On the Theory of Matchgate Computations

Jin-Yi Cai *
Computer Sciences Dept.
University of Wisconsin
Madison, WI 53706. USA.
jyc@cs.wisc.edu

Vinay Choudhary †
Computer Sciences Dept.
University of Wisconsin
Madison, WI 53706. USA.
vinchr@cs.wisc.edu

Pinyan Lu‡
Dept. of Computer Sc. & Tech.
Tsinghua University
Beijing, 100084, P. R. China
lpy@mails.tsinghua.edu.cn

Abstract

Valiant has proposed a new theory of algorithmic computation based on perfect matchings and Pfaffians. We study the properties of matchgates—the basic building blocks in this new theory. We give a set of algebraic identities which completely characterizes these objects for arbitrary numbers of inputs and outputs. These identities are derived from Grassmann-Plücker identities. The 4 by 4 matchgate character matrices are of particular interest. These were used in Valiant's classical simulation of a fragment of quantum computations. For these 4 by 4 matchgates, we use Jacobi's theorem on compound matrices to prove that the invertible matchgate matrices form a multiplicative group. Our results can also be expressed in the theory of Holographic Algorithms in terms of realizable standard signatures. These results are useful in establishing limitations on the ultimate capabilities of Valiant's theory of matchgate computations and Holographic Algorithms.

1 Introduction

Recently Valiant [12] has introduced a new method of designing algorithms based on perfect matchings and *Pfaffians*. The basic building blocks in this new theory are called *matchgates*. Each matchgate defines a *character matrix*, with entries defined in terms of the Pfaffian, which captures the properties of the matchgate under the consideration of (perfect) matchings when certain input and/or output nodes are retained or removed. (Formal definitions will be given in the next section.)

These matchgates can be combined to form *matchcircuits*. Certain global properties of these matchcircuits can be interpreted as realizing computations which, *prima facie*, take exponential time. However, due to the way the matchcircuits are constructed and the algebraic properties of the Pfaffian, these properties can actually be computed in polynomial time in the size of the matchcircuit. The crucial observation behind this is a compositional theorem, which is algebraic in nature, and states that the product of the characters of two constituent matchgates is the character of a composite matchgate. Matchcircuits represent a new algorithmic method to construct polynomial time algorithms performing certain seemingly exponential time computations. Valiant [12] used these matchcircuits to show that a nontrivial, though restricted, fragment of quantum circuits can be simulated classically in polynomial time. It is not clear at the moment what is the class of all quantum circuits that can be simulated classically in this framework. More generally it is not clear what are the ultimate capabilities and limitations of this new class of algorithms.

Subsequently, Valiant [13] further introduced the notion of Holographic Algorithms. This theory is also based on matchgates, but with the additional ingredient of a choice of a set of linear basis vectors, through which the computation can be expressed and interpreted. In this theory the matchgates used are restricted to be *planar matchgates*. Instead of a character matrix, a planar matchgate is associated with a *signature*. The computation is ultimately carried out by the elegant FKT method [6, 7, 10]. Valiant obtained polynomial time holographic algorithms for a number of problems, minor variations of which are NP-hard. The new algorithms in this framework are quite exotic, e.g., in [16] a certain restricted counting problem for SAT is shown be #P-hard and its mod 2 version is $\oplus$P-hard, and yet its mod 7 version is solvable in P by holographic algorithms. Again the ultimate capabilities and limitations of holographic algorithms are not clear at this time. It is precisely this uncertainty that is most exciting to us.

Will this new algorithmic paradigm lead to a collapse of complexity classes? The kinds of algorithms that are produced by matchgate computations are quite unlike any-

*Supported by NSF CCR-0208013 and CCR-0511679.
†Supported by NSF CCR-0208013.
‡Supported by NSF CCR-0511679 and by the National Natural Science Foundation of China Grant 60553001 and the National Basic Research Program of China Grant 2007CB807900, 2007CB807901.

thing before (aside from quantum algorithms). Valiant suggested [13], "any proof of P $\neq$ NP may need to explain, and not only to imply, the unsolvability" of NP-hard problems using this approach. Our paper is a systematic investigation of the capabilities and limitations of the basic building blocks of this theory, namely the matchgates.

It turns out that there is a rich internal structure to the matchgates as expressed by the algebraic properties of Pfaffian. In [12, 11], Valiant has found 5 equations, called matchgate identities, which are necessary conditions for all 4 by 4 matchgate characters. With a slight restriction, these 5 matchgate identities are also sufficient for the case of 4 by 4 characters. The paper [8] also discusses matchgates as related to quantum computing. The 4 by 4 matchgate characters are important because they are used in the simulation of quantum circuits.

The main results of this paper are concerned with this internal structure, and provide a fairly complete picture of general matchgates. The aim of this paper is theory-building, not problem solving. We believe a solid foundation for the theory is needed to obtain further positive, and more importantly, negative results.

We state our main findings. It turns out that matchgates of every size form an algebraic variety. We first find a symmetry as realized by a group action on the rows and columns of the 4 by 4 character matrices, and express matchgate identities in terms of determinantal minors. Then we find a total of 10 matchgate identities. We prove that they constitute a complete set of matchgate identities for 4 by 4 characters. Then we use Jacobi's theorem on compound matrices to prove that the invertible 4 by 4 matchgate matrices form a multiplicative group. That it is closed under matrix multiplication is used in [12] as the basis for the quantum simulation. Here we prove that if the character matrix is invertible, its inverse is also the character matrix of some matchgate.

More importantly we give results for general matchgates. We define matchgate identities for matchgates with arbitrary k-inputs and l-outputs. Then we show that a set of *useful* Grassmann-Plücker identities [11] gives a complete set of matchgate identities for any general matchgate.

Combined with results from [1], these characterizations also apply to planar matchgates and their (standard) signatures in the holographic algorithm framework. These have been used as a foundation in the investigation of matchgrid computations and holographic algorithms [4, 5]. In particular we include here a characterization of symmetric signatures, which follows from these matchgate identities.

Our results have important implications for both upper and lower bounds. 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. An interesting consequence of our proof is that when a required matchgate exists, it can be realized by a weighted complete graph consisting of essentially the external nodes plus at most one omittable node. Thus the design of a required matchgate boils down to the choice of $\binom{k+l}{2}$ weights, where k and l are the numbers of input and output nodes. This makes it feasible both to search, and in case of non-existence to prove that this is so. The first negative results (lower bounds) in this area all rely on this result [1, 16] (a preliminary version of this paper appeared as ECCC TR06-018.) In [1] we used results here to give non-existence theorems for certain holographic algorithms. In a paper titled "Accidental Algorithms" [16] Valiant showed a surprising mod 7 counting problem solvable in P, as well as some lower bounds for certain Satisfiability problem using holographic algorithms. The lower bound proof relies on the results proved here. In [3] we show, using results developed here and in [1], that mod 7 is the only modulus for which Valiant's "Accidental Algorithm" exists for that problem. In [4, 5], the characterization theorems of general matchgates developed in this paper, namely Matchgate Identities, are also used in an essential way. The results presented here serve as a foundation for an in-depth study of the rich theory of matchcircuit and holographic algorithms.

2 Background

Before we can describe our results, we will require quite a few definitions. Most of these definitions have been introduced by Valiant in [12, 13, 11]. We will give a brief recap here.

We will be dealing with weighted undirected graphs $G = (V, E, W)$, which are represented by skew-symmetric adjacency matrices M. The Pfaffian of an $n \times n$ skew-symmetric matrix M is a polynomial function computable in polynomial time, satisfying $(\mathrm{Pf}(M))^2 = \det(M)$. We assume the reader is acquainted with Pfaffians and Pfaffian Sums; otherwise please take a brief look at the first section of Appendix. We omit the definitions of Pfaffians and Pfaffian Sums here, and our recap of other definitions is brief. We remark that the use of Pfaffian Sums is only needed when one allows the so-called omittable nodes. For the most part one can ignore this complication, and consider only matchgates without omittable nodes and consequently no Pfaffian Sums, but only Pfaffians.

