 = -S a_1^1$. But this makes $\det M = 0$.

Now assume that Γ is an even matchgate. Consider the subsets with $k-1$ elements. All the entries $u_{Z-\{i\}}$, $1 \leq i \leq k$, are zero. This gives us the following set of equations.

$$\text{For every } i,\ 1 \leq i \leq k: \qquad a_0^0 (a_0^1)^{k-1} + w_i a_1^0 (a_0^1)^{k-1} + \sum_{j \neq i} w_j a_0^0 a_1^1 (a_0^1)^{k-2} \quad = \quad 0$$

Dividing throughout by $(a_0^1)^{k-2}$ and then adding up, we obtain

$$k a_0^0 a_0^1 + S(a_1^0 a_0^1 + (k-1) a_0^0 a_1^1) \quad = \quad 0 \tag{8}$$

Note that we can now conclude $S \neq 0$ otherwise $a_0^0 a_0^1$ will be zero.

We further consider all subsets with 1 element. All the entries $u_{\{i\}}$, $1 \leq i \leq k$, are zero and we get the following set of equations.

$$\text{For every } i,\ 1 \leq i \leq k: \qquad a_0^1 (a_0^0)^{k-1} + w_i a_1^1 (a_0^0)^{k-1} + \sum_{j \neq i} w_j a_1^0 a_0^1 (a_0^0)^{k-2} \quad = \quad 0$$

Dividing throughout by $(a_0^0)^{k-2}$ and then adding up, we obtain

$$k a_0^0 a_0^1 + S(a_0^0 a_1^1 + (k-1) a_0^1 a_1^0) \quad = \quad 0 \tag{9}$$

From equations (8) and (9), we get

$$S(a_0^0 a_1^1 + (k-1) a_0^1 a_1^0) \quad = \quad S(a_0^1 a_1^0 + (k-1) a_0^0 a_1^1)$$

Since we already have $S \neq 0$, then for $k \neq 2$, we have $a_0^0 a_1^1 = a_1^0 a_0^1$, which gives $\det M = 0$ again. This is a contradiction.

$\square$

Proof of Theorem 5.2

We prove that for any $k > 3$, the Not-All-Equal gate can not be realized as a signature by any matchgate over any basis of two linearly independent vectors.

Theorem 8.2. *Given $k > 3$, there is no linearly independent basis $\boldsymbol{\beta}$ such that there is a recognizer Γ having k external nodes with $valR(\Gamma, x_1 \otimes, \ldots, \otimes, x_k)$ equal to*

1. 0*, if* $x_1 = \ldots = x_k$*, and*

2. 1*, otherwise.*

We'll use the following simple lemmas.

Lemma 8.1. *Let* $AX + BY = 1$ *be a linear equation where both* A *and* B *are non-zero. Suppose, for some* x *and* y*,* $(1,1), (x,y)$ *and* (x^2, y^2) *are all solutions of this equation. Then* $x = y = 1$*.*

Proof. We have the following equalities.

$$\begin{aligned} A + B &= 1 & (10)\\ Ax + By &= 1 & (11)\\ Ax^2 + By^2 &= 1 & (12) \end{aligned}$$

First we show that none of x and y can be zero. Suppose $x = 0$. Then from (11) and (12) and $B \neq 0$, we get $y = 1$ and $B = 1$. Then $A = 0$ by (10), contrary to assumption. Similarly $y \neq 0$.

Now suppose any one of x or y is 1. Then, from the first two equations, the other is also 1. If none of them is 1, we subtract the first two equations to get $A(x-1) = -B(y-1)$ and subtract the last two to get $Ax(x-1) = -By(y-1)$. Now we can divide these two equations to get $x = y$. And then, from the first and second equations, we have $x = y = 1$, nonetheless. □

Lemma 8.2. *Suppose* a*,* b*,* c*,* d *are such that* $a + b = c + d = 1$ *and* $abcd \neq 0$*. Also, assume that* $ad - bc \neq 0$*. Let* $x = \frac{c^2}{a^2}$ *and* $y = \frac{d^2}{b^2}$*. Suppose* $(X,Y) = (1,1)$ *and* $(X,Y) = (x,y)$ *are solutions of the linear equation* $AX + BY = 1$ *where both* A *and* B *are non-zero. Then,* $x \neq 0, 1$ *and* $y \neq 0, 1$*.*

Proof. It is clear that x and y are non-zero because $abcd \neq 0$. Since $(1,1)$ and (x,y) are solutions of $AX + BY = 1$, we have $x = 1$ if and only if $y = 1$. Suppose $x = y = 1$. The only choices are $a = c, b = -d$ or $a = -c, b = d$ otherwise $ad - bc = 0$. But from the fact that $a + b = c + d = 1$, $a = c$ implies $b = d$ and vice-versa. This is impossible as none of a, b, c and d is zero. □

Proof of theorem 8.2. Let $n = (n_0, n_1), p = (p_0, p_1)$. Suppose Γ is a recognizer with the property stated in Theorem 8.2. The signature of Γ w.r.t. $\boldsymbol{\beta}$ is $u_\beta = (1, 0, \ldots, 0, 1)^t$. The standard signature u of Γ can be written as $u = M^{\otimes k} u_\beta$ where M is the matrix $\begin{bmatrix} p_1 & -n_1 \\ -p_0 & n_0 \end{bmatrix}$. Let $a = p_1, b = -n_1, c = -p_0, d = n_0$. Denote by

$$\sigma_i = (a+b)^{k-i}(c+d)^i - a^{k-i}c^i - b^{k-i}d^i,$$

for $0 \leq i \leq k$. Then, a moment reflection in terms of the tensor product equation $u = M^{\otimes k} u_\beta$ shows that the standard signature can be written in the symmetric form

$$[\sigma_0, \sigma_1, \ldots, \sigma_i, \ldots, \sigma_k].$$

It suffices to show that there do not exist a, b, c and d with $\Delta = ad - bc \neq 0$ such that u as given above is the standard signature of a recognizer. Assume to the contrary that for some values of a, b, c and d, there is such a recognizer Γ. We will use the *parity* conditions and the *matchgate identities* to arrive at a contradiction. We consider three different cases.

