THEORY OF COMPUTING, Volume 10 (7), 2014, pp. 167–197
www.theoryofcomputing.org

RESEARCH SURVEY

# Matchgates Revisited

Jin-Yi Cai* Aaron Gorenstein

Received May 17, 2013; Revised December 17, 2013; Published August 12, 2014

**Abstract:** We study a collection of concepts and theorems that laid the foundation of matchgate computation. This includes the signature theory of planar matchgates, and the parallel theory of characters of not necessarily planar matchgates. Our aim is to present a unified and, whenever possible, simplified account of this challenging theory. Our results include: (1) A direct proof that the Matchgate Identities (MGI) are necessary and sufficient conditions for matchgate signatures. This proof is self-contained and does not go through the character theory. (2) A proof that the MGI already imply the Parity Condition. (3) A simplified construction of a crossover gadget. This is used in the proof of sufficiency of the MGI for matchgate signatures. This is also used to give a proof of equivalence between the signature theory and the character theory which permits omittable nodes. (4) A direct construction of matchgates realizing all matchgate-realizable symmetric signatures.

**ACM Classification:** F.1.3, F.2.2, G.2.1, G.2.2

**AMS Classification:** 03D15, 05C70, 68R10

**Key words and phrases:** complexity theory, matchgates, Pfaffian orientation

## 1 Introduction

Leslie Valiant introduced *matchgates* in a seminal paper [24]. In that paper he presented a way to encode computation via the Pfaffian and Pfaffian Sum, and showed that a non-trivial, though restricted, fragment of quantum computation can be simulated in classical polynomial time. Underlying this magic is a way to encode certain quantum states by a classical computation of perfect matchings, and to simulate certain

*Supported by NSF CCF-0914969 and NSF CCF-1217549.

 DOI: 10.4086/toc.2014.v010a007

quantum gates by the so-called matchgates. These matchgates are weighted graphs, not necessarily planar, and are equipped with input and output nodes, as well as the so-called omittable nodes. Each matchgate is associated with a *character*, whose entries are defined in terms of a Pfaffian and Pfaffian Sum.

Three years later, there was great excitement when Valiant invented holographic algorithms [26], where he also introduced planar matchgates. These matchgates are planar graphs, have a subset of vertices on the outer face designated as external nodes, and are each associated with a *signature*. The entries of a signature are defined in terms of the perfect matching polynomial, $\mathrm{PerfMatch}(\cdot)$. For planar weighted graphs, this quantity can be computed by Kasteleyn's well-known algorithm [14] (a. k. a. FKT algorithm [21]) in polynomial time, which uses the Pfaffian and a Pfaffian orientation.

Holographic algorithms (for examples, see [26, 25, 7]) are quite exotic, and use a quantum-like superposition of fragments of computation to achieve custom-designed cancellations. The two basic ingredients of holographic algorithms from [26] are matchgates and holographic transformations. A number of concrete problems are shown to be polynomial-time computable by this novel technique, even though they appear to require exponential time, and minor variations of which are NP-hard. They challenge our perceived boundary of what polynomial-time computation can do. Since we do not really have any reasonable absolute lower bounds that apply to unrestricted computational models, our faith in such well-known conjectures such as $\mathsf{P} \neq \mathsf{NP}$ or $\mathsf{P} \neq \mathsf{P}^{\#\mathsf{P}}$ is based primarily on the inability of existing algorithmic techniques to solve NP-hard or #P-hard problems in polynomial time. To maintain this faith, it is imperative that we gain a better understanding of what the new methodology can or cannot do. To quote Valiant [26], "any proof of $\mathsf{P} \neq \mathsf{NP}$ may need to explain, and not only to imply, the unsolvability" of NP-complete or #P-complete problems by this methodology. It becomes apparent that there is a fundamental problem of what are the intrinsic limitations of matchgates, and what is the relationship between characters of general matchgates and signatures of planar matchgates.

In [23], Valiant showed that the character of every 2-input 2-output matchgate must satisfy five polynomial identities, called the *Matchgate Identities*. Valiant used this to show that certain quantum gates cannot be simulated by the characters of general matchgates. In a sequence of two papers [1, 2] a general study of the character theory and the signature theory of matchgates was undertaken. These papers achieved the following general results: Firstly, there is essentially an equivalence between the character theory and the signature theory of matchgates, and secondly, a set of *useful Grassmann-Plücker identities* together with the Parity Condition are a necessary and sufficient condition for a sequence of values to be the signature of a planar matchgate. (The notion of "useful" was defined in [2].) This set of useful Grassmann-Plücker identities will be called Matchgate Identities (MGI) in the general sense. Along the way they also established a concrete characterization of symmetric signatures, which are signatures whose entries only depend on the Hamming weight of the index.

However, this proof is long and indirect. In particular the proof for the signature theory of planar matchgates goes through characters. Additionally, there is a subtle gap in the proof that every planar matchgate signature must satisfy the Matchgate Identities. The gap has to do with the non-uniform and exponentially many ways in which the induced Pfaffian orientations on subgraphs of a planar graph can introduce a correction factor $(-1)$ to Pfaffian values, relative to perfect matchings. We note that Pfaffian orientations are themselves an important topic [22], and resolving this gap also leads to the first result to our knowledge concerning the behavior of Pfaffian orientations of subgraphs under node removal.

In this paper we present a full, self-contained proof that the MGI characterize planar matchgate signatures. This proof does not involve character theory or any non-planar matchgate. Moreover, we include a short proof demonstrating that the MGI imply the Parity Condition. Previously this was presented as a separate requirement for matchgates, but now we show that the MGI entirely characterize matchgate signatures. We then revisit and clarify the equivalence between planar matchgates and the original general matchgates. Along the way we introduce a concise matchgate for the "crossover gadget," using only real weights 1 and $-1$. Previously the only known such gadget uses complex values. Finally, it has been known that the MGI greatly simplify for symmetric signatures. By the general theory any symmetric sequence satisfying the MGI must be realizable as the signature of a planar matchgate. Previously this existence was only known by going through the entire equivalence proof of characters and signatures, which also uses the only known "crossover gadget." In this paper, we present a simple, direct construction of a planar matchgate realizing any symmetric sequence satisfying the MGI.

The most intricate part of this paper is the proof that planar matchgate signatures must satisfy the MGI. The strategy is as follows: we first establish identities for Pfaffian minors implied by the Grassmann-Plücker identities. Then we want to map the signature entries of the MGI term-by-term to the factors appearing in the new identities. However, such a mapping involves an individualized (per-factor) sign change. The presence of this sign change is a consequence of Pfaffian orientations. To compute the signature of a matchgate $G$, we assume it has a fixed Pfaffian orientation $\overrightarrow{G}$. This induces a natural Pfaffian orientation for every subgraph, $\overrightarrow{G^{\alpha}}$, where $\alpha$ is a bitstring specifying a removal pattern of the external nodes from $G$. A Pfaffian orientation may introduce an extra $(-1)$ factor, a "sign change," to the corresponding perfect matching value. The sign change of $\overrightarrow{G^{\alpha}}$ depends on $\alpha$, so the presence or absence of the "sign change" may itself change between different external node removals.

Thus, our main goal is to show that the *change* of the sign change occurs in a pattern such that the MGI still hold. We do so using Theorem 4.3. Essentially, it proves the following. For any two fixed bit positions $i < j$ referencing the external nodes, let $b_i b_j \in \{0,1\}^2$ be the bit pattern on these two bits. Then, while the sign change may be different for different values of $b_i b_j$, *the change of sign change* when we go from $b_i b_j$ to $\overline{b_i}\,\overline{b_j}$ is always the same, independent of the removal pattern on the other external nodes. This is succinctly expressed as a *quadruple product identity*. Moreover, this is in fact the strongest statement we can say about a pair of nodes and their change of signs (see Figure 1). Fortunately this is also sufficient to prove the MGI.

This paper is organized as follows. In Section 2 we define all the concepts and terminology in the signature theory of planar matchgates. We will also prove that MGI imply the Parity Condition. We will restrict discussion to planar matchgates pertaining to signature theory here. The terminology having to do with general (not necessarily planar) matchgates and characters will be delayed until Section 6. In Section 3 we will give a self-contained proof of some known identities. This is partly for the convenience of the readers, and partly to give simplified proofs when possible. For example, the earlier proof of Theorem 3.2 from [10] goes through skew-symmetric bilinear forms and operators acting on the exterior algebra of a module over some commutative ring. Here we present a direct, elementary proof. In Section 4 we prove that every matchgate signature satisfies the MGI. In Section 5 we prove that the MGI are also sufficient conditions for a signature to be realizable as a matchgate signature. Here we also give the simplified construction of a crossover gadget. In Section 6 we discuss the character theory. In Section 7 we give the direct construction for matchgates realizing symmetric signatures. Some concluding remarks are in Section 8.

## 2 Preliminaries

**Matchgate, PerfMatch definitions** A matchgate is an undirected weighted plane graph $G$ with $k$ distinguished "external" nodes on its outer face, ordered in a clockwise order. (We will see shortly that without loss of generality we may assume the graph $G$ is connected. Therefore it is a plane graph, i. e., a planar graph given with a particular planar embedding, and the outer face is both uniquely defined and has a connected boundary.) Without loss of generality, we assume all edge weights are non-zero; zero weighted edges can be deleted. The weights can be from any field $\mathbb{F}$. We define the perfect matching polynomial, $\mathrm{PerfMatch}(G)$, as the following:

$$\mathrm{PerfMatch}(G) = \sum_{M \in \mathcal{M}(G)} \prod_{e \in M} w(e) \tag{2.1}$$

where $\mathcal{M}(G)$ is the set of all perfect matchings in $G$ and $w(e)$ is the weight of edge $e$ in $G$. For each length-$k$ bitstring $\alpha$, $G$ defines a subgraph $G^{\alpha}$ obtained from $G$ by the following operation: For all $1 \le i \le k$, if the $i$-th bit $\alpha_i$ of $\alpha$ is 1, then we remove the $i$-th external node and all its incident edges. Thus, $G^{00\ldots0} = G$, and $G^{11\ldots1}$ is $G$ with *all* external nodes removed.

**Signature, perfect matching term definitions** We define the signature of the matchgate $G$ as the vector $\Gamma_G = (\Gamma_G^{\alpha})$, indexed by $\alpha \in \{0,1\}^k$, as follows:

$$\Gamma_G^{\alpha} = \mathrm{PerfMatch}(G^{\alpha}) = \sum_{M \in \mathcal{M}(G^{\alpha})} \prod_{e \in M} w(e)\,. \tag{2.2}$$

For a perfect matching $M \in \mathcal{M}(G^{\alpha})$ we define $\Gamma_G^{\alpha}(M) = \prod_{e \in M} w(e)$ as the *perfect matching term*, equal to the product of the edge weights for the matching $M$. Where $G$ is clear, we omit the subscript $G$, and write $\Gamma^{\alpha}$ for $\Gamma_G^{\alpha}$, and $\Gamma^{\alpha}(M)$ for $\Gamma_G^{\alpha}(M)$.

**Pfaffian orientations, induced Pfaffian orientations** For a plane graph $G$, the value $\mathrm{PerfMatch}(G)$ can be computed using Kasteleyn's algorithm [14] via the Pfaffian. A *Pfaffian orientation* on $G$ is an assignment of a direction to each edge of $G$ in such a way that each face, except possibly the outer face, has an odd number of clockwise oriented edges when one traverses the boundary of the face. Such an orientation is easy to compute for any plane graph. Note that any "bridge edge" (an edge both sides of which belong to the same face) can be oriented arbitrarily, and the traversal of the face will count the edge twice, once clockwise and once counter-clockwise. Under a *Pfaffian orientation*, defined below, on $G$, the Pfaffian of a skew-symmetric matrix defined by $G$ and the orientation is equal to $\pm\mathrm{PerfMatch}(G)$. We fix a single Pfaffian orientation for $G$ and call the directed graph $\overrightarrow{G}$. Note that $\overrightarrow{G}^{\alpha}$, which is obtained from $\overrightarrow{G}$ by removing some vertices and their incident edges according to $\alpha$, is *also* Pfaffian-oriented. This is because we only remove zero or more vertices on the outer face, and the removal of these vertices and their incident edges does not create any *non-outer face*. Thus a single fixed Pfaffian orientation for $G$ induces a set of Pfaffian orientations, one for each $G^{\alpha}$. We consider a Pfaffian orientation for $G$ is fixed, and each $G^{\alpha}$ inherits the induced Pfaffian orientation.

**Skew-symmetric matrix** Now we assume the vertices of $G$ are labeled by a totally ordered set, for example, $1 < 2 < \ldots < n$. Given an orientation on $G$, we define a skew-symmetric adjacency matrix $A = A_{\overrightarrow{G}}$ for $\overrightarrow{G}$ as follows. Let $(u,v)$ be a directed edge from $u$ to $v$ in $\overrightarrow{G}$. Then $A_{u,v} = w(\{u,v\})$, and $A_{v,u} = -w(\{u,v\})$, where $w(\{u,v\})$ is the weight of the corresponding edge in $G$. The diagonal and all other locations $(u,v)$ not corresponding to an edge in the matrix $A$ are set to 0. As a result, the lower-left triangle of $A$ is the negation of the upper-right triangle.

