On the Theory of Matchgate Computations

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

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

Abstract

Valiant has proposed a new theory of algorithmic computation based on perfect matchings and the Pfaffian. We study the properties of *matchgates*—the basic building blocks in this new theory. We give a set of algebraic identities which completely characterize these objects in terms of the Grassmann-Plücker identities. In the important case of 4 by 4 matchgate matrices, which was used in Valiant's classical simulation of a fragment of quantum computations, we further realize a group action on the character matrix of a matchgate, and relate this information to its compound matrix. Then we use Jacobi's theorem to prove that in this case the invertible matchgate matrices form a multiplicative group. These results are useful in establishing limitations on the ultimate capabilities of Valiant's theory of matchgate computations and his closely related theory of Holographic Algorithms.

1 Introduction

In a most striking development, Valiant [11] has introduced a completely new method of organizing certain computations based on the graph theoretic notion of perfect matching and the related algebraic construct called the Pfaffian. The central objects in this new theory are called *matchgates*. These are essentially graphs with certain nodes designated as inputs or outputs. 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*. The global properties of these matchcircuits can be interpreted as realizing certain computations which would seem to take exponential time in the size of the circuit. However, due to the way the matchcircuits are constructed and the algebraic properties of Pfaffians defining the character matrices of the constituent matchgates, these global properties of the matchcircuits 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. Thus matchcircuits can be seen as a new algorithmic method to construct polynomial time algorithms performing certain seemingly exponential time computations. Valiant [11] used these matchcircuits to show that a non-trivial, though still quite restricted, fragment of quantum circuits can be simulated classically in polynomial time. It is not very 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. To understand that, we must first have a better understanding of the matchgates.

Subsequently, in another ground breaking paper, Valiant [12] further introduced the notion of Holographic Algorithms. This theory is also based on matchgates and their properties, 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, however, the matchgates used are restricted to be *planar matchgates*. Instead of a character matrix, a planar matchgate is associated with a signature matrix. Then the computation is expressed via the elegant Fisher-Kasteleyn-Temperley method [6, 7, 8] for planar perfect matchings. Valiant was able to use this theory to devise polynomial time algorithms for several problems, for which certain minor variations are known to be NP-complete or NP-hard (or even #P-hard). Again the ultimate capabilities and limitations of Holographic Algorithms are not clear at this moment. But it can be safely said that Valiant's new theory has pushed outward the boundary of what is known to be polynomial time computable, and it holds the promise of becoming a new algorithmic design paradigm.

In the most optimistic outlook (or some may call it imprudently unrealistic), this new algorithmic paradigm may ultimately lead to a collapse of complexity classes. The kinds of algorithms that are produced by the method of matchgates are quite unlike anything before and almost exotic. If our collective belief in NP $\neq$ P is based on our sense and experience that the usual algorithmic paradigms are insufficient for NP-hard problems, then at a minimum, no one who has examined these new algorithms in some detail will feel comfortable to say that these fall under the same category, and therefore can be safely regarded as inadequate for NP-hard problems by our erstwhile experience. Of course the final truth may be that these algorithms do not in fact lead to any collapse of complexity classes. But even in this eventuality, as Valiant suggested in [12], "any proof of P $\neq$ NP may need to explain, and not only to imply, the unsolvability" of NP-hard problems using this approach. Regardless of how one views its likely final outcome, we think the investigation of the capabilities and limitations of the new algorithms is an extremely worthwhile scientific goal.

It is also clear that in order to gain a better understanding of this capability and limitation, one must first gain a better understanding of its most basic building blocks, namely the matchgates themselves.

It turns out that there is a rich internal structure to the matchgates as expressed by the algebraic properties of the Pfaffian. The main results of this paper are concerned with this internal structures of matchgates and their characters. We believe that the results in this paper provide a fairly complete picture of these matchgates. Indeed Valiant has already initiated this study [11, 10]. In particular Valiant exhibited 5 equations, called matchgate identities, which are necessary conditions for the important class of all 4 by 4 matchgate character matrices. This is the class of matchgates which was used in Valiant's classical simulation of a fragment of quantum computations. With a slight restriction on the character matrices, Valiant also showed that these 5 matchgate identities are sufficient.