Case 1. k is odd.

First assume Γ is odd, i.e. all even positions in the symmetric standard signature are zero. When we count from zero up to k, this gives us the following set of equations:

$$\begin{aligned}
(a+b)^k - a^k - b^k &= 0 \\
(a+b)^{k-2}(c+d)^2 - a^{k-2}c^2 - b^{k-2}d^2 &= 0 \\
&\vdots \\
(a+b)(c+d)^{k-1} - ac^{k-1} - bd^{k-1} &= 0
\end{aligned}$$

Note that since $k > 3$, we have at least three equations. For the moment, assume $a+b=0$. Then $a \neq 0$ because $\Delta \neq 0$. Therefore, from the second equation, $c^2 = d^2$. So, $c = \pm d$. But $c \neq -d$ as $\Delta \neq 0$. So $c = d \neq 0$. Now we'll use matchgate identity to show that this is not possible. Let us fix $k-4$ external nodes to 1. What remains is a four-input matchgate. The only matchgate identity which isn't trivially satisfied is the following:

$$\sigma_{k-4}\sigma_k = \sigma_{k-2}^2. \tag{13}$$

This comes from the set of 10 matchgate identities for the 4 by 4 (naked) character matrices (See Section 2.4. For naked characters, one must change the entries by deleting the modifiers, which amounts to multiplying a -1 in the 3rd row and the 3rd column. In this case where entries only depend on cardinalities, the middle 2 by 2 determinant is zero.) Substituting $b=-a$, $d=c$ in the above, we get $\sigma_{k-4} = -2a^4c^{k-4}$, $\sigma_{k-2} = -2a^2c^{k-2}$, and $\sigma_k = (2c)^k - 2c^k$. Using the fact that $a, c \neq 0$, we arrive at a contradiction. Therefore, $a+b \neq 0$.

Now consider what happens if $c+d=0$. If so, $c \neq 0$ because $\Delta \neq 0$. Then the last equation from the above set of equations gives $a+b=0$ which makes $\Delta = 0$.

We can now assume that $a+b, c+d \neq 0$. By using Proposition 4.3 from [16], we can scale a, b, c, d such that $a+b = c+d = 1$. Again, we first consider the case when $abcd = 0$. If $a = 0$, then $b = 1$, and from the second equation, $d^2 = 1$. $d = 1$ would make $c = 0$ and therefore $\Delta = 0$. So $d = -1$ and $c = 2$. Again, we substitute these values into the matchgate identity (13) to get a contradiction. The case when $b = 0$ is symmetric. Now, consider $c = 0$. This means $d = 1$. The last equation gives $b = 1$ and so $a = 0$ which makes $\Delta = 0$. The case $d = 0$ is symmetric.

The only case left is $a+b = 1, c+d = 1$ and $abcd \neq 0$. Let $x = c^2/a^2$ and $y = d^2/b^2$. Let $A = a^k, B = b^k$. We see that the equation $AX + BY = 1$ has solutions

$$(1,1), (x,y), (x^2,y^2), \ldots, (x^{\frac{k-1}{2}}, y^{\frac{k-1}{2}}).$$

By Lemma 8.2, $x \neq 0, 1$ and $y \neq 0, 1$. Since $k > 3$ and odd, $\frac{k-1}{2} \geq 2$. Then, by Lemma 8.1, we have $x = y = 1$. That is a contradiction.

The other case is when Γ is even. In that case, we get the same set of equations except that a, b are replaced by c, d and vice-versa. The matchgate identity we use in that case is obtained by fixing $k-4$ external nodes to 0. The proof for odd k is complete.

Case 2. $k \geq 6$ and k is even.

In this case, the proofs when Γ is even or odd are slightly different. We'll consider them one by one. The basic strategy is similar to what we saw earlier. First assume that Γ is odd. In this case, we have the following set of equations:

$$\begin{aligned}
(a+b)^k - a^k - b^k &= 0\\
(a+b)^{k-2}(c+d)^2 - a^{k-2}c^2 - b^{k-2}d^2 &= 0\\
&\vdots\\
(a+b)^2(c+d)^{k-2} - a^2c^{k-2} - b^2d^{k-2} &= 0\\
(c+d)^k - c^k - d^k &= 0
\end{aligned}$$

If $a+b=0$, then the first equation gives $a^k = -b^k = -(-a)^k = -a^k$. This means $a=b=0$ which makes $\Delta = 0$. The case $c+d=0$ is symmetric.

We now assume, after scaling appropriately using Proposition 4.3 from [16], that $a+b=c+d=1$. Again we first consider the case when $abcd=0$. If $a=0$, then $b=1$ and by the second equation, $d^2=1$ which upon substituting in the last equation gives $c^k=0$ because k is even. This makes $\Delta=0$. The cases when $b=0$, $c=0$ or $d=0$ are symmetric.

Now, we have $a+b=c+d=1$ and $abcd \neq 0$. Let $x = c^2/a^2$ and $y = d^2/b^2$. Let $A=a^k, B=b^k$. We see that the equation $AX+BY=1$ has solutions

$$(1,1), (x,y), (x^2,y^2), \dots, (x^{\frac{k}{2}}, y^{\frac{k}{2}}).$$

By Lemma 8.2), $x \neq 0,1$ and $y \neq 0,1$. Since $k \geq 4$, $\frac{k}{2} \geq 2$. Therefore, by Lemma 8.1, we get that $x=y=1$. That is a contradiction.

