# Jordan-Wigner formalism for arbitrary 2-input 2-output matchgates and their classical simulation

Richard Jozsa[1], Akimasa Miyake[2] and Sergii Strelchuk[1]

[1] *DAMTP, Centre for Mathematical Sciences, University of Cambridge, Wilberforce Road, Cambridge CB3 0WA, U.K.*

[2] *Center for Quantum Information and Control, Department of Physics and Astronomy, University of New Mexico, 1919 Lomas Blvd NE, Albuquerque NM 87131, USA.*

**Abstract**

In Valiant's matchgate theory, 2-input 2-output matchgates are $4 \times 4$ matrices that satisfy ten so-called matchgate identities. We prove that the set of all such matchgates (including non-unitary and non-invertible ones) coincides with the topological closure of the set of all matrices obtained as exponentials of linear combinations of the 2-qubit Jordan-Wigner (JW) operators and their quadratic products, extending a previous result of Knill. In Valiant's theory, outputs of matchgate circuits can be classically computed in poly-time. Via the JW formalism, Terhal & DiVincenzo and Knill established a relation of a unitary class of these circuits to the efficient simulation of non-interacting fermions. We describe how the JW formalism may be used to give an efficient simulation for all cases in Valiant's simulation theorem, which in particular includes the case of non-interacting fermions generalised to allow arbitrary 1-qubit gates on the first line at any stage in the circuit. Finally we give an exposition of how these simulation results can be alternatively understood from some basic Lie algebra theory, in terms of a formalism introduced by Somma et al.

## 1 Introduction

The theory of matchgate computations was introduced by Valiant in [1] and used to provide a striking new class of efficient (i.e. poly-time) classical algorithms for a variety of computational tasks [2]. General matchgates can have $k$ inputs and $l$ outputs, being then represented by matrices of size $2^k \times 2^l$. Here we will be concerned only with 2-input 2-output matchgates and hereafter the term 'matchgate' will always mean '2-input 2-output matchgate'.

In some cases, matchgates can be unitary and Valiant also identified a corresponding novel class of classically efficiently simulatable quantum circuits [1]. Soon thereafter Terhal & DiVincenzo [3] and Knill [4] showed that there is a connection between a class of Valiant's unitary matchgate circuits and the physics of non-interacting fermions (and see [6] for a further exposition). The evolution of non-interacting fermions can be classically efficiently simulated [5, 3] by using the formalism of Jordan-Wigner (JW) operators [8] (that gives

a representation of fermionic modes in terms of standard qubits), and this provided a quantum physical interpretation of part of Valiant's results. In this paper we will further extend and study the relationship between Valiant's matchgate theory and the Jordan-Wigner formalism of quantum physics.

Our results are organised as follows. In Section 2 and the Appendix we will prove an equivalence between arbitrary 2-input 2-output matchgates (including non-unitary and non-invertible ones) and the JW formalism for two qubit lines, viz. the set of all such matchgates will be seen to coincide with the topological closure of the set of all matrices obtained as exponentials of linear combinations of the 2-qubit Jordan-Wigner (JW) operators and their quadratic products, extending a previous result of Knill [4]. Then in Section 3 we will see that the classical simulation of all cases of matchgate circuits in Valiant's simulation theorem [1], can be carried out using the Jordan-Wigner formalism. Finally in Section 4 we will give an exposition of how all these simulation results can also be alternatively understood using some basic Lie algebra theory, as an example of a more abstract formalism introduced by Somma et al. [7].

In fermionic physics it is usual to impose conservation of the parity of the number of fermions (the boson-fermion superselection rule). In the JW formalism this corresponds to considering quantum processes whose hamiltonians involve only even degree products of the JW operators, and the case of so-called non-interacting fermions corresponds to allowing only purely quadratic terms. It may be shown [3] [6] that in the matchgate formalism, the latter case is equivalent to considering poly-sized circuits of unitary 2-qubit matchgates of the following form, each acting on two nearest-neighbour (n.n.) qubit lines:

$$G(V,W) = \begin{pmatrix} p & 0 & 0 & q \\ 0 & w & x & 0 \\ 0 & y & z & 0 \\ r & 0 & 0 & s \end{pmatrix} \qquad V = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \quad W = \begin{pmatrix} w & x \\ y & z \end{pmatrix}. \tag{1}$$

Here $V$ and $W$ are both in $SU(2)$ or both in $U(2)$ with the same determinant and "n.n." is with respect to any fixed chosen linear ordering of the qubit lines. We will refer to gates of this form acting on n.n. qubits as *fermionic* matchgates. However Valiant's matchgate formalism includes further unitary circuits that do not respect the boson-fermion superselection rule; an interesting example is the following: we can have circuits of fermionic matchgates together with arbitrary 1-qubit gates applied on the *first* qubit line at any stage within the circuit. We will see (as also outlined in [4], and in accordance with our general JW-matchgate equivalence), that they may be represented in terms of hamiltonians that have *linear* as well as quadratic JW terms. Furthermore these seemingly more general hamiltonians can in fact be seen as special cases of purely quadratic ones in a slightly enlarged setting.