It turns out that these matchgates 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 these 5 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, by showing that they are both necessary and sufficient for any 4 by 4 matchgate character matrix without any assumptions. We further relate this information to the compound matrix of the character matrix. (A compound matrix consists of entries which are determinantal minors of a fixed order of the original matrix.) Then we use Jacobi's theorem on compound matrices to prove that the invertible 4 by 4 matchgate matrices form a multiplicative group. It was easy to show that this set is closed under matrix multiplication, as was noted in [11]. Here we prove that if the character matrix is invertible, its inverse is also the character matrix of some matchgate.

We then define matchgate identities for general k-input, l-output matchgates, and find matchgate identities for these general matchgates. We show that a set of the so-called Grassmann-Plücker identities [2, 10] give a complete set of matchgate identities for any general matchgate. A $2^k \times 2^l$ matrix is the character matrix of a matchgate if and only if it satisfies all these matchgate identities derived from the Grassmann-Plücker identities.

By definition, even with a fixed number of input and output nodes (such as the class of 2-input, 2-output matchgates giving arise to the 4 by 4 character matrices), 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 the proof of these characterizations of general matchgates is that when a requisite matchgate exists, it can be realized by a weighted complete graph consisting of essentially the external nodes plus at most one omittable node. Thus, in some sense, the design of a requisite matchgate boils down to the choice of $\binom{k+l}{2}$ weights, where $k + l$ is the number of input and output nodes. This makes it feasible both to search, and in case of non-existence to prove that it does not exist, by an algorithmic process.

We believe that a thorough understanding of the capabilities and limitations of matchgates is essential to delineate the final domain of matchcircuit computations. We note that our results on matchgates also apply to planar matchgates and the corresponding notion of signature matrices. In fact in a forth coming paper [4], we will prove an equivalence theorem of matchgates/matchcircuits with character matrices on the one hand and planar matchgates/matchgrids with signature matrices on the other. Therefore the results presented in this paper also serve as the first step in the study of the limitation of Holographic Algorithms. We will show that using these matchgate identities (and other properties) we can establish the impossibility of certain 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 [11] and [10]. We will give a brief recap here.

2.1 Graphs and Pfaffian

Let $G = (V, E, W)$ be a weighted undirected graph, where V is the set of vertices represented by integers, E is the set of edges and W are the weights of the edges. In general, $V = \{k_1, \ldots, k_n\}$ where $k_1 < \ldots < k_n$. We represent the graph by 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.

2.2 Grassmann-Plücker Identities

Let M be a skew-symmetric matrix, and $A = \{i_1, \ldots, i_r\}$ where $i_1 < \ldots < i_r$. Consistent with our notation, $\mathrm{Pf}_M(i_1, \ldots, i_r)$, 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 $\{i_1, \ldots, i_r\}$. And obviously, $\mathrm{Pf}_M[i_1, \ldots, i_r]$ is just another notation for $\mathrm{Pf}(M[A])$. 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 identities.

Theorem 2.1. *[2, 3] 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 identities (generated by I and J),*

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

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.

2.3 Matchgates and Matchcircuits

A *matchgate* Γ is a quadruple (G, X, Y, T) where $G = (V, E, W)$ is a graph, $X \subseteq V$ is a set of *input* nodes, $Y \subseteq V$ is a set of *output* nodes, and $T \subseteq V$ is a set of *omittable* nodes such that X, Y and T are pairwise disjoint, and $\forall i \in T$, 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 of a matchgate fragment, we assume that $\lambda_i = 1$, if $i \in T$, and 0 otherwise. We say that a matchgate Γ has *normal numbering* if the numbers of nodes in V are consecutive from 1 to $|V|$ and X, Y have minimal and maximal numbers, respectively.