The other case is when Γ is even. In this case, we have the following set of equations:

$$\begin{aligned}
(a+b)^{k-1}(c+d) - a^{k-1}c - b^{k-1}d &= 0\\
(a+b)^{k-3}(c+d)^3 - a^{k-3}c^3 - b^{k-3}d^3 &= 0\\
&\vdots\\
(a+b)(c+d)^{k-1} - ac^{k-1} - bd^{k-1} &= 0
\end{aligned}$$

If $a+b=0$, the first equation gives $a^{k-1}(c-d)=0$. Since we already have $a \neq 0$, we get $c=d$. We'll use matchgate identity to show that this is not possible. Let us fix $k-4$ external nodes to 1. What remains is a four-input matchgate. The only matchgate identity which isn't trivially satisfied is the following:

$$\sigma_{k-4}\sigma_k = \sigma_{k-2}^2 \tag{14}$$

Substituting $b=-a$, $d=c$ in the above, and using the fact that $a,c \neq 0$, we arrive at a contradiction. Therefore, $a+b \neq 0$. The case when $c+d=0$ is symmetric.

So we have $a+b, c+d \neq 0$. Again, after scaling appropriately, we assume that $a+b=c+d=1$. As before, we first consider the case when $abcd=0$. If $a=0$, then $b=1$ and by the first equation, $d=1$ which means $c=0$ and $\Delta=0$. The cases when $b=0$, $c=0$ or $d=0$ are symmetric.

Now, we have $a+b=c+d=1$ and $abcd \neq 0$. Let $x=c^2/a^2$ and $y=d^2/b^2$. Let $A=a^{k-1}c, B=b^{k-1}d$. The equation $AX+BY=1$ has solutions

$$(1,1), (x,y), (x^2,y^2), \dots, (x^{\frac{k-2}{2}}, y^{\frac{k-2}{2}}).$$

By Lemma 8.2, $x \neq 0,1$ and $y \neq 0,1$. Since $k \geq 6$, $\frac{k-2}{2} \geq 2$. Therefore, by Lemma 8.1, we get that $x=y=1$ which is not true.

Case 3. $k = 4$.

Again we distinguish the cases when Γ is even or odd. When Γ is odd, the proof for the case $k \geq 6$ holds because the set of parity constraints gives at least three equations.

To prove that Γ can't be even, we have to do a little more work because we get only the following two equations using parity.

$$\begin{aligned} (a+b)^3(c+d) - a^3c - b^3d &= 0 & (15) \\ (a+b)(c+d)^3 - ac^3 - bd^3 &= 0 & (16) \end{aligned}$$

First part of the proof for the case $k \geq 6$ also works here and we can conclude that $a+b = c+d = 1$ and $abcd \neq 0$. For the time being, assume that $a^3 \neq (1-a)^3$. Now we substitute $b = 1-a$, $d = 1-c$ in (15) gives $c = \frac{1-(1-a)^3}{a^3-(1-a)^3}$. Putting this in (16) gives the following equation in a:

$$\left[(1-(1-a)^3)^3 - (a^3-1)^3\right] a = (a^3-(1-a)^3)^3 - (a^3-1)^3 \tag{17}$$

So, either $a^3 = (1-a)^3$ or a satisfies (17). We conclude that a satisfies the following equation:

$$(a^3-(1-a)^3)\left\{\left[(1-(1-a)^3)^3-(a^3-1)^3\right]a - (a^3-(1-a)^3)^3 - (a^3-1)^3\right\} = 0 \tag{18}$$

There is a symmetry effected by a reflection at $1/2$, namely $x \mapsto 1-x$. This suggests that we replace the variable a by the new variable x where $a = 1/2 + x$. Then (17) factors into

$$\frac{x(2x+1)(2x-1)(4x^2+7)(16x^4+7)}{16}$$

with roots $x = 0, \pm 1/2, \pm\sqrt{7}i/2, \frac{\pm 7^{1/4} \pm 7^{1/4} i}{2}$. Similarly the factor $a^3 - (1-a)^3 = (1/2+x)^3 - (1/2-x)^3 = \frac{x}{2}(3-4x^2)$, with roots 0 and $\pm\frac{\sqrt{3}}{2}$.

Symmetrically, c, b and d also satisfy the same equation (18).

Now consider the only non-trivial matchgate identity.

$$((a+b)^4 - a^4 - b^4)((c+d)^4 - c^4 - d^4) = ((a+b)^2(c+d)^2 - a^2c^2 - b^2d^2)^2 \tag{19}$$

After substituting $b = 1-a$, $d = 1-c$ in (19) and simplifying using the fact that $a \neq c$ because otherwise $\Delta = 0$, we get the following equation in a and c.

$$(a+c-2)^2 + 4ac(a+c-ac) = 0 \tag{20}$$

What remains is to consider all pairs a, c of solutions to (18). Substitute these into (20) we verify that none works. This can be done explicitly.

□

Symmetric signatures in b2

Here we discuss the symmetric signatures that can be realized in the basis **b2**. We will obtain a closed form for such signatures, thereby proving Theorem 6.1.