## 2 General matchgates and the JW formalism

In this section we will be concerned with just two qubit lines and $4 \times 4$ matrices. We will label rows and columns of $4 \times 4$ matrices $B$ by 1, 2, 3, 4 which will correspond respectively to 00, 01, 10, 11 when $B$ is viewed as operating on the space of two qubits.

The Jordan-Wigner operators for $n$ qubit lines are defined in eq. (5) below and for two qubit lines we have simply

$$c_1 = XI \quad c_2 = YI \quad c_3 = ZX \quad c_4 = ZY \tag{2}$$

where $I$ is the identity and $X, Y, Z$ are the standard Pauli matrices, and we have omitted all tensor product symbols (so e.g. $XI$ is shorthand for $X \otimes I$).

For matchgates, it was shown in [9] that a $4\times4$ matrix $B$ is a 2-input 2-output matchgate if and only if it satisfies the following ten *matchgate identities*:

$$\begin{aligned}
M_1 &= B_{11}B_{44} - B_{14}B_{41} - B_{22}B_{33} + B_{23}B_{32} = 0\\
M_2 &= B_{21}B_{44} - B_{22}B_{43} + B_{23}B_{42} - B_{24}B_{41} = 0\\
M_3 &= B_{31}B_{44} - B_{32}B_{43} + B_{33}B_{42} - B_{34}B_{41} = 0\\
M_4 &= B_{13}B_{44} - B_{14}B_{43} - B_{23}B_{34} + B_{24}B_{33} = 0\\
M_5 &= B_{12}B_{44} - B_{14}B_{42} - B_{22}B_{34} + B_{24}B_{32} = 0\\
M_6 &= B_{11}B_{24} - B_{12}B_{23} + B_{13}B_{22} - B_{14}B_{21} = 0\\
M_7 &= B_{11}B_{42} - B_{12}B_{41} - B_{21}B_{32} + B_{22}B_{31} = 0\\
M_8 &= B_{12}B_{43} - B_{13}B_{42} - B_{21}B_{34} + B_{24}B_{31} = 0\\
M_9 &= B_{11}B_{34} - B_{12}B_{33} + B_{13}B_{32} - B_{14}B_{31} = 0\\
M_{10} &= B_{11}B_{43} - B_{13}B_{41} - B_{21}B_{33} + B_{23}B_{31} = 0
\end{aligned}$$

Let $\mathcal{MG}$ be the set of all 2-input 2-output matchgates, which is thus a closed set in the space of all $4 \times 4$ complex matrices.

We will prove a correspondence between $\mathcal{MG}$ and $4\times4$ matrices obtained as exponentials $e^A$ of linear combinations of the $c_i$'s and quadratic terms $c_ic_j$'s i.e. $A = \sum \alpha_i c_i + \sum \beta_{ij} c_i c_j$ with $\alpha_i, \beta_{ij} \in \mathbb{C}$. However to obtain the matchgate identities as written above we will need to reverse the order of the tensor product in the JW operators and use

$$\tilde{c}_1 = IX \quad \tilde{c}_2 = IY \quad \tilde{c}_3 = XZ \quad \tilde{c}_4 = YZ. \tag{3}$$

If we were to proceed instead with the JW operators directly (e.g. as was done in [4] for a setting of five matchgate identities) we would obtain matrices $e^A$ that do not satisfy the identities above, but instead satisfy a set of identities obtained by changing row and column labels via $1,2,3,4 \to 1,3,2,4$ or $00,01,10,11 \to 00,10,01,11$ corresponding to reversing the role of the two qubits. For example instead of $M_2 = 0$ above we would obtain $B_{31}B_{44} - B_{33}B_{42} + B_{32}B_{43} - B_{34}B_{41} = 0$ (viz. eq. (3) in [4]).