2.1 Grassmann-Plücker Identities

Let M be a skew-symmetric matrix, and $A = \{i_1, \ldots, i_r\}$ where $i_1 < \ldots < i_r$. $\mathrm{Pf}_M(i_1, \ldots, i_r)$, or when M is clear from the context, simply $\mathrm{Pf}(i_1, \ldots, i_r)$ or $\mathrm{Pf}(A)$, is defined

as the Pfaffian of the matrix obtained by restricting M to rows and columns present in A, namely $i_1, \ldots, i_r$. When the set notation A is used, we implicitly assume the indices are in increasing order. If $i_1, \ldots, i_r$ are not in increasing order, the sign will vary according to the parity of the permutation $\begin{pmatrix} 1 & 2 & \ldots & r \\ i_1 & i_2 & \ldots & i_r \end{pmatrix}$, e.g., $\mathrm{Pf}_M(i_2, i_1, \ldots, i_r) = -\mathrm{Pf}_M(i_1, i_2, \ldots, i_r)$ and so on. If $i_1, i_2, \ldots, i_r$ are not all distinct, then $\mathrm{Pf}_M(i_1, \ldots, i_r)$ is defined to be zero. The notation $\mathrm{Pf}_M[i_1, \ldots, i_r]$ will denote the Pfaffian after removing the rows and columns of $\{i_1, \ldots, i_r\}$. Note that $\mathrm{Pf}_M[i_1, \ldots, i_r]$ is the same as $\mathrm{Pf}(M[A])$, where $M[A]$ denotes the matrix M with rows and columns from A removed. Also, in the index list, we denote by $\hat{i}$, the omission of index i. For example, $\mathrm{Pf}(1, 2, \hat{3}, 4, 5) = \mathrm{Pf}(1, 2, 4, 5)$ etc.

The following theorem states the Grassmann-Plücker (GP) identities.

Theorem 2.1. *[9] For any $n \times n$ skew-symmetric matrix M, and for any $I = \{i_1, \ldots, i_K\} \subseteq [n]$ and $J = \{j_1, \ldots, j_L\} \subseteq [n]$, the following is called the Grassmann-Plücker identity (generated by I and J),*

$$0 = \sum_{l=1}^{L} (-1)^l \mathrm{Pf}(j_l, i_1, \ldots, i_K)\mathrm{Pf}(j_1, \ldots, \hat{j_l}, \ldots, j_L)$$

$$+ \sum_{k=1}^{K} (-1)^k \mathrm{Pf}(i_1, \ldots, \hat{i_k}, \ldots, i_K)\mathrm{Pf}(i_k, j_1, \ldots, j_L). \quad (1)$$

We will use the notation $\mathrm{Pf}(t \circ I)$ to denote the Pfaffian $\mathrm{Pf}(t, i_1, \ldots, i_K)$, assuming $I = \{i_1, \ldots, i_K\}$ is listed in increasing order.

2.2 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 $\forall i \in T$, 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 saturate all the unomittable nodes and also an arbitrary (possibly empty) subset of T. Whenever we refer to the Pfaffian Sum (denoted by PfS) of a matchgate fragment, we assume that $\lambda_i = 1$, if $i \in T$, and 0 otherwise (See the definition of Pfaffian Sum in the Appendix). 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 $Z = X' \cup Y'$. E.g., if $X = \{1, 2\}$ and $Y = \{n - 1, n\}$, where $n = |V|$ is the number of vertices in Γ. Then the ordering of rows is $\emptyset, \{1\}, \{2\}, \{1, 2\}$, and the ordering of columns is $\emptyset, \{n\}, \{n - 1\}, \{n - 1, n\}$.

A *matchcircuit* is a way of combining matchgates using 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. The edges above or below a matchgate are referred to as *parallel* edges. The attachment of modifiers to a character is to ensure that all "overlaps" in the evaluation of the Pfaffian of the entire matchcircuit works out properly. Figure 2 shows a typical matchcircuit. We do not present the detailed definition here because we won't be dealing too much with matchcircuits. Note that the relative ordering of all the vertices are carefully placed in a layered matchcircuit, and is schematically depicted in Figure 2 as well as in Figure 1. In Figure 1, one can verify that every edge on the top line outside of the matchgates Γ_1, Γ' and Γ_4 (there are 16 of them) always incurs collectively an

even number of overlaps with all such edges from the bottom line, except those 2 parallel edges above Γ_2 and Γ_3 (see Theorem 3.2). We refer the reader to [12] 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.

In [13] Valiant also introduced *planar matchgates* in the framework of holographic algorithms. A planar matchgate Γ with m external nodes comes with a planar embedding, where the external nodes are ordered counter-clockwise on the external face. For a planar matchgate Γ with m external nodes, we assign a *standard signature* which has 2^m entries

$$G^{i_1 i_2 \dots i_m} = \mathrm{PerfMatch}(G - Z),$$

where $\mathrm{PerfMatch}(G - Z) = \sum_M \prod_{(i,j)\in M} w_{ij}$, is a sum over all perfect matchings M in $G - Z$, and Z is the subset of removed external nodes having the characteristic sequence $\chi_Z = i_1 i_2 \dots i_m$. (If there are omittable nodes in Γ they must be on the external face, and then the sum over M may range over matchings which saturate all the unomittable nodes.) PerfMatch is called the perfect matching polynomial.

In many ways, the definitions for planar matchgates and signatures are more intuitive than general matchgates and characters. It is a remarkable fact proved in [1] that these two categories of objects are essentially the same. Planar matchgates and signatures have seen more research activities; but this does not render the character theory useless. In fact the only way we know how to prove the fundamental structural properties of signatures is through results of this paper, in terms of the character theory with Pfaffians. Also certain constructions of planar matchgates and signatures are known to exist (by our general theory) and are explicitly known only via the proof of the general realizability theorem in this paper (followed by transformations from [1]). In short, what we prove here for matchgates and characters apply to planar matchgates and standard signatures, and that is the only known proof route for these theorems on signatures.

3 2-input 2-output Matchgates

3.1 Complete Set of Identities

In [11], Valiant presented a set of five equations on the entries of the character matrix of 2-input, 2-output matchgates. These were called matchgate identities. (In the explicit listing of Valiant's equations, we will retain Valiant's notation and number the rows and columns of the 4 by 4 character matrix from 1 to 4, instead of 0 to 3 written in binary bits 00 to 11, as from Sec. 2.2.) It was shown that the character of every 2-input, 2-output matchgate satisfies these equations. Furthermore, if a matrix B satisfies all these identities and an additional constraint, namely $B_{44} \neq 0$, then there is a matchgate having character B.

Let Γ be a 2-input, 2-output matchgate having character B. Assume that the matchgate is normally numbered and its character is normally ordered. Then Valiant's five matchgate identities are quoted as follows [11]:

$$\begin{aligned}
B_{11}B_{44} - B_{22}B_{33} - B_{14}B_{41} + B_{23}B_{32} &= 0\\
B_{21}B_{44} - B_{22}B_{43} - B_{41}B_{24} + B_{23}B_{42} &= 0\\
B_{31}B_{44} + B_{33}B_{42} - B_{41}B_{34} - B_{32}B_{43} &= 0\\
B_{13}B_{44} + B_{33}B_{24} - B_{14}B_{43} - B_{23}B_{34} &= 0\\
B_{12}B_{44} - B_{22}B_{34} - B_{14}B_{42} + B_{32}B_{24} &= 0
\end{aligned}$$

It turns out that there are interesting symmetries buried in this set of identities. For example, $B_{11}B_{44} - B_{14}B_{41}$ is the determinant of the submatrix of B obtained by removing rows and columns 2 and 3. And the first matchgate identity asserts that this is equal to the minor of B at rows and columns 2 and 3.

We will express this in a more compact notation. Denote by $D(ij, kl)$ the determinant of the 2×2 submatrix of B consisting of rows i and j, and columns k and l, i.e., $D(ij, kl)$ is the following determinant, where $i < j$ and $k < l$,

$$\begin{vmatrix} B_{ik} & B_{il} \\ B_{jk} & B_{jl} \end{vmatrix}$$

We note that all five identities above can be written as the determinant of a 2×2 matrix being equal to the determinant of another 2×2 matrix. These matrices are (not necessarily contiguous) sub-matrices of the character matrix. In this notation, we can write the identities above as

$$\begin{aligned}
&D(14,14) = D(23,23) \quad D(24,14) = D(24,23)\\
&D(34,14) = D(34,23) \quad D(14,34) = D(23,34)\\
&D(14,24) = D(23,24)
\end{aligned}$$

The symmetry is as follows: We consider the set of $\binom{4}{2}$ unordered pairs of $\{1,2,3,4\}$, denoted by $S = \{\{1,2\},\{1,3\},\{1,4\},\{2,3\},\{2,4\},\{3,4\}\}$. An involution ρ flips the pair $\{1,4\}$ and $\{2,3\}$, and leaves everything else fixed. Thus ρ is the permutation

$$\begin{pmatrix} \{1,2\} & \{1,3\} & \{1,4\} & \{2,3\} & \{2,4\} & \{3,4\} \\ \{1,2\} & \{1,3\} & \{2,3\} & \{1,4\} & \{2,4\} & \{3,4\} \end{pmatrix}$$

In terms of this ρ, the above five identities can all be written as

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

where the ordered pair (of unordered pairs) $(p,q) = (14,14),(24,14),(34,14),(14,34)$ and $(14,24)$, respectively.