We have already defined the matrices M and $A = (a_{i,j})$. The expression of $a_{i,j}$ in Lemma 6.1 can be obtained by considering the number of ways two subsets I and J of cardinality i and j respectively can intersect each other. In fact, these a_{ij} can be expressed by the Krawtchouk polynomials [11]. $P_k^n(x)$ is defined as:

$$P_k^n(x) = \sum_{j=0}^{k} (-1)^j \binom{x}{j}\binom{n-x}{k-j}$$

From Lemma 6.1, we see that $a_{ij} = P_i(j)$.

Suppose we want to realize the symmetric signature $[x_0, x_1, \ldots, x_n]$ by a generator. By the notation from Section 6, this means that the standard signature we want is $(x_0, \ldots, x_n)M$, where M is the $(n+1) \times 2^n$ matrix. From which we know, the standard signature is also a symmetric signature and the symmetric form can be written as $[z_0, z_1, \ldots, z_n] = (x_0, x_1, \ldots, x_n)A$, where A was also defined in Section 6. We need to consider various cases. Before that, let's prove a lemma that will be useful later.

Lemma 8.3. *Suppose Γ is an even matchgate, with symmetric standard signature $[z_0, \ldots, z_n]$. Then, for all odd i, $z_i = 0$, and there exist r_1 and r_2 not both zero, such that for every even $k \geq 2$,*

$$r_1 z_{k-2} = r_2 z_k$$

Proof. We use matchgate identities to prove the lemma. Let k be odd. Let Z, U be the sets of external and internal nodes, respectively. To prove that $z_0 : z_2 = z_{k-1} : z_{k+1}$, we use the Grassmann-Plücker identity generated by the two sets, $I = (Z - I') \cup U$ and $J = (Z - J') \cup U$, where I' is a singleton set, say $I' = \{a\}$ and a is an external node, and J' is a set of k external nodes other than a. The resulting matchgate identity is as follows:

$$z_0 z_{k+1} = \sum_{k \text{ times}} (\pm) z_2 z_{k-1}$$

where the sign of the terms in the right hand side alternates, beginning with a $+$. Therefore, $z_0 z_{k+1} = z_2 z_{k-1}$. If $z_0, z_2, \ldots$ are all non-zero, we can choose $r_1 = \frac{z_2}{z_0}, r_2 = 1$ and we're done.

Now suppose $z_k = 0$ for some even k. For the moment assume $k \leq n - 4$. We give some more matchgate identities which will imply that all of $z_0, z_2, \ldots$, except one extremal value, are zero. Let I_1 be a set of k external nodes. Let a, b, c, d be four external nodes not in I_1. Let $I' = I_1 \cup \{a\}$ and $J' = I_1 \cup \{b, c, d\}$. Consider the Grassmann-Plücker identity generated by $I = (Z - I') \cup U$ and $J = (Z - J') \cup U$. This gives us $z_k z_{k+4} = z_{k+2}^2$. From these identities, we can conclude that if $z_k = 0$ for some even then $z_{k'}$ is zero for all even k' except possibly the two extremes z_0 and z_{n^*}, where $n^* = 2\lfloor n/2 \rfloor$, which is n if n is even, and $n-1$ if n is odd. From the identity $z_0 z_{n^*} = z_{n^*-2} z_2$ that we found earlier, we can conclude that at most one of them can be non-zero. If $z_0 \neq 0$ is the only non-zero, we can choose $r_1 = 0, r_2 = 1$ and if z_{n^*} is the only non-zero, we can choose $r_1 = 1, r_2 = 0$. (Of course it is also possible that all $z_i = 0$.) □

Lemma 8.4. *Suppose Γ is an odd matchgate, with symmetric standard signature $[z_0, \ldots, z_n]$. Then for all even i, $z_i = 0$, and there exist r_1 and r_2 not both zero, such that for every odd $k \geq 3$,*

$$r_1 z_{k-2} = r_2 z_k$$

Proof. We again use matchgate identities for the proof. Let k be even. Let Z, U be the sets of external and internal nodes, respectively. To prove that $z_1 : z_3 = z_{k-1} : z_{k+1}$, we use the Grassmann-Plücker identity generated by the two sets, $I = (Z - I') \cup U$ and $J = (Z - J') \cup U$, where I' is a set of two elements, say $I' = \{a, b\}$ and a, b are external nodes, and J' is a set of k external nodes such that $b \in J'$ and $a \notin J'$. The resulting matchgate identity is as follows:

$$z_1 z_{k+1} = \sum_{k-1 \text{ times}} (\pm) z_3 z_{k-1}$$

where the sign of the terms in the right hand side alternates, beginning with a +. Therefore, $z_1 z_{k+1} = z_3 z_{k-1}$. If $z_1, z_3, \ldots$ are all non-zero, then we can choose $r_1 = \frac{z_3}{z_1}$ and $r_2 = 1$, and we're done. What remains is the case when z_k is zero for some odd k. In this case, we need more matchgate identities as in the proof of Lemma 8.3 to finish the proof. These identities can be obtained by the same method as described there. □

It follows from the characterization theorem for matchgates, that the requirements of Lemma 8.3, and Lemma 8.4 are both necessary and sufficient. Because the signatures are symmetric, it can be proved that the set of useful Grassmann-Plücker Identities considered here is a complete set.

Proof of theorem 6.1. We will need to consider various cases. First we will obtain a set of equations for each case. Later we will see how to solve these equations.

Case 1: n is odd and an even matchgate Γ realizes the signature.