Thus introduce the eleven linear and quadratic reversed JW operators (up to overall constants and writing $\tilde{c}_0$ for $\tilde{c}_i\tilde{c}_j$ with $i = j$):

$$\begin{array}{llllll}
\tilde{c}_0 = II & & & & & \\
\tilde{c}_1 = IX & \tilde{c}_2 = IY & \tilde{c}_3 = XZ & \tilde{c}_4 = YZ & & \\
\tilde{c}_1\tilde{c}_2 = IZ & \tilde{c}_1\tilde{c}_3 = XY & \tilde{c}_1\tilde{c}_4 = YY & \tilde{c}_2\tilde{c}_3 = XX & \tilde{c}_2\tilde{c}_4 = YX & \tilde{c}_3\tilde{c}_4 = ZI
\end{array} \tag{4}$$

Let $\mathcal{L}$ be the (complex) linear span of these eleven $4\times4$ matrices, which is an 11-dimensional Lie algebra (with the standard matrix product commutator as Lie bracket).
Let $\mathcal{G} = \{e^A : A \in \mathcal{L}\}$ be the corresponding Lie group. Note that by definition, all elements

of $\mathcal{G}$ are invertible matrices but $\mathcal{G}$ is not topologically closed; for example $\lim_{t\to\infty} e^{t(IZ-II)} = \lim_{t\to\infty} e^{t(IZ)}/e^t = I\otimes|0\rangle\langle 0| \notin \mathcal{G}$, or even more simply $\lim_{t\to\infty} e^{A-tII} = \lim_{t\to\infty} e^A/e^t$ which is the zero matrix.

Let $\mathcal{MG}^* = \{B \in \mathcal{MG} : B \text{ is invertible}\}$. Then we have:

**Theorem 1. (a)** *$\mathcal{MG}^*$ is dense in $\mathcal{MG}$;* **(b)** *$\mathcal{MG}^* = \mathcal{G}$.*
*Thus $\mathcal{MG} = \overline{\mathcal{G}}$ (where the overline denotes topological closure).*

In the Appendix we give a full proof of this Theorem, utilising and extending some methods introduced in [4]. The argument contains some further results of possible independent interest e.g. a geometrical interpretation of the matchgate identities, given in Theorem 6 in the Appendix.

# 3 Classical simulation of matchgate circuits

We now introduce the full Jordan-Wigner formalism and describe how it may be used to provide an efficient classical simulation of the matchgate circuits treated in [1].

The Jordan-Wigner operators for $n$ qubit lines are the $2n$ Pauli product operators (omitting tensor product symbols $\otimes$ throughout):

$$\begin{array}{llll} c_1 = X\,I\ldots I & c_3 = Z\,X\,I\ldots I & c_{2k-1} = Z\ldots Z\,X\,I\ldots I & \text{etc.} \\ c_2 = Y\,I\ldots I & c_4 = Z\,Y\,I\ldots I & c_{2k} = Z\ldots Z\,Y\,I\ldots I & \text{etc.} \end{array} \tag{5}$$

Here $k$ ranges from 1 to $n$, and the Pauli $X$ and $Y$ operators are in the $k^{\text{th}}$ slot for $c_{2k-1}$ and $c_{2k}$. We say that the operators $c_{2k-1}$ and $c_{2k}$ are associated to the $k^{\text{th}}$ qubit line. These $n$-qubit operators are Hermitian and satisfy the Clifford algebra anti-commutation relations:

$$\{c_\mu, c_\nu\} \equiv c_\mu c_\nu + c_\nu c_\mu = 2\delta_{\mu\nu} I \quad \mu,\nu = 1,\ldots,2n. \tag{6}$$

We begin by establishing some algebraic properties of Clifford algebras and later we will apply these to the representation provided by the JW operators.

## 3.1 Quadratic and linear terms in a Clifford algebra

Let $c_\mu$, $\mu = 1,\ldots,m$ be any $m$ symbols (now abstract Clifford algebra generators rather than the JW representation above) that satisfy the Clifford algebra anti-commutation relations $\{c_\mu, c_\nu\} \equiv c_\mu c_\nu + c_\nu c_\mu = 2\delta_{\mu\nu} I \quad \mu,\nu = 1,\ldots,m$.

Let $\mathcal{L}_1$ denote the complex linear span of the $c_\mu$'s and let $\mathcal{L}_2$ be the complex linear span of all purely quadratic terms $c_\mu c_\nu$. Let $\mathcal{L}_{1\oplus 2} = \mathcal{L}_1 \oplus \mathcal{L}_2$ be the linear span of all linear and quadratic terms. Note that from the Clifford algebra anti-commutation relations, $\mathcal{L}_1$, $\mathcal{L}_2$ and $\mathcal{L}_{1\oplus 2}$ respectively have dimensions $m$, $\binom{m}{2}+1$ and $\binom{m}{2}+m+1$.