It turns out that we may apply the permutation ρ to any ordered pair (p,q), where $p,q \in S$. In order that $(\rho(p),\rho(q))$ is not identical to (p,q), (lest we get a trivial statement,) we must have at least either p or q (or both) equal to $\{1,4\}$ or $\{2,3\}$. In terms of a permutation group, we have an action by the involution $\rho \times \rho$ on the set $S \times S$, which has 10 non-trivial orbits of two elements each (and 16 fixed points).

This suggests that there are 10 matchgate identities. It turns out that indeed one can prove these 10 matchgate identities are all valid for all 2-input 2-output matchgates. The proof uses the Grassmann-Plücker identities and is omitted here. Here are the 5 additional identities:

$$\begin{array}{ll} D(12,14) = D(12,23) & D(13,14) = D(13,23) \\ D(14,12) = D(23,12) & D(14,13) = D(23,13) \\ D(14,23) = D(23,14) & \end{array}$$

More succinctly,

$$D(p,q) = D(\rho(p),\rho(q)), \tag{2}$$

for any $(p,q) \in S \times S$.

Theorem 3.1. *If B is the character matrix of a 2-input 2-output matchgate over any field F, then B satisfies the 10 matchgate identities.*

Now we show the completeness of these identities. (From now on, it will be more convenient to use binary bit strings to index rows and columns as stated in Sec. 2.2. Thus, in the next Theorem, rows and columns are indexed from $0 = 00$ to $3 = 11$.)

Theorem 3.2. *Let B be a 4×4 matrix over a field F satisfying the 10 matchgate identities. Then there exists a matchgate Γ such that $\chi(\Gamma) = B$.*

Proof. The main idea of this proof is simple. If B is identically 0 then it is trivially realizable. If $B_{11,11} \neq 0$, we can use the proof from [12]. If $B_{11,11} = 0$ but some other entry is not 0, then we try to transform B to B' such that $B'_{11,11} \neq 0$, while still satisfying all the 10 matchgate identities. The proof below is not the most efficient for this special case of 4 by 4. But this method can be generalized to prove Theorem 4.2.

Our general technique is to compose matchgates to form a matchcircuit, which is then transformed into a matchgate that realizes the given matrix.

We assume B is not the zero matrix, and suppose $B_{rc} \neq 0$. Let r be written as a binary bit string in $\{0,1\}^2$. Let $\overline{r} = r \oplus 11$ be the bit-wise XOR of r with 11. Define a bijection $\alpha_r : \{0,1\}^2 \to \{0,1\}^2$, which maps $x \mapsto x \oplus \overline{r}$. It is clear that $\alpha_r(r) = 11$, and α_r is an involution, i.e., $\alpha_r = \alpha_r^{-1}$. Also its action on any bit of x is independent of other bits. Let α_c be similarly defined in terms of $c \in \{0,1\}^2$. Let B' be the matrix obtained after applying the transformations α_r and α_c, respectively, to the (indices of) rows and columns of B. We now have, $B'_{11,11} \neq 0$. Since α_r and α_c are their own inverses, applying them to B' yields B.

It can be verified (essentially because the actions of ρ and that of α_r and of α_c commute) that the above set (2) of matchgate identities is invariant under any such transformation. If B satisfies the matchgate identities, then so does B'. From the construction in [12] there is a matchgate Γ' that realizes B'. Now to construct the matchgate Γ to realize B, we first make a matchcircuit Γ'' with character matrix B as shown in Figure 1. Each of the matchgates $\Gamma_1, \Gamma_2, \Gamma_3, \Gamma_4$ is either $\Gamma^{(1)}$ or $\Gamma^{(2)}$, defined below, depending on whether that bit of r (or c) is 1 or 0. All the parallel edges above any gate equal to $\Gamma^{(2)}$ are given weight -1. (This factor of -1 is needed to compensate for an odd number of overlaps.) Here, $\Gamma^{(1)}$, $\Gamma^{(2)}$ are 1-input, 1-output matchgates where $\Gamma^{(1)}$ simply "transmits" its input and $\Gamma^{(2)}$ "flips" its input. The character matrix of $\Gamma^{(1)}$ is the identity matrix and the character matrix of $\Gamma^{(2)}$ is $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. More concretely, $\Gamma^{(2)}$ consists of a single edge of weight 1; $\Gamma^{(1)}$ consists of a path of 2 edges each of weight 1.

The Main Theorem in [12] (the basis for the quantum simulation) can be extended to prove the Extended Main Theorem, given in the Appendix. It can be verified that the construction here satisfies the conditions of the Extended Main Theorem. Therefore, the character matrix of this matchcircuit is the product of the character matrices of the five constituent matchgates, each extended to two inputs, two outputs. (Here "extending" a one-bit matchgate to two bits means algebraically a tensor product with the 2 by 2 identity matrix.) This product is B. To see that, we look at the matchcircuit in a slightly different way. The overall action of the matchcircuit on its inputs is the composition of the actions of the matchgates. The action of Γ' is described by B'. Therefore, the character matrix of Γ'' is B.

Now the matchgate Γ is obtained by deleting the input and output nodes of the matchcircuit and the edges incident to them. The new leftmost/rightmost nodes are now considered as input/output nodes. The edges that we deleted have no overlap among themselves, and they are now considered as external edges of the matchgate Γ. Recall that 1 and 0 have opposite meanings with respect to deletion of external nodes in matchgates and matchcircuits, and since matchgates are assumed to have external edges while matchcircuits don't, the character of Γ is exactly the same as that of Γ''. Hence Γ realizes B. □

3.2 Group Property

We show that the subset of invertible character matrices of two input, two output matchgates forms a multiplicative group. It is relatively easy to see that the product of two character matrices is itself a character matrix [12] by composing two matchgates in sequence. The composed matchgate has the product matrix as its character matrix, because enumerating all (perfect) matchings in the composed matchgate is precisely reflected by matrix multiplication. This is an essential ingredient in Valiant's classical simulation of a fragment of quantum computation. Here we prove a more surprising result that the inverse of a character is also a character. We hope that this will provide a better understanding of the scope of what is computable by these matchgates, including the scope of quantum operations they can simulate.

Let A be an $m \times n$ matrix. A minor of order k of A is the determinant of a k by k submatrix of A. The k^{th} compound matrix of A is a matrix $A^{[k]}$ of order $\binom{m}{k} \times \binom{n}{k}$, where we arrange all the minors of A of order k in lexicographic order.

The matchgate identities have an elegant expression in terms of the compound.

Theorem 3.3. *If B is a 4×4 character matrix of a matchgate, then the matchgate identities state precisely that $B^{[2]}$ is invariant under the following operation: simultaneously interchange row 3 with row 4 and column 3 with column 4.*

Proof. The relevant rows and columns are illustrated below. The proof follows from the matchgate identities.

$$\begin{bmatrix} & & D(12,14) & D(12,23) & & \\ & & D(13,14) & D(13,23) & & \\ D(14,12) & D(14,13) & D(14,14) & D(14,23) & D(14,24) & D(14,34) \\ D(23,12) & D(23,13) & D(23,14) & D(23,23) & D(23,24) & D(23,34) \\ & & D(24,14) & D(24,23) & & \\ & & D(34,14) & D(34,23) & & \end{bmatrix}$$

□

Theorem 3.4. *Let B be a 4×4 matrix over a field F that satisfies the matchgate identities. Suppose that B is invertible. Then B^{-1} also satisfies the matchgate identities.*

We omit the proof here, which uses Jacobi's Theorem on compound matrices. (It is also possible to give a brute force verification by computer algebra, using the results from the previous section that the 10 matchgate identities are necessary and sufficient.)