Since the matchgate Γ is even, $z_j = 0$ whenever j is odd.

$$\sum_{i=0}^{n} a_{ij} x_i = 0, \qquad j = 1, 3, \ldots, n. \tag{21}$$

Using Lemma 6.1 and the fact that j is odd, $a_{n-i,j} x_{n-i} = (-1)^j a_{ij} x_{n-i} = -a_{ij} x_{n-i}$. Therefore,

$$a_{ij} x_i + a_{n-i,j} x_{n-i} = a_{ij}(x_i - x_{n-i})$$

Let us introduce new variable $y_i = x_i - x_{n-i}$, where $i = 0, 1, \ldots, \frac{n-1}{2}$ which now satisfy the following set of equations:

$$\sum_{i<n/2} a_{ij} y_i = 0, \qquad j = 1, 3, \ldots, n.$$

Note that there are $\frac{n+1}{2}$ equations. As $(n+1)$-dimensional vectors, all the column vectors in $A = (a_{ij})$, for $j = 0, 1, \ldots$, are linearly independent. In particular then, they are linearly independent for odd $j = 1, 3, \ldots, n$. By Lemma 6.1, the truncated vectors of dimension $\frac{n+1}{2}$ (where row index $0 \le i \le \frac{n-1}{2}$) appearing in the above equations, for $j = 1, 3, \ldots, n$, is still linearly independent.
Since the number of variables is also $\frac{n+1}{2}$, the only solution is $y_i = 0$ for $i = 0, 1, \ldots, \frac{n-1}{2}$. Therefore,

$$x_i = x_{n-i}, \qquad i = 0, 1, \ldots, \frac{n-1}{2}. \tag{22}$$

When j is even, we have,

$$\begin{aligned} z_j &= \sum_{i=0}^{n} a_{ij} x_i \\ &= \sum_{i=0}^{\frac{n-1}{2}} a_{ij} x_i + \sum_{i=\frac{n+1}{2}}^{n} a_{ij} x_i \end{aligned}$$

$$
\begin{aligned}
&= \sum_{i=0}^{\frac{n-1}{2}} a_{ij}x_i + \sum_{i=\frac{n+1}{2}}^{n} a_{n-i,j}x_i \qquad \text{(by Lemma 6.1)} \\
&= \sum_{i=0}^{\frac{n-1}{2}} a_{ij}x_i + \sum_{i=0}^{\frac{n-1}{2}} a_{ij}x_{n-i} \\
&= \sum_{i=0}^{\frac{n-1}{2}} a_{ij}(x_i + x_{n-i}) \\
&= 2\sum_{i=0}^{\frac{n-1}{2}} a_{ij}x_i \qquad \text{(by using (22))}
\end{aligned}
$$

Now we use Lemma 8.3 to get the following set of equations.

$$
r_1 \sum_{i<\frac{n}{2}} a_{ij}x_i = r_2 \sum_{i<\frac{n}{2}} a_{i,j+2}x_i, \qquad j = 0, 2, \ldots, n-3. \tag{23}
$$

We have a set of $\frac{n-1}{2}$ equations in $\frac{n+1}{2}$ variables other than r_1, r_2.

Case 2: n is odd and an odd matchgate Γ realizes the signature.

In this case, z_j is zero for all even j. Using an analysis similar to the above, we will get $x_i = -x_{n-i}$ and will eventually obtain the following set of equations by using Lemma 8.4.

$$
r_1 \sum_{i<\frac{n}{2}} a_{ij}x_i = r_2 \sum_{i<\frac{n}{2}} a_{i,j+2}x_i, \qquad j = 1, 3, \ldots, n-2. \tag{24}
$$

Again we have a set of $\frac{n-1}{2}$ equations in $\frac{n+1}{2}$ variables other than r_1, r_2.

Case 3: n is even and an even matchgate Γ realizes the signature.

As before, since the matchgate Γ is even, $z_j = 0$ whenever j is odd.

$$
\sum_i a_{ij}x_i = 0, \qquad j = 1, 3, \ldots, n-1. \tag{25}
$$

From Lemma 6.1, we get $a_{\frac{n}{2}j} = -a_{\frac{n}{2}j}$ and therefore, $a_{\frac{n}{2}j} = 0$ for odd j. Using Lemma 6.1 again, and the fact that j is odd, $a_{n-i,j}x_{n-i} = (-1)^j a_{ij}x_{n-i} = -a_{ij}x_{n-i}$. Therefore,

$$
a_{ij}x_i + a_{n-i,j}x_{n-i} = a_{ij}(x_i - x_{n-i})
$$

As in Case 1, we can introduce new variables $y_i = x_i - x_{n-i}$, and rewrite the equations which are linearly independent because the original equations (25) are linearly independent. Since we have $\frac{n}{2}$ equations in as many variables, we conclude that the only solution is $y_i = 0$ which implies

$$
x_i = x_{n-i}, \qquad i = 0, 1, \ldots, \frac{n}{2} - 1. \tag{26}
$$

Using the above, when j is even, we can write z_j as:

$$
z_j \;=\; 2\sum_{i=0}^{\frac{n}{2}-1} a_{ij}x_i + a_{\frac{n}{2}j}x_{\frac{n}{2}}, \qquad j = 0, 2, \ldots, n.
$$

Now we can use a new variable $x_i = x'_i$, except $x_{\frac{n}{2}} = 2x'_{\frac{n}{2}}$. Then we can use Lemma 8.3 to get the following set of equations.

$$r_1 \sum_{i \leq \frac{n}{2}} a_{ij} x'_i = r_2 \sum_{i \leq \frac{n}{2}} a_{i,j+2} x'_i, \qquad j = 0, 2, \ldots, n-2. \tag{27}$$

We have a set of $\frac{n}{2}$ equations in $\frac{n}{2}+1$ variables other than r_1, r_2.

Case 4: n is even and an odd matchgate Γ realizes the signature.