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

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

A *matchcircuit* is a way of combining matchgates using what are called connecting edges. Informally, all inputs/outputs of constituent matchgates have an external edge. The external edges are connected to each other with an odd number of connecting edges. The matchgates are arranged in a layered fashion from left to right where the connecting edges separate these layers. Figure 2 shows a typical matchcircuit. We do not present the detailed definition here due to space constraints and because we won't be dealing too much with matchcircuits. We refer the reader to [11] 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.

3 2-input 2-output Matchgates

3.1 A Complete Set of Matchgate Identities

In [10], 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 2.3.) 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 [10]:

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

It turns out that there are interesting symmetries buried in this set of identities. For example, the terms $B_{11}B_{44} - B_{14}B_{41}$ 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

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

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

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

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 realized 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 is omitted here for space limitations, but uses essentially the same techniques as in [10]. 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,

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

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

Theorem 3.1. *If B is the character matrix of a 2-input 2-out 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 2.3. 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. For the proof, we will use the construction of [11] as a black-box. We will compose matchgates to form a matchcircuit which has the same character matrix but with rows and columns permuted. Then we will transform this matchcircuit to a matchgate that realizes the given matrix.

Now, if B is the zero matrix, then there is a trivial matchgate that realizes it. Otherwise let's assume that $B_{rc} \neq 0$. 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, $B'_{44} \neq 0$. 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 of matchgate identities is invariant under any such transformation. If B satisfies the matchgate identities, then so does B'. From the construction in [11] 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 $\Gamma^{(2)}$ depending on whether that bit of i (or j) 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; see Appendix for details. It is possible to give a more efficient proof in this case, but the general method is used in the proof of Theorem 4.2.) 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 $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

The Main theorem in [11] can be extended to prove the Extended Main Theorem, given in appendix. It can be verified that construction 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 that we imagine the matchgate to act on two bits, where its action on the bits (in the matchcircuit) that are not its inputs is considered to be identity. This product is nothing but B. To see that, we look at the matchcircuit in a slightly different way. The overall action of the matchcircuit on its inputs is just 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 meaning 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. $\square$

3.2 Group Property

Now we will study a very interesting property of 2-input, 2-output matchgates. 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 [11] 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 ultimately which quantum operations can they simulate.

To get to this result, we will need to consider what is known as the compound of a matrix [1]. Then the proof will follow from Jacobi's theorem [1] which relates the compound of a matrix to the compound of its inverse. First we introduce some notation. Let A be an $m \times n$ matrix.

- $A(i_1, \ldots, i_k; j_1, \ldots, j_k)$: The determinant of the submatrix consisting of rows $i_1, \ldots, i_k$ and columns $j_1, \ldots, j_k$ of A. Here it is assumed that $1 \leq i_1 < \ldots < i_k \leq m$, and $1 \leq j_1 < \ldots < j_k \leq n$. It is called a minor of order k.
- $A^{[k]}$: The k^{th} compound matrix of A is a matrix of order $\binom{m}{k} \times \binom{n}{k}$, where we arrange all the minors of A of order k in lexicographic order.

We define the matrices J_n and K_n as the following $n \times n$ matrices:

$$J_{ij} = \begin{cases} (-1)^{i-1} & \text{if } i = j \\ 0 & \text{otherwise} \end{cases}$$

$$K_{ij} = \begin{cases} 1 & \text{if } i = n - j + 1 \\ 0 & \text{otherwise} \end{cases}$$

We are now ready to state Jacobi's theorem [1].

Theorem 3.3. [Jacobi's Theorem] *Let A be an invertible $n \times n$ matrix over a field F. Then,*

$$(A^{-1})^{[k]} = \frac{1}{|A|} K (J A^t J)^{[n-k]} K$$

where $J = J_n$ and $K = K_m$ for $m = \binom{n}{k}$, and $|A|$ denotes the determinant of A.