In case when B is not an invertible matrix, we have the following:

Corollary 3.1. *Let B be a 4×4 matrix over a field F that satisfies the matchgate identities. Then $\mathrm{adj}(B)$ also satisfies the matchgate identities.*

4 General Matchgates

We now move on to general k-input, l-output matchgates. Specifically, our goal is to find out whether there is a set of equations that completely characterizes the characters of general matchgates, just like the 10 equations we obtained for 2-input, 2-output matchgates.

Basically, what we aim to prove is that the GP identities characterize all the character matrices. But we have to be careful. There are various kinds of Pfaffians that occur in the GP identities. In particular, there are Pfaffians of submatrices obtained by deleting rows and columns corresponding to some internal nodes of the matchgate. These Pfaffians do not correspond to any entries of the character matrix. We have to carefully choose the identities that we want to classify as *matchgate identities* for general matchgates.

Consider a normally numbered, normally ordered k-input, l-output matchgate Γ having $n \geq k + l$ vertices. We will only consider matchgates without omittable nodes; the case with matchgates having omittable nodes will be discussed in the Appendix. Let M be its skew-symmetric adjacency matrix. Its character matrix B is a $2^k \times 2^l$ matrix with rows and columns indexed from 0 through $2^k - 1$ and $2^l - 1$, respectively. Let U be the set of nodes which are not inputs or outputs. Since there are no omittable node, each entry of B is either 0 or the Pfaffian of a submatrix multiplied with the modifier. Let $i_1 = 1, \ldots, i_k = k$ be the inputs of Γ and let $o_1 = n, \ldots, o_l = n-l+1$ be its outputs.

We need to introduce a little more compact notation. Given a row index r where $0 \leq r \leq 2^k - 1$. Let X' be the subset of inputs corresponding to the 1's in the binary expansion of r. We will use r to refer to the index r as well as the set X' whenever the intended meaning is clear from the context. For example, $\mathrm{Pf}_M[X']$ and $\mathrm{Pf}_M[r]$ denote the same thing. Similar notation applies to the column indices. Also, note that row indices and column indices refer to disjoint set of nodes in Γ. So we can combine these two together. For example, if r is a row index and c is a column index, then $\mathrm{Pf}_M[rc]$ denotes the Pfaffian of M with all rows and columns corresponding to the 1's in r and c deleted. For any entry of the character B, the modifier μ depends only on the row index and the column index. Let μ_r denote the contribution of row index r to the modifier value, and let μ_c denote the contribution of the column index. The modifier at entry B_{rc} is $\mu_{rc} = \mu_r \mu_c$. In this notation, we can write $B_{rc} = \mu_{rc} \mathrm{Pf}_M[rc]$ or simply $B_{rc} = \mu_{rc} \mathrm{Pf}[rc]$.

Now consider all the GP identities stated in (1) obtained from subsets I and J of $\{1, \ldots, n\}$. To be able to consider this as a matchgate identity (i.e. in terms of the entries of the character matrix instead of the Pfaffians), it needs to satisfy the following two properties:

1. Every non-zero Pfaffian of (1) should be the Pfaffian of a submatrix obtained by deleting only (rows and

columns corresponding to) some inputs and outputs of Γ.

2. The GP identity should be independent of n. (The identity may depend on k and l, but not on the number of internal nodes.)

The first property can be satisfied if we restrict ourselves to the GP identities obtained from I and J such that $U \subseteq I \cap J$. Any such GP identity will be referred to as *useful*.

Lemma 4.1. *If $U \subseteq I \cap J$, then all non-zero Pfaffians in the GP identity are Pfaffians with only some inputs or outputs deleted.*

Proof. All the summands in a GP identity are products of two Pfaffians which are on subsets obtained by moving some element from I to J or from J to I. If any element of U is moved from I to J (or from J to I), then that will appear twice in J (or I) and hence that term is zero. If any other element is moved, both the Pfaffians contain all of U, having only some inputs or outputs deleted. □

To prove that all the useful GP identities are independent of n is slightly more difficult. First we have to state a little more precisely what we mean by being independent of n. For this purpose, first we represent all the Pfaffians in a GP identity by the indices that are deleted, rather than using the indices that are retained as in (1). In other words, we use the $\mathrm{Pf}[\ ]$ notation instead of $\mathrm{Pf}(\ )$. All the indices that now appear are indices of inputs or outputs. We replace these indices by the symbols $i_1, \ldots i_k$, and $o_1, \ldots, o_l$. We claim that the GP identity is now independent of n. Basically this means that the coefficient of every term in the sum (which is either $+1$ or -1) is independent of n. We note that the number of terms clearly only depends on k and l, being determined by the respective subsets of $\{i_1, \ldots i_k\}$ and $\{o_1, \ldots, o_l\}$.

Lemma 4.2. *All the useful GP identities are independent of n.*

Proof. Let I and J be supersets of U. Suppose $i'_1 < \ldots < i'_a$ are the inputs in I and $o'_1 > \ldots > o'_b$ are the outputs in I. Similarly, let $i''_1 < \ldots < i''_c$ and $o''_1 > \ldots > o''_d$ be the inputs and outputs in J. Consider the GP identity obtained from I and J. Let's look at a term where input i'_e is moved from I to J. The case of moving from J to I is symmetric. This term can be written as

$$(-1)^e \mathrm{Pf}(I - \{i'_e\})\mathrm{Pf}(i'_e \circ J).$$

(Recall that in this notation the elements in J, but not i'_e, are assumed to be listed in increasing order.) To write this term in $\mathrm{Pf}[\ ]$ notation, we have to first arrange the terms in the second Pfaffian in increasing order. This requires moving i'_e to its appropriate position in J. This position depends on the input i'_e and the inputs $i''_1, \ldots, i''_c$ in J which is independent of n. The sign $(-1)^e$ only depends on the inputs in I which is again independent of n. Therefore, the coefficient of this term is independent of n.

Now let's consider what happens when we move an output o'_f from I to J. The term in the GP identity is

$$(-1)^{a+|U|+b-f+1}\mathrm{Pf}(I - \{o'_f\})\mathrm{Pf}(o'_f \circ J).$$

The only part in $(-1)^{a+|U|+b-f+1}$ which depends on n is $(-1)^{|U|}$. Again, we need to move o'_f to its correct position so that the indices in the second Pfaffian are in increasing order. This involves moving o'_f across all inputs in J, all elements of U, and some of the outputs in J. Again, the only part that depends on n is moving across elements of U which contributes a sign $(-1)^{|U|}$. The overall sign is, therefore, independent of n. □

Now we know that all the useful GP identities are truly *matchgate identities*. We still need to replace the Pfaffians by entries of the character B. To do that, we'll need some notation. Suppose I is a superset of U. We want to define the sign μ_I. Let I_R be the set of inputs not in I. Let I_C be the set of outputs not in I. Consider I_R as binary bits, μ_{I_R} is defined earlier as a $\pm$ contribution to the modifier. Similarly μ_{I_C} is defined. Then we let $\mu_I = \mu_{I_R}\mu_{I_C}$. Given an input t, let α_t^I be the number of inputs *in* I less than t and β_t^I be the number of inputs more than t which are *not in* I.

Fix some I and J such that $U \subseteq I \cap J$, As before, suppose $i'_1 < \ldots < i'_a$ are the inputs and $o'_1 > \ldots > o'_b$ are the outputs in I and $i''_1 < \ldots < i''_c$ and $o''_1 > \ldots > o''_d$ are the inputs and outputs in J. The non-zero terms in the GP identity generated by I and J will only involve moving some $t \in I \Delta J$, the symmetric difference. Now consider an input $t \in I - J$. The term corresponding to moving t from I to J can be written as: (where we write $B_* = B_{I_R \cup \{t\}, I_C}$ and $B_{**} = B_{J_R - \{t\}, J_C}$, and for notational convenience, we write the negation of (1) i.e., starting the sum with $+$)

$$\begin{aligned}
& (-1)^{\alpha_t^I}\mathrm{Pf}(I - \{t\})\mathrm{Pf}(t \circ J) \\
= \ & (-1)^{\alpha_t^I}(-1)^{\alpha_t^J}\mathrm{Pf}(I - \{t\})\mathrm{Pf}(J \cup \{t\}) \\
= \ & (-1)^{\alpha_t^I}(-1)^{\alpha_t^J}\mu_I(-1)^{\alpha_t^I}(-1)^{\beta_t^I}B_*\mathrm{Pf}(J \cup \{t\}) \\
= \ & (-1)^{\alpha_t^J}\mu_I(-1)^{\beta_t^I}B_*\mathrm{Pf}(J \cup \{t\}) \\
= \ & (-1)^{\alpha_t^J}\mu_I(-1)^{\beta_t^I}B_*\mu_J(-1)^{\alpha_t^J}(-1)^{\beta_t^J}B_{**} \\
= \ & (-1)^{\beta_t^I}(-1)^{\beta_t^J}\mu_I\mu_J B_* B_{**}
\end{aligned}$$

