ELSEVIER

Theoretical Computer Science 289 (2002) 457–471

Theoretical Computer Science

www.elsevier.com/locate/tcs

Expressiveness of matchgates ☆

Leslie G. Valiant

Division of Engineering and Applied Sciences, Harvard University, Cambridge, MA 02138, USA

Received March 2001; accepted June 2001
Communicated by A. Razborov

Abstract

Matchgates have been used to simulate classically in polynomial time assemblies of quantum gates. In this paper it is shown that every matchgate for 2-input 2-output functions has to obey a certain set of five polynomial identities. It is also shown that no matchgate can realize a nontrivial control gate for any number of inputs. On the other hand, it is proved that classical Boolean formulae can be expressed as matchcircuits of polynomial size. © 2002 Elsevier Science B.V. All rights reserved.

1. Introduction

Quantum circuits as defined by Deutch [3] offer a model of computation for which no polynomial time simulation by classical computers is known, but for which the possibility of physical realization is currently open. A subclass of these circuits was defined in [9], for which, in contrast, polynomial time classical simulation is provable. The definition of this subclass involves a restriction on the gates used, to so-called *matchgates*, as well as restrictions on the manner in which these are interconnected. The purpose of this current paper is to understand the implications of the restrictions on the gates.

First we show that for all 2-qubit matchgates, the 4×4 matrix that describes the gate is constrained by five polynomial relations that we call the *matchgate identities*. In [9] it was shown that as long as entry $(4,4)$ of the matrix is nonzero, every 4×4 matrix satisfying exactly these identities can be realized.

☆ This research was supported in part by grant NSF-CCR-98-77049 and by the National Security Agency (NSA) and Advanced Research and Development Activity (ARDA) under Army Research Office (ARO) Contract No. DAAD19-01-1-0506.

E-mail address: valiant@deas.harvard.edu (L.G. Valiant).

0304-3975/02/$ - see front matter © 2002 Elsevier Science B.V. All rights reserved.
PII: S0304-3975(01)00325-5

We go on to consider a consequence of these relations to *control gates*. These are gates where the value of one input, the control input, emerges from the gate unchanged as one of the outputs, but controls how the other, controlled, inputs are mapped to the other outputs. A nontrivial example is the control-NOT gate [1, 5] which flips the controlled input if and only if the control input has value 1. We regard a control inputs as being trivial if its effect on the controlled inputs is the same multiplicative factor for all values of the controlled gates. We show that for any number of inputs no matchgate can realize a nontrivial control gate.

The generic power of control gates is illustrated by the fact that when they are strung together into a long chain one can have a single control input influence an arbitrary number of other variables. Since scalable general quantum computers have yet to be built, our result poses a specific more limited challenge: can arbitrarily long chains of control gates be built that require only polynomially growing resources? A negative answer would suggest that the obstacles that have been encountered in constructing scalable quantum computers may be related to the constraints on quantum gates that matchgates impose. A positive answer, on the other hand, would be a useful building block, for example, for Shor's integer factorization algorithm [7] where nondeterministically chosen single bits influence operations on arbitrary length numbers.

Finally, we obtain the following further characterization of matchgates. We show that for every Boolean n-variable formula and an input for it, one can construct a matchcircuit that effectively evaluates the formula on that input. Further the matchcircuits so constructed lie in a class that can be predicted classically in time polynomial in the size of the formula.

2. Definitions

2.1. Graph-theoretic definitions

We describe some standard graph-theoretic notions and their relation to the Pfaffian of a matrix [2, 4].

A weighted undirected graph, or simply a *graph*, G is a triple (V,E,W) where V is a set of *vertices* each represented by a distinct positive integer, E is a set of *edges* or unordered pairs (i,j) of the vertices $i,j \in V$, and W is the set of *weights*, each weight $w(i,j)$ corresponding to the edge $(i,j) \in E$. For example, $V=\{1,2,3\}$, $E=\{(1,2),(2,3),(1,3)\}$, $w(1,2)=w(2,3)=w(1,3)=2$, is the complete graph on three vertices in which every edge has weight 2.

An $n \times n$ matrix B is *skew-symmetric* if for all i,j $(1 \leqslant i,j \leqslant n)$ $B(i,j)=-B(j,i)$. The *matrix of the graph* $G=(V,E,W)$ where $V=\{1,2,\ldots,n\}$ is the $n \times n$ matrix $M(G)$ where the (i,j) entry $M(G)(i,j)$ is defined to equal

(i) $w(i,j)$ if $i<j$,
(ii) $-w(i,j)$ if $i>j$, and
(iii) 0 otherwise.

In the more general case that $V=\{k_1,k_2,\ldots,k_n\}$ where $k_1<k_2<\cdots<k_n$, weight $w(k_i,k_j)$ replaces $w(i,j)$ in (i) and (ii) in this definition. For brevity, we shall abbreviate $M(G)$ by G whenever it is clear that a matrix is intended.

The Pfaffian of an $n\times n$ skew-symmetric matrix B is defined to be zero if n is odd, one if $n=0$, and if n is even with $n=2k$ and $k>0$ then it is defined as

$$\mathrm{Pf}(B)=\sum_{\pi}\varepsilon_\pi w(i_1,i_2)w(i_3,i_4)\cdots w(i_{2k-1},i_{2k}),$$

where

(i) $\pi=[i_1,i_2,i_3,\ldots,i_{2k}]$ is a permutation on $[1,2,\ldots,n]$,

(ii) summation is over all such permutations π where further
$i_1<i_2, i_3<i_4,\ldots,i_{2k-1}<i_{2k}$, and
$i_1<i_3<i_5<\cdots<i_{2k-1}$, and

(iii) $\varepsilon_\pi\in\{-1,1\}$ is the sign of the permutation π, i.e., it is -1 or $+1$ according to whether the number of transpositions or swaps of pairs of distinct elements i_j, i_k, needed to reorder π to the identity permutation is odd or even. (An equivalent definition in this context 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 $i_{2s-1}<i_{2r-1}<i_{2s}<i_{2r}$. Note that it is implicit here that $i_{2r-1}<i_{2r}$ and $i_{2s-1}<i_{2s}$.)