Corollary 3.1. *Let A, J and K be as above, then*

$$(\text{adj } A)^{[k]} = |A|^{k-1} K (J A^t J)^{[n-k]} K$$

Here adj A *denotes the adjoint of A.*

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

Theorem 3.4. *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 3.5. *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.*

Proof. We will make use of Jacobi's Theorem and Theorem 3.4. By Jacobi's Theorem, we have

$$(B^{-1})^{[2]} = \frac{1}{|B|} K (JB^t J)^{[2]} K$$

where $J = J_4$ and $K = K_6$. Now note that the matchgate identities are symmetric with respect to rows and columns and hence, are invariant under transpose. So B^t also satisfies the identities. Clearly, J satisfies the identities. By Theorem 3.2, B^t and J are realizable as the character matrices of some 2-input 2-output matchgates. Therefore so is $C = JB^t J$. It follows that C also satisfies the identities. This means that $C^{[2]}$ is invariant under simultaneous interchange of row 3 with row 4 and column 3 with column 4. Multiplication by K on the left and right is nothing but a simultaneous reversal of rows/columns. So $KC^{[2]}K$ is $C^{[2]}$ with rows and columns in reverse order. Hence $KC^{[2]}K$ is also invariant under simultaneous interchange of row 3 with row 4 and column 3 with column 4. Therefore, B^{-1} satisfies the matchgate identities. ☐

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

Corollary 3.2. *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.*

Proof. When B is not invertible, by Corollary 3.1, $(\mathrm{adj}\ B)^{[2]} = 0$. Hence adj B satisfies the matchgate identities. ☐

4 General Matchgates

4.1 Identities for 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 Grassmann-Plücker identities characterize all the character matrices. But we have to be careful. There are various kinds of Pfaffians that occur in the Grassmann-Plücker 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 anti-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 the matrix 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 the Grassmann-Plücker identity 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), we need it to satisfy the following two properties:

1. Every non-zero Pfaffian should be the Pfaffian of a submatrix obtained by deleting only (rows and columns corresponding to) some inputs and outputs of Γ.

2. The Grassmann-Plücker identity should be independent of n.

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

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

Proof. All the summands in a Grassmann-Plücker 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, or have only some inputs or outputs deleted. ☐

To prove that all the useful Grassmann-Plücker 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 Grassmann-Plücker identity by the indices that are deleted, rather than using the indices that are retained as in 1. In other words, we use Pf[] notation instead of 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 Grassmann-Plücker 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.

Lemma 4.2. *All the useful Grassmann-Plücker identities are independent of n.*

Proof. Let I be a superset of U. Suppose $i'_1 < \ldots < i'_a$ are the inputs in I and $o'_1 > \ldots > o'_b$ be the outputs in I. Similarly, let $i''_1 < \ldots < i''_c$ and $o''_1 > \ldots > o''_d$ be the outputs in J where J is another superset of U. Consider the Grassmann-Plücker 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 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 Grassmann-Plücker identity is

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

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 Grassmann-Plücker 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 z_t^I be the number of inputs *in* I less than t and o_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 Grassmann-Plücker 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 $B_{**} = B_{J_R-\{t\},J_C}$)

$$\begin{aligned}
& (-1)^{z_t^I}\text{Pf}(I-\{t\})\text{Pf}(t\circ J) \\
= \;& (-1)^{z_t^I}(-1)^{z_t^J}\text{Pf}(I-\{t\})\text{Pf}(J\cup\{t\}) \\
= \;& (-1)^{z_t^I}(-1)^{z_t^J}\mu_I(-1)^{o_t^I}(-1)^{z_t^I}B_*\text{Pf}(J\cup\{t\}) \\
= \;& (-1)^{z_t^J}\mu_I(-1)^{o_t^I}B_*\text{Pf}(J\cup\{t\}) \\
= \;& (-1)^{z_t^J}\mu_I(-1)^{o_t^I}B_*\mu_J(-1)^{z_t^J}(-1)^{o_t^J}B_{**} \\
= \;& (-1)^{o_t^I}(-1)^{o_t^J}\mu_I\mu_J B_* B_{**}
\end{aligned}$$

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

$$(-1)^{o_t^I}(-1)^{o_t^J}B_{I_R\cup\{t\},I_C}B_{J_R-\{t\},J_C} \tag{2}$$

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

The above form will allow us to prove an important property of the Grassmann-Plücker 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 Grassmann-Plücker identities. We have the following lemma.