In this case, z_j is zero for all even j. This case differs from Case 3 in the same way as Case 2 differs from Case 1. The analysis is similar to the above. We begin with the equations

$$\sum_i a_{ij} x_i = 0, \qquad j = 0, 2, \ldots, n. \tag{28}$$

As before, $a_{ij}x_i + a_{n-i,j}x_{n-i} = a_{ij}(x_i + x_{n-i})$, and we introduce new variables $y_i = x_i + x_{n-i}$, for $i = 0, \ldots, \frac{n}{2}-1$ and $y_{\frac{n}{2}} = x_{\frac{n}{2}}$. We will get $x_i = -x_{n-i}$ and $x_{\frac{n}{2}} = 0$. Now we use Lemma 8.4 to get the following set of equations.

$$r_1 \sum_{i < \frac{n}{2}} a_{ij} x_i = r_2 \sum_{i < \frac{n}{2}} a_{i,j+2} x_i, \qquad j = 1, 3, \ldots, n-3. \tag{29}$$

Now we show how to solve the equations we obtained above. We will then obtain the complete set of symmetric signatures that can be realized in basis **b2**. We use the fact that a_{ij}'s can be represented in terms of the Krawtchouk polynomials defined earlier.

$$P_k^n(x) = \sum_{j=0}^{k} (-1)^j \binom{x}{j} \binom{n-x}{k-j}.$$

We will drop the superscript n when it is clear from the context. From Lemma 6.1, we see that $a_{ij} = P_i(j)$. These polynomials satisfy the following *orthogonality* relation [11].

$$\sum_{i=0}^{n} \binom{n}{i} P_r(i) P_s(i) = 2^n \binom{n}{r} \delta_{rs}. \tag{30}$$

Also, $\binom{n}{i} P_s(i) = \binom{n}{s} P_i(s)$. Therefore, we conclude that

$$\sum_s \frac{1}{\binom{n}{s}} a_{si} a_{sj} = \begin{cases} \frac{2^n}{\binom{n}{i}} & i = j \\ 0 & i \neq j \end{cases} \tag{31}$$

Lemma 8.5. *For n odd and $i \equiv j \bmod 2$,*

$$\sum_{s < \frac{n}{2}} \frac{1}{\binom{n}{s}} a_{si} a_{sj} = \begin{cases} \frac{2^{n-1}}{\binom{n}{i}} & i = j \\ 0 & i \neq j \end{cases} \tag{32}$$

Proof. The proof follows by using equation (31) and Lemma 6.1 ∎

Lemma 8.6. *For n even and $i \equiv j \bmod 2$,*

$$\sum_{s \le \frac{n}{2}} \frac{1}{\binom{n}{s}} a'_{si} a'_{sj} = \begin{cases} \frac{2^{n-1}}{\binom{n}{i}} & i = j \\ 0 & i \ne j \end{cases} \tag{33}$$

where $a'_{i,j} = a_{i,j}$, except $a'_{\frac{n}{2},j} = a_{\frac{n}{2},j}/\sqrt{2}$.

In the following we will assume n is odd. The case for n even is similar. Therefore, if we define $\hat{a}_{ij} = \frac{a_{ij}}{\sqrt{\binom{n}{i}}}$, then the column vectors $\hat{a}_j = [\hat{a}_{ij}]_{0 \le i \le n/2}$ are orthogonal vectors, among all even j or among all odd j, and it has square norm $\| \hat{a}_j \|_2^2 = \frac{2^{n-1}}{\binom{n}{j}}$. Let $\hat{a}_j^0 = \frac{1}{\|\hat{a}_j\|} \hat{a}_j$ be a set of orthonormal vectors (among all even or all odd j).

Now we show how to solve the equations (23) in Case 1 above. Let us define $y_i = x_i \sqrt{\binom{n}{i}}$, $i = 0, 1, \ldots, \frac{n-1}{2}$. We can re-write these equations as

$$r_1 \sum_{i < \frac{n}{2}} \hat{a}_{ij} y_i = r_2 \sum_{i < \frac{n}{2}} \hat{a}_{i,j+2} y_i \qquad j = 0, 2, \ldots, n-3. \tag{34}$$

Then,

$$r_1 \| \hat{a}_j \| \langle y, \hat{a}_j^0 \rangle = r_2 \| \hat{a}_{j+2} \| \langle y, \hat{a}_{j+2}^0 \rangle \tag{35}$$

Hence, in terms of the basis $\hat{a}_j^0$'s, $j = 0, 2, \ldots, n-1$, we can write y as

$$y = \lambda \left(r_2^{\frac{n-1}{2}}, r_1 r_2^{\frac{n-3}{2}} \sqrt{\binom{n}{2}}, r_1^2 r_2^{\frac{n-5}{2}} \sqrt{\binom{n}{4}}, \ldots, r_1^{\frac{n-1}{2}} \sqrt{\binom{n}{n-1}} \right) \tag{36}$$

Therefore, $x_i = \frac{1}{\sqrt{\binom{n}{i}}} y_i$ can be written as

$$x_i = \frac{\lambda}{2^{\frac{n-1}{2}} \binom{n}{i}} \left[r_2^{\frac{n-1}{2}} a_{i0} + r_1 r_2^{\frac{n-3}{2}} \binom{n}{2} a_{i2} + \ldots + r_1^{\frac{n-1}{2}} \binom{n}{n-1} a_{i,n-1} \right] \tag{37}$$