A *matching* $E^*\subseteq E$ of G is a set of edges such that if (i,j), (r,s) are distinct edges in E^* then i,j,r,s are all distinct vertices. In a graph with an even number $2k$ of nodes a matching E^* is *perfect* if it contains k edges. (In other words, every $i\in V$ is an endpoint of, or is *saturated* by, some edge in E^*.)

We shall use the following graph-theoretic interpretation of the Pfaffian. If B is the matrix of the graph G then there is a one-to-one correspondence between monomials in the Pfaffian and perfect matchings in G. The monomial $w(i_1,i_2)\,w(i_3,i_4)\cdots w(i_{2k-1},i_{2k})$ in Pf (G) corresponds to the perfect matching $\{(i_1,i_2),(i_3,i_4),\ldots,(i_{2k-1},i_{2k})\}$ in G. The coefficient ε_π of this monomial will be the parity of the numbers of overlapping pairs of edges, in the sense defined above.

For an $n\times n$ matrix B and any set $A=\{i_1,\ldots,i_r\}\subseteq\{1,\ldots,n\}$ we denote by $B[A]$ the $(n-r)\times(n-r)$ matrix obtained by deleting from B all the rows and columns indexed by A. The following is from [8].

Definition. The *Pfaffian Sum* of an $n\times n$ skew-symmetric matrix B is a polynomial over indeterminates $\lambda_1\cdots\lambda_n$ such that

$$\mathrm{PfS}(B)=\sum_{A}\left(\prod_{i\in A}\lambda_i\right)\mathrm{Pf}(B[A]).$$

Summation here is over the various principal minors obtained from B by deleting some subset A of the indices. In this paper we shall only need the instances in which each λ_i is fixed to be 0 or 1. The i for which $\lambda_i=0$ can be thought of as the *unomittable*

indices, and those with $\lambda_i = 1$ as the *omittable* indices. Then for this *(0,1)-case* the Pfaffian Sum is simply the sum of the $\mathrm{Pf}(B[A])$ over those A that contain only omittable indices. This is the only case we need in this paper.

2.2. Matchgates

We shall simulate each quantum or other gate by what we call a matchgate.

A *matchgate* Γ is a quadruple (G, X, Y, T) where G is a graph (V, E, W), $X \subseteq V$ is a set of *input* vertices, $Y \subseteq V$ is a set of *output* vertices, and $T \subseteq V$ is a set of *omittable* vertices such that (i) X, Y and T are all disjoint, and (ii) $\forall i \in T$ if $j \in X$ then $j < i$ and if $j \in Y$ then $j > i$.

The matchings we consider will be those that saturate all the unomittable nodes, i.e. $V - T$, and also some, possibly empty, subset of T. Whenever we refer to the Pfaffian Sum of a matchgate fragment, such as G' in the following paragraph, we shall assume the substitutions $\lambda_i = 1$ if $i \in T$, and $\lambda_i = 0$ otherwise.

We call $X \cup Y$ the *external* nodes. For $Z \subseteq X \cup Y$ we define the *character* $\chi(\Gamma, Z)$ of Γ with respect to Z to be the product

$$\mu(\Gamma, Z)\mathrm{PfS}(G'),$$

where: (a) $G' = (V - Z, E', W')$ where further E' is the restriction of E to edges with both endpoints in $V - Z$, and W' is the corresponding restriction of W, and (b) the *modifier* $\mu(\Gamma, Z) \in \{-1, 1\}$ counts the parity of the number of overlaps between matched edges in E' and matched external edges. The external edges are the edges that link each matchgate to the rest of the circuit. We consider there to exist one external edge from each node in $X \cap Z$ and from each node in $Y \cap Z$. The other endpoint of each of the former is some node of lower index than any in V, and of each of the latter is some node of index higher than any in V.

The character of a matchgate, therefore, takes into account overlaps between its internal edges and the external edges that link its external nodes to the rest of the circuit. The significance of condition (ii) in the definition of matchgates is that it guarantees that the modifier $\mu(\Gamma, Z)$ is always well defined: for any fixed Z the external edges that arise are uniquely defined, but it has to be guaranteed that the parity of the overlap of any one such external edge with *every* matching of E' that saturates all the unomittable nodes is the same. Condition (ii) achieves this by not allowing an omittable node in the gate to be numbered intermediate between the endpoints of an external edge. (That case might produce different overlap parity for the given external edge and the various internal matchings depending on whether the omittable node was in the matching.) To verify this, note that if for $i \in X \cap Z$ there are r nodes $j > i$ where $j \in V - Z$, then the parity of the overlap of the external edge from i with the internal edges is the parity of r.

We define the *character* $\chi(\Gamma)$ of Γ to be the vector of $2^{|X \cup Y|}$ values of $\chi(\Gamma, Z)$ for the various $2^{|X \cup Y|}$ possible choices of Z. Often it is useful to think of the character as a $2^{|X|} \times 2^{|Y|}$ matrix where the rows represent the subsets of the inputs X, and

the columns the subsets of the outputs Y. Matchgates with $|X|=|Y|=k$ can then be regarded as matrix transformations defined by the character matrix. For example, $k=1$ corresponds to one bit 2×2 matrix transformations and $k=2$ corresponds to two bit 4×4 transformations. In all cases, we need to specify a correspondence between subsets of X and the rows of the matrix, and another correspondence between subsets of Y and the columns of the matrix. In this paper we shall assume that this correspondence is a normal ordering, as defined below.