Lemma 4.3. *Given any b, $1 \le b \le k$, ρ_b is a permutation on the Grassmann-Plücker identities.*

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 Grassmann-Plücker identity generated by I and J, then $G_2 = \rho_b(G_1)$ is the Grassmann-Plücker 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 $binJ' - I'$ from J' to I'. The other cases when $b \notin I \cup J$ or $b \in J - I$ are symmetric.

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 $(-1)^{o_t^I + o_t^J}$ and of the corresponding term in G_2 is $(-1)^{o_t^{I'} + o_t^{J'}}$. Our analysis depends on b. First, if b is an output vertex, or an input such that $b \leq t$, then $o_t^I = o_t^{I'}$ and $o_t^J = o_t^{J'}$ 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 o_t^I and $o_t^{I'}$, and also exactly once in o_t^J and $o_t^{J'}$. Thus, it is counted exactly twice among $o_t^I, o_t^J, o_t^{I'}, o_t^{J'}$. It follows that in any case, the sum $o_t^I + o_t^J + o_t^{I'} + o_t^{J'}$ 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. $\square$

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. Final induced transformation on the Grassmann-Plücker identities is still a permutation. 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 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 Grassmann-Plücker 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 vertices with an edge of weight α between them. This will have character B.

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 anti-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 $\chi(\Gamma)$. Now we proceed by downward induction on the total Hamming weight $H(r) + H(c)$. Consider any other entry B_{rc} such that $H(r) + H(c)$ is less than $k + l - 2$. Let $a_1 < \ldots < a_m$ be the bits that are 1 in rc. Let $1 \leq a' \leq k + l$ be an index not equal to any of these.

Consider the Grassmann-Plücker identity with $I = \{1, \ldots, k+l\} - \{a_1, \ldots, a_m, a'\}$ and $J = \{a'\}$. This identity looks like the following:

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

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 more than m. Since B is equal to $\chi(\Gamma)$ on all such entries and since B and $\chi(\Gamma)$ both satisfy the Grassmann-Plücker identities, we see that $B_{ij} = \chi(\Gamma)_{ij}$.

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 Grassmann-Plücker 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. $\square$

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 ([11]). We need to change the definition of useful Grassmann-Plücker 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 Grassmann-Plücker identities are independent of n and the analog of theorem 4.1 that input/output bit-flips induce a permutation on the Grassmann-Plücker identities. The completeness theorem is proved in the appendix.

From the proofs of theorem 4.2 and theorem 6.1 (in the appendix), we see that if $B_{2^k-1,2^l-1}$ is non-zero, then 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 Conclusions and Future Work

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 interesting results concerning the building blocks of his theory, namely the matchgates. We believe that it is essential to gain a better understanding of these matchgates before one can get a full picture of matchgate computations. Even for 2-input 2-output matchgates, it is not clear what the full extent of its computational capabilities. It is hoped that results in this paper will pave the way for some in-depth study of these matchgate computations. In a forth coming paper [4], we will present some negative results of holographic algorithms based on these necessary and sufficient conditions on matchgates.

One structural question remains for the general matchgates. We believe that non-singular 2^k by 2^k matchgate characters also form a group. The group property is likely to suggest deeper symmetries of these matchgate computations.

Acknowledgments

We would like to thank Leslie Valiant for very encouraging comments and discussions, especially while both he and the first author visited Beijing. We 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.

References

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

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

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

[4] Jin-Yi Cai, V. Choudhary. Some Results on Matchgates and Holographic Algorithms. To appear.

[5] Jin-Yi Cai, V. Choudhary. Valiant's Holant Theorem and Matchgate Tensors (Extended Abstract). Electronic Colloquium on Computational Complexity Report TR05-118.

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

[9] L. G. Valiant: Negation can be Exponentially Powerful. Theor. Comput. Sci. 12: 303-314 (1980).