Here in the first equality the factor $(-1)^{\alpha_t^J}$ comes from moving t in $t \circ J$ to its proper place in $J \cup \{t\}$. In the second equality we replace $\mathrm{Pf}(I - \{t\})$ by $\mu_I B_*$, but we need to make an additional modification on the modifier μ_I by the

factor $(-1)^{\alpha_t^I}(-1)^{\beta_t^I}$. The two factors $(-1)^{\alpha_t^I}$ cancel in the third equality. In the fourth equality we replace $\mathrm{Pf}(J\cup\{t\})$ by $\mu_J B_{**}$, but again we need to make an additional modification on the modifier μ_J by the factor $(-1)^{\alpha_t^J}(-1)^{\beta_t^J}$. Finally the two factors $(-1)^{\alpha_t^J}$ cancel in the fifth equality.

Since μ_I and μ_J appear in all terms of this GP identity, we can drop this term. So, the term obtained by moving input t from I to J can be written as

$$(-1)^{\beta_t^I}(-1)^{\beta_t^J} B_{I_R\cup\{t\},I_C} B_{J_R-\{t\},J_C}. \qquad (3)$$

We can write a similar expression when t is an output.

The above form will allow us to prove an important property of the GP identities. Let b be an input bit position between 1 and k. Consider a permutation σ_b on the rows of the character matrix B which, given a row r, maps it to row r' such that r and r' differ only in the b^{th} bit. I.e. σ_b flips the b^{th} bit. This induces a transformation ρ_b on the GP identities. We have the following lemma.

Lemma 4.3. *Given any b, $1 \le b \le k$, ρ_b is a permutation on the GP identities. Similarly ρ_b is a permutation for any output node b.*

Proof. Given a set I. Define the set $I' = I\Delta\{b\}$ to be the symmetric difference. We claim the following: If G_1 is the GP identity generated by I and J, then $G_2 = \rho_b(G_1)$ is the GP identity generated by I' and J'.

First, let's forget about the signs of the terms appearing in G_1 and G_2. Then G_1 maps to G_2 term-for-term. Consider the case when $b \in I \cap J$. Then, any non-zero term in G_1 involves moving an element $t \neq b$, from I to J (or from J to I). This term maps to the term in G_2 that is obtained by moving t from I' to J' (or from J' to I'). This also holds when $b \in I - J$ and $t \neq b$. The term obtained by moving $b \in I - J$ from I to J maps to the term obtained by moving $b \in J' - I'$ from J' to I'. The other cases when $b \notin I \cup J$ or $b \in J - I$ are similar.

Now we need to show that the signs are also the same. For now, let's consider a term in G_1 obtained by moving an input t from I to J. As we saw above, the sign of this term in G_1 is $(-1)^{\beta_t^I+\beta_t^J}$ and of the corresponding term in G_2 is $(-1)^{\beta_t^{I'}+\beta_t^{J'}}$. Our analysis depends on b. First, if b is an output vertex, or an input such that $b \le t$, then $\beta_t^I = \beta_t^{I'}$ and $\beta_t^J = \beta_t^{J'}$ because these only depend on the inputs more than t. And if $b > t$ is an input vertex, then b is counted exactly once in β_t^I together with $\beta_t^{I'}$, and also exactly once in β_t^J together with $\beta_t^{J'}$. Thus, it is counted exactly twice among $\beta_t^I, \beta_t^J, \beta_t^{I'}, \beta_t^{J'}$. It follows that in any case, the sum $\beta_t^I + \beta_t^J + \beta_t^{I'} + \beta_t^{J'}$ is always even. Therefore, the signs are also the same.

The case when t is an output node is similar and is omitted here. This completes the proof. □

Observe that now we can allow a permutation of the matrix entries which is a composition of several input/output bit-flips because all these are independent of each other. The final induced transformation on the GP identities is still a permutation on the set of GP identities. This gives the following theorem.

Theorem 4.1. *If B is a $2^k \times 2^l$ matrix that satisfies all the matchgate identities. Let B' be the matrix obtained from B by applying, possibly more than one, bit-flips on the rows and columns. Then B' also satisfies the matchgate identities.*

Now we are ready to prove the completeness theorem. We say that a $2^k \times 2^l$ matrix B is realizable if there is a matchgate Γ such that $\chi(\Gamma) = B$. We say that a matrix is even (odd) if $B_{ij} = 0$ whenever $H(i) + H(j)$ is odd (even) where $H(i)$ denotes Hamming weight, i.e., the number of 1's in the binary expansion of i. The character matrix of a matchgate without omittable nodes is either even or odd depending on whether n is even or odd.

Theorem 4.2. *Let k, l be non-negative integers. Let B be a $2^k \times 2^l$ matrix which is either even or odd. Then B is the character matrix of a k-input, l-output matchgate Γ if and only if B satisfies all the useful GP identities.*

Proof. We only need to prove the "if" part. If the matrix B is identically zero, it is realizable by a matchgate. So we can assume that B is not identically zero.

First assume that $B_{2^k-1,2^l-1} = 1$. If $B_{2^k-1,2^l-1} = \alpha$ is non-zero but not 1, then we can simply divide all the entries in B by α. Once we obtain a matchgate for that, we add two new internal vertices with an edge of weight α between them. The two new vertices have consecutive indices so that there are no overlaps with anything else. This will have character B.

For $B_{2^k-1,2^l-1} = 1$, the matchgate Γ is a complete graph on $k + l$ vertices. It has k inputs and l outputs (and no internal nodes). Suppose i and j are two vertices. Consider the row r and column c such that $rc = \{1, \ldots, k + l\} - \{i, j\}$, i.e. the entry B_{rc} of the matrix corresponds to all nodes except i and j being deleted. The weight of the edge (i, j) is simply $\mu_{rc} B_{rc}$. Let the skew-symmetric adjacency matrix of Γ be M.

We claim that the character matrix of Γ, $\chi(\Gamma)$, is equal to B. By construction, all the entries of B with total Hamming weight (i.e. B_{rc} where the total number of 1's in rc is) at least $k + l - 2$ are equal to those in $\chi(\Gamma)$. (By convention, the Pfaffian of a 0 by 0 matrix is 1.) Now we proceed by downward induction on the total Hamming weight $H(r) + H(c)$. Consider any entry B_{rc} such that $m = H(r) + H(c)$ is less than $k + l - 2$, and assume that the claim holds for all entries of weight $> m$. Let $a_1 < \ldots < a_m$ be the bits that are 1 in rc. Let $1 \le a' \le k + l$ be an index

not equal to any of these. Consider the GP identity with $I = \{1, \ldots, k+l\} - \{a_1, \ldots, a_m, a'\}$ and $J = \{a'\}$. This identity is of the form:

$$\begin{aligned} & \mathrm{Pf}_M[a_1, \ldots, a_m]\mathrm{Pf}_M() \\ = & \sum_{b \neq a', a_1, \ldots, a_m} (\pm)\mathrm{Pf}_M[b, a', a_1, \ldots, a_m]\mathrm{Pf}_M(b, a') \end{aligned}$$

Note that $\mathrm{Pf}_M() = 1 = \chi(\Gamma)_{2^k-1,2^l-1} = B_{2^k-1,2^l-1}$. The right hand side is a sum of products of two terms. Each term is the Pfaffian of M with a superset of $a_1, \ldots, a_m$ removed. These correspond to entries of $\chi(\Gamma)$ and B in positions with total Hamming weight strictly more than m. (Note that $k + l - 2 > m$.) Since B is equal to $\chi(\Gamma)$ on all such entries and since B and $\chi(\Gamma)$ both satisfy the GP identities, we see that $B_{rc} = \chi(\Gamma)_{rc}$. This completes the proof for the case $B_{2^k-1,2^l-1} \neq 0$.