We say that matchgate $\Gamma=(G,X,Y,T)$ with $G=(V,E,W)$ has *normal numbering* if the numbering of V is consecutive and X,Y have minimal and maximal numbers, respectively. Formally, $V=\{1,2,\ldots,|V|\}$ and $\forall i\in X,\forall j\in Y$ and $\forall k\notin X\cup Y$ it is the case that $i<k<j$.

We say that the character matrix B of a matchgate Γ has *normal ordering* if the rows and columns are ordered in ascending and descending order, respectively, in the natural binary set ordering. Formally, if $X'\subseteq X=\{1,\ldots,k\}$ we let $\mathrm{bin}(X')$ denote the k-bit binary number whose ith bit from the left is 1 or 0 according to whether $i\in X'$. Then in a normal ordering the $(j+1)$st row denotes X' iff $j=\mathrm{bin}(X')$. For the outputs if $Y'\subseteq Y=\{n-k+1,\ldots,n\}$ where $n=|V|$, we let $\mathrm{binR}(Y')$ be the k-bit binary number whose ith bit from the left is 1 or 0 according to whether $n-i+1\in Y'$. Then in a normal ordering the $(j+1)$st column denotes Y' where $j=\mathrm{binR}(Y')$.

2.3. Control gates

A k-qubit gate over bits $\{x_1,\ldots,x_k\}$ is a *control gate* if, with x_k as the control bit, it maps any pure state $\underline{v}=\{v_1,\ldots,v_k\}\in\{0,1\}^k$ to a linear combination $\sum\alpha_i\underline{v}^{(i)}$ of pure states such that for all i where $\alpha_i\neq 0$, it is the case that the value of x_k in $\underline{v}^{(i)}$ is v_k. In other words, the value v_k of the control bit x_k is always preserved.

A control gate is *trivial* iff there is a constant c such that for all pairs $\underline{v}^+,\underline{v}^-\in\{0,1\}^k$ such that $\underline{v}^+,\underline{v}^-$ differ only in the kth bit, and there $x_k=1$ in $\underline{v}^+$ and $x_k=0$ in $\underline{v}^-$, it is the case that the pure state $\underline{v}^+$ gets mapped by the gate to c times the state to which $\underline{v}^-$ is mapped.

An example of a nontrivial control gate is the 2-qubit control-NOT gate that inverts or leaves unchanged one bit depending on whether the other (control) bit is 1 or 0 [1, 5]. Chaining together the control bits of n control-NOT gates enables one to simultaneously invert or leave unchanged n bits depending on the value of a single input.

For a control matchgate to have normal numbering we require in addition to the above that the control input be the highest numbered input, and the control output the lowest numbered output.

It should be clear that for a control matchgate with normal numbering, if B is its normally ordered character matrix and if B is

$$\begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix},$$

where $B_{11}, B_{12}, B_{21}, B_{22}$ are $2^{k-1} \times 2^{k-1}$ blocks, then $B_{12} = B_{21} = 0$. The reason is that if any entry in B_{12} or B_{21} were nonzero, then that would correspond to a $\underline{v}$ (corresponding to the row) mapping to $\underline{v}B$ that has nonzero coefficient for a column $\underline{v}'$ such that the input control variable, x_k disagrees in value from the output control variable, a situation that, by definition, is not allowed for a control gate.

We note also that a control gate so represented is trivial if B_{22} is a constant multiple of B_{11}.

3. The Grassmann–Plücker identity

For skew symmetric matrix A we define $\mathrm{Pf}_A(i_1,\ldots,i_k)$ as follows: If $i_1 < i_2 < \cdots < i_k$ then $\mathrm{Pf}_A(i_1,\ldots,i_k)$ is the Pfaffian of the $k \times k$ matrix obtained by restricting A to the rows and columns indexed by $i_1,\ldots,i_k$. The parity will vary according to the parity of the order of the indices. Hence $\mathrm{Pf}_A(i_1,i_2,\ldots,i_k) = -\mathrm{Pf}_A(i_2,i_1,\ldots,i_k)$, etc. If $i_1,\ldots,i_k$ are not distinct then $\mathrm{Pf}_A(i_1,\ldots,i_k) = 0$. In general, where the matrix A is understood we abbreviate $\mathrm{Pf}_A(i_1,\ldots,i_k)$ to $\mathrm{Pf}(i_1,\ldots,i_k)$. Also in the index list we denote by $\hat{i}$ the omission of index i. Hence, for example, $\mathrm{Pf}(3,1,2,3) = 0$, $\mathrm{Pf}(1,\ldots,\hat{3},\ldots,5) = \mathrm{Pf}(1,2,4,5)$, $\mathrm{Pf}(3,1,\ldots,\hat{2},\hat{3},\ldots,5) = -\mathrm{Pf}(1,3,4,5)$ and $\mathrm{Pf}(3,2,1,4) = -\mathrm{Pf}(1,2,3,4)$.

The Grassman–Plücker identity [4] is:

Theorem 1. *For any skew symmetric matrix A*

$$\sum_{l=1}^{L}(-1)^l Pf(j_l,i_1,\ldots,i_K).\,Pf(j_1,j_2,\ldots,j_{l-1},\hat{j}_l,j_{l+1},\ldots,j_L) + \sum_{k=1}^{K}(-1)^k Pf(i_1,\ldots,i_{k-1},\hat{i}_k,i_{k+1},\ldots,i_K).\,Pf(i_k,j_1,\ldots,j_L) = 0.$$

Proof (Murota [4]). By the definition of Pfaffian

$$\mathrm{Pf}(j_l,i_1,\ldots,i_K) = \sum_{k=1}^{K}(-1)^{k-1}.\mathrm{Pf}(j_l,i_k).\,\mathrm{Pf}(i_1,\ldots,\hat{i}_k,\ldots,i_K),$$

$$\mathrm{Pf}(i_k,j_1,\ldots,j_L) = \sum_{l=1}^{L}(-1)^{l-1}.\mathrm{Pf}(i_k,j_l).\,\mathrm{Pf}(j_1,\ldots,\hat{j}_l,\ldots,j_L).$$

Substituting these in the left-hand side of the statement of the theorem and using $\mathrm{Pf}(j_l,i_k) + \mathrm{Pf}(i_k,j_l) = 0$ gives the result. □

For $n \times n$ skew-symmetric matrix A we now define $\mathrm{Pf}_A[j_1,\ldots,j_l]$ as $\mathrm{Pf}_A(i_1,\ldots,i_{n-l})$ where $\{j_1,\ldots,j_l\} \cup \{i_1,\ldots,i_{n-l}\} = \{1,\ldots,n\}$ and $i_1 < i_2 < \cdots < i_{n-l}$. We suppress the A where this is understood.