Now we will try to obtain a closed form for the above expression. For the sake of clarity, let's substitute $r_1 = t_1^2$ and $r_2 = t_2^2$. Denoting by S_i the expression in the bracket, we get,

$$\begin{aligned}
S_i &= \sum_{j \text{ even}} \binom{n}{j} t_1^j t_2^{n-1-j} a_{ij} \\
&= \sum_{j \text{ even}} \binom{n}{j} t_1^j t_2^{n-1-j} \left(\sum_{0 \le s \le i,j} (-1)^s \binom{j}{s} \binom{n-j}{i-s} \right) \\
&= \sum_s \sum_{j \text{ even},\ j \ge s} (-1)^s t_1^j t_2^{n-1-j} \frac{n!}{s!(i-s)!(j-s)!(n-i-j+s)!} \\
&= \sum_s (-1)^s \frac{n!}{s!(i-s)!(n-i)!} \left(\sum_{j \text{ even},\ j \ge s} \frac{(n-i)!}{(j-s)!(n-i-j+s)!} t_1^j t_2^{n-1-j} \right) \\
&= \sum_s (-1)^s \frac{n!}{s!(i-s)!(n-i)!} t_1^s t_2^{i-s-1} \left(\sum_{j \text{ even},\ j \ge s} \frac{(n-i)!}{(j-s)!(n-i-j+s)!} t_1^{j-s} t_2^{n-i-j+s} \right) \\
&= \sum_s (-1)^s \binom{n}{i} \binom{i}{s} t_1^s t_2^{i-s-1} \left(\sum_{j \text{ even},\ j \ge s} \frac{(n-i)!}{(j-s)!(n-i-j+s)!} t_1^{j-s} t_2^{n-i-j+s} \right)
\end{aligned}$$

Now the sum within parentheses is

$$\sum_{j \text{ even},\ j\geq s} \frac{(n-i)!}{(j-s)!(n-i-j+s)!} t_1^{j-s} t_2^{n-i-j+s} \quad = \quad \begin{cases} \frac{(t_2+t_1)^{n-i}+(t_2-t_1)^{n-i}}{2} & \text{if } s \text{ is even.} \\ \frac{(t_2+t_1)^{n-i}-(t_2-t_1)^{n-i}}{2} & \text{if } s \text{ is odd.} \end{cases}$$

Therefore, we have,

$$\begin{aligned} S_i/\binom{n}{i} &= \sum_{s \text{ even}} \binom{i}{s} t_1^s t_2^{i-s-1} \left(\frac{(t_2+t_1)^{n-i}+(t_2-t_1)^{n-i}}{2} \right) \\ &\quad - \sum_{s \text{ odd}} \binom{i}{s} t_1^s t_2^{i-s-1} \left(\frac{(t_2+t_1)^{n-i}-(t_2-t_1)^{n-i}}{2} \right) \\ &= \frac{1}{2t_2} \left((t_2+t_1)^{n-i} + (t_2-t_1)^{n-i} \right) \left(\sum_{s \text{ even}} \binom{i}{s} t_1^s t_2^{i-s} \right) \\ &\quad - \frac{1}{2t_2} \left((t_2+t_1)^{n-i} - (t_2-t_1)^{n-i} \right) \left(\sum_{s \text{ odd}} \binom{i}{s} t_1^s t_2^{i-s} \right) \\ &= \frac{1}{2t_2} \left((t_2+t_1)^{n-i} + (t_2-t_1)^{n-i} \right) \left(\frac{(t_2+t_1)^i + (t_2-t_1)^i}{2} \right) \\ &\quad - \frac{1}{2t_2} \left((t_2+t_1)^{n-i} - (t_2-t_1)^{n-i} \right) \left(\frac{(t_2+t_1)^i - (t_2-t_1)^i}{2} \right) \\ &= \frac{1}{2t_2} \left((t_2+t_1)^{n-i}(t_2-t_1)^i + (t_2-t_1)^{n-i}(t_2+t_1)^i \right) \end{aligned}$$

The statement in the Theorem follows.
The other equations can be solved similarly.

$\square$

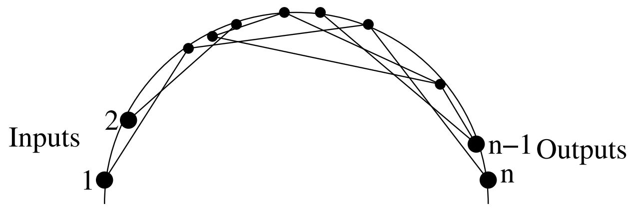

Figure 1: An example of converting a 2-input, 2-output matchgate to a planar matchgate.

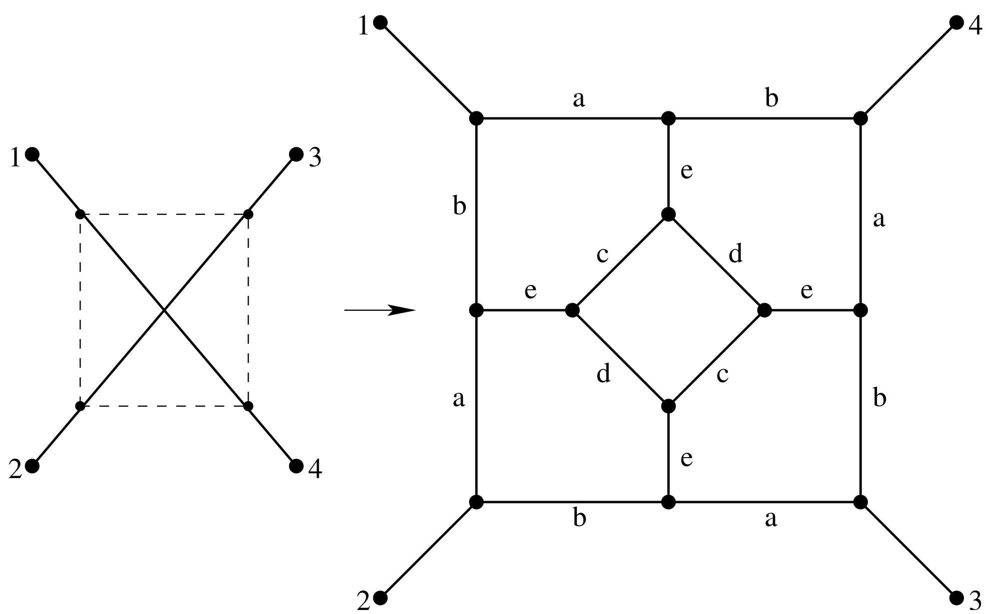

Figure 2: The gadget used to replace crossovers. Here $a = 1, b = i, c = d = -1/2, e = \sqrt{i}$, where $i = \sqrt{-1}$. The gadget was from [16] by Valiant.