**Theorem 2.** *Let $T = e^A$ for $A = \sum_{\mu,\nu} a_{\mu\nu}\, c_\mu c_\nu \in \mathcal{L}_2$ be the exponential of any purely quadratic expression in the $c_\mu$'s. Then $\mathcal{L}_1$ is preserved under conjugation by $T$.*

**Proof** The terms in $A$ with $\mu = \nu$ contribute only an overall scalar multiple for $T$, giving a trivial conjugation action on $\mathcal{L}_1$. Thus (recalling also that $c_\mu c_\nu = -c_\nu c_\mu$) we may assume

without loss of generality that $a_{\mu\nu}$ is anti-symmetric. For that case, a simple proof of the Theorem is given in [6] (theorem 4.1 there) for the case of $m$ even and $a_{\mu\nu}$ being real and anti-symmetric (guaranteeing there that $A$ is hermitian for hermitian $c_\mu$'s). But it is easy to see that the proof extends without change to the general case of arbitrary anti-symmetric complex $a_{\mu\nu}$'s. For each $c_\mu$ we get $Tc_\mu T^{-1} = \sum_\nu K_{\mu\nu}\, c_\nu$ with $[K_{\mu\nu}] = \exp(-4[a_{\mu\nu}])$, where square brackets denote matrices with the given entries. □

**Remark 1.** Note that Theorem 2 also implies the preservation of $\mathcal{L}_2$ since $TMNT^{-1} = (TMT^{-1})(TNT^{-1})$ for any $M, N \in \mathcal{L}_1$ □.

Below we will be interested in extending the exponent to include linear terms:

$$A = \sum_{\mu,\nu} a_{\mu\nu}\, c_\mu c_\nu + \sum_\sigma b_\sigma c_\sigma \quad \in \mathcal{L}_{1\oplus 2}.$$

But neither $\mathcal{L}_1$ nor $\mathcal{L}_2$ is closed under conjugation by these extended $e^A$'s. However we can view any such extended exponent as a *purely quadratic* expression with one extra generator:

**Theorem 3.** *Let $c_\mu$ for $\mu = 1, \ldots, m$ be as above and let $c_0$ be a further symbol satisfying*

$$\{c_0, c_\mu\} = 2\delta_{0\mu} I \quad \text{for } \mu = 0, 1, \ldots, m$$

*extending the set of c's to $m+1$ generators. Introduce*

$$d_0 = c_0 \text{ and } \quad d_\mu = ic_\mu c_0 \text{ for } \mu = 1, \ldots, m.$$

*(The optional factor i here is just to have all d's hermitian if the c's were.) Then*
*(a) $\{d_\mu, d_\nu\} = 2\delta_{\mu\nu} I \quad \mu, \nu = 0, 1, \ldots, m.$*
*(b) A general purely quadratic expression in the $d_\mu$'s for $\mu = 0, 1, \ldots, m$*

$$\tilde{A} = \sum_{\mu,\nu=0}^{m} \tilde{a}_{\mu\nu} d_\mu d_\nu \in \mathcal{L}_2(d'\text{s}) \tag{7}$$

*is the same as a general quadratic* plus linear *expression in the $c_\mu$'s for $\mu = 1, \ldots, m$*

$$A = \sum_{\mu,\nu=1}^{m} a_{\mu\nu}\, c_\mu c_\nu + \sum_{\sigma=1}^{m} b_\sigma c_\sigma \quad \in \mathcal{L}_{1\oplus 2}(c'\text{s}). \tag{8}$$

*In fact $a_{\mu\nu} = \tilde{a}_{\mu\nu}$ for $\mu, \nu = 1, \ldots, m$ and $b_\sigma = i(\tilde{a}_{\sigma 0} - \tilde{a}_{0\sigma})$.*

**Proof** (a) follows immediately from the anti-commutation relations of the $c$'s and the definition of the $d$'s in terms of the $c$'s. For (b) we note that if $\mu, \nu \neq 0$ then $d_\mu d_\nu = -c_\mu c_0 c_\nu c_0 = c_\mu c_0 c_0 c_\nu = c_\mu c_\nu$ and $d_\mu d_0 = ic_\mu c_0 c_0 = ic_\mu$. Inserting these into eq. (7) gives eq. (8) with the claimed relations between the coefficients. □

Theorem 3 with Remark 1 immediately gives:

**Corollary 1.** *$\mathcal{L}_{1\oplus 2}$ is closed under conjugation by $e^A$ for any $A \in \mathcal{L}_{1\oplus 2}$.*

In Section 4 below we will see an alternative demonstration of this fact, using properties of Lie algebras.

### 3.2 Review of classical simulation of fermionic matchgate circuits

Now set $m = 2n$ and let $c_\mu$ for $\mu = 1, \ldots, 2n$ be the JW hermitian operators on $n$ qubits.