Theorem 2. *For any skew-symmetric $n \times n$ matrix A:*

(i) if $1 \leqslant i < j < k < l \leqslant n$ then

$$\mathrm{Pf}[\ ]\mathrm{Pf}[i,j,k,l] - \mathrm{Pf}[i,j]\mathrm{Pf}[k,l] + \mathrm{Pf}[i,k]\mathrm{Pf}[j,l] - \mathrm{Pf}[i,l]\mathrm{Pf}[j,k] = 0.$$

(ii) if $1 \leqslant i < j < k < l \leqslant n$ then

$$\mathrm{Pf}[j,k,l]\mathrm{Pf}[i] - \mathrm{Pf}[i,k,l]\mathrm{Pf}[j] + \mathrm{Pf}[i,j,l]\mathrm{Pf}[k] - \mathrm{Pf}[i,j,k]\mathrm{Pf}[l] = 0.$$

(iii) if $1 \leqslant i < k < m < j \leqslant n$ and $\mathrm{Pf}[i,k] = \mathrm{Pf}[i,j] = 0$ then

$$\mathrm{Pf}[i,m]\mathrm{Pf}[k,j] + \mathrm{Pf}[\ ]\mathrm{Pf}[i,j,k,m] = 0.$$

Proof. We use the abbreviations $I = \{i_1, \ldots, i_K\}, J = \{j_1, \ldots, j_L\}$ and apply the respective substitutions given below to the Grassmann–Plücker identity, omitting terms which equal zero because their index set contains repetitions.

(i) Consider $I = \{\ldots, \hat{i}, \ldots\}$ and $J = \{\ldots, \hat{j}, \ldots, \hat{k}, \ldots, \hat{l}, \ldots\}$. In other words $|I| = n-1$ and $|J| = |n-3|$. Then Theorem 1 gives

$$\begin{aligned}
&(-1)^i \mathrm{Pf}(i, \ldots, \hat{i}, \ldots)\mathrm{Pf}(\ldots, \hat{i}, \ldots, \hat{j}, \ldots, \hat{k}, \ldots, \hat{l}, \ldots) \\
&\quad + (-1)^{j-1}\mathrm{Pf}(\ldots, \hat{i}, \ldots, \hat{j}, \ldots)\mathrm{Pf}(j, \ldots, \hat{j}, \ldots, \hat{k}, \ldots, \hat{l}, \ldots) \\
&\quad + (-1)^{k-1}\mathrm{Pf}(\ldots, \hat{i}, \ldots, \hat{k}, \ldots)\mathrm{Pf}(k, \ldots, \hat{j}, \ldots, \hat{k}, \ldots, \hat{l}, \ldots) \\
&\quad + (-1)^{l-1}\mathrm{Pf}(\ldots, \hat{i}, \ldots, \hat{l}, \ldots)\mathrm{Pf}(l, \ldots, \hat{j}, \ldots, \hat{k}, \ldots, \hat{l}, \ldots) = 0.
\end{aligned}$$

We now put into increasing order the indices of the first factor of the first term, and of the second factors of the last three terms. This will contribute a new multiplicative term of $(-1)^{i-1}, (-1)^{j-1}, (-1)^{k-2}$ and $(-1)^{l-3}$ to the four terms, respectively. The resulting signs of the four terms will be therefore $(-1)^{i+i-1} = -1, (-1)^{j-1+j-1} = 1, (-1)^{k-1+k-2} = -1$ and $(-1)^{l-1+l-3} = 1$, respectively. This gives the desired result.

(ii) Consider $I = \{\ldots\}$ and $J = \{\ldots, \hat{i}, \ldots, \hat{j}, \ldots, \hat{k}, \ldots, \hat{l}, \ldots\}$ so that $|I| = n$, and $|J| = n-4$. Then Theorem 1 gives

$$\begin{aligned}
&(-1)^i \mathrm{Pf}(\ldots, \hat{i}, \ldots,)\mathrm{Pf}(i, \ldots, \hat{i}, \ldots, \hat{j}, \ldots, \hat{k}, \ldots, \hat{l}, \ldots) \\
&\quad + (-1)^j \mathrm{Pf}(\ldots, \hat{j}, \ldots,)\mathrm{Pf}(j, \ldots, \hat{i}, \ldots, \hat{j}, \ldots, \hat{k}, \ldots, \hat{l}, \ldots) \\
&\quad + (-1)^k \mathrm{Pf}(\ldots, \hat{k}, \ldots,)\mathrm{Pf}(k, \ldots, \hat{i}, \ldots, \hat{j}, \ldots, \hat{k}, \ldots, \hat{l}, \ldots) \\
&\quad + (-1)^l \mathrm{Pf}(\ldots, \hat{l}, \ldots,)\mathrm{Pf}(l, \ldots, \hat{i}, \ldots, \hat{j}, \ldots, \hat{k}, \ldots, \hat{l}, \ldots) = 0.
\end{aligned}$$

Putting the indices in increasing order in the second factor of each of the four terms introduces multipliers of $(-1)^{i-1}, (-1)^{j-2}, (-1)^{k-3}$ and $(-1)^{l-4}$, respectively. Combining these with the multipliers of the four terms gives coefficients of $-1, 1, -1$ and 1 respectively, as needed.