**Pfaffian** The Pfaffian of an $n \times n$ matrix, where $n \geq 2$ is even, is defined as follows:

$$\mathrm{Pf}(A) = \sum_{\pi} \varepsilon_\pi A_{i_1,i_2} A_{i_3,i_4} \cdots A_{i_{n-1},i_n} \tag{2.3}$$

where the sum is over all permutations

$$\pi = \begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix}$$

such that $i_1 < i_2$, $i_3 < i_4$, $\ldots$, $i_{n-1} < i_n$ and $i_1 < i_3 < i_5 < \ldots < i_{n-1}$. The term $\varepsilon_\pi$ is $-1$ or 1 depending on whether the parity of $\pi$ is odd or even, respectively. We note that there is a natural 1-1 correspondence between permutations $\pi$ in this *canonical* expression and partitions of $[n]$ into disjoint pairs, which are potential perfect matchings. A permutation $\pi$ corresponds to an actual perfect matching iff all the pairs are edges. It is known and easy to verify that the sign $\varepsilon_\pi$ can also be computed by the parity of the number of overlapping pairs ($+1$ if it is even, $-1$ if it is odd). We say $\{i_{2k-1}, i_{2k}\}$ and $\{i_{2\ell-1}, i_{2\ell}\}$ is an overlapping pair iff $i_{2k-1} < i_{2\ell-1} < i_{2k} < i_{2\ell}$ or $i_{2\ell-1} < i_{2k-1} < i_{2\ell} < i_{2k}$.

We note that the term $\varepsilon_\pi A_{i_1,i_2} A_{i_3,i_4} \cdots A_{i_{n-1},i_n}$ is the same for any listing of the partition $[n] = \{i_1, i_2\} \cup \{i_3, i_4\} \cup \ldots \cup \{i_{n-1}, i_n\}$, where

$$\pi = \begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix},$$

independent of the ordering of the pairs, as well as the order within each pair. We also note that this definition is valid for any linear order on the vertices; it need not be the set of consecutive integers from 1 to $n$. This is particularly relevant when we consider the Pfaffian of $\overrightarrow{G}^\alpha$, where the vertices will inherit the labeling from $G$.

As convention, if $n$ is odd, then $\mathrm{Pf}(A) = 0$; if $n$ is zero, then $\mathrm{Pf}(A) = 1$.

**Relating Pf to PerfMatch** If $A = A_{\overrightarrow{G}}$, we call $\varepsilon_\pi A_{i_1,i_2} A_{i_3,i_4} \cdots A_{i_{n-1},i_n}$ a *Pfaffian term*. As observed, there is a 1-to-1 correspondence between all non-zero Pfaffian terms and perfect matchings in $\mathcal{M}(G)$. If $M$ is a perfect matching, we denote the corresponding Pfaffian term by $\mathrm{Pf}_{\overrightarrow{G}}(M)$. A perfect matching term has the same value, up to a $\pm$ sign, as the corresponding Pfaffian term. In other words, $\mathrm{Pf}_{\overrightarrow{G}}(M) = \pm\Gamma_G(M)$. They may indeed differ, even under a Pfaffian orientation. The heart of the FKT algorithm is the proof that for the skew symmetric matrix of a Pfaffian-oriented graph, either every pair of corresponding terms are the same, or every pair of corresponding terms differ by a sign. Thus, $\mathrm{Pf}(A_{\overrightarrow{G}}) = \pm \mathrm{PerfMatch}(G)$. This equality is an equality of polynomials: Given a Pfaffian oriented $\overrightarrow{G}$, there exists an $\varepsilon = \pm 1$, such that

$$\mathrm{Pf}(A_{\overrightarrow{G}}) = \varepsilon\, \mathrm{PerfMatch}(G) \tag{2.4}$$

and if (2.4) holds for one set of edge weights, then *every* Pfaffian term is $\varepsilon$ times its corresponding perfect matching term, for every set of weights.

**Pfaffian signature definition** As the orientation in $\overrightarrow{G}$ induces a Pfaffian orientation for all $G^{\alpha}$, we can naturally refer to $\overrightarrow{G^{\alpha}}$. Note that $\overrightarrow{G^{\alpha}} = \overrightarrow{G}^{\alpha}$, the oriented graph obtained by $\overrightarrow{G}$ after removing some vertices and incident edges according to $\alpha$, in the same way as before. Also note that $A_{\overrightarrow{G^{\alpha}}}$ is obtained from $A_{\overrightarrow{G}}$ by removing the appropriate columns and rows indicated by $\alpha$. We abbreviate $\mathrm{Pf}(A_{\overrightarrow{G^{\alpha}}})$ as $\mathrm{Pf}^{\alpha}_{\overrightarrow{G}}$. Where $\overrightarrow{G}$ is clear, we just write $\mathrm{Pf}^{\alpha}$. With a given Pfaffian orientation on the plane graph $G$, and a given labeling of its $k$ external nodes in clockwise order, we define the Pfaffian Signature of $\overrightarrow{G}$ to be the vector $(\mathrm{Pf}^{\alpha})$ indexed by $\alpha \in \{0,1\}^k$. Each $\mathrm{Pf}^{\alpha}$ is a sum of Pfaffian terms, by the definition of $\mathrm{Pf}(A_{\overrightarrow{G^{\alpha}}})$, under the induced Pfaffian orientation.

Critically, equation (2.4) is a term by term equation: For every $\alpha \in \{0,1\}^k$, there exists $\varepsilon(\alpha) \in \{-1,1\}$, such that for all $M \in \mathcal{M}(G^{\alpha})$,

$$\mathrm{Pf}_{\overrightarrow{G^{\alpha}}}(M) = \varepsilon(\alpha)\Gamma_{G^{\alpha}}(M)\,. \tag{2.5}$$

**Matchgate Identities** We state the Matchgate Identities, or MGI.

**Theorem 2.1.** *Let $\Gamma$ be the signature of a matchgate with $k$ external nodes. For any length-$k$ bitstrings $\alpha, \beta \in \{0,1\}^k$, let $\alpha \oplus \beta \in \{0,1\}^k$ be their bitwise XOR, and let $P = \{p_1, \ldots, p_\ell\}$, where $p_1 < \ldots < p_\ell$, be the subset of $[k]$ whose characteristic sequence is $\alpha \oplus \beta$. Here $p_i$ is the $i$-th bit where $\alpha$ and $\beta$ differ. Then, the signature $\Gamma$ satisfies:*

$$\sum_{i=1}^{\ell} (-1)^i \Gamma^{\alpha \oplus e_{p_i}} \Gamma^{\beta \oplus e_{p_i}} = 0\,, \tag{2.6}$$

*where $e_j$ denotes a length-$k$ bitstring with a 1 in the $j$-th index, and 0 elsewhere.*

We will show that this is a complete characterization of what vectors can be planar matchgate signatures.

**Parity Condition** A perfect matching has an even number of vertices. Therefore it follows that $\mathrm{PerfMatch}(G^{\alpha}) = 0$, whenever $G^{\alpha}$ has an odd number of vertices. Thus, either for all $\alpha$ of odd Hamming weight, or for all $\alpha$ of even Hamming weight, $\Gamma^{\alpha} = 0$.

**Matchgate Identities imply Parity Condition** Here we show that this Parity Condition is a consequence of MGI.

**Theorem 2.2.** *If a vector $\Gamma$ obeys the MGI, then it also obeys the Parity Condition.*

*Proof.* For a contradiction assume $\Gamma^{\alpha} \neq 0$ and $\Gamma^{\beta} \neq 0$, for some $\alpha$ and $\beta$ of even and odd Hamming weight respectively. We define $\widetilde{\Gamma}$ by $\widetilde{\Gamma}^{\gamma} = \Gamma^{\gamma \oplus \alpha}$. Since $\gamma \oplus \gamma' = (\gamma \oplus \alpha) \oplus (\gamma' \oplus \alpha)$, if the vector $\Gamma$ obeys the MGI then the vector $\widetilde{\Gamma}$ also obeys the MGI. Also $\widetilde{\Gamma}^{00\ldots0} = \Gamma^{\alpha} \neq 0$ and $\widetilde{\Gamma}^{\beta \oplus \alpha} = \Gamma^{\beta} \neq 0$. Note that $\beta \oplus \alpha$ has an odd Hamming weight.

Let $\beta' = \{p_1, \ldots, p_\ell\}$ be of minimum odd Hamming weight such that $\widetilde{\Gamma}^{\beta'} \neq 0$, where $\ell \geq 1$. Now invoke the MGI on the bitstrings $00\ldots0 \oplus e_{p_1}$ and $\beta' \oplus e_{p_1}$. That gives

$$0 = -\widetilde{\Gamma}^{00\ldots0}\widetilde{\Gamma}^{\beta'} + \sum_{i=2}^{\ell}(-1)^i \widetilde{\Gamma}^{00\ldots0\oplus e_{p_1}\oplus e_{p_i}}\widetilde{\Gamma}^{\beta'\oplus e_{p_1}\oplus e_{p_i}}\,. \tag{2.7}$$

If $\ell = 1$ then the sum $\sum_{i=2}^{\ell}$ is vacuous, and we have a contradiction. So $\ell \geq 2$ and we consider each term in the sum $\sum_{i=2}^{\ell}$. Observe that for every $2 \leq i \leq \ell$, $\beta' \oplus e_{p_1} \oplus e_{p_i}$ has an odd Hamming weight *less* than that of $\beta'$, hence $\widetilde{\Gamma}^{\beta'\oplus e_{p_1}\oplus e_{p_i}} = 0$. Thus the sum $\sum_{i=2}^{\ell}$ is zero but $\widetilde{\Gamma}^{00\ldots0}\widetilde{\Gamma}^{\beta'} \neq 0$, a contradiction. □

Nonetheless, in further development of the signature theory, our experience is that the Parity Condition is a good criterion to apply first.

**The sign** MGI were first introduced by Valiant in [23] in the context of proving certain 2-input 2-output quantum gate cannot be realized by a matchgate. It was shown that 2-input 2-output matchgates must satisfy certain identities which are named the Matchgate Identities. These identities are actually concerned with *characters* of matchgates. These so-called characters are defined directly in terms of Pfaffians, and their underlying matchgates need not be planar by definition. In the case of 2-input 2-output matchgates, these character values constitute a 4 by 4 matrix, called a character matrix. Subsequently in [1] and [2], this theory is generalized to matchgates of an arbitrary number of external nodes. The ultimate result is that there is an equivalence of matchgate characters (of not necessarily planar matchgates) and matchgate signatures (of planar matchgates). See Section 6. Furthermore Matchgate Identities (together with the Parity Condition) are a necessary and sufficient condition for a vector of values to be the signature of a (planar) matchgate. In fact, by Theorem 2.2, the Matchgate Identities already logically imply the Parity Condition.

The existing proof of the equivalence of being a matchgate signature and satisfaction of MGI (together with parity requirements) is quite long and indirect. In particular it goes through characters. More importantly, there is a gap in the existing proof that Matchgate Identities are a necessary condition for a matchgate signature. The gap is to exactly account for the change of signs from Pfaffians to signatures. We will rectify this situation. Our new proof is direct and self-contained; we show that Matchgate Identities are a necessary condition for matchgate signatures without going through characters.

We will first establish the Pfaffian Signature Identities.

**Theorem 2.3.** *Let $\overrightarrow{G}$ be a plane graph with a Pfaffian orientation and $k$ external nodes. For any length-$k$ bitstrings $\alpha, \beta \in \{0,1\}^k$, let $\alpha \oplus \beta \in \{0,1\}^k$ be their bitwise XOR, and let $P = \{p_1, \ldots, p_\ell\}$, where $p_1 < \ldots < p_\ell$, be the subset of $[k]$ whose characteristic sequence is $\alpha \oplus \beta$. Then,*

$$\sum_{i=1}^{\ell}(-1)^i \operatorname{Pf}^{\alpha\oplus e_{p_i}} \operatorname{Pf}^{\beta\oplus e_{p_i}} = 0\,. \tag{2.8}$$

Because of the "sign change" between $\operatorname{Pf}^{\alpha}$ and $\Gamma^{\alpha}$, this statement does not immediately imply Theorem 2.1. We need to know that the extra $-1$ factors between $\operatorname{Pf}^{\alpha}$ and $\Gamma^{\alpha}$ appear in just such a pattern that the $-1$ factors all cancel each other in the Matchgate Identities in (2.6) *relative to* the Pfaffian Signature Identities in (2.8). Before doing so, we will prove Theorem 2.3.

## 3 Proving the Pfaffian signature identities

Theorem 2.3 will follow from the Grassmann-Plücker Identities over Pfaffian minors of a matrix. We state the following definition of the Grassmann-Plücker Identities for a skew-symmetric matrix $A$. In writing $\mathrm{Pf}(i_1, i_2, \ldots, i_K)$ we mean the Pfaffian of the $K \times K$ matrix whose rows and columns are the $i_1, i_2, \ldots, i_K$-th rows and columns of $A$, in that order. The order matters: $\mathrm{Pf}(i_1, i_2, \ldots) = -\mathrm{Pf}(i_2, i_1, \ldots)$, for instance. In particular, if there are two identical rows and columns, the Pfaffian is 0. When we write $\mathrm{Pf}(i_1, i_2, \ldots, \widehat{i_k}, \ldots, i_K)$, the $\widehat{i_k}$ means that $i_k$ is explicitly excluded from that list.

**Theorem 3.1** (The Grassmann-Plücker Identities)**.** *Let $I = \{i_1, i_2, \ldots, i_K\}, J = \{j_1, j_2, \ldots, j_L\}$ be subsets of indices of a skew-symmetric $A$, where $i_1 < i_2 < \ldots < i_K$ and $j_1 < j_2 < \ldots < j_L$. Then*

$$\sum_{\ell=1}^{L} (-1)^{\ell-1} \mathrm{Pf}(j_\ell, i_1, \ldots, i_K) \mathrm{Pf}(j_1, \ldots, \widehat{j_\ell}, \ldots, j_L) + \sum_{k=1}^{K} (-1)^{k-1} \mathrm{Pf}(i_1, \ldots, \widehat{i_k}, \ldots, i_K) \mathrm{Pf}(i_k, j_1, \ldots, j_L) = 0\,. \tag{3.1}$$

Theorem 3.1 has the following short proof [23, 19] originally from [20].