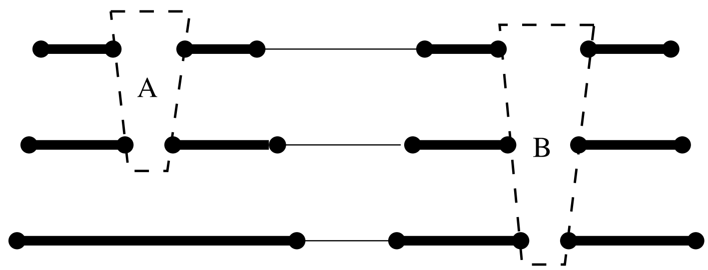

Figure 3: An example of a matchcircuit consisting of two matchgates A and B. The internal structures of A and B are not shown.

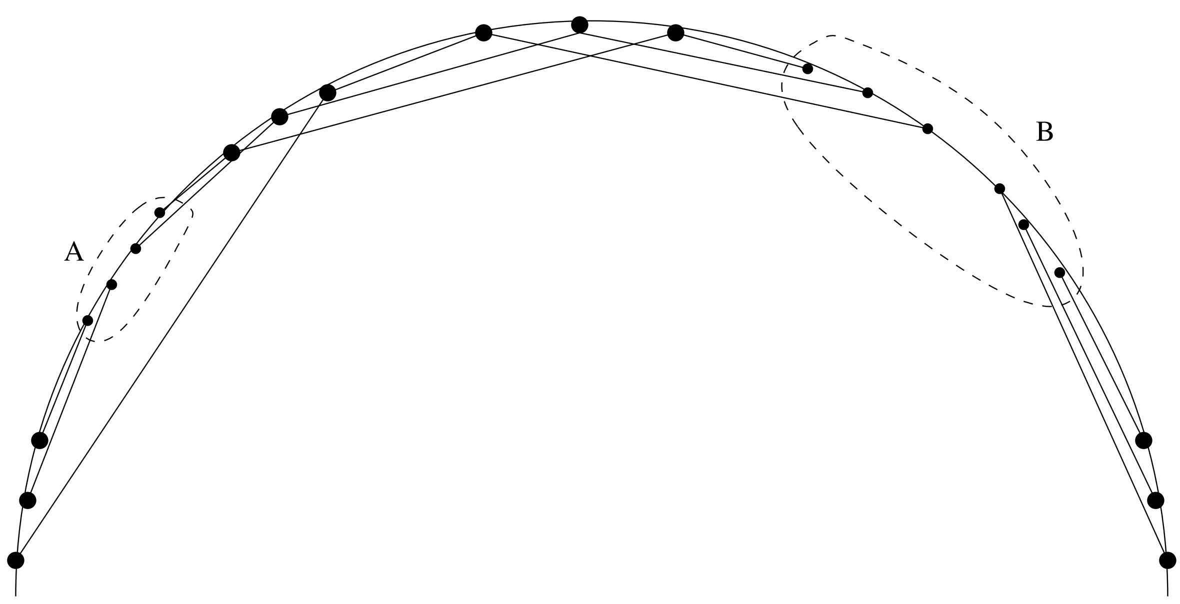

Figure 4: A planar matchgate equivalent to the matchcircuit shown in Figure 3. The dotted curves enclose the planar matchgates equivalent to the matchgates A and B from the matchcircuit. Each of these, when magnified, looks like Figure 1.

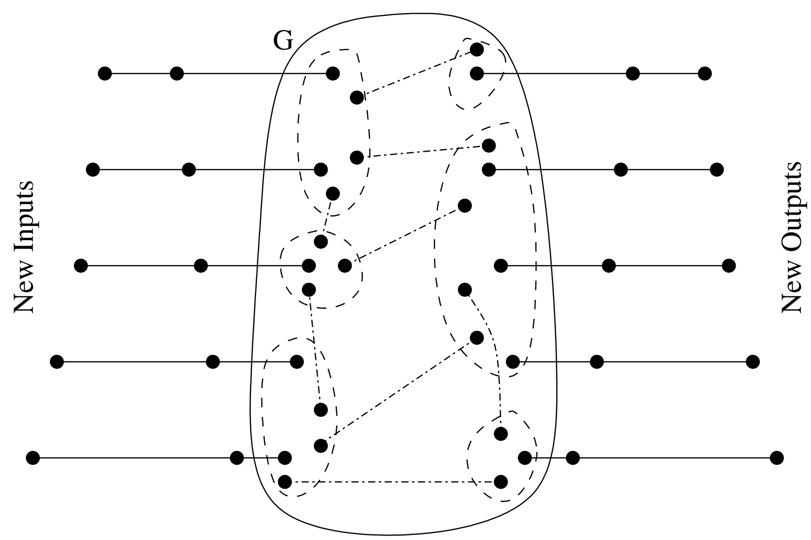

Figure 5: Constructing a matchcircuit from a planar matchgrid.