(iii) Now consider $I-\{\ldots,\hat{i},\ldots\}$ and $J=\{\ldots,\hat{k},\ldots,\hat{m},\ldots,\hat{j}\ldots\}$ so that $|I|=n-1$ and $|J|=n-3$. Then Theorem 1 yields

$$\begin{aligned}&(-1)^{i}\mathrm{Pf}(i,\ldots,\hat{i},\ldots)\mathrm{Pf}(\ldots,\hat{i},\ldots,\hat{k},\ldots,\hat{m},\ldots,\hat{j},\ldots)\\&\quad+(-1)^{k-1}\mathrm{Pf}(\ldots,\hat{i},\ldots,\hat{k},\ldots)\mathrm{Pf}(k,\ldots,\hat{k},\ldots,\hat{m},\ldots,\hat{j},\ldots)\\&\quad+(-1)^{m-1}\mathrm{Pf}(\ldots,\hat{i},\ldots,\hat{m},\ldots)\mathrm{Pf}(m,\ldots,\hat{k},\ldots,\hat{m},\ldots,\hat{j},\ldots)\\&\quad+(-1)^{j-1}\mathrm{Pf}(\ldots,\hat{i},\ldots,\hat{j},\ldots)\mathrm{Pf}(j,\ldots,\hat{k},\ldots,\hat{m},\ldots,\hat{j},\ldots)=0.\end{aligned}$$

Putting into increasing order the indices of the first factor of the first term, and the second factors of the last three terms introduces new multiplicative factors of $(-1)^{i-1},(-1)^{k-1},(-1)^{m-2}$ and $(-1)^{j-3}$. Hence combining these with the existing multipliers gives coefficients of $-1,1,-1$ and 1. But the second and third terms vanish by virtue of the assumptions that $\mathrm{Pf}[i,k]=Pf[i,j]=0$.

The result follows. □

4. The matchgate identities

We shall now show that the entries of the character matrix of a 2-qubit matchgate are constrained by five polynomial relations.

Theorem 3. *If B is a normally ordered character matrix of a normally numbered 2-input 2-output matchgate then B obeys the following set of identities.*

$$\begin{aligned}&B(1,1)B(4,4)-B(2,2)B(3,3)-B(1,4)B(4,1)+B(2,3)B(3,2)=0,\\&B(2,1)B(4,4)-B(2,2)B(4,3)-B(4,1)B(2,4)+B(2,3)B(4,2)=0,\\&B(3,1)B(4,4)+B(3,3)B(4,2)-B(4,1)B(3,4)-B(3,2)B(4,3)=0,\\&B(1,3)B(4,4)+B(3,3)B(2,4)-B(1,4)B(4,3)-B(2,3)B(3,4)=0,\\&B(1,2)B(4,4)-B(2,2)B(3,4)-B(1,4)B(4,2)+B(3,2)B(2,4)=0.\end{aligned}$$

Before proceeding to the proof let us observe that it was shown in [9] that as long as $B(4,4)\neq 0$ any matchgate satisfying exactly these five identities can be realized. Hence this gives a good characterization of which character matrices are realizable.

Proof of Theorem 3. From Theorem 3 in [9] we know that any matchgate can be replaced by one with an even number of nodes and exactly one omittable node, and having the same character matrix.

We shall appeal to Theorem 2(i) and (ii) where $1\leqslant i<j<k<l\leqslant n$. Hence if the inputs are $\{i,j\}$ and the outputs $\{k,l\}$, then in a normal ordering the rows will be ordered $\{\},\{i\},\{j\},\{i,j\}$ and the columns $\{\},\{l\},\{k\},\{k,l\}$.

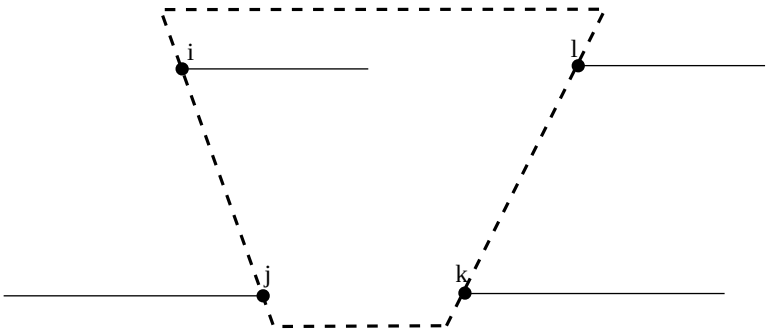

Fig. 1. Nodes $\{i,j\}$ and $\{k,l\}$ are the input and output nodes, respectively, of a matchgate. The four edges shown are the matched edges to these nodes for the $\{j\}$, $\{k,l\}$ contribution, namely $B(3,4)$, to the character matrix. Here the overlap between internal and external edges is odd, since the only such contribution is the overlap between the external edge to j and the internal edge from i.

Then Theorem 2(i) can be rewritten as

$$(\mu)B(1,1)B(4,4)-(\mu)B(4,1)B(1,4)+(\mu)B(2,3)B(3,2)-(\mu)B(2,2)B(3,3)=0,$$

where (μ) denotes the modifier contribution of the corresponding term. Fig. 1 illustrates that the contribution of the modifier for $B(3,4)$ is -1. It is easy to see that -1 contributions come also from $B(3,1), B(3,2), B(3,4), B(1,3)$, $B(2,3)$ and $B(4,3)$, and that the remaining contributions are $+1$. Hence the above rewriting of Theorem 2(i) yields $+1$ values for all four modifiers (μ), and hence is equivalent to

$$B(1,1)B(4,4)-B(4,1)B(1,4)+B(2,3)B(3,2)-B(2,2)B(3,3)=0,$$

which is exactly the first matchgate identity, as required.