*Proof of Theorem 3.1.* From the definition of Pfaffian:

$$\mathrm{Pf}(j_\ell, i_1, \ldots, i_K) = \sum_{k=1}^{K} (-1)^{k-1} \mathrm{Pf}(j_\ell, i_k) \mathrm{Pf}(i_1, \ldots, \widehat{i_k}, \ldots, i_K)\,, \tag{3.2}$$

$$\mathrm{Pf}(i_k, j_1, \ldots, j_L) = \sum_{\ell=1}^{L} (-1)^{\ell-1} \mathrm{Pf}(i_k, j_\ell) \mathrm{Pf}(j_1, \ldots, \widehat{j_\ell}, \ldots, j_L)\,, \tag{3.3}$$

and also

$$\mathrm{Pf}(j_\ell, i_k) + \mathrm{Pf}(i_k, j_\ell) = 0\,. \tag{3.4}$$

The proof is completed by substituting these into the left-hand side of equation (3.1). □

There is another form of these identities which is more closely related to the Pfaffian Signature Identities. We state this theorem next. An earlier proof of Theorem 3.2 appears in [10]. They go through skew-symmetric bilinear forms and operators acting on the exterior algebra $\Lambda(M)$ of an $R$-module $M$ over some commutative ring $R$. Here we present a direct, elementary proof.

**Theorem 3.2.** *Let $A, I, J$ be as above. For a subset $S$ of indices of $A$, we write $\mathrm{Pf}(S)$ when $S$ is listed in increasing order. Let $D = I \triangle J = \{k_1, \ldots, k_m\}$ (listed in increasing order) be the symmetric difference of $I, J$. Then*

$$\sum_{s=1}^{m} (-1)^{s-1} \mathrm{Pf}(I \triangle \{k_s\}) \mathrm{Pf}(J \triangle \{k_s\}) = 0\,. \tag{3.5}$$

*Proof of Theorem 3.2.* We prove Theorem 3.2 by Theorem 3.1.

Considering a term in equation (3.1), and let $x$ be the element being moved from the index set of one Pfaffian to another. If $x \in I \cap J$, clearly the term is 0. It follows that there is a one-to-one correspondence between the remaining terms in equations (3.1) and (3.5). All that remains is showing that each such term in equation (3.1) has the same sign as its counterpart in (3.5).

Suppose $x \in J - I$. In that case, the term in equation (3.1) is

$$(-1)^z \operatorname{Pf}(x, i_1, \ldots, i_K) \operatorname{Pf}(j_1, \ldots, \hat{x}, \ldots, j_L) \tag{3.6}$$

where $z$ is the number of elements in $J$ preceding $x$, equivalently those elements in $J$ less than $x$. We write $z = a + b$, where

$$a = |\{y \mid y \in J - I, y < x\}|, \tag{3.7}$$

$$b = |\{y \mid y \in J \cap I, y < x\}|, \tag{3.8}$$

and we also define

$$c = |\{y \mid y \in I - J, y < x\}|. \tag{3.9}$$

When we put the indices in $\operatorname{Pf}(x, i_1, \ldots, i_K)$ in increasing order we move $x$ along until it is in the sorted order, we move $x$ exactly $b + c$ times. Thus

$$\operatorname{Pf}(x, i_1, \ldots, i_K) = (-1)^{b+c} \operatorname{Pf}(I \cup \{x\}) \tag{3.10}$$

and so it follows that

$$(-1)^z \operatorname{Pf}(x, i_1, \ldots, i_K) = (-1)^{a+c} \operatorname{Pf}(I \cup \{x\}). \tag{3.11}$$

It is clear that $a + c$ is precisely the number of those in $D$ preceding $x$, exactly the sign in front of the corresponding term in (3.5).

The argument for the case $x \in I - J$ is symmetric. □

Now we are ready to prove Theorem 2.3.

*Proof of Theorem 2.3.* We prove Theorem 2.3 by Theorem 3.2. For a matchgate $G$, let $\alpha, \beta$ be two bitstrings of length $k$, where $k$ is the number of external nodes in $G$. The $i$-th bit of $\alpha$, denoted $\alpha_i$, corresponds to the $i$-th external node in $G$ in clockwise order.

Let $U$ be the set of all internal (that is, not external) nodes in $G$. We define $I = \{v_i \mid \alpha_i = 0\} \cup U$, where $v_i$ is the label of the node in $G$ which is the $i$-th external node referenced by $\alpha_i$. Similarly let $J = \{v_i \mid \beta_i = 0\} \cup U$. Observe that $I \triangle J = \{v_i \mid \alpha_i \neq \beta_i\}$. It follows that there is a term-for-term correspondence between equation (3.5) of Theorem 3.2 and equation (2.8) of Theorem 2.3. □

# 4 Matchgates satisfy Matchgate Identities

We will now prove that while $\operatorname{Pf}^\alpha$ may differ from $\Gamma^\alpha$ by a sign depending on $\alpha$, the differences occur in just such a pattern that they cancel in the MGI. This will allow us to conclude that the Pfaffian Signature Identities (2.8) differ from the MGI (2.6) by a global $\pm 1$ factor, thus proving the Matchgate Identities.

**Definition 4.1.** For any $M^\alpha \in \mathcal{M}(G^\alpha)$, where $G^\alpha$ has the orientation $\overrightarrow{G^\alpha}$, we define the *sign* of the perfect matching $M^\alpha$ to be:

$$\operatorname{sgn}(M^\alpha) = \frac{\operatorname{Pf}_{\overrightarrow{G^\alpha}}(M^\alpha)}{\Gamma_{G^\alpha}(M^\alpha)} \in \{-1, 1\}. \tag{4.1}$$

Recall that it is a polynomial equality that the Pfaffian is equal to $\pm$PerfMatch, under a Pfaffian orientation. Thus we can conclude that, for $\mathrm{Pf}_{\overrightarrow{G^{\alpha}}}(M^{\alpha})$ and $\Gamma_{G^{\alpha}}(M^{\alpha})$, the value of $\mathrm{sgn}(M^{\alpha})$ is the same $\pm 1$ for every perfect matching $M^{\alpha} \in \mathcal{M}(G^{\alpha})$. This allows us to define a very useful function:

**Definition 4.2.** For any $\alpha$ such that $\mathcal{M}(G^{\alpha}) \neq \emptyset$, we take any $M^{\alpha} \in \mathcal{M}(G^{\alpha})$ and define the function $\delta$:

$$\delta(\alpha) = \mathrm{sgn}(M^{\alpha}) = \frac{\mathrm{Pf}_{\overrightarrow{G^{\alpha}}}(M^{\alpha})}{\Gamma_{G^{\alpha}}(M^{\alpha})}. \tag{4.2}$$

Note that $\delta(\alpha)$ is well-defined; the value is independent of the choice of $M^{\alpha} \in \mathcal{M}(G^{\alpha})$. It is defined whenever $\mathcal{M}(G^{\alpha}) \neq \emptyset$. Recall that we have a fixed Pfaffian orientation for $G$ and a fixed induced orientation for all $G^{\alpha}$.

We are ready to state the key theorem which implies the MGI.

**Theorem 4.3.** *Let $1 \le i < j \le k$. Let $b, c \in \{0,1\}$ and denote $\overline{b} = 1-b$, $\overline{c} = 1-c$. For any strings $u, \tilde{u} \in \{0,1\}^{i-1}$, $v, \tilde{v} \in \{0,1\}^{j-i-1}$, and $w, \tilde{w} \in \{0,1\}^{k}$, the following is true:*

$$\delta(ubvcw)\delta(u\overline{b}v\overline{c}w) = \delta(\tilde{u}b\tilde{v}c\tilde{w})\delta(\tilde{u}\overline{b}\tilde{v}\overline{c}\tilde{w}) \tag{4.3}$$

*when all four $\delta$ terms involved are defined.*

Note that the only equality we claim here is the pairwise product being the same. The individual $\delta$ terms can vary; for example there are cases when the above equation resolves to $(1)(-1) = (-1)(1)$ (see Figure 1). The theorem asserts that if flipping two fixed bits changes the "sign change" $\delta$ for some $u, v, w$, then it will change the sign change for all $u, v, w$ of the same lengths whenever $\delta$ is defined. It is an invariance of *the change of sign change*.

Since each factor in (4.3) is $\pm 1$, this equation can also be equivalently expressed as the following *quadruple product identity*:

$$\delta(ubvcw)\delta(u\overline{b}v\overline{c}w)\delta(\tilde{u}b\tilde{v}c\tilde{w})\delta(\tilde{u}\overline{b}\tilde{v}\overline{c}\tilde{w}) = 1. \tag{4.4}$$

**Theorem 4.3 implies the MGI** Before proving Theorem 4.3 we show how it proves Theorem 2.1.

If there are no non-zero terms in a particular MGI indexed by $\alpha, \beta \in \{0,1\}^k$, then the MGI is trivial.

There is a 1-1 correspondence between the non-zero terms in (2.6) and (2.8). Since (2.8) is an equality, if there are non-zero terms in (2.6), then there are at least two such terms. Consider all non-zero terms in (2.6), and let each non-zero term from the Pfaffian identity (2.8) be divided by its corresponding MGI term in (2.6). The ratio is of the form

$$\frac{\mathrm{Pf}^{\alpha \oplus e_i}\,\mathrm{Pf}^{\beta \oplus e_i}}{\Gamma^{\alpha \oplus e_i}\Gamma^{\beta \oplus e_i}} = \delta(\alpha \oplus e_i)\delta(\beta \oplus e_i), \tag{4.5}$$

where $i$ is a bit location where $\alpha_i \neq \beta_i$. Consider any two such terms and form the *product* of the two products of the pairs. This quadruple product has the form

$$\delta(\alpha \oplus e_i)\delta(\beta \oplus e_i)\delta(\alpha \oplus e_j)\delta(\beta \oplus e_j) \tag{4.6}$$

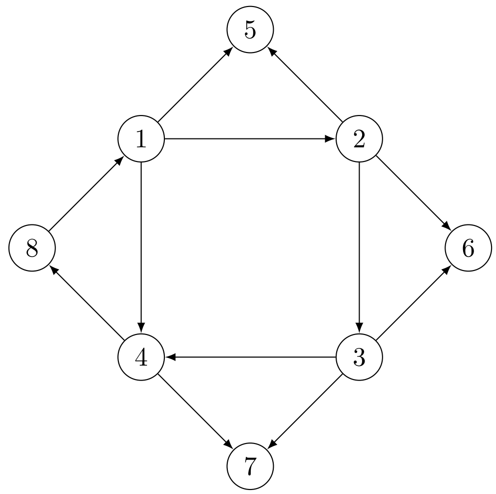


Figure 1: This graph is an example of a nontrivial instance of equation (4.3). All edge weights are 1. Let the external nodes be $5,6,7,8$. Observe that $\delta(0000)=1, \delta(1100)=-1, \delta(0011)=-1, \delta(1111)=1$. Thus, if we let $b,c$ refer to the first two external nodes, $u,v$ both be the empty string, and $w=00$ and $\tilde{w}=11$, we get the situation where equation (4.3) becomes $(1)(-1)=(-1)(1)$.

for some $1 \leq i < j \leq k$, which is the same as

$$\delta(\alpha \oplus e_i)\delta(\alpha \oplus e_j)\delta(\beta \oplus e_j)\delta(\beta \oplus e_i)\,. \tag{4.7}$$

Let $\alpha_\ell$ be the $\ell$-th bit in $\alpha$ ($1 \leq \ell \leq k$). Recall that $\alpha_i = \overline{\beta_i}, \alpha_j = \overline{\beta_j}$. Letting $b = \overline{\alpha_i}$ and $c = \alpha_j$, we see that we can use Theorem 4.3 to conclude that the product of the first two terms equals the product of the other two terms in (4.7), and so the whole product must be 1. This implies that all Pfaffian identity terms differ from their corresponding MGI terms by the same global $\pm 1$ constant. Note that $\delta$ is not defined exactly when that term in the MGI is 0 (and the corresponding Pfaffian Signature Identity term is also 0), so it is sufficient to consider only those terms in the MGI where the relevant $\delta$ is defined.

Theorem 2.1 is proved assuming Theorem 4.3.

Now we will prove Theorem 4.3. We first prove for the case $b=c=0$. The proof for the case $b=1, c=0$ is similar with only a few extra complications. The other cases follow by symmetry.

**Preprocessing** In the following, and for the rest of the paper, all newly-introduced edges have weight 1 unless otherwise specified. We assume that $G$ is preprocessed in the following way: First we append a path of length 2 from each external node in $G$. For the $i$-th external node, we will connect it to a new node called $\hat{i}$, which is then connected to another new node called $i$. The new nodes $1,2,\ldots,k$ are now considered external nodes, and are labeled as such within the graph. All other nodes, including all original nodes and all $\hat{1},\hat{2},\ldots,\hat{k}$ are non-external nodes. The node $\hat{i}$ will be given the label $2k+1-i$. Thus $\hat{1},\hat{2},\ldots,\hat{k}$ are ordered reversely $2k > 2k-1 > \ldots > k+1$ respectively. All other nodes (the original nodes of $G$) are labeled arbitrarily starting from $2k+1$. The modified graph will now be called $G$. Now

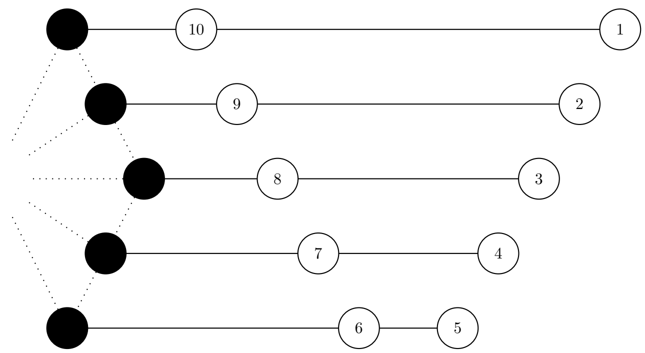


Figure 2: An example of preprocessing.

all external nodes are at the end of a path of length at least 2. It is easy to check that the signature $\Gamma$ is not changed. As an example of the preprocessing for $k = 5$, consider Figure 2.