**Theorem 4.** *Consider any purely quadratic hermitian expression (hamiltonian)*

$$H = i \sum_{\mu,\nu=1}^{2n} h_{\mu\nu} c_\mu c_\nu \quad \textit{with } h_{\mu\nu} \textit{ real and anti-symmetric.}$$

*Then $U = e^{iH}$ is unitary and*
*(a) all fermionic matchgates $G(V, W)$ (acting on any pair of n.n. lines) with $\det V = \det W = 1$ arise in this way. For qubit lines $k, k+1$ we use only the corresponding four $c_\mu$'s, having $\mu = 2k-1, 2k, 2k+1, 2k+2$.*
*(b) any such $U = e^{iH}$ is expressible as a circuit of 2-qubit fermionic matchgates, of circuit size $O(n^3)$.*

The proof of this Theorem is given in section 5 of [6]. Note that in Theorem 4(a) the case of fermionic matchgates eq. (1) with $\det V = \det W \neq 1$ can be readily included by allowing $H$ to also contain quadratic terms $c_\mu c_\nu$ with $\mu = \nu$, thus allowing the identity $II$ on the two qubit lines as a further term in $H$.

Now let $\mathcal{C}$ be any (poly-sized) circuit of 2-qubit fermionic matchgates, with input a *product* state $|\psi_0\rangle$ and output being a final $Z$-measurement on a line $k$, and with no intermediate measurements allowed. If $p_0, p_1$ are the output probabilities then

$$p_0 - p_1 = \langle Z_k \rangle = \langle \psi_0 | \, \mathcal{C}^\dagger Z_k \mathcal{C} \, | \psi_0 \rangle$$

where $Z_k$ is $Z$ on the $k^{\text{th}}$ line and its expectation value $\langle Z_k \rangle$ is taken in the final state $\mathcal{C} \, |\psi_0\rangle$. Now $Z_k = -ic_{2k-1}c_{2k}$ and by Theorem 2 (or rather Remark 1) the linear span of pure quadratic terms in the $c$'s is preserved under conjugation by $\mathcal{C}$. Thus successively conjugating by the 2-qubit gates of $\mathcal{C}$ (taken in reverse order) we finally arrive at

$$\mathcal{C}^\dagger Z_k \mathcal{C} = \sum_{\mu,\nu=1}^{2n} \alpha_{\mu\nu} c_\mu c_\nu \tag{9}$$

where the coefficients $\alpha_{\mu\nu}$ can be computed in poly$(n)$ time via successive $2n \times 2n$ matrix multiplications, effecting the conjugation action of the sequence of 2-qubit gates. Then noting that the sum in eq. (9) has only $O(n^2)$ terms and that the $c_\mu c_\nu$'s are product operators, and $|\psi_0\rangle$ is a product state, we see that we can compute $p_0 - p_1$ in poly$(n)$ time, giving the efficient classical simulation.

### 3.3 Inclusion of 1-qubit gates on the first line (and more)

Consider now allowing also *linear* terms in the hamiltonian

$$\tilde{H} = i \sum_{\mu,\nu=1}^{2n} h_{\mu\nu} c_\mu c_\nu + \sum_{\sigma=1}^{2n} k_\sigma c_\sigma$$

with $k_\sigma$ also real to keep $H$ hermitian. Note that the $e^{i\tilde{H}}$'s include all previous 2-qubit fermionic matchgates as well as further gates which in fact include arbitrary 1-qubit gates $U_1$ on the first qubit line. To see this, recall that the Pauli operators for line 1 are given by

$$X_1 = c_1 \quad Y_1 = c_2 \quad Z_1 = -ic_1c_2$$

so any $U_1 = e^{i(\alpha X_1 + \beta Y_1 + \gamma Z_1)}$ is now included. There are still further gates involving linear terms in the $c_\sigma$'s with $\sigma > 2$ which generally act across all the first $k$ lines when $\sigma = 2k-1, 2k$ are used.

One way to perform the efficient simulation of these more general circuits is to use the construction in Theorem 3 to reduce the problem to the case of a purely quadratic hamiltonian and then carry out the classical simulation exactly as in Section 3.2. We can explicitly construct the extra $c_0$ operator by introducing an extra fermionic mode (qubit line) labelled $n+1$ to the right of the existing lines viz. $1, 2 \ldots, n, n+1$, and set $c_0 = Z \ldots ZX$ where $X$ acts on line $n+1$ and there are $n$ $Z$'s i.e. $c_0$ is just the first JW operator for the new fermionic mode. The previous $2n$ JW operators are all extended by the identity on the new line to recognise the new mode. Thus it is immediate that this $c_0$ satisfies the required anti-commutation relations with $c_\mu$, $\mu = 1, \ldots, 2n$. Alternatively we can obtain the extra generator working just within $n$ qubit lines by setting $c_0 = Z \ldots Z = (-i)^n c_1 c_2 \ldots c_{2n-1} c_{2n}$, which is easily checked to have the required anti-commutation relations. With either choice of $c_0$ we then construct $d_\mu$ for $\mu = 0, 1, \ldots, n$ as in Theorem 3 and as they are still all product operators, we can apply the method of Section 3.2 to achieve the efficient simulation.