The remaining four matchgate identities all derive from Theorem 2(ii). We denote the omitted node by m, so that $1\leqslant i<j<m<k<l\leqslant n$. In each of the four cases, we delete one of these five nodes from the matchgate so that the matrix size becomes odd, and apply Theorem 2(ii) to the remaining four of the indices i,j,m,k,l.

For the first of these four identities, we omit i and apply Theorem 2(ii) to $j<m<k<l$ so that effectively we substitute $i=j, j=m, k=k, l=l$, to get

$$\mathrm{Pf}_A[m,k,l]\mathrm{Pf}_A[j]-\mathrm{Pf}_A[j,k,l]\mathrm{Pf}_A[m]+\mathrm{Pf}_A[j,m,l]\mathrm{Pf}_A[k]-\mathrm{Pf}_A[j,m,k]\mathrm{Pf}_A[l]=0,$$

where $A=B[i]$. Hence, with respect to B itself this relation is

$$\begin{aligned}&\mathrm{Pf}[i,m,k,l]\mathrm{Pf}[i,j]-\mathrm{Pf}[i,j,k,l]\mathrm{Pf}[i,m]+\mathrm{Pf}[i,j,m,l]\mathrm{Pf}[i,k]\\&\quad-\mathrm{Pf}[i,j,m,k]\mathrm{Pf}[i,l]=0.\end{aligned}$$

This is equivalent to

$$(\mu)B(2,4)B(4,1)-(\mu)B(4,4)B(2,1)+(\mu)B(4,2)B(2,3)-(\mu)B(4,3)B(2,2).$$

Noting that of these factors only $B(4,3)$ and $B(2,3)$ introduce -1 modifiers gives

$$B(2,1)B(4,4) - B(2,2)B(4,3) - B(4,1)B(2,4) + B(2,3)B(4,2) = 0,$$

which is exactly as required.

For the second of the last four identities, we omit j and apply Theorem 2(ii) to $i<m<k<l$ so that effectively we substitute $i=i, j=m, k=k, l=l$ to get

$$\mathrm{Pf}_A[m,k,l]\mathrm{Pf}_A[i] - \mathrm{Pf}_A[i,k,l]\mathrm{Pf}_A[m] + \mathrm{Pf}_A[i,m,l]\mathrm{Pf}_A[k] - \mathrm{Pf}_A[i,m,k]\mathrm{Pf}_A[l] = 0$$

for $A = B[j]$. With respect to the original matrix we need to omit j:

$$\begin{aligned}&\mathrm{Pf}[j,m,k,l]\mathrm{Pf}[i,j] - \mathrm{Pf}[i,j,k,l]\mathrm{Pf}[j,m] + \mathrm{Pf}[i,j,m,l]\mathrm{Pf}[j,k]\\ &\quad - \mathrm{Pf}[i,j,m,k]\mathrm{Pf}[j,l] = 0.\end{aligned}$$

This is equivalent to

$$(\mu)B(3,4)B(4,1) - (\mu)B(4,4)B(3,1) + (\mu)B(4,2)B(3,3) - (\mu)B(4,3)B(3,2) = 0.$$

Since among these factors $B(3,4)B(3,1), B(4,3)$ and $B(3,2)$ are the ones that introduce -1 factors in the modifier, this is exactly the identity we need.

For the third of the last four identities we omit k and apply Theorem 2(ii) to $i<j<m<l$ so that effectively we substitute $i=i, j=j, k=m, l=l$ to get for the original matrix,

$$\begin{aligned}&\mathrm{Pf}[j,m,k,l]\mathrm{Pf}[i,k] - \mathrm{Pf}[i,m,k,l]\mathrm{Pf}[j,k] + \mathrm{Pf}[i,j,k,l]\mathrm{Pf}[m,k]\\ &\quad - \mathrm{Pf}[i,j,m,k]\mathrm{Pf}[k,l] = 0.\end{aligned}$$

This gives

$$(\mu)B(3,4)B(2,3) - (\mu)B(2,4)B(3,3) + (\mu)B(4,4)B(1,3) - (\mu)B(4,3)B(1,4) = 0.$$

Among the factors $B(3,4), B(2,3), B(1,3)$ and $B(4,3)$ contribute -1 to the modifier. Adjusting for these we get the required identity.

For the final identity we omit l and apply Theorem 2(ii) to $i<j<m<k$, so that effectively we substitute $i=i, j=j, k=m, l=k$. We obtain for the original matrix:

$$\begin{aligned}&\mathrm{Pf}[j,m,k,l]\mathrm{Pf}[i,l] - \mathrm{Pf}[i,m,k,l]\mathrm{Pf}[j,l] + \mathrm{Pf}[i,j,k,l]\mathrm{Pf}[m,l]\\ &\quad - \mathrm{Pf}[i,j,m,l]\mathrm{Pf}[k,l] = 0.\end{aligned}$$

This gives

$$(\mu)B(3,4)B(2,2) - (\mu)B(2,4)B(3,2) + (\mu)B(4,4)B(1,2) - (\mu)B(4,2)B(1,4) = 0.$$

Among these factors $B(3,4)$ and $B(3,2)$ contribute modifiers of -1, and this gives the last identity. □

5. Control gates

We shall show that in a normally numbered character matrix of a control gate, the top left block can differ from the bottom right block by at most a constant factor, or, in other words, the effect of the control bit is the same constant for all states of the remaining bits.

For the 2-qubit case this result follows immediately from the matchgate identities. After substitution of $B(1,3)=B(1,4)=B(2,3)=B(2,4)=B(3,1)=B(3,2)=B(4,1)=B(4,2)=0$ the first, second and fifth identity become

$$B(1,1)B(4,4) = B(2,2)B(3,3),$$
$$B(2,1)B(4,4) = B(2,2)B(4,3), \quad \text{and}$$
$$B(1,2)B(4,4) = B(2,2)B(3,4),$$

which establish the claim.