Now suppose B is not identically zero but $B_{2^k-1,2^l-1} = 0$. Let B_{ij} be a non-zero entry in B. We use bit-flips to map i and j to $2^k - 1$ and $2^l - 1$ respectively to get a matrix B' such that $B'_{2^k-1,2^l-1} \neq 0$. By Theorem 4.1, B' also satisfies the GP identities. Let Γ' be a matchgate that realizes B'. Then we can construct Γ that realizes B by using a construction similar to what we used in the 2-input, 2-output case, as shown in Figure 1. □

Actually, the proof of the above theorem also works in the case when we allow omittable nodes too i.e. the matrix is neither even nor odd. First note that any matchgate is equivalent to a matchgate with an even number of nodes and exactly one omittable node which has a number less than the output nodes but more than all other nodes ([12]). We need to change the definition of useful GP identity to mean that every Pfaffian has only some inputs/outputs and possibly, the omittable node deleted. In that case, we can interpret any such Pfaffian as a Pfaffian sum of the matchgate with some inputs/outputs deleted which then corresponds to the character entries. By using similar arguments, we can prove that all useful GP identities are independent of n and the analog of theorem 4.1 that input/output bit-flips induce a permutation on the GP identities. The completeness theorem is proved in the Appendix.

From the proofs of theorem 4.2 and theorem 7.1 (in the appendix), we see that we need only $O(k + l)$ vertices to realize B. This is interesting because in the definition of matchgates, we allow a k-input, l-output matchgate to have an arbitrary number of internal nodes. We now know that any such matchgate is equivalent to another with only $O(k+l)$ nodes. This makes it possible to prove the non-existence of certain matchgates.

Corollary 4.1. *Let Γ be any k-input, l-output matchgate. Then there is another matchgate Γ' having only $O(k + l)$ vertices such that $\chi(\Gamma) = \chi(\Gamma')$.*

5 Realizability of Signatures

In [13] Valiant introduced the theory of Holographic Algorithms. Here the basic objects are planar matchgates and their signatures. (In this paper we do not consider signatures of a planar matchgate under a basis transformation. Without this transformation, we only consider the *standard* signatures as defined in Sec. 2. Also for simplicity in the following discussion we will not consider omittable nodes.) These planar matchgates are connected to form matchgrids which are the counter parts to matchcircuits. As mentioned earlier in Section 2, we have accomplished a unification of the matchcircuit/character theory and the matchgrid/signature theory in [1].

Roughly speaking, this unification is accomplished as follows. Given a planar matchgate with a signature G, defined by the perfect matching polynomial PerfMatch, one uses the FKT algorithm to show that each entry of G is equal to a corresponding Pfaffian of the submatrix of a *single* skew-symmetric matrix M, where the submatrix is obtained by removing the appropriate rows and columns of M. The skew-symmetric matrix M is obtained from the given skew-symmetric adjacency matrix of the planar matchgate graph, by running the FKT algorithm. The FKT algorithm is applied once to the planar matchgate graph with no vertex removed; but conceptually one can think of it being applied simultaneously to the exponentially many induced subgraphs of the matchgate with various external nodes removed. By the property of the FKT algorithm, which only assigns a ± 1 factor to each edge, this gives a single consistent weighted altered graph. To each entry of the signature G, the corresponding Pfaffian of the submatrix becomes an entry of the character of a matchgate, without the modifier. This is called the naked character in [1].

In many ways, it is simpler to discuss the structural properties of a naked character [1] than a character with the modifiers, in particular with the Matchgate Identities. The modifiers μ are defined in order to account for additional crossovers when matchgates are connected within a matchcircuit. But in terms of the character matrix, the modifiers amount to a multiplication of a ± 1 factor along every row and every column, where the value of each row (column) factor is determined by the row (column) index. Thus the set of all Matchgate Identities is transformed to the set of Matchgate Identities for naked characters, in a one-to-one fashion.

Now we discuss the technically more interesting reverse direction from (naked) characters to signatures. We take a general (not necessarily planar) matchgate Γ with a naked character $\chi(\Gamma)$, and realize it as the signature of a planar matchgate. This is done by a specific embedding of all the vertices of Γ on a semi-circle [1], and then replacing each physical crossing of a pair of edges by a crossover gadget from [13]. This produces a planar matchgate Γ'. One then

argues that the PerfMatch value for each signature entry of Γ' is the same as the corresponding Pfaffian value of the naked character of Γ.

It follows that Theorem 4.2 also applies to planar matchgates and their signatures. More specifically, a set of values can be the standard signature of a planar matchgate (without omittable nodes) iff they satisfy all the parity requirements and all the *useful* Grassmann-Plücker identities. Thus, we have the following three categories of objects all equivalent to each other: Signatures of planar matchgates, naked characters of planar matchgates, and naked characters of general (not necessarily planar) matchgates. And of course, characters and naked characters are related to each other by the modifiers (which are, in some sense, external to the matchgates). The character theory can be viewed as primarily algebraic, while signatures of planar matchgates can be viewed as its geometric realization. Another useful observation derived from this dual perspective is that one can really unify the notions of input and output nodes of a general matchgate; the salient feature is its circular ordering as external nodes of a planar matchgate represented by its signature.

However, there is a subtle point concerning the equivalence of signatures and (naked) characters expressed as Pfaffians. To a signature tensor G satisfying all the Matchgate Identities (and the parity requirements), Theorem 4.2 gives a realization via the character of a complete graph without internal nodes. (Technically this is the case with $G^{11\ldots1} = 1$. In general, we need to "flip" some external nodes, thus introduce a linear number of internal nodes.) However, the realization as a planar matchgate for the signature G may have some internal nodes, necessitated by the introduction of the cross-over gadgets (see below). Thus it is *not* the case that we can realize G as a signature without internal nodes. If G has arity m, this process may introduce $O(m^2)$ internal nodes.

Let's consider exactly how Matchgate Identities are expressed for the signatures. Let G be the signature of a planar matchgate with m external nodes. Since each signature entry can be viewed as a Pfaffian (via the FKT) we have one *useful* Grassmann-Plücker identity for each pair of subsets I and J both containing all the internal nodes. It is clear that the only non-zero terms in the Grassmann-Plücker identity involve moving elements in the symmetric difference $I \Delta J$, which is a subset of the external nodes. We now ignore the internal nodes and consider I and J as subsets of the external nodes, (under a circular shift) identified with $[m] = \{1, 2, \ldots, m\}$. Suppose

$$I \Delta J = \{i_1, \ldots, i_{k_1}, i_{k_1+1}, \ldots, i_{k_2}, i_{k_2+1}, \ldots, i_{k_3}, \ldots\},$$

where $i_1 < \cdots < i_{k_1} < i_{k_1+1} < \cdots < i_{k_2} < i_{k_2+1} < \cdots < i_{k_3} < \ldots$ in the order of the index set $\{1, 2, \ldots, m\}$, and where $i_1, \ldots, i_{k_1} \in I - J$, $i_{k_1+1}, \ldots, i_{k_2} \in J - I$, $i_{k_2+1}, \ldots, i_{k_3} \in I - J$, and so on.

Every non-zero term in (1) involves moving either an element from $I - J$ to J or from $J - I$ to I. For i_j, $j = 1, \ldots, k_1$, the term in (1) is $(-1)^j \mathrm{Pf}(I - \{i_j\})\mathrm{Pf}(i_j \circ J)$. Note that i_j is already in its right place with respect to J within $i_j \circ J$. For $i_j, j = k_1 + 1, \ldots, k_2$, the term in (1) is $(-1)^{j-k_1}\mathrm{Pf}(i_j \circ I)\mathrm{Pf}(J - \{i_j\})$. When we move i_j to its right place with respect to I within $i_j \circ I$, namely k_1 places to the right, this incurs $(-1)^{k_1}$. Thus the term becomes $(-1)^j \mathrm{Pf}(I \cup \{i_j\})\mathrm{Pf}(J - \{i_j\})$, where $I \cup \{i_j\}$ is assumed to be in increasing order.