The efficient simulation of our more general circuits may also be seen even without introducing the extra operator $c_0$, by using Corollary 1 directly – we just apply the method of Section 3.2 to $\mathcal{L}_{1\oplus 2}$ replacing $\mathcal{L}_2$, noting that $\mathcal{L}_{1\oplus 2}$, like $\mathcal{L}_2$, has a basis of product operators (viz. the JW $c_\mu$'s and $c_\mu c_\nu$'s) and it is also of polynomial dimension $O(n^2)$.

**Remark 2.** Note that this classical simulation method does not depend on $\tilde{H}$ being hermitian and $e^{i\tilde{H}}$ being unitary. Indeed we can replace $\tilde{H}$ by any general complex linear combination $A$ as in eq. (8) and efficiently compute the quantity $p_0 - p_1$ for the corresponding, now non-unitary, circuit of gates $e^A$. In this setting, general purely quadratic exponents for n.n. lines (cf. Theorem 4(a)) will give gates of the form $G(V, W)$ as in eq. (1) with $V$ and $W$ now being arbitrary invertible $2 \times 2$ matrices satisfying $\det V = \det W$. □

The fact that $\mathcal{L}_{1\oplus 2}$ is preserved under conjugation by 1-qubit gates acting on the first line (which provides the key extension beyond the purely non-interacting fermion case) may also be seen by elementary means: any 1-qubit gate can be written as a sequence of products of phase gates $P_\alpha = \mathrm{diag}(1 \;\; e^{i\alpha})$ and Hadamard gates $H$. Now $P_\alpha \otimes I$ is easily verified to be a fermionic 2-qubit matchgate so we need only consider $H$ on line 1. But $H$ has a very simple conjugation action on the Pauli operators $X, Y$ and $Z$ so its conjugation action on the JW $c_\mu$'s and $c_\mu c_\nu$'s (which are all Pauli products) is very easily computed directly to confirm preservation of $\mathcal{L}_{1\oplus 2}$.

### 3.4 JW formalism for Valiant's simulation theorem

In this section we show that the simulation above for circuits of exponentials of elements from $\mathcal{L}_{1\oplus 2}$, includes all of the invertible matchgate cases given in the Main Theorem of [1]

(ibid. page 1245) i.e. circuits comprising the following kinds of gates:
(a) any diagonal 2-qubit matchgate (acting on any pair of qubit lines);
(b) any matchgate $B$ acting on n.n. lines, with $B$ having non-zero entries only in the positions $B_{11}$, $B_{22}$, $B_{33}$, $B_{44}$, $B_{14}$, $B_{41}$, $B_{23}$ and $B_{32}$ (i.e. as in the structure of our fermionic matchgates);
(c) any 2-qubit matchgate acting on the first two lines.

According to Theorem 1, any invertible 4x4 matchgate is the exponential of a linear combination of $c_\mu$'s and $c_\mu c_\nu$'s, with $\mu, \nu = 1, 2, 3, 4$ corresponding to the JW operators for two qubit lines. Viewing these two lines as the first two of $n$ lines, we immediately have (c).

For (a) we note that the matchgate identities imply that $B$ is a diagonal matchgate iff $B_{11}B_{44} = B_{22}B_{33}$ so $B$ is the exponential of a linear combination of the commuting matrices $ZI$, $IZ$ and $II$. If the gate acts on lines $k$ and $l$ (with $k < l$) then, noting that $Z_k I_l = c_{2k-1}c_{2k}$, $I_k Z_l = c_{2l-1}c_{2l}$ and $I_k I_l = c_{2k}c_{2k}$ (where $Z_k$ denotes $Z$ acting on the $k^{\text{th}}$ line and identity on all other lines etc.), we see that $B$ is the exponential of an element of $\mathcal{L}_{1\oplus 2}$.

Finally for (b), the matchgate identities imply that any matchgate $B$ satisfying the given non-zero entry conditions, has the form $G(V, W)$ with $\det V = \det W$. Then Theorem 4(a) (or more generally its non-unitary extension given in Remark 2) implies that all such gates are again exponentials of elements of $\mathcal{L}_{1\oplus 2}$, which completes all the cases.

## 4 A Lie algebra perspective

The existence of all of the above efficient classical simulations can also be seen, perhaps even more simply, from some basic Lie algebra theory, as an application of the formalism introduced in [7]. Here we will give an elementary exposition of this view and its application to matchgate circuits.