In the general k-qubit case we have the following:

Theorem 4. *If B is a normally ordered character matrix of a normally numbered k-qubit control matchgate then for some constant c for all i,j $(1\leqslant i,j\leqslant 2^{k-1})$*

$$B(i,j)=cB(N+i,N+j),$$

where $N=2^{k-1}$.

Proof. Consider elements $B(i,j)$ and $B(u,v)$ for $1\leqslant i,j,u,v\leqslant N$. Define $H(r,s)$ for $1\leqslant r,s\leqslant N$ to be the Hamming distance between the code words for $r-1,s-1$ when represented in standard binary notation. Thus, if $r\neq s, 1\leqslant H(r,s)\leqslant k-1$.

We claim that

$$\frac{B(i,j)}{B(N+i,N+j)}=\frac{B(u,v)}{B(N+u,N+v)}, \tag{5.1}$$

which is sufficient for the theorem. We shall prove this claim for the two cases: (i) $i=u$ and $H(j,v)=1$, and (ii) $j=v$ and $H(i,u)=1$. The claim for general i,j,u,v then clearly follows by induction on $H(i,u)+H(j,v)$.

Without loss of generality it is sufficient to consider case (ii). Suppose that the binary numerals for $i-1$ and $u-1$ differ in the tth bit in their standard binary representations and that the tth bit for $u-1$ is 1. We consider the four matchgate fragments with the input and output nodes corresponding to 1 digits in either $(i-1,j-1)$, or in $(u-1,v-1)$, being deleted. Further, we consider each of these two situations in the two cases that both or neither of the control nodes are deleted.

Consider the matchgate that corresponds to $(i-1,j-1)$ being omitted but the control nodes being retained. By virtue of Theorem 3 in [9] we can assume that this like any matchgate is realized by an even number of nodes, among which one is omittable and has index, say, m. Apply Theorem 2(iii) for $t<k<m<n-k+1$, where

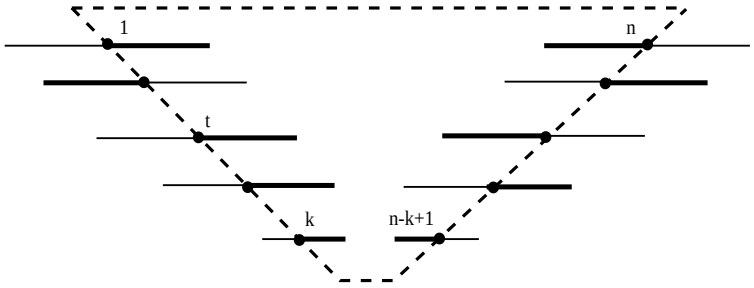

Fig. 2. Illustration of the parity differences analysed in the proof of Theorem 4. Nodes $\{1,\ldots,k\}$ are the input nodes of the matchgate and nodes $\{n-k+1,\ldots,n\}$ the outputs. Nodes k and $n-k+1$ correspond to the control bit. The bold lines show matched edges. In this instances, for the (i,j) case with control equal to zero, seven external nodes are matched internally and the rest externally. If the control bits were set to 1 then the number of internally matched edges would decrease by 2. The (u,v) case would differ only in that node t would be matched externally.

$\mathrm{Pf}[t,n-k+1]=\mathrm{Pf}[m,n-k+1]=\mathrm{Pf}[k,m]=\mathrm{Pf}[t,k]=0$ since the original gate was a control gate and these Pfaffians each correspond to the input control bit k having a different value from the output control bit $n-k+1$. The result is

$$\mathrm{Pf}[k,n-k+1]\mathrm{Pf}[t,m]=-\mathrm{Pf}[\ ]\mathrm{Pf}[t,k,m,n-k+1].$$

The four factors in this expression equal, respectively,

$$B(N+i,N+j),B(u,v),B(i,j),B(N+u,N+v).$$

To establish claim (5.1) it remains to verify that an odd number of these four factors are associated with a modifier of (-1).

To see this, note that the number of internal connections to external nodes for $\mathrm{Pf}[\ ]$ and for $\mathrm{Pf}[k,n-k+1]$ have the same parity, but they are of opposite parity to the number of such internal connections for $\mathrm{Pf}[t,m]$ and for $\mathrm{Pf}[t,k,m,n-k+1]$. In the example shown in Fig. 2 the four values are 7,5,6 and 4 respectively. We need to examine the overlaps of these internally matched edges with the externally matched edges in each of the four cases. Now within each of the two pairs $Pf[],Pf[k,n-k+1]$ and $Pf[t,m],Pf[t,k,m,n-k+1]$ the only differences in overlaps are those occurring between the external edges at k and $n-k+1$, on the one hand, and the internal edges at the remaining input/output nodes, on the other. Hence for the pair for which the number of such internal edges is even, the modifiers are the same, but for the other pair the modifiers are different. The result follows. □

6. Expressing Boolean formulae as matchgates

It is an open problem as to whether classical Boolean circuits can be simulated by matchcircuits of polynomial size. As observed in [9] not all the classical Boolean

functions over two variables have matchgates under the direct encoding. What we shall show is that there is nevertheless a simulation of classical circuits as long as these are restricted to have a tree geometry, or, in other words, the circuits are formulae, or, equivalently, have logarithmic depth. The simulation is by matchcircuits with 2-input 2-output gates, but has the property that the input values of the formula are mapped to the internal structure rather than to the input values of the matchcircuits.