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

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

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

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

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

Appendix

Extended Main Theorem

Let $\Gamma = (G, X, Y, T)$ be a matchgate. Let us call Γ, an *even* matchgate if $PfS(G \backslash Z)$ is zero whenever $Z \subseteq X \cup Y$ has odd size and call it *odd* if $PfS(G \backslash Z)$ 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 6.1. [Extended Main Theorem] *Consider a matchcircuit Γ composed of gates as in [11]. 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 [11] 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 [11] □

Identities for Matchgates with Omittable Nodes

Lemma 6.1. *Consider any Grassmann-Plücker 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 6.2. *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 Grassmann-Plücker 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 anti-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 Grassmann-Plücker 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:

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

Note that $Pf_M() = 1 = A_{2^k-1, 2^l-1} = B_{2^k-1, 2^l-1}$. 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 Grassmann-Plücker identities, we see that $B_{ij} = A_{ij}$. This completes the proof. □

Figures

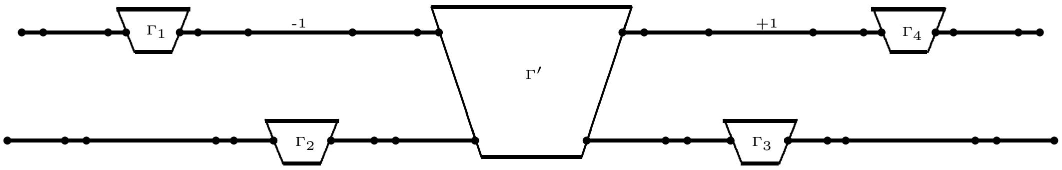

Figure 1: The figure shows the matchcircuit Γ'' used in the proof of theorem 3.2. Suppose α_r flips the second bit only and α_c flips the first bit only. Then Γ_2 and Γ_4 are equal to $\Gamma^{(2)}$ i.e. they flip their input; and Γ_1 and Γ_3 simply transmit their input. Therefore, the parallel edge 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.

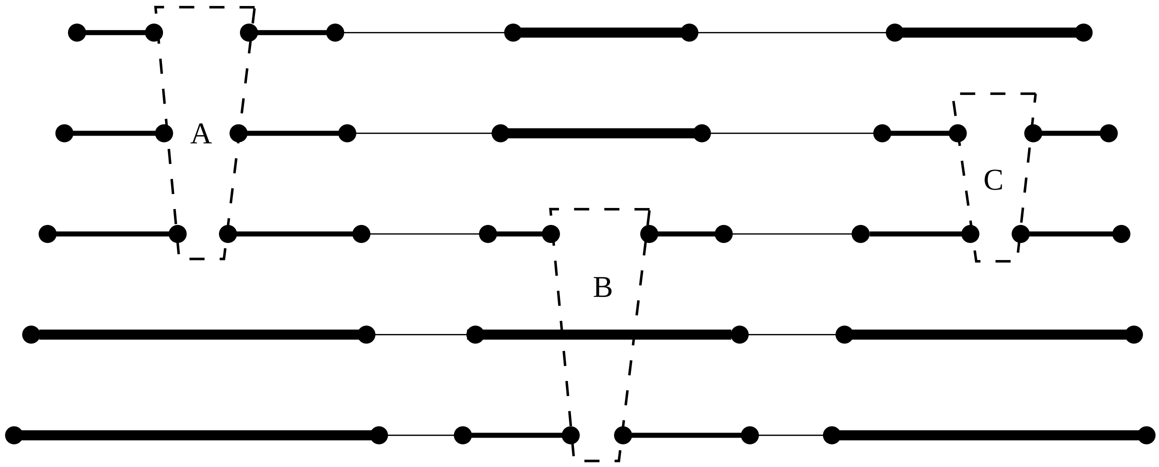

Figure 2: An example of a matchcircuit composed of matchgates A, B and C. A is a 3-input, 3-output matchgate while B and C are 2-input, 2-output matchgates. The boldest line represent *parallel* edges, the lightest represent *connecting* edges and the rest are *external* edges. The nodes in the matchcircuit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