Second, we make $G$ a connected graph. If the graph is already connected then we do nothing. Suppose it is not connected and there are several connected components $G_i$. Consider a clockwise traversal of all the external nodes. We may consider the planar embedding is on the sphere with one fixed point in the outer face designated as $\infty$. We temporarily connect each external node to $\infty$ by non-intersecting paths. As we clockwise-traverse from one external node to the next, if they belong to different components $G_i$ and $G_j$, we can connect one non-external node $u$ from $G_i$ to one non-external node $v$ from $G_j$ by a path of length 2: $u, e = \{u,w\}, w, e' = \{w,v\}, v$, together with one extra node $w'$ and an edge $\{w,w'\}$. This gadget can be made disjoint from all the temporary paths to $\infty$, and also disjoint from each other. In any perfect matching, $w$ is matched to $w'$ and therefore this gadget has no effect on the signature. Then we remove the temporary paths to $\infty$. The reasons for this construction are to make the matchgate graph (1) connected, and (2) its outer face uniquely well-defined for the given planar embedding, with a connected boundary.

Lastly, we concern ourselves with the orientation $\overrightarrow{G}$ for $G$. The $k$ external nodes are labeled clockwise 1 through $k$ exactly in that order. When we index $G$ with a length-$k$ bitstring $\alpha$, the bits in $\alpha$ refer to the external nodes in $G$ in this clockwise order. The neighbor $\hat{i}$ of $i$ is labeled $2k+1-i$. Then we let $\overrightarrow{G}$ be any Pfaffian orientation of $G$. Note that the orientation of *bridge* edges (edges that are not part of any cycle) have no bearing on the orientation being a Pfaffian orientation, and therefore can be arbitrary. In particular, for each $\{i,\hat{i}\}$ edge (being a bridge edge) we assume it is oriented in the order $(i,\hat{i})$: from low to high.

With our graph so preprocessed, we are ready to prove our theorem. For every bit values $b$ and $c$, and strings $u,v,w$, for brevity we will use $G^{bc}$ to refer to the graph $G^{ubvcw}$, suppressing $u,v,w$.

*Proof for the case $b = 0, c = 0$.* We assume that $\delta(u0v0w)$ and $\delta(u1v1w)$ are both defined (for the particular $u,v,w$).

Hence there exists a perfect matching in $G^{00}$, call it $M^{00}$. Similarly there exists a perfect matching in $G^{11}$, call it $M^{11}$. Let $e^* = \{i, j\}$ be a new edge (recall that $i < j$ are the external nodes referenced by $b,c$). This is an undirected edge placed in the outer face. Define the graph $G^* = G^{00} \cup \{e^*\}$, having the same set of vertices as $G^{00}$ and one extra edge $e^*$. See Figure 3. This introduces a new non-outer

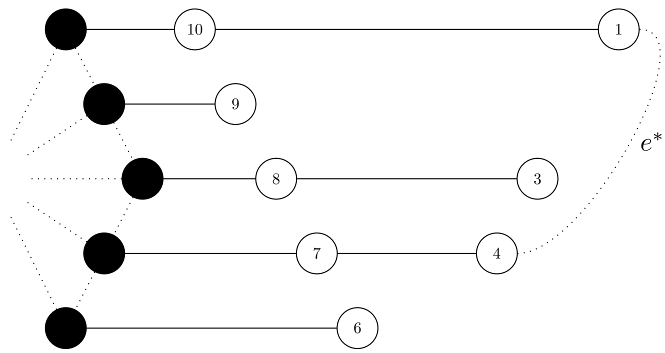


Figure 3: Adding $e^*$ in the $b=0, c=0$ case. In this example $i=1$, $j=4$, and $bvc = 0100$.

face, consisting of the segment from external nodes $i$ to $j$ (corresponding to $bvc$) followed by $e^*$. The segment has a path from $i$ to $j$ through all the external nodes $\ell$ or its neighbor $\hat{\ell}$ referenced in $v$ because the boundary of the outer face is connected. Viewed from within the new non-outer face just formed by this path and $e^*$, the segment $bvc$ is traversed in counter-clockwise direction.

By adding $e^*$ we have exactly one more face in $G^*$ compared to $G$, as well as compared to $G^{00}$ and $G^{11}$. Let $\overrightarrow{G^*} = \overrightarrow{G^{00}} \cup \{\overrightarrow{e^*}\}$ with $\overrightarrow{e^*}$ oriented either as $(i,j)$ or as $(j,i)$, such that that new face has an odd number of clockwise oriented edges, as demanded by Kasteleyn's algorithm to produce a Pfaffian orientation. We note that each existing bridge edge $\{\ell, \hat{\ell}\}$ corresponding to a bit 0 in $v$ contributes exactly one extra clockwise oriented edge in the traversal around the boundary of the new face, since it is traversed in both directions exactly once. We define $M^* = M^{11} \cup \{e^*\}$. Note that $M^* \in \mathcal{M}(G^*)$ and we may also consider $M^{00} \in \mathcal{M}(G^*)$.

We shall use $M^*$ as an intermediate step to understand how $\delta(u0v0w)$ and $\delta(u1v1w)$ are related. Our goal is to show that their product is a function entirely of $i$, $j$ and $\overrightarrow{G}$, and independent of $u$, $v$ and $w$, thus proving our theorem.

**Claim:** The signs of $M^*$ and $M^{00}$ are the same. Formally:

$$\frac{\mathrm{Pf}_{\overrightarrow{G^{00}}}(M^{00})}{\Gamma_{G^{00}}(M^{00})} = \frac{\mathrm{Pf}_{\overrightarrow{G^*}}(M^{00})}{\Gamma_{G^*}(M^{00})} = \frac{\mathrm{Pf}_{\overrightarrow{G^*}}(M^*)}{\Gamma_{G^*}(M^*)}. \tag{4.8}$$

The first equality follows from the fact that adding the edge $e^*$ to $G^{00}$ does not change the Pfaffian term nor the perfect matching term, both corresponding to the perfect matching $M^{00}$, since $M^{00}$ does not contain the edge $e^*$. The second equality follows from the fact that *all* perfect matchings in a Pfaffian-oriented graph must have the same sign. terms in a Pfaffian-oriented graph must have the same sign.

Now we compare $M^*$ and $M^{11}$. The perfect matching terms are the same, $\Gamma_{G^*}(M^*) = \Gamma_{G^{11}}(M^{11})$, since the additional edge $e^*$ has weight 1. We write out their Pfaffian terms explicitly. For $\mathrm{Pf}_{\overrightarrow{G^{11}}}(M^{11})$ we will write it in the canonical form where the listing of matched edges are given according to the stipulation after (2.3). Note that the nodes of $G^{11}$ are linearly ordered by the induced order from that of $G$. For $\mathrm{Pf}_{\overrightarrow{G^*}}(M^*)$ we will write it by appending the extra matched pair $\{i,j\}$ in the order $i<j$ at the end.

(4.9)

$$\mathrm{Pf}_{\overrightarrow{G^{11}}}(M^{11}) = \varepsilon_{\pi_1} A_{x_1,x_2} A_{x_3,x_4} \cdots A_{x_{n-1},x_n} \tag{4.10}$$

and

$$\mathrm{Pf}_{\overrightarrow{G^*}}(M^*) = \varepsilon_{\pi_2} A_{x_1,x_2} A_{x_3,x_4} \cdots A_{x_{n-1},x_n} A_{i,j} \tag{4.11}$$

where $x_1 < x_2, x_3 < x_4, \ldots, x_{n-1} < x_n$, $x_1 < x_3 < \ldots < x_{n-1}$. The value $A_{i,j} = \pm 1$, and it is $+1$ if $\overrightarrow{e^*}$ is oriented as $(i,j)$ and it is $-1$ if it is oriented as $(j,i)$, according to Kasteleyn's algorithm. The sign of the permutation $\varepsilon_{\pi_1}$ counts the parity of the overlapping pairs among $\{\{x_1,x_2\},\{x_3,x_4\},\ldots,\{x_{n-1},x_n\}\}$. The sign $\varepsilon_{\pi_2}$ counts the parity of the overlapping pairs among $\{\{x_1,x_2\},\{x_3,x_4\},\ldots,\{x_{n-1},x_n\},\{i,j\}\}$. Thus $\varepsilon_{\pi_2}/\varepsilon_{\pi_1} = (-1)^z$, where $z$ is the number of overlaps between $\{i,j\}$ and the edges in $M^{11}$.

We account for these two sources of change in values separately.

Consider $\varepsilon_{\pi_2}/\varepsilon_{\pi_1}$. To form an overlapping pair with $\{i,j\}$, a pair must be an edge with one label between $i$ and $j$ and one label outside. Vertices with a label between $i$ and $j$ correspond exactly to the external nodes within the segment $v$ that are not removed. These external nodes must be matched within $M^{11}$ to a node of a label greater than $j$. It follows that $z$ is precisely the number of 0's within $v$.

Now consider $A_{i,j}$. It is $-1$ if $e^*$ is oriented high-to-low in $\overrightarrow{G^*}$, and 1 otherwise. Let $f(\overrightarrow{G},i,j)$ be this value when the orientation of $e^*$ is made to the graph $G^{11\ldots1\oplus e_i \oplus e_j}$—the graph obtained from $G$ with all external nodes removed except $i$ and $j$—according to Kasteleyn's algorithm. Relative to this, if the orientation of $e^*$ is made to the graph $G^*$, the orientation is changed according to the parity of the number of zeros in $v$, the removal pattern within the segment between $i$ and $j$. More precisely, each 0 within $v$ adds one more bridge edge of the form $\{\ell,\hat{\ell}\}$ where $i < \ell < j$ and changes the orientation of $e^*$ exactly once. Hence the value $A_{i,j}$ is precisely $f(\overrightarrow{G},i,j)(-1)^z$, where, again $z$ is the number of 0's within $v$.

Returning to our Pfaffian terms:

$$\mathrm{Pf}_{\overrightarrow{G^{11}}}(M^{11}) = \varepsilon_{\pi_1} A_{x_1,x_2} A_{x_3,x_4} \cdots A_{x_{n-1},x_n} \tag{4.12}$$

and

$$\begin{aligned} \mathrm{Pf}_{\overrightarrow{G^*}}(M^*) &= \varepsilon_{\pi_2} A_{x_1,x_2} A_{x_3,x_4} \cdots A_{x_{n-1},x_n} A_{i,j} && (4.13)\\ &= \varepsilon_{\pi_1} A_{x_1,x_2} A_{x_3,x_4} \cdots A_{x_{n-1},x_n} f(\overrightarrow{G},i,j)\,. && (4.14) \end{aligned}$$

Note that the two factors $(-1)^z$ are canceled. So the sign difference between $\delta(u0v0w)$ and $\delta(u1v1w)$ is entirely a function of $\overrightarrow{G}$ and $i,j$, and not the constituent $u,v,w$. □

*Proof for the case $b=1, c=0$.* Following the idea of $M^{00}$ and $M^{11}$ from the previous proof, we define $M^{01}$ and $M^{10}$ in the graphs $G^{01}, G^{10}$ respectively. Recall that the neighbor of $i$ is $\hat{i}$, and the neighbor of $j$ is $\hat{j}$, $\{i,\hat{i}\} \in M^{01}$ and $\{j,\hat{j}\} \in M^{10}$, and that they are specially labeled such that $i < j < \hat{j} < \hat{i}$. We define a new edge $e^* = \{j,\hat{i}\}$, and $G^* = G^{10} \cup \{e^*\}$. See Figure 4. The edge $e^*$ is drawn on the outer face of $G^{10}$ so that $G^*$ is a plane graph with one more non-outer face. We orient $G^*$ to $\overrightarrow{G^*}$, namely to orient the edge $e^*$ appropriately as before by Kasteleyn's algorithm. Let $M^* = (M^{01} - \{i,\hat{i}\}) \cup \{e^*\}$.

We claim, using the same reasoning from the previous proof, that $M^*$ and $M^{10}$ have the same sign.

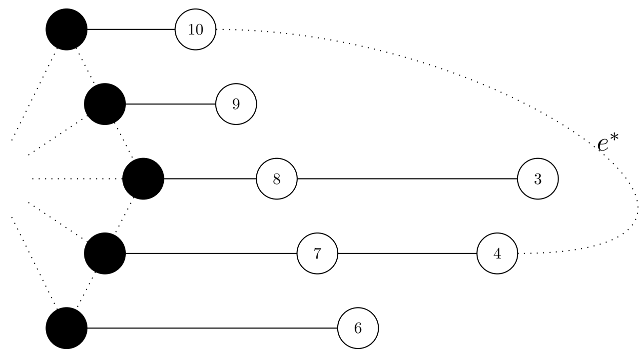


Figure 4: Adding $e^*$ in the $b = 1, c = 0$ case. In this example $\hat{\imath} = 10$, $j = 4$, and $bvc = 1100$.

$$\frac{\mathrm{Pf}_{\overrightarrow{G^{10}}}(M^{10})}{\Gamma_{G^{10}}(M^{10})} = \frac{\mathrm{Pf}_{\overrightarrow{G^*}}(M^{10})}{\Gamma_{G^*}(M^{10})} = \frac{\mathrm{Pf}_{\overrightarrow{G^*}}(M^*)}{\Gamma_{G^*}(M^*)}\,. \tag{4.15}$$

The first equality is because $M^{10}$ does not contain the edge $e^*$ which was added to $G^{10}$ to obtain $G^*$. The second equality is because $M^{10}$ and $M^*$ are both perfect matchings in a Pfaffian oriented graph $\overrightarrow{G^*}$.