Theorem 5. *There is a deterministic polynomial time mapping g from descriptions of Boolean formulae F and input vectors $\underline{x}$ for them, to matchcircuits M composed of 2-input 2-output gates and having integer weights, such that*

$$F(\underline{x}) = 1 \text{ if and only if } \mathrm{PfS}(M) \neq 0.$$

Proof. We shall compose three mappings to obtain g. The first will map a Boolean formula F over $\{x_1,\ldots,x_n\}$ to a directed acyclic graph $G=(V,E)$ with two distinguished vertices $s,t\in V$ and with the edges labelled by $\{0,1,x,\bar{x}_1,\ldots,x_n,\bar{x}_n\}$ such that for any $\underline{x}\in\{0,1\}^n, F(\underline{x})=1$ if and only if there is a directed path in G from s to t that has nonzero weight when the actual values of $\underline{x}$ are substituted for the edge labels. Further, this map is such that each value of $\underline{x}$ such that $F(\underline{x})=1$ will induce exactly one such directed path from s to t. Graph G is obtained by considering the evaluation of formula F using up to $p=\log|F|$ pebbles or registers according to any fixed pebbling strategy (e.g [6]). The $2^{p+1}|F|$ nodes of G will represent the 2^{p+1} possible register values at each of the $|F|$ points in the evaluation. The edges represent a legal step in the evaluation. The nodes s,t will correspond respectively to the initial configuration in the pebbling strategy, and the final configuration with a pebble only on the output node, and that pebble having value one.

The second mapping will map $\{G=(V,E),s,t\}$ to a bipartite graph $G^*(V^*,E^*)$ such that G^* has exactly as many perfect matchings as there are directed paths from s to t in G. The mapping (see [8]) maps $V=\{1,\ldots,n\}$ to $V^*=\{1,\ldots,2n\}$. For each $(i,j)\in E$ there is an edge $(i,n+j)$ in G^* with the same label. In E^* there is an edge $(t,n+s)$ labelled 1 where $s,t\in V$ are the source and target of the directed path in G, and an edge $(i,n+i)$ labelled 1 for every $i\in\{1,\ldots,n\}-\{s,t\}$.

For a formula F, we finally construct the associated matchcircuit as follows: If $G^*(F)$ has nodes $X\cup Y$ and edges $E\subseteq X\times Y$ then the matchcircuit works on $|X\cup Y|$ bits labelled by the nodes of $X\cup Y$. For each edge in $G^*(F)$ between nodes i,j in $G^*(F)$ will label x we place a 2-input 2-output matchgate with character matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ x & 0 & 0 & 1 \end{pmatrix}$$

to link the bits representing i and j. Note that such a matchgate is realizable since the matrix satisfies the matchgate identities and has a nonzero (4,4) entry. In particular Proposition 3 in [9] gives a construction for it.

The intention is that all the inputs of the matchcircuit are given value 1. The values of the two input bits to any gate either pass through the gate unchanged, or if they both have value 1 they can be both "switched off" to output value 0, by virtue of the x entry in position (4,1). Hence, the outputs of the circuit can all simultaneously acquire value 0 if and only if there is a perfect matching in $G^*(F)$.

Hence, if in the matchcircuit described the x entries take the appropriate $\{0,1\}$ values, whether constant or as imposed by the input vector $\underline{x}$ of the formula F, and if all the inputs are set to 1 and all the outputs set to zero, then the Pfaffian of the resulting matchcircuit will be nonzero if and only if the value of $F(\underline{x})$ is 1. This follows immediately from the Matchcircuit Theorem [9] since each perfect matching in G^* corresponds to a distinct set $S=\{S_1,\ldots,S_m\}$ of node sets of the m matchgates that are matched by external edges. Hence that theorem implies that if G^* has no perfect matching then $\mathrm{PfS}=0$ and if it has one such matching then $\mathrm{PfS}=\varepsilon_S\in\{-1,1\}$ for some S. □

Corollary 1. *The theorem holds for DSPACE*$(\log(n))$ *in place of Boolean formulae F, and, if the reduction g is allowed to be randomized, also for NSPACE*$(\log(n))$.

Proof. Computations in *NSPACE*$(\log(n))$ for a fixed input length n can be mapped to a directed acyclic graph G in which the edges are labeled by $\{0,1,x_1,\bar{x}_1,\ldots,x_n,\bar{x}_n\}$, and in which computations are in one to one correspondence with paths from distinguished node s to distinguished node t. In turn G will be mapped to G^* with the edges similarly labeled. Now by the Matchcircuit Theorem in [9] each perfect matching in G^* will contribute the product of the weights of the corresponding G^* edges, but with a 1 or -1 multiplier depending on the sign of the matching.

If the computation is from *DSPACE*$(\log(n))$ then there is just one perfect matching and the result follows. Otherwise we shall choose different new variables to correspond to each occurrence of x_i or $\bar{x}_i$ having a positive value. Since PfS is a polynomial of polynomial degree in terms of these new variables, a random choice of integer substitutions from a fixed range of $\mathrm{O}(\log n)$ bit integers will make PfS nonzero with high probability, as required. □

Acknowledgements

I thank Rocco Servedio for his helpful comments on this paper.

References

[1] A. Barenco, et al., Elementary gates for quantum computation, Phys. Rev. A 52 (5) (1995) 3457–3467.
[2] R.A. Brualdi, H.J. Ryser, Combinatorial Matrix Theory, Cambridge University Press, Cambridge, 1991.
[3] D. Deutsch, Quantum computational networks, Proc. R. Soc. Lond. A 425 (1989) 73–90.
[4] K. Murota, Matrices and Matroids for Systems Analysis, Springer, Berlin, 2000.

[5] M.A. Nielsen, I.L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, Cambridge, 2000.
[6] J.E. Savage, Models of Computation, Addison-Wesley, Reading, MA, 1998.
[7] P.W. Shor, Algorithms for quantum computation: discrete logarithms and factoring, SIAM J. Comput. 26 (5) (1997) 1489–1509.
[8] S. Skyum, L.G. Valiant, A complexity theory based on boolean algebra, J. ACM 32 (2) (1985) 484–502.
[9] L.G. Valiant, Quantum circuits that can be simulated classically in polynomial time, SIAM J. Computing, to appear; Extended abstract in Proc. 33rd ACM Symp. on Theory of Computing, ACM Press, New York, 2001 pp. 114–123.