To motivate this approach, consider first the different and well-studied issue of the efficient classical simulation of Clifford circuits [11, 10, 12]. The basic Clifford gates (not to be confused with the Clifford algebras above) are defined to be the Hadamard gate $H$, phase gate $S = \text{diag}\,(1\ i)$ and the controlled-$Z$ gate $CZ$. A Clifford circuit is any circuit of these gates and a Clifford operation is any such resulting unitary operation on $n$ qubits. Suppose we have a (poly-sized) Clifford circuit on $n$ qubits with overall Clifford operation $C$, and input state $|\psi_{\text{in}}\rangle = |\alpha_1\rangle \ldots |\alpha_n\rangle$ being any product state, and output being the result of a standard measurement on the first qubit of the final state $|\psi_{\text{out}}\rangle = C\,|\psi_{\text{in}}\rangle$. Then (a variant of) the Gottesman-Knill theorem asserts that this quantum process may be classically efficiently simulated, in the sense that the output probabilities $p_0$ and $p_1$ may be classically computed in poly($n$) time.

The key property upon which this result rests, is the fact that Clifford operations conjugate the set of tensor products of 1-qubit Pauli operations into itself i.e. if $P_1, \ldots, P_n$ are any 1-qubit Pauli operations and $C$ is any Clifford operation then there exist 1-qubit Pauli operations $P'_i$ such that $C^\dagger(P_1 \otimes \ldots \otimes P_n)C = k(P'_1 \otimes \ldots \otimes P'_n)$ where $k = \pm 1$ or $\pm i$. Furthermore the update rule for determining all $n$ of the $P'_i$'s (and $k$) from the $P_i$'s is computable classically in $O(n)$ time if $C$ is a basic Clifford gate. This property then easily

gives the classical simulation result for Clifford circuits [13, 12] viz. we have

$$p_0 - p_1 = \langle Z \otimes I \otimes \ldots \otimes I \rangle_{\text{out}} = \langle \psi_{\text{in}} | \, C^\dagger (Z \otimes I \otimes \ldots \otimes I) C \, | \psi_{\text{in}} \rangle \, . \tag{10}$$

Now if the size of the circuit is $N = \text{poly}(n)$ then $C = C_N \ldots C_2 C_1$ where each $C_i$ is a basic Clifford gate. So successive conjugation by the $C_i$'s (taken in reverse order) in eq. (10) gives $P_i'$'s with

$$p_0 - p_1 = \langle \psi_{\text{in}} | \, P_1' \otimes \ldots \otimes P_n' \, | \psi_{\text{in}} \rangle = \prod_{i=1}^{n} \langle \alpha_i | \, P_i' \, | \alpha_i \rangle \, .$$

Each of the $n$ terms in the latter product can be computed in constant time (ignoring issues of precision which will add at most a poly overhead) and the identities of the $P_i'$'s in $NO(n)$ time so $p_0$ and $p_1$ can be computed in classical $NO(n) + O(n)$ time i.e. poly$(n)$ time.

Now let us isolate the key ingredients that make the above simulation efficient, with a view to generalisation. Consider the following features:
**(S1)**: for each $n$ we have a structure $\mathcal{S}_n$ (above, the Pauli group on $n$ qubits) whose elements have classical poly$(n)$ sized descriptions;
**(S2)**: we have a class $\mathcal{U}_n$ of gates (above, the Clifford gates) that preserve $\mathcal{S}_n$ under conjugation, and the conjugation update rule is computable in classical poly$(n)$ time;
**(S3)**: for a suitable class of input states $|\psi_{\text{in}}\rangle$ (say product states or computational basis states) we have $\langle \psi_{\text{in}} | \, A \, | \psi_{\text{in}} \rangle$ being computable in poly$(n)$ time for any $A \in \mathcal{S}_n$;
**(S4)**: $\mathcal{S}_n$ contains observables of interest e.g. $Z \otimes I \otimes \ldots \otimes I$.

Clearly if these features are satisfied then we will have a classical simulation result for circuits of gates from $\mathcal{U}_n$ and expectation values of observables $A \in \mathcal{S}_n$ (that we have used above to obtain our output probabilities). Note that $\mathcal{S}_n$ need not be a group; in fact in [14] it has been pointed out that the JW simulation of fermionic matchgate circuits can be viewed as an example of the above features with $\mathcal{S}_n$ being a vector space (of linear (or quadratic) terms in a Clifford algebra). But more generally we seek further natural occurrences of these features in other mathematical contexts, with an aim of identifying new classes of classically simulatable quantum circuits.