Now we only need to compare $M^*$ and $M^{01}$. The perfect matching terms are the same, $\Gamma_{G^*}(M^*) = \Gamma_{G^{01}}(M^{01})$, since both edges $e^*$ and $\{i, \hat{\imath}\}$ have weight 1. We shall use the same approach as before to analyze the Pfaffian terms. Once again we write their Pfaffian terms explicitly:

$$\mathrm{Pf}_{\overrightarrow{G^{01}}}(M^{01}) = \varepsilon_{\pi_1} A_{x_1,x_2} A_{x_3,x_4} \cdots A_{x_{n-1},x_n} A_{i,\hat{\imath}} \tag{4.16}$$

and

$$\mathrm{Pf}_{\overrightarrow{G^*}}(M^*) = \varepsilon_{\pi_2} A_{x_1,x_2} A_{x_3,x_4} \cdots A_{x_{n-1},x_n} A_{j,\hat{\imath}} \tag{4.17}$$

where the labels of the matching edges satisfy $x_1 < x_2, x_3 < x_4, \ldots, x_{n-1} < x_n$, $x_1 < x_3 < \ldots < x_{n-1}$, and $\varepsilon_{\pi_1}$ and $\varepsilon_{\pi_2}$ count the parity of the number of overlapping pairs among the matching edges in $M^{01}$ and $M^*$ respectively. To compute $\varepsilon_{\pi_2}/\varepsilon_{\pi_1}$, we only need to account for the parities of the number of overlapping pairs between $\{i, \hat{\imath}\}$ and the other matching edges in $M^{01}$, and between $\{j, \hat{\imath}\}$ and the other matching edges in $M^*$. As a necessary condition, any such an overlapping edge must have at least one end point strictly less than $\hat{\imath}$. Let us account for all edges $\{x, y\}$ with the minimum label $\min\{x, y\} < \hat{\imath}$. Those with $\min\{x, y\} < i$ are not overlapping edges since each has a unique neighbor with label greater than $\hat{\imath}$. The unique edge with $\min\{x, y\} = i$ is $\{i, \hat{\imath}\}$ in $G^{01}$, which is not present in $G^*$. The edges with $i < \min\{x, y\} < j$ are of the form $\{\ell, \hat{\ell}\}$. They are in 1-1 correspondence with the 0's in $v$, and do contribute an overlapping pair in $M^*$ but *not* in $M^{01}$. The node $j$ is not present in $G^{01}$, and the edge $e^* = \{j, \hat{\imath}\}$ has $\min\{x, y\} = j$, and is in $M^*$. All edges with $j < \min\{x, y\} < \hat{\imath}$ either do not contribute to an overlap in both $M^{01}$ and $M^*$ (when $j < \min\{x, y\} \le k$), or do contribute to an overlap in both $M^{01}$ and $M^*$ (when $k < \min\{x, y\} < \hat{\imath}$). The conclusion is that $\varepsilon_{\pi_2}/\varepsilon_{\pi_1} = (-1)^z$, where $z$ is the number of 0's in $v$.

Now consider $A_{i,\hat{i}}$ and $A_{j,\hat{i}}$. Because we oriented the bridge edge $\{i,\hat{i}\}$ from low to high, we know that $A_{i,\hat{i}}$ is 1. We now need only consider $A_{j,\hat{i}}$. By the same reasoning as in the previous proof we conclude

$$A_{j,\hat{i}} = f(\overrightarrow{G},i,j)(-1)^z, \tag{4.18}$$

where $f(\overrightarrow{G},i,j)$ is the $\pm 1$ value for $A_{j,\hat{i}}$ when we introduce the edge $\{j,\hat{i}\}$ to the graph obtained from $G$ with all external nodes removed *except* $j$, according to Kasteleyn's algorithm.

Our conclusion is the same:

$$\mathrm{Pf}_{\overrightarrow{G^{01}}}(M^{01}) = \varepsilon_{\pi_1} A_{x_1,x_2} A_{x_3,x_4} \cdots A_{x_{n-1},x_n} A_{i,\hat{i}} \tag{4.19}$$

$$= \varepsilon_{\pi_1} A_{x_1,x_2} A_{x_3,x_4} \cdots A_{x_{n-1},x_n} \tag{4.20}$$

and

$$\mathrm{Pf}_{\overrightarrow{G^*}}(M^*) = \varepsilon_{\pi_2} A_{x_1,x_2} A_{x_3,x_4} \cdots A_{x_{n-1},x_n} A_{j,\hat{i}} \tag{4.21}$$

$$= \varepsilon_{\pi_1} A_{x_1,x_2} A_{x_3,x_4} \cdots A_{x_{n-1},x_n} f(\overrightarrow{G},i,j), \tag{4.22}$$

again with the two factors $(-1)^z$ canceled. The second line follows from the fact that $A_{i,\hat{i}} = 1$. Again we conclude that the difference in sign between $ubvcw$ and $u\bar{b}v\bar{c}w$ is entirely a function of $\overrightarrow{G}$ and $i, j$, and not of $u, v, w$. $\square$

With this, the proof of Theorem 2.1 is complete, namely (planar) matchgate signatures satisfy the Matchgate Identities.

# 5 MGI imply matchgate-realizable

Any signature of a matchgate must satisfy the Matchgate Identities. In this section, we show that any $\Gamma \in (\mathbb{F}^2)^{\otimes k} = \mathbb{F}^{2^k}$ satisfying the Matchgate Identities can be realized as the signature of a matchgate with $k$ external nodes. Thus MGI are not only necessary but also sufficient conditions for matchgate signatures.

Consider a length $2^k$ vector $\Gamma$ indexed by $\{0,1\}^k$ satisfying MGI. If it is the all-zeros vector then it is trivially realizable. So assume there is at least one non-zero value.

**Preprocessing** Assume $\Gamma^\beta \neq 0$, for some $\beta \in \{0,1\}^k$. Define $\Gamma'^\alpha = \Gamma^{\alpha\oplus\overline{\beta}}/\Gamma^\beta$, where $\overline{\beta} = \beta \oplus 11\ldots1$. Thus, $\Gamma'^{11\ldots1} = 1$, and $\Gamma'$ also satisfies the MGI. In this section we will create a matchgate $G'$ with signature $\Gamma'$. Given such a $G'$, we can create a matchgate $G$ with signature $\Gamma$ as follows: First we add two new non-external nodes $u, v$ to $G'$ and an edge $\{u, v\}$ of weight $\Gamma^\beta$. Those two nodes are not connected to any other nodes—in effect they contribute exactly a factor $\Gamma^\beta$ to each perfect matching term. Then, if the $i$-th bit of $\overline{\beta}$ is one, we add a new edge $\{v_i, v_i'\}$ of weight one to the $i$-th external node $v_i$, and making $v_i'$ the new $i$-th external node. It follows that the signature of $G$ is exactly $\Gamma$.

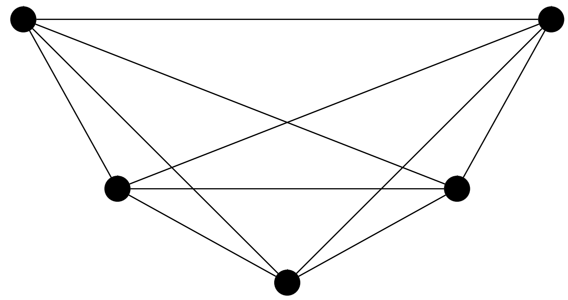

Figure 5: The embedding for $K_5$.

**Construction** We now show that we can realize $\Gamma$ satisfying MGI and $\Gamma^{11\ldots 1} = 1$. Let $K_k$ denote the complete graph on $k$ vertices. The labels of $K_k$ are ordered $1 < 2 < \ldots < k$, and correspond to the bit positions in the index for $\Gamma$. We place the nodes of $K_k$ on a convex curve, as illustrated in Figure 5. The nodes are arranged in clockwise order by their index, and two edges cross each other geometrically in the drawing of the graph iff their labels form an overlapping pair as defined before algebraically. (We assume the $k$ nodes are placed in general position, so that any pair of crossing edges intersect at a unique point. There are exactly $\binom{k}{4}$ such intersection points.) For each $\alpha$ of Hamming weight $k-2$, note that $K_k^\alpha$ has exactly one edge left. For each such $\alpha$, set the weight of the unique edge in $K_k^\alpha$ to be $\Gamma^\alpha$. This defines a weight for every edge of $K_k$.

**Equality with Pfaffian** We first prove the following equality: Let $\mathrm{Pf}(K_k^\alpha)$ be the Pfaffian value of the skew-symmetric matrix representing $K_k^\alpha$ where the nodes of $K_k^\alpha$ have the induced order from $1 < 2 < \ldots < k$. Then for all $\alpha \in \{0,1\}^k$:

$$\mathrm{Pf}(K_k^\alpha) = \Gamma^\alpha . \tag{5.1}$$

It follows that the $\binom{k}{2}$ edge weights of $K_k$ determine the $2^k$ values of any $\Gamma$ satisfying MGI.

Equation (5.1) holds for any $\alpha$ of Hamming weight $k-\ell$, for any odd $\ell$. The left-hand side would be a Pfaffian of a matrix with an odd number of rows and columns, hence 0, and the right-hand side would be 0 by the Parity Condition, Theorem 2.2. Now we consider the case when $\ell$ is even.

Clearly (5.1) holds for any $\alpha$ of Hamming weight equal to $k-2$. By assumption $\Gamma$ satisfies the Matchgate Identities (2.6). Inductively, consider $\alpha$ with Hamming weight $k-\ell$ for some even $\ell > 2$. Let $\{p_1, \ldots, p_\ell\}$ be the set of indices listed in increasing order $p_1 < \ldots < p_\ell$, where $\alpha$ has the bit 0. These are the bit positions where $\alpha$ differs from $1^k$. Consider the MGI on $\alpha \oplus e_{p_1}$ and $1^k \oplus e_{p_1}$:

$$\Gamma^\alpha \Gamma^{11\ldots 1} = \sum_{i=2}^{\ell} (-1)^i \Gamma^{\alpha \oplus e_{p_1} \oplus e_{p_i}} \Gamma^{1^k \oplus e_{p_1} \oplus e_{p_i}} . \tag{5.2}$$

As $\Gamma^{11\ldots 1} = 1$, we see that $\Gamma^\alpha$ is defined by higher Hamming weight terms.

Thus all lower Hamming weight terms of $\Gamma$ are determined by those of weight $k-2$. However we observe that, by Theorem 3.2, the Pfaffian values also satisfy exactly the same identities as MGI. By induction, it follows that $\mathrm{Pf}(K_k^\alpha) = \Gamma^\alpha$ for all $\alpha$.

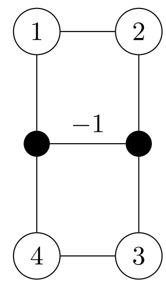


Figure 6: The crossover gadget. The external nodes are those labeled, and all edge weights are 1, except the edge labeled $-1$.

**Planarizing $K_k$** We want to show next that there exists a *planar* matchgate $G$ with signature $\Gamma_G = \Gamma$. We construct such a $G$ from $K_k$. Consider the convex embedding of $K_k$. For $k \geq 4$ it has some edge crossings, as shown in Figure 5. The planar graph $G$ is created by replacing each edge crossing with a *crossover gadget* from Figure 6. The crossover gadget is itself a matchgate $X$ with the following signature:

$$X^{0000} = 1\,, \tag{5.3}$$
$$X^{0101} = 1\,, \tag{5.4}$$
$$X^{1010} = 1\,, \tag{5.5}$$
$$X^{1111} = -1\,, \tag{5.6}$$

and for all other $\beta \in \{0,1\}^4$, $X^\beta = 0$. We note that even though geometrically this gadget is only symmetric under a rotation of $\pi$ (but not $\pi/2$), its signature is invariant under a cyclic permutation, and thus functionally it is symmetric under a rotation of $\pi/2$. Now we replace every crossing of a pair of edges in the embedded $K_k$ by a copy of $X$. For example, this replacement by the crossover gadget changes Figure 5 to Figure 7. If an edge $\{i, j\}$ in $K_k$ crosses some other edges (this happens for every non-adjacent $i$ and $j$ in the cyclic sense), then this replacement breaks the edge $\{i, j\}$ into several parts. If $\{i, j\}$ crosses $t \geq 0$ other edges, then it is replaced by $t+1$ edges (outside of crossover gadgets)—we will call them the *$i$-$j$-passage*—in addition to $t$ copies of the crossover gadget. Of course one copy of the crossover gadget is used for both edges of a pair of crossing edges in this replacement. Define $I$ to be the set of all edges in $G$ that are *not* part of a crossover gadget. Then each edge $\{i, j\}$ in $K_k$ defines a unique subset of edges in $I$, which is the *$i$-$j$-passage*. It is clear that $I$ is a disjoint union of these $i$-$j$-passages, over all $\binom{k}{2}$ pairs $1 \leq i < j \leq k$. Finally we choose one edge in each $i$-$j$-passage to have the weight $\Gamma^{[k]-\{i,j\}}$, namely the edge weight of $\{i, j\}$ in $K_k$. To be specific, we will choose this edge to be the one adjacent to $i$, the lower indexed external node of $\{i, j\}$. All other edges of $I$ are assigned weight one. See Figure 8. This defines our planar matchgate $G$ with external nodes $1 < 2 < \ldots < k$.

We claim that $\Gamma_G = \Gamma$.