In this way it is easy to see that all the useful matchgate identities on a realizable standard signature G of arity m can be expressed as follows:

Matchgate Identities for Signatures: A pattern α is an m-bit string, i.e., $\alpha \in \{0,1\}^m$. A position vector $P = \{p_i\}, i \in [l]$, is a subsequence of $\{1, 2, \ldots, m\}$, i.e., $p_i \in [m]$ and $p_1 < p_2 < \cdots < p_l$. We also use p to denote the m-bit string, whose $(p_1, p_2, \ldots, p_l)$-th bits are 1 and others are 0. Let $e_i \in \{0,1\}^m$ be the pattern with 1 in the i-th bit and 0 elsewhere. Let $\alpha + \beta$ denote the pattern obtained from bitwise XOR the patterns α and β. Then for any pattern $\alpha \in \{0,1\}^m$ and any position vector $P = \{p_i\}, i \in [l]$, we have the following identity:

$$\sum_{i=1}^{l} (-1)^i G^{\alpha + e_{p_i}} G^{\alpha + p + e_{p_i}} = 0. \tag{4}$$

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

$$\sum_{i=1}^{l} (-1)^i G^{\alpha + e_{p_i}} G^{\beta + e_{p_i}} = 0. \tag{5}$$

Theorem 4.2 says that a tensor $\mathbf{G} = (G^{i_1, \ldots, i_m})$ is realizable as the standard signature of some planar matchgate iff it satisfies all the parity requirements and (4) for all α and P (or equivalently (5) for all α and β).

A signature is called a *symmetric signature* if its entries only depend on the cardinality of the subset of removed external vertices. Let z_i be the value with a subset of cardinality i removed. Then a symmetric signature can be denoted more succinctly as $[z_0, \ldots, z_m]$. In the framework of holographic algorithms, symmetric signatures are particularly important, because they have a clear combinatorial meaning. For standard symmetric signatures we have

Lemma 5.1. *Suppose Γ is an even matchgate with symmetric standard signature $[z_0, \ldots, z_m]$. Then for all odd i, $z_i = 0$, and there exist r_1 and r_2 not both zero, such that for every even $2 \le k \le m$,*

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

Proof. The parity condition is obvious.

For $m \leq 3$ the condition $r_1 z_{k-2} = r_2 z_k$ is always satisfiable for some r_1 and r_2 not both zero.

Let $m \geq 4$, we use matchgate identities (4). Consider the pattern 1000α where α has Hamming weight $2i$, and $0 \leq 2i \leq m-4$. Let the position vector be $11110\ldots0$. Then (4) gives

$$\begin{aligned} 0 \quad &= G^{0000\alpha}G^{1111\alpha} - G^{1100\alpha}G^{0011\alpha} \\ &\quad + G^{1010\alpha}G^{0101\alpha} - G^{1001\alpha}G^{0110\alpha}. \end{aligned}$$

It follows from symmetry that the last two terms cancel and we get $z_{2i}z_{2i+4} = (z_{2i+2})^2$.

Also, if m is even then consider the pattern 1000α and the position vector 1111β, where $\alpha = 0^{m-4}$ and $\beta = 1^{m-4}$. Then we have

$$\begin{aligned} 0 = G^{0000\alpha}G^{1111\beta} - G^{1100\alpha}G^{0011\beta} \\ + G^{1010\alpha}G^{0101\beta} - G^{1001\alpha}G^{0110\beta} \pm \ldots. \end{aligned}$$

The terms cancel except the first two, from which we get $z_0 z_m = z_2 z_{m-2}$.

Similarly if m is odd, we consider the pattern $1000\ldots0$ and the position vector $1111\ldots10$ and we can get $z_0 z_{m-1} = z_2 z_{m-3}$.

The lemma follows from this. □

Similarly one can prove

Lemma 5.2. *Suppose Γ is an odd matchgate, with symmetric standard signature $[z_0, \ldots, z_m]$. Then for all even i, $z_i = 0$, and there exist r_1 and r_2 not both zero, such that for every odd $3 \leq k \leq m$,*

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

Using the fact that the signatures are symmetric, it can be proved that the set of useful Grassmann-Plücker Identities considered here already constitutes a complete set. It follows from the characterization theorem for matchgates, that the requirements of Lemma 5.1, and Lemma 5.2 are both necessary and sufficient.

Another way to express this is

Theorem 5.1. *A symmetric signature $[z_0, \ldots, z_m]$ of a planar matchgate with* even *cardinality is realizable iff for all odd i, $z_i = 0$, and there exist constants r_1, r_2 and λ, such that $z_{2i} = \lambda \cdot (r_1)^{\lfloor m/2 \rfloor - i} \cdot (r_2)^i$, for $0 \leq i \leq \lfloor \frac{m}{2} \rfloor$.*

A symmetric signature $[z_0, \ldots, z_m]$ of a planar matchgate with odd *cardinality is realizable iff for all even i, $z_i = 0$, and there exist constants r_1, r_2 and λ, such that $z_{2i-1} = \lambda \cdot (r_1)^{\lceil m/2 \rceil - i} \cdot (r_2)^{i-1}$, for $1 \leq i \leq \lceil \frac{m}{2} \rceil$.*

Given an array of values forming a kind of geometric progression as above, the general theory guarantees that there exists a planar matchgate whose signature is the given array. It is a curious fact that the only construction realizing this planar matchgate is via the general proof, and thus via Pfaffian, as follows: We first construct a complete graph with every edge having the same weight. This is given by the proof of Theorem 4.2. For that graph it can be checked that the Pfaffian values are the correct values, as in a (naked) character. Then the planar embedding and the crossover gadget from [1, 13] are used to produce a planar matchgate with the given signature. In particular there will be some $O(m^2)$ extra internal nodes if m is the number of external nodes (arity) of the matchgate. We do not know of any direct construction of a planar matchgate with the given signature, even for this simple case.

6 Conclusions

Valiant's new theory of matchgate computations is an extraordinarily fresh attempt at exploring and devising new algorithmic approaches to problems. It has already yielded highly non-trivial results, such as his classical simulation of a fragment of quantum circuits, and his holographic algorithms. But a full account of the capabilities of matchgate computations is far from being clear. We presented in this paper some fundamental results concerning the building blocks of his theory, namely the matchgates. Our goal here is theory-building, not so much as problem-solving. We believe that it is essential to gain a better understanding of these matchgates before one can get a full picture of matchgate computations [1, 16]. It is hoped that results in this paper will pave the way for some in-depth study of Valiant's new theory. In [1], we applied our results on matchgates to obtain some negative results of holographic algorithms. In [16] Valiant has obtained some important lower bound for holographic algorithms using results of this paper.

References

[1] Jin-Yi Cai and Vinay Choudhary. Some Results on Matchgates and Holographic Algorithms. In Proceedings of ICALP 2006, Part I. LNCS vol. 4051. pp 703-714. Also available at ECCC TR06-048, 2006.

[2] Jin-Yi Cai and V. Choudhary. Valiant's Holant Theorem and Matchgate Tensors (Extended Abstract). In Proceedings of TAMC 2006: LNCS vol. 3959, pp 248-261. Also available at ECCC Report TR05-118.

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

[4] Jin-Yi Cai and Pinyan Lu. Holographic Algorithms: From Art to Science. To appear in STOC 2007. Also available at ECCC Report TR06-145.

[5] Jin-Yi Cai and Pinyan Lu. Bases Collapse in Holographic Algorithms. In these proceedings. Also available at ECCC Report TR07-003.

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

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

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

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

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

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

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

[13] 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 ECCC Report TR05-099.

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

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

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

Acknowledgments

We would like to thank Leslie Valiant for very encouraging comments and discussions. We also thank Andrew Yao, and his group of students in Tsinghua University, for listening to the lectures by the first author on this material. We also thank in particular Rakesh Kumar and Anand Kumar Sinha for many interesting discussions on this and related topics, and to the anonymous referees for their helpful comments.

Appendix

Graphs and Pfaffians

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 a skew-symmetric matrix M, called the (skew-symmetric adjacency) matrix of G, where $M(i,j) = w(k_i, k_j)$ if $i < j$, $M(i,j) = -w(k_i, k_j)$ if $i > j$, and $M(i,i) = 0$. From here on, we will use G to represent both the graph and its matrix, whenever the meaning is clear from the context.

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

- $\pi = \begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix}$, is a permutation.
- summation is over all permutations π where $i_1 < i_2, i_3 < i_4, \ldots, i_{2k-1} < i_{2k}$ and $i_1 < i_3 < \ldots < i_{2k-1}$, 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 $(\mathrm{Pf}(M))^2 = \det(M)$.

A matching is a subset of edges such that no two edges share a common vertex. A vertex is said to be saturated if there is a matching edge incident to it. A perfect matching is a matching which saturates all vertices.

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 $w(i_1, i_2) \ldots w(i_{2k-1}, i_{2k})$ in $\mathrm{Pf}(M)$ corresponds to the perfect matching $\{(i_1, i_2), \ldots, (i_{2k-1}, i_{2k})\}$ 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 $A = \{i_1, \ldots, i_r\} \subseteq \{1, \ldots, n\}$, 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 $\lambda_1, \lambda_2, \ldots, \lambda_n$ 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.