In our motivating discussion above (and throughout the paper) we are considering only non-adaptive circuits i.e. we do not allow intermediate measurements within the circuit, followed by adaptive choices of subsequent gates depending on earlier measurement outcomes. Furthermore, for matchgate circuits we consider only unitary circuits, without intermediate measurements, having measurements only at the end to provide output probabilities. The computational power of such unitary matchgate circuits has been shown in [16] to coincide with that of space-bounded quantum computation, and further results on the ability of these circuits to compute Boolean functions have been given in [17]. Some classical simulation results for adaptive matchgate circuits have been given in [3]. In [12] the simulation complexity for adaptive and non-adaptive Clifford circuits has been discussed. It is shown there that non-adaptive Clifford circuits with product state inputs can be classically efficiently simulated (essentially by the method above) whereas if the circuits are allowed become adaptive then they become universal for quantum computation. (The latter result depends on special properties of Clifford gates, such as the fact that CNOT is Clifford.) This suggests that the formalism we are developing here may not have any generic extension to the case of adaptive circuits.

Somma et al. [7] have identified an occurrence arising naturally in the theory of representations of Lie algebras and Lie groups. Here we will give an exposition of this formalism and describe how it relates to our original issue of the classical simulation of matchgate circuits. We will not need abstract Lie algebra theory and we begin with the concrete setting of a *finite-dimensional matrix Lie algebra* $\mathcal{A}$ viz. a vector space $\mathcal{A}$ of matrices (of some finite dimension $d$, not to be confused with the size of the matrices) that is closed under the commutator (or bracket operation) $[A, B] = AB - BA$ (defined in terms of the usual matrix product). If $B_1, \ldots, B_d$ is a basis of matrices for $\mathcal{A}$ then we have the associated *structure constants* $c_{ij}^k$ given by

$$[B_i, B_j] = \sum_{k=1}^{d} c_{ij}^k B_k.$$

Introduce the set of all exponentials $\mathcal{E} = \{e^A : A \in \mathcal{A}\}$ (where the matrix exponential is the sum $\sum_{k=0}^{\infty} A^k/k$). Note that all elements of $\mathcal{E}$ are invertible and $\mathcal{E}$ is closed under inverses. Let $\mathcal{G}$ be the matrix group generated by $\mathcal{E}$. $\mathcal{G}$ is in fact a Lie group with Lie algebra $\mathcal{A}$ (cf. [15] §8.3) but we will not explicitly need this fact here – for our key result, Lemma 1 below, it will suffice to know just that $\mathcal{A}$ is closed under commutators. However it is interesting to note that in a more abstract setting of Lie group representation theory, Lemma 1 amounts to an instance of a fundamental general result (cf. [15]) viz. that the Lie algebra $\mathcal{A}$ carries a natural representation of the Lie group $\mathcal{G}$. This is the adjoint representation in which each $G \in \mathcal{G}$ acts linearly on $\mathcal{A}$ by conjugation, and for us an important ingredient of this result is the fact that $\mathcal{A}$ is always preserved under conjugation by such $G$'s:

**Theorem 5.** *(Adjoint representation of a Lie group on its Lie algebra.) With $\mathcal{A}$ and $\mathcal{G}$ as above, for all $G \in \mathcal{G}$ and $B \in \mathcal{A}$ we have that $B' = GBG^{-1}$ is in $\mathcal{A}$ and the resulting linear map $B \to B'$ on $\mathcal{A}$ for each $G \in \mathcal{G}$, provides a representation of $\mathcal{G}$ on $\mathcal{A}$.*

We will further need to assess the complexity of computing the update $B \to B'$, as given in the following Lemma (whose proof also implicitly shows that $\mathcal{A}$ is preserved under conjugation by $G \in \mathcal{G}$).

**Lemma 1.** *The conjugation action of $e^A$ on $\mathcal{A}$ can be classically computed (to $m$ digits of accuracy) in poly$(m, d)$ time (where $d$ is the dimension of $\mathcal{A}$).*

**Proof** Let $B_1, \ldots, B_d$ be a basis for $\mathcal{A}$ and write $A = \sum \xi_j B_j$. We aim to compute $a_{ij}$ defined by $e^A B_i e^{-A} = \sum_{ij} a_{ij} B_j$ which will suffice to fully characterise the adjoint action of $e^A$. To this end, introduce

$$B_i(t) = e^{tA} B_i e^{-tA}$$

so $B_i(0) = B_i$ and we get

$$\frac{dB_i(t)}{dt} = [A, B_i(t)] = \sum_{jk} \xi_j c_{ji}^k B_k(t)$$

so if $\underline{B}(t) = (B_1(t), \ldots, B_d(t))^T$ then

$$\frac{d\underline{B}(t)}{dt} = M\