Fix any $\alpha \in \{0,1\}^k$. For any $S \subseteq I$, define $\mathcal{M}_S(G^\alpha)$ to be the subset of all perfect matchings $M' \in \mathcal{M}(G^\alpha)$ such that $M' \cap I = S$. Every perfect matching $M \in \mathcal{M}(K_k^\alpha)$ defines a collection of $i$-$j$-passages, for all $\{i, j\} \in M$. Let $S(M)$ be the union of these $i$-$j$-passages. Clearly the perfect matching

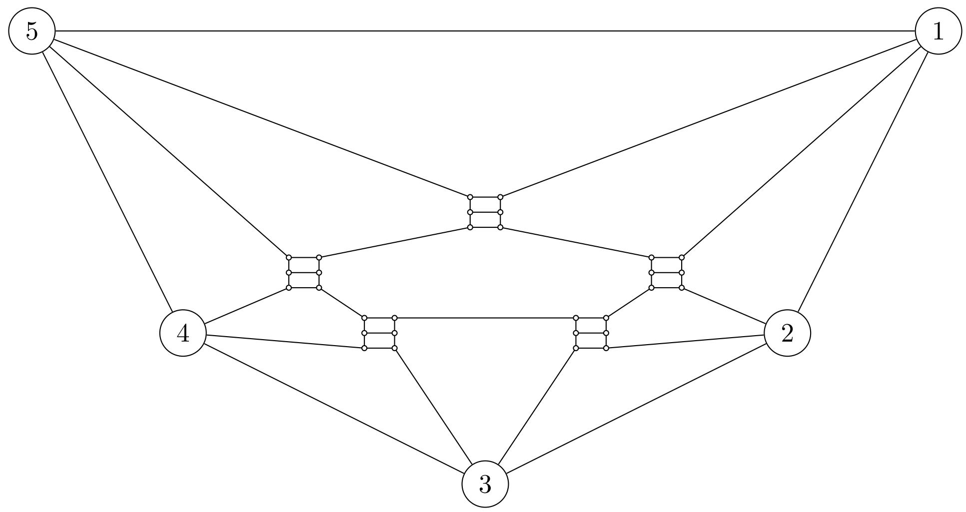


Figure 7: The graph from Figure 5 with the crossovers replaced by crossover gadgets from Figure 6.

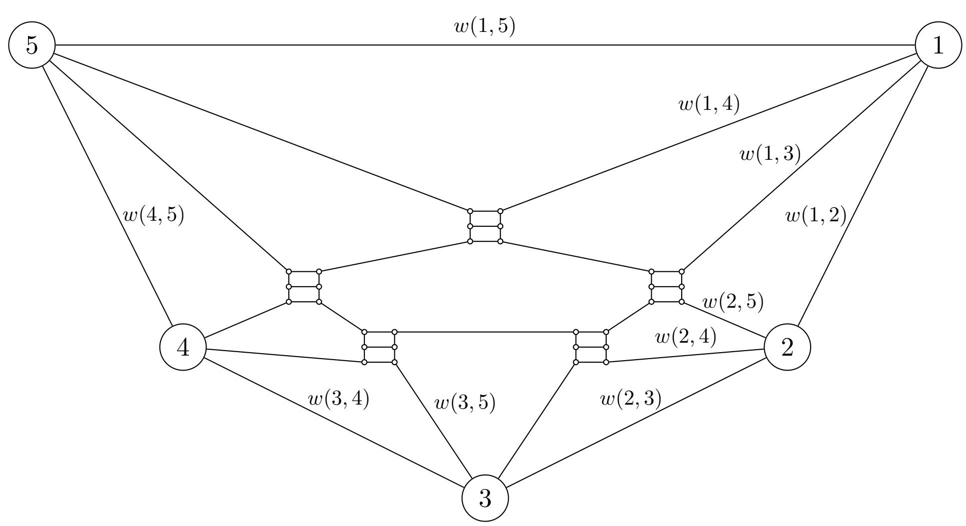


Figure 8: The "planarized" $K_5$ with edge weights. The unlabeled edges have weight 1. For notational simplicity, in the figure we use the notation $w(i,j)$ for $w(\{i,j\})$.

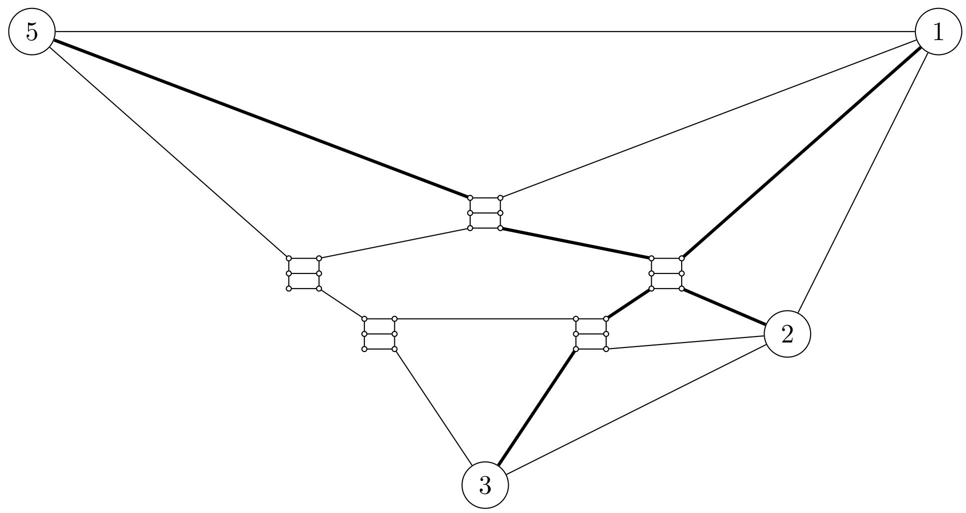


Figure 9: The thick edges comprise $S(M)$ for $G^{00010}$, where $M = \{\{1,3\},\{2,5\}\}$.

$M \in \mathcal{M}(K_k^\alpha)$ can be recovered from $S(M)$, and is unique for the given $S(M)$. There is a 1-1 correspondence between $M$ and $S(M)$. As an example, we consider $M = \{\{1,3\},\{2,5\}\} \in \mathcal{M}(K_5^{00010})$. The set $S(M)$ for $G^{00010}$ is indicated in Figure 9.

We will show that, for the purpose of computing the signature entry $\Gamma_G^\alpha$, we only need to consider those perfect matchings $M' \in \mathcal{M}(G^\alpha)$ that satisfy the following property:

**Property:** There exists an $M \in \mathcal{M}(K_k^\alpha)$, such that

$$M' \cap I = S(M)\,. \tag{5.7}$$

This is a consequence of properties of the crossover gadget. If $i$ is an external node in $G^\alpha$, then any $M' \in \mathcal{M}(G^\alpha)$ must contain a unique edge $e'$ adjacent to $i$. There is a unique $j$, which is another external node in $G$, such that $e'$ belongs to the $i$-$j$-passage. Then by the properties of the crossover gadgets along this $i$-$j$-passage, we may assume $M'$ contains all edges of this $i$-$j$-passage, saturating $j$. In particular $j$ belongs to $G^\alpha$. All other $M'$ collectively contribute 0, since the evaluation of the crossover gadget $X$ will be 0. More generally, in the computation of $\Gamma_G^\alpha = \sum_{M' \in \mathcal{M}(G^\alpha)} \prod_{e' \in M'} w(e')$, we classify all $M' \in \mathcal{M}(G^\alpha)$ according to $M' \cap I$. If $S \neq S(M)$ for any $M \in \mathcal{M}(K_k^\alpha)$, then

$$\sum_{M' \in \mathcal{M}(G^\alpha):\ M' \cap I = S} \ \prod_{e' \in M'} w(e') = 0\,. \tag{5.8}$$

In fact, for any $M' \in \mathcal{M}(G^\alpha)$ such that $M' \cap I = S$ which is not $S(M)$ for any $M \in \mathcal{M}(K_k^\alpha)$, it must be the case that at some crossover gadget $X$, $S$ induces an external removal pattern $\beta \notin \{0000, 0101, 1010, 1111\}$. Then $X^\beta = 0$, and (5.8) follows.

Thus we restrict to those perfect matchings $M' \in \mathcal{M}(G^\alpha)$ that satisfy the property (5.7). For any

$M \in \mathcal{M}(K_k^\alpha)$, it is clear that

$$\sum_{M' \in \mathcal{M}_{S(M)}(G^\alpha)} \prod_{e' \in M'} w(e') = (-1)^{c(M)} \prod_{e \in M} w(e)\,, \tag{5.9}$$

where $c(M)$ counts the number of copies of $X$ where the external removal pattern is $\beta = 1111$. Thus $c(M)$ is exactly the number of overlapping pairs in $M$. It follows that

$$\begin{aligned}
\Gamma_G^\alpha &= \sum_{M' \in \mathcal{M}(G^\alpha)} \prod_{e' \in M'} w(e') && (5.10)\\
&= \sum_{S \subseteq I} \sum_{M' \in \mathcal{M}_S(G^\alpha)} \prod_{e' \in M'} w(e') && (5.11)\\
&= \sum_{M \in \mathcal{M}(K_k^\alpha)} \sum_{M' \in \mathcal{M}_{S(M)}(G^\alpha)} \prod_{e' \in M'} w(e') && (5.12)\\
&= \mathrm{Pf}(K_k^\alpha)\,. && (5.13)
\end{aligned}$$

The last equality is because each Pfaffian term in $\mathrm{Pf}(K_k^\alpha)$ has exactly the same sign as in (5.9). Hence $\Gamma_G = \Gamma$ follows from this and (5.1).

**Theorem 5.1.** *Let $\mathbb{F}$ be any field. Any $\Gamma \in (\mathbb{F}^2)^{\otimes k}$ satisfying the Matchgate Identities is the signature of a matchgate with k external nodes. The matchgate has $O(k^4)$ nodes. If $\Gamma^{11\ldots1} = 1$, achievable by a normalization for every nonzero $\Gamma$, there exists a skew-symmetric matrix $M \in \mathbb{F}^{k\times k}$ such that $\Gamma^\alpha = \mathrm{Pf}(M^\alpha)$, where $M^\alpha$ is the matrix obtained from M by deleting all rows and columns belonging to the subset denoted by $\alpha$.*

# 6 Character

In [24] Valiant showed that a fragment of quantum computation could be simulated in polynomial time through the *character* of general (not-necessarily-planar) matchgates. The notion of a general matchgate and its character ultimately inspired planar matchgates and their signatures. The character is directly based on the notion of the Pfaffian, and what counting problems are expressible in that form.

Historically, the proof that the MGI characterize planar matchgate signatures went through character theory. In the new proof presented in this paper we bypassed the need for character and general matchgates. In this section we discuss character to show that the character of a general matchgate is essentially equivalent to the signature of a planar matchgate. While prior work expressed this equivalence in principle, the explicit statement in Theorem 6.1 is new.

## 6.1 Definitions

**The Pfaffian of an undirected graph** For an undirected, labeled, weighted graph $G = (V, E, W)$ there is a skew-symmetric matrix $M_G$. For $i < j$, we define $(M_G)_{i,j} = w(\{i, j\})$, the weight of the edge $\{i, j\} \in E$. If that edge does not exist, we say the weight is 0. For $i > j$, we define $(M_G)_{i,j} = -w(\{i, j\})$. We define $\mathrm{Pf}(G) = \mathrm{Pf}(M_G)$.

**General matchgate** A general matchgate $G = (V, E, W)$ is an undirected, labeled, weighted graph with three designated subsets of $V$. The set $X \subseteq V$ is the set of *input* nodes, the set $Y \subseteq V$ is the set of *output* nodes, and the set $T \subseteq V$ is the set of omittable nodes. These three subsets are disjoint. The nodes in $X \cup Y$ are called *external nodes*. They also define a (possibly nonempty) fourth subset $U = V - (X \cup Y \cup T)$.

The ordered labeling of the nodes of $G$ obey some rules: $\forall i \in X$, $\forall j \in T : i < j$, and $\forall j \in T$, $\forall \ell \in Y$ : $j < \ell$. In other words, ordered from low-to-high, the input nodes $X$ come first, then the omittable nodes $T$, and finally the output nodes $Y$. The remaining nodes can be interspersed throughout the ordering.

**The omittable nodes** For $G$ with a set of omittable nodes $T$, we define the "Pfaffian Sum," PfS, as follows:

$$\mathrm{PfS}(G) = \sum_{W \subseteq T} \mathrm{Pf}(G - W) \tag{6.1}$$

where the sum is over all subsets $W$ of $T$, and $G - W$ is the graph obtained from $G$ with all nodes in $W$ and their incident edges removed.

We can express this solely in terms of Pfaffians as well. Let $I$ be the index set of $M_G$. Define $\lambda_i = 1$ if $i$ is an index corresponding to an omittable node, and $\lambda_i = 0$ otherwise. Then,

$$\mathrm{PfS}(G) = \sum_{A \subseteq I} \left( \prod_{i \in A} \lambda_i \right) \mathrm{Pf}(M_G[A]) \tag{6.2}$$

where the sum is over all subsets $A$ of $I$, and $M_G[A]$ is the matrix obtained from $M_G$ with the rows and columns indexed by $A$ removed. It was shown in [24] that, for a size-$n$ graph:

$$\mathrm{PfS}(G) = \begin{cases} \mathrm{Pf}(M_G + \Lambda^{(n)}) & \text{if } n \text{ even,} \\ \mathrm{Pf}(M_G^+ + \Lambda^{(n+1)}) & \text{if } n \text{ odd,} \end{cases} \tag{6.3}$$

where $\Lambda^{(n)}$ is a simple matrix constructed from the $\lambda_i$ values and $M_G^+$ is $M_G$ with an additional final row, column of all zeros. Thus the Pfaffian Sum $\mathrm{PfS}(G)$ is also computable in polynomial time. This "omittable node" feature seems to be quite different from what has been presented for planar matchgate signatures. However, we shall see that it ultimately does not add more power.

**The character of a matchgate** Consider any $Z \subseteq X \cup Y$, a subset of the *external nodes* of $G$. A general matchgate is ultimately part of a larger *matchcircuit*, and the external nodes in $G$ are connected to external edges. The following is from [24], "[w]e consider there to exist one external edge from each node in $X \cap Z$ and from each node in $Y \cap Z$. The other endpoint of each of the former is some node of lower index than any in $V$ and of each of the latter is some node of index higher than any in $V$."

The character of a matchgate $G$ is defined as

$$\chi(G, Z) = \mu(G, Z)\,\mathrm{PfS}(G - Z)\,. \tag{6.4}$$

The term $\mu(G, Z)$ is called the *modifier value*. It is one of $\pm 1$, and corresponds to the parity of the overlapping pairs between matching edges in $E$ and external edges. Recall that the number of overlapping pairs is computed as a function of node labels. Due to the rules of index ordering, this value is determined by $(G,Z)$, and is independent of the particular matching in $\mathrm{PfS}(G-Z)$. Thus $\mu(G,Z)$ is well-defined for any $(G,Z)$.

We also define the *naked character* $\check{\chi}$ of a matchgate, without the modifier.

$$\check{\chi}(G,Z) = \mathrm{PfS}(G-Z)\,. \tag{6.5}$$

For brevity and consistency, we write $\chi_G^\alpha = \chi(G,Z)$, where $\alpha$ is the characteristic bitstring of $Z$. The naked character will be referred to as $\check{\chi}_G^\alpha$. Where $G$ is clear we may omit it.

**Matchcircuits** These matchgates, not necessarily planar, were designed to show that the evaluation of some quantum circuits could be done in polynomial time. Matchgates can be combined into *matchcircuits* in specific ways. The composition is helped by the modifiers; in fact their sole purpose is to make this composition nicely expressible as a Pfaffian. We will not go into this detail; please see [24]. From another perspective, a matchcircuit is simply a larger matchgate with a modifier value set to a constant 1, as there are no more edges external to the entire matchcircuit. The naked character of a matchcircuit is its character.

## 6.2 Equivalence of naked characters and signatures

We will prove the following theorem:

**Theorem 6.1.** *For a general matchgate $G$ with $k$ external nodes, there exist two planar matchgates $G_1$ and $G_2$ such that for all $\alpha \in \{0,1\}^k$,*

$$\check{\chi}_G^\alpha = \Gamma_{G_1}^\alpha + \Gamma_{G_2}^\alpha\,. \tag{6.6}$$

*Proof.* $G$ may not be a planar graph. We draw it by placing its nodes on a semi-circle arc. The nodes appear in a clockwise ordering, ordered exactly by their labels in the graph. The edges are drawn as chords inside the semi-circle arc. If we place the nodes in general position, then any pair of intersecting chords intersect at a unique point. Observe that two edges $(u,v),(x,y)$, where $u<v$ and $x<y$, cross in the drawing exactly when $u<x<v<y$ or $x<u<y<v$, i. e., exactly when they form an overlapping pair. This arrangement is very similar to the planar matchgate construction in Section 5.

We start by replacing every crossing of chords by the planar crossover gadget from Figure 6. For the purpose of this proof, we may consider $G$ as a subgraph of some $K_n$. After each crossing has been replaced by the crossover gadget we have a planar matchgate $G'$. We consider $X\cup T\cup Y$ as its external nodes. Let $\Gamma'$ be its signature. Let $\alpha \in \{0,1\}^{|X\cup T\cup Y|}$ indicate a bit removal pattern, and let $\beta$ and $\gamma$ be its restrictions to $X\cup Y$ and $T$ respectively. The same proof in Section 5 shows that

$$\Gamma'^\alpha = \mathrm{Pf}(G^\beta - W_\gamma)\,, \tag{6.7}$$

where $W_\gamma$ is the subset of $T$ indicated by $\gamma$.

Fix any $\beta \in \{0,1\}^{|X\cup Y|}$, such that $G^\beta$ has an even number of nodes. Then we only need to consider $\gamma \in \{0,1\}^{|T|}$ of even Hamming weight in the sum (6.7). Similarly, if $G^\beta$ has an odd number of nodes, then we only need to consider $\gamma$ of odd Hamming weight in (6.7).

The following idea is from [26, p. 1952]. There exists a planar matchgate $H$ with $t=|T|$ external nodes such that for any $\gamma \in \{0,1\}^{|T|}$ of even Hamming weight, $H^\gamma = 1$, and for any bitstring $\gamma$ of odd

Hamming weight, $H^\gamma = 0$ (see Section 7). Clearly $H$ has an even number of nodes, since $H^{00\dots0} = 1$. We define the planar matchgate $G'_1$ by attaching $H$ to the set $T$ of $G'$ on the side of the semi-circle arc *opposite* to all the intersecting chords in the embedding of $G$. Each node in $T$ is connected to a distinct external node of $H$ by an edge of weight 1. We note that composing $G'$ with $H$ in this fashion does not introduce any more edge crossings, and all external nodes $X \cup Y$ still remain on the outer face.

For all $\beta$ where $G_1'^\beta$ has an even number of nodes, which happens exactly when $G^\beta$ has an even number of nodes, the following hold:

$$\Gamma^\beta_{G'_1} = \sum_{W_{\text{even}}} \Gamma^\beta_{G'-W_{\text{even}}} = \sum_{\text{even } \gamma} \Gamma^{\alpha(\beta,\gamma)}_{G'} = \sum_{\text{even } \gamma} \operatorname{Pf}(G^\beta - W_\gamma) = \check{\chi}^\beta_G\,, \tag{6.8}$$

where the sum over $W_{\text{even}}$ is for all even-sized subsets of $T$, and $\alpha(\beta,\gamma)$ is the bit string in $\{0,1\}^{|X\cup T\cup Y|}$ formed by concatenating $\beta$ and $\gamma$, in the proper order. If $G_1'^\beta$ has an odd number of nodes, then $\Gamma^\beta_{G'_1} = 0$.

There also exists a planar matchgate $H'$ of arity $t = |T|$ such that for any $\beta$ of odd Hamming weight, $H'^\beta = 1$, and for any bitstring $\beta$ of even Hamming weight, $H'^\beta = 0$ (see Section 7). Use $H'$ instead of $H$ we can define a planar matchgate $G'_2$, which will have the signature values equal to the naked character values of $G$ for all $\beta$ for which $G^\beta$ has an odd number of nodes. If $G_2'^\beta$ has an even number of nodes, then $\Gamma^\beta_{G'_2} = 0$.

This completes the proof. □

Note that a matchcircuit is itself a large general matchgate with only a naked character. Thus, its character is also expressible as the sum of two signatures of planar matchgates.

# 7 Symmetric signatures

We return to planar matchgate signatures. We say a signature is *even* if it is the signature of an even matchgate, i. e., a matchgate with an even number of nodes. An even signature has nonzero values only for indices of even Hamming weight. We define an *odd* signature similarly. A signature $\Gamma$ of a matchgate is *symmetric* if, for all $\alpha,\beta$ of equal Hamming weight, $\Gamma^\alpha = \Gamma^\beta$. In other words, the value of a signature entry is only a function of how many 1's are in its index, not their particular pattern. These signatures are important because they have a clear combinatorial meaning. We write a symmetric arity-$k$ signature in the following form $[z_0, z_1, \dots, z_k]$, where $z_i$ is the value of the signature for an index of Hamming weight $i$. The symmetric signatures that obey the MGI have a very concise description, which we prove next.

**Theorem 7.1.** *If $[z_0,\dots,z_k]$ is an even symmetric matchgate signature, then $z_i = 0$ for all odd i, and there exist $r_1$ and $r_2$ not both zero such that for all even $i \geq 2$:*

$$r_1 z_{i-2} = r_2 z_i\,. \tag{7.1}$$

*Conversely, every sequence of values satisfying these conditions is an even symmetric matchgate signature. The statement for odd symmetric signatures is analogous.*

*Stated equivalently, a sequence is a symmetric matchgate signature iff it takes the following form: Alternate entries of $[z_0,\dots,z_k]$ are zero and the entries at the other alternate positions form a geometric progression.*

*Proof.* By the Parity Condition, all odd parity entries of the signature of an even matchgate are zero. Consider any *even* $i$ and $j$, where $0 \le i < j \le k$. We invoke the MGI for $\alpha = 1^i 1 0^{k-i}, \beta = 1^i 0 1^{j-i-1} 0^{k-j}$. We use the exponentiation notation here to denote repetition. The string $\alpha$ has an odd Hamming weight $i+1$ and $\beta$ has an odd Hamming weight $j-1$. Note that $i$ and $j$ being both even implies that $j-i-1 \ge 1$. Using the fact that $\Gamma$ is symmetric, the MGI under $\alpha, \beta$ can be simplified (where the set $P$ defined in Theorem 2.1 is $\{i+1, \ldots, j\}$, having cardinality $\ell = j-i$):

$$\sum_{k=1}^{\ell} (-1)^k \Gamma^{\alpha \oplus e_{p_k}} \Gamma^{\beta \oplus e_{p_k}} = -z_i z_j + \sum_{k=2}^{\ell} (-1)^k z_{i+2} z_{j-2} = 0 \,. \tag{7.2}$$

Rearranging the second equality, we get:

$$z_i z_j = \sum_{k=2}^{\ell} (-1)^k z_{i+2} z_{j-2} \,. \tag{7.3}$$

There are an odd number ($j-i-1 \ge 1$) of terms in the sum, and the terms alternate their signs and begin with a $+$, so we conclude that

$$z_i z_j = z_{i+2} z_{j-2} \,. \tag{7.4}$$

In particular, if $i$ is even and $0 \le i \le k-4$, then

$$z_i z_{i+4} = z_{i+2}^2 \,. \tag{7.5}$$

If $z_{i+2} \ne 0$, then both $z_i \ne 0$ and $z_{i+4} \ne 0$. This means that if any even indexed entry that is not the first or the last even indexed entry (call it a non-extremal entry) is nonzero, then all even indexed entries are nonzero. In this case, the geometric progression is established, with common ratio $z_{i+2}/z_i = z_{i+4}/z_{i+2}$, for even $0 \le i \le k-4$.

Suppose all non-extremal even indexed entries are zero. If $k \le 3$ then the theorem is self-evident. Suppose $k \ge 4$. Let $k^* \le k$ be the maximum even index. Then $k^* \ge 4$ and we have

$$z_0 z_{k^*} = z_2 z_{k^*-2} \,. \tag{7.6}$$

Note that $k^* - 2 \ge 2$ and therefore it is non-extremal. It follows that $z_0 z_{k^*} = 0$ and therefore at most one extremal even indexed entry can be nonzero. It is also easy to verify that a sequence satisfying the conditions of this theorem also satisfies MGI, and hence is a matchgate signature. (See Section 7.1 for a direct construction.) This completes the proof for even signatures. The proof for odd signatures is similar. The theorem follows. □

Explicitly, there are just four cases for symmetric signatures:

1. $[a^k b^0, 0, a^{k-1} b, 0, a^{k-2} b^2, 0, \ldots, a^0 b^k]$ (arity $2k+1$);
2. $[a^k b^0, 0, a^{k-1} b, 0, a^{k-2} b^2, 0, \ldots, a^0 b^k, 0]$ (arity $2k+2$);
3. $[0, a^k b^0, 0, a^{k-1} b, 0, a^{k-2} b^2, 0, \ldots, a^0 b^k]$ (arity $2k+2$);
4. $[0, a^k b^0, 0, a^{k-1} b, 0, a^{k-2} b^2, 0, \ldots, a^0 b^k, 0]$ (arity $2k+3$).

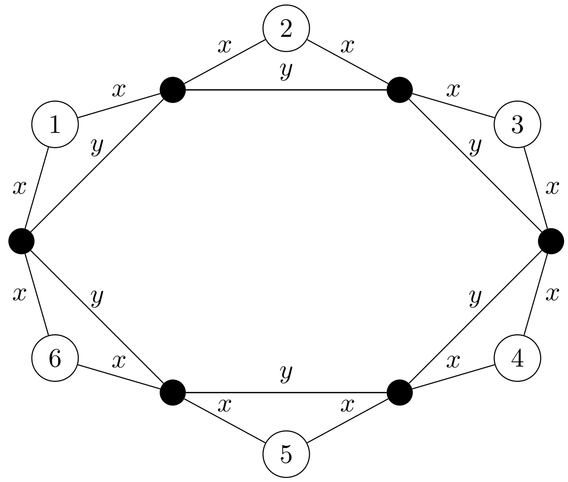


Figure 10: A matchgate for an even, symmetric, arity-6 signature.

### 7.1 Matchgates for symmetric signatures

We have already demonstrated how to build a planar matchgate realizing any MGI-satisfying signature, through a planarizing procedure. Up until now the only known construction of a matchgate realizing an arbitrary symmetric signature is through this general procedure. This is unsatisfactory, since they ought to have more symmetry. However it is difficult to imagine a geometric construction that is planar and symmetric for all pairs of external nodes $1 \le i < j \le k$, if $k \ge 4$. Now we will present a simple and direct construction for symmetric signatures, when the underlying field $\mathbb{F}$ is the complex numbers $\mathbb{C}$ (or any algebraically closed field). The constructed matchgates are not geometrically symmetric for all pairs of external nodes, but functionally they are, in terms of the signatures.

We present two closely related matchgate constructions, one for even symmetric signatures, and the other for odd, which is a simple modification of the even signature case. Our constructions for both these cases work regardless if the signature has odd or even arity.

In Figure 10 we have an example of a planar matchgate for an even, arity-6 signature. Its design can be described as a cycle of triangles which share vertices (each triangle has two weight $x$ edges, and a weight $y$ base). For odd signatures, the construction is changed very slightly, as shown in Figure 11. The only modification is to delete one external node in a matchgate for an even symmetric signature of arity one higher.

More specifically, to construct in general an even matchgate $G$ of arity $k$, we first take $k$ triangles with vertices $\{a_i, b_i, c_i\}$ $(1 \le i \le k)$. The edges $\{a_i, b_i\}$ and $\{a_i, c_i\}$ have weight $x$, and $\{b_i, c_i\}$ has weight $y$. We link them in a cycle, identifying $c_i$ with $b_{i+1}$, where the index is counted modulo $k$. The matchgate $G$ has $k$ external nodes $\{a_1, \ldots, a_k\}$, and a total of $2k$ nodes.

Consider any $\alpha \in \{0,1\}^k$ of even Hamming weight. $\alpha_i = 0$ iff $a_i$ remains in $G^\alpha$. If $\alpha = 1^k$, then $G^\alpha$ is a cycle of length $k$. If $k$ is odd, of course $G^\alpha$ has no perfect matchings. If $k$ is even, there are exactly two perfect matchings, each having weight $y^{k/2}$.

Now assume $\alpha \neq 1^k$. Then $\alpha$ cyclically alternates between consecutive 0's (called a *0-run*) and

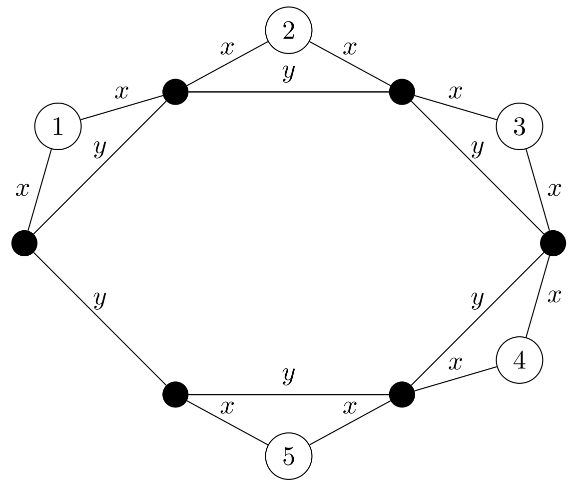


Figure 11: A matchgate for an odd, symmetric, arity-5 signature.

consecutive 1's (called a *1-run*). Each $a_i$ that remains in $G^\alpha$ must be matched to either $b_i$ (we call it *left-match*) or $c_i = b_{i+1}$ (we call it *right-match*), both with weight $x$. Consider any 0-run. It is clear that either all $a_i$ within this 0-run left-match or all right-match. Next consider a 1-run of $m$ 1's; it is between two 0-runs. If $m$ is even, then the path of $m$ edges all with weight $y$ forces the two neighboring 0-runs to take either both left-match or both right-match. Moreover, both possibilities are realizable, and in each case the 1-run contributes a weight $y^{m/2}$. If $m$ is odd, then the path of $m$ edges forces the two neighboring 0-runs to take opposite types of left-match and right-match. Again both possibilities are realizable; in one case the 1-run contributes a weight $y^{(m-1)/2}$, and in another case it contributes a weight $y^{(m+1)/2}$. Furthermore, for two 1-runs $1^m$ and $1^{m'}$ both of odd length and are consecutive in the sense that the only 1-runs in between are of even length, they contribute a combined weight $y^{(m+m')/2}$. Since $\alpha$ has an even Hamming weight $|\alpha|$, there is an even number of 1-runs of odd length. Hence together the 1-runs contribute a weight $y^{|\alpha|/2}$. There are exactly two perfect matchings in $G^\alpha$, each uniquely determined by the left-match or right-match choice of any particular $a_i$ in $G^\alpha$. It follows that the signature value is $\Gamma^\alpha = 2x^{k-|\alpha|}y^{|\alpha|/2}$. Clearly by choosing $x$ and $y$ suitably, we can realize an arbitrary even symmetric signature.

The construction for odd symmetric signatures is to remove one external node in the matchgate for an even symmetric signature of arity one higher. By the general form of odd symmetric signatures, being a sub-signature $[z_1, \ldots, z_n]$ of an even symmetric signature $[z_0, z_1, \ldots, z_n]$, the proof is complete.

# 8 Conclusion

Substantial work has been built on top of MGI in the signature theory of matchgates [7, 6, 17, 5, 16, 15, 8, 18, 9, 13]. In particular, a number of complexity dichotomy theorems have been proved that use this understanding of what matchgates can and cannot compute. A general theme of these theorems asserts that a wide class of locally constrained counting problems can be classified into three types: (1) Those that are computable in polynomial time for general graphs; (2) Those that are #P-hard for general graphs but computable in polynomial time over planar graphs; and (3) Those that remain #P-hard for planar graphs. Moreover type (2) occurs precisely for problems which can be described by signatures that are realizable by planar matchgates after a holographic transformation. This theme is generally proved for symmetric signatures [15, 9, 13]. For not-necessarily-symmetric signatures, these are only proved in special cases [4]. This paper provides a firm foundation for this theory and for future explorations.

**Acknowledgements** We would like to thank the referees and the editor for many constructive comments.

## References


[1] JIN-YI CAI AND VINAY CHOUDHARY: Some results on matchgates and holographic algorithms. *Int. J. Software and Informatics*, 1(1):3–36, 2007. See at IJSI. Preliminary version in ICALP'06. See also at ECCC. 168, 173

[2] JIN-YI CAI, VINAY CHOUDHARY, AND PINYAN LU: On the theory of matchgate computations. *Theory Comput. Syst.*, 45(1):108–132, 2009. Preliminary version in CCC'07. See also at ECCC. [doi:10.1007/s00224-007-9092-8] 168, 173

[3] JIN-YI CAI, HENG GUO, AND TYSON WILLIAMS: A complete dichotomy rises from the capture of vanishing signatures: extended abstract. In *Proc. 45th STOC*, pp. 635–644. ACM Press, 2013. See also at arXiv. [doi:10.1145/2488608.2488687]

[4] JIN-YI CAI, MICHAEL R. KOWALCZYK, AND TYSON WILLIAMS: Gadgets and anti-gadgets leading to a complexity dichotomy. In *Proc. 3rd Symp. Innovations in Theoretical Computer Science (ITCS'12)*, pp. 452–467. ACM Press, 2012. See also at arXiv. [doi:10.1145/2090236.2090272] 194

[5] JIN-YI CAI AND PINYAN LU: Holographic algorithms: The power of dimensionality resolved. *Theoret. Comput. Sci.*, 410(18):1618–1628, 2009. Preliminary version in ICALP'07. See also at ECCC. [doi:10.1016/j.tcs.2008.12.047] 193

[6] JIN-YI CAI AND PINYAN LU: On blockwise symmetric signatures for matchgates. *Theoret. Comput. Sci.*, 411(4-5):739–750, 2010. Preliminary version in FCT'07. See also at ECCC. [doi:10.1016/j.tcs.2009.10.012] 193

[7] JIN-YI CAI AND PINYAN LU: Holographic algorithms: From art to science. *J. Comput. System Sci.*, 77(1):41–61, 2011. Preliminary version in STOC'07. See also at ECCC. [doi:10.1016/j.jcss.2010.06.005] 168, 193

[8] JIN-YI CAI AND PINYAN LU: Signature theory in holographic algorithms. *Algorithmica*, 61(4):779–816, 2011. Preliminary version in ISAAC'08. [doi:10.1007/s00453-009-9383-3] 193

[9] JIN-YI CAI, PINYAN LU, AND MINGJI XIA: Holographic algorithms with matchgates capture precisely tractable planar #CSP. In *Proc. 51st FOCS*, pp. 427–436. IEEE Comp. Soc. Press, 2010. See also at arXiv. [doi:10.1109/FOCS.2010.48] 193, 194

[10] ANDREAS W.M. DRESS AND WALTER WENZEL: A simple proof of an identity concerning Pfaffians of skew symmetric matrices. *Advances in Mathematics*, 112(1):120–134, 1995. [doi:10.1006/aima.1995.1029] 169, 174

[11] HENG GUO, SANGXIA HUANG, PINYAN LU, AND MINGJI XIA: The complexity of weighted Boolean #CSP modulo *k*. In *Proc. 28th Symp. Theoretical Aspects of Comp. Sci. (STACS'11)*, pp. 249–260. Schloss Dagstuhl, 2011. [doi:10.4230/LIPIcs.STACS.2011.249]

[12] HENG GUO, PINYAN LU, AND LESLIE G. VALIANT: The complexity of symmetric Boolean parity Holant problems. *SIAM J. Comput.*, 42(1):324–356, 2013. Preliminary version in ICALP'11. [doi:10.1137/100815530]

[13] HENG GUO AND TYSON WILLIAMS: The complexity of planar Boolean #CSP with complex weights. In *Proc. 40th Internat. Colloq. on Automata, Languages and Programming (ICALP'13)*, pp. 516–527. Springer, 2013. See also at arXiv. [doi:10.1007/978-3-642-39206-1_44] 193, 194

[14] PIETER WILLEM KASTELEYN: Graph theory and crystal physics. In FRANK HARARY, editor, *Graph Theory and Theoretical Physics*, pp. 43–110. Academic Press, 1967. 168, 170

[15] MICHAEL KOWALCZYK: *Dichotomy Theorems for Holant Problems*. Ph. D. thesis, University of Wisconsin–Madison, 2010. Available at author's home page. [ACM:2049085] 193, 194

[16] JOSEPH M. LANDSBERG, JASON MORTON, AND SERGUEI NORINE: Holographic algorithms without matchgates. *Linear Algebra and its Applications*, 438(2):782–795, 2013. See also at arXiv. [doi:10.1016/j.laa.2012.01.010] 193

[17] ANGSHENG LI AND MINGJI XIA: A theory for Valiant's matchcircuits (extended abstract). In *Proc. 25th Symp. Theoretical Aspects of Comp. Sci. (STACS'08)*, pp. 491–502. Schloss Dagstuhl, 2008. See also at arXiv. [doi:10.4230/LIPIcs.STACS.2008.1368] 193

[18] JASON MORTON: Pfaffian circuits. Technical report, 2010. [arXiv:1101.0129] 193

[19] KAZUO MUROTA: *Matrices and Matroids for Systems Analysis*. Volume 20 of *Algorithms and Combinatorics*. Springer, 2000. [doi:10.1007/978-3-642-03994-2] 174

[20] YASUHIRO OHTA: *Bilinear Theory of Soliton*. Ph. D. thesis, University of Tokyo, 1992. 174

[21] HAROLD N. V. TEMPERLEY AND MICHAEL E. FISHER: Dimer problem in statistical mechanics–an exact result. *Philosophical Magazine*, 6(68):1061–1063, 1961. [doi:10.1080/14786436108243366] 168

[22] ROBIN THOMAS: A survey of Pfaffian orientations of graphs. In MARTA SANZ-SOLÉ, JAVIER SORIA, JUAN LUIS VARONA, AND JOAN VERDERA, editors, *Proceedings of the International Congress of Mathematicians*, volume 3, pp. 963–984, Madrid, 2006. European Mathematical Society Publishing House. [doi:10.4171/022-3/47] 168

[23] LESLIE G. VALIANT: Expressiveness of matchgates. *Theoret. Comput. Sci.*, 289(1):457–471, 2002. [doi:10.1016/S0304-3975(01)00325-5] 168, 173, 174

[24] LESLIE G. VALIANT: Quantum circuits that can be simulated classically in polynomial time. *SIAM J. Comput.*, 31(4):1229–1254, 2002. Preliminary version in STOC'01. [doi:10.1137/S0097539700377025] 167, 187, 188, 189

[25] LESLIE G. VALIANT: Accidental algorithms. In *Proc. 47th FOCS*, pp. 509–517. IEEE Comp. Soc. Press, 2006. [doi:10.1109/FOCS.2006.7] 168

[26] LESLIE G. VALIANT: Holographic algorithms. *SIAM J. Comput.*, 37(5):1565–1594, 2008. Preliminary version in FOCS'04. See also at ECCC. [doi:10.1137/070682575] 168, 189

## AUTHORS

Jin-Yi Cai
Professor
University of Wisconsin–Madison, WI
jyc@cs.wisc.edu
http://pages.cs.wisc.edu/~jyc/

Aaron Gorenstein
University of Wisconsin–Madison, WI
agorenst@cs.wisc.edu
http://pages.cs.wisc.edu/~agorenst/

## ABOUT THE AUTHORS

JIN-YI CAI grew up in Shanghai, China, and attended schools there. He studied mathematics at Fudan University (class of 77), where his first interest was analysis. He continued his studies at Temple University, where he was greatly influenced by Donald J. Newman. It was during that period that he came in contact with complexity theory. He also realized that a trick he had "invented," to the displeasure of some of his teachers, was really a matter about the complexity of proofs and would fit nicely within this theory. His trick was to reduce all Euclidean geometry problems, for which he could not always find a clever proof quickly enough, to a computational problem via coordinates, replacing the need for cleverness.

He studied complexity theory at Cornell University under the guidance of Juris Hartmanis, and received his Ph. D. in 1986. Then he held faculty positions at Yale University (1986-1989), Princeton University (1989-1993), and SUNY Buffalo (1993-2000). He is currently a Professor of Computer Science at the University of Wisconsin–Madison. He was a Sloan Fellow and a Guggenheim Fellow. He was elected a Fellow of the ACM in 2001. His main research interest is complexity theory. He has published over 100 research papers.

AARON GORENSTEIN first realized he wanted to study computer science after taking some introductory courses at Boston University. During his college studies at the University of Rochester, he decided to focus on theory after taking an algorithms course. Under his advisor Lane Hemaspaandra, Aaron pursued his interest in complexity theory and graduated from Rochester with a B. S. and M. S. in computer science. He is currently a graduate student studying under Jin-Yi Cai at the University of Wisconsin–Madison. When not studying computer science, he enjoys practicing the piano and reading historical nonfiction.