Extended Main Theorem

In this Appendix, we give an extension of the Main Theorem proved by Valiant in [12]. It is a minor extension which was needed in Section 3.

Let $\Gamma = (G, X, Y, T)$ be a matchgate. Let us call Γ, an *even* matchgate if $\mathrm{PfS}(G \backslash Z)$ is zero whenever $Z \subseteq X \cup Y$ has odd size and call it *odd* if $\mathrm{PfS}(G \backslash Z)$ is zero whenever $|Z|$ is even. Let us modify the definition of a matchcircuit to allow parallel edges to have weight -1. Then we can prove the following *Extended Main Theorem*.

Theorem 7.1. [Extended Main Theorem] *Consider a matchcircuit Γ composed of gates as in [12]. Suppose that every gate is:*

1. *a gate with diagonal character matrix,*
2. *an even gate applied to consecutive bits $x_i, x_{i+1}, \ldots, x_{i+j}$ for some $j \geq 0$,*
3. *an odd gate applied to consecutive bits $x_i, x_{i+1}, \ldots, x_{i+j}$ for some $j \geq 0$, or*
4. *an arbitrary gate on bits $x_1, \ldots, x_j$ for some $j \geq 1$.*

Suppose also that every parallel edge above any odd matchgate, if any, has weight -1 and all other parallel edges have weight 1. Then the character matrix of Γ is the product of the character matrices of the constituent matchgates, each extended to as many inputs/outputs as those of Γ.

Proof. The only kind of overlap that we need to worry about in the proof of the Main Theorem in [12] is that between parallel and external edges of a matchgate. By the definition of an odd gate, the only non-zero in its character matrix can be in positions which correspond to an odd number of inputs/outputs being matched externally. Any parallel edge above a matchgate has an overlap with any of its external edges that are present. Since only those matchings make a non-zero contribution when there are an odd number nodes matched externally, any such parallel edge overlaps with an odd number of external edges; thus contributing a $-$ sign which cancels with its own weight of -1. The rest of the proof is exactly as in [12] □

Identities for Matchgates with Omittable Nodes

Lemma 7.1. *Consider any GP identity such that all the Pfaffians appearing in it are Pfaffians of sub-matrices with some input/output nodes and/or the omittable node deleted. Remove any terms which have an odd number of indices deleted. Write each remaining term as a Pfaffian sum of a matrix with a subset of inputs/outputs deleted. Then it is a useful identity and is independent of n. Therefore, it is a matchgate identity.*

Theorem 7.2. *Let k, l be non-negative integers. Let B be a $2^k \times 2^l$ matrix. Then B is the character matrix of a k-input, l-output matchgate Γ if and only if B satisfies all the GP identities.*

Proof. The proof is almost the same as for the case without omittable nodes. As earlier, let's assume, WLOG, that $B_{2^k-1,2^l-1} = 1$. The matchgate Γ is a complete graph $k + l + 1$ vertices. It has k inputs and l outputs and one omittable node. The weight of the edge joining nodes i and j is the appropriate modifier times the entry of the matrix B which corresponds to i, j being deleted. Note that now, this entry might have total Hamming weight (as far as inputs/outputs are concerned) either $k + l - 1$ or $k + l - 2$, depending on whether either i or j is the omittable node or not. Let the skew-symmetric adjacency matrix of Γ be M. We claim that the character matrix of Γ, say A, is equal to B. By definition, all the entries of B with total Hamming weight at least $k + l - 2$ are equal to those in A. Now we proceed by downward induction on the total Hamming weight $H(i) + H(j)$. Consider any other entry B_{ij} such that $H(i) + H(j)$ is less than $k + l - 2$.

Let $a_1 \leq \ldots \leq a_r$ be the bits that are 1 in i and j. Depending on the parity of r, we either need to delete the omittable node, say a, or keep it. Let S be the set of nodes that we need to delete to get this entry of B. Let $1 \leq a' \leq k + l$ be an index not in S. Consider the GP identity with $I = \Gamma - S \cup \{a'\}$ which we'll denote by $I = \{\hat{S}, \hat{a'}\}$ and let $J = \{a'\}$. This identity looks like the following:

$$\mathrm{Pf}_M[S]\mathrm{Pf}_M() = \sum_{b \in I} (\pm)\mathrm{Pf}_M[\{b, a'\} \cup S]\mathrm{Pf}_M(b, a')$$

Note that $\mathrm{Pf}_M() = 1 = A_{2^k-1,2^l-1} = B_{2^k-1,2^l-1}$. The right hand side is a sum of products of two terms. Each term is the Pfaffian sum of M with a superset of $a_1, \ldots a_r$ removed. These correspond to entries of A and B in positions with total Hamming weight more than r. Since B is equal to A on all such entries and since B satisfies the GP identities, we see that $B_{ij} = A_{ij}$. This completes the proof. □

Figures

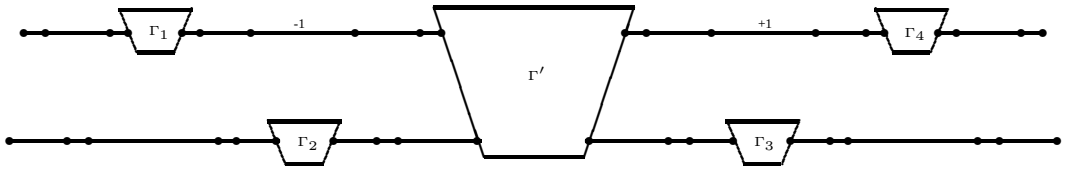

Figure 1. The figure shows the matchcircuit Γ'' used in the proof of theorem 3.2. Suppose α_r flips the second bit only and α_c flips the first bit only. Then Γ_2 and Γ_4 are equal to $\Gamma^{(2)}$ i.e. they flip their input; and Γ_1 and Γ_3 simply transmit their input. Therefore, the parallel edge above Γ_2 has weight -1 and all other parallel edges, in particular the one above Γ_3 have weight 1. In the general case when there are k-inputs and l-outputs, if any matchgate flips its input, all the parallel edges above it have a weight -1.

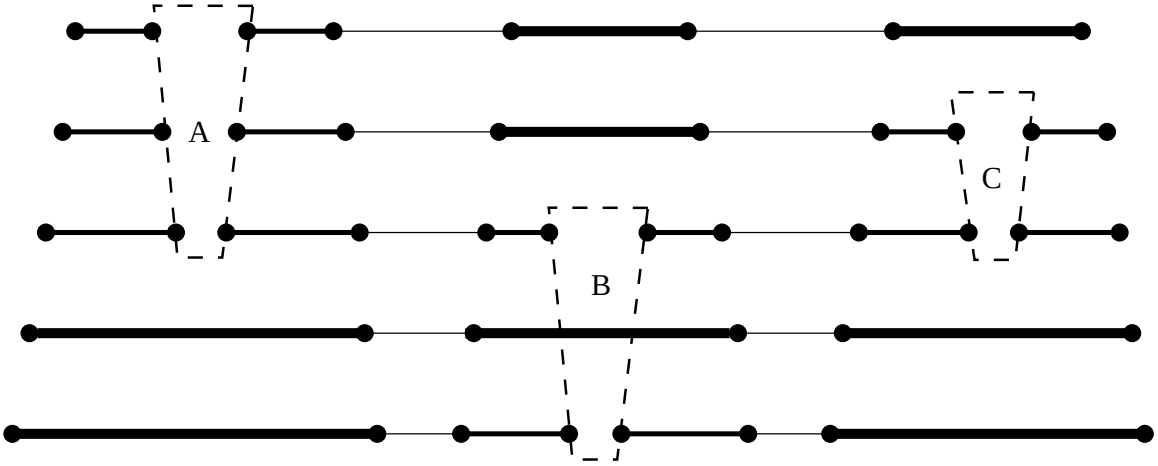

Figure 2. An example of a matchcircuit composed of matchgates A, B and C. A is a 3-input, 3-output matchgate while B and C are 2-input, 2-output matchgates. The boldest line represent *parallel* edges, the lightest represent *connecting* edges and the rest are *external* edges. The nodes in the matchcircuit are numbered in increasing order from left to right. The five leftmost nodes are its *inputs* and the five rightmost ones are its *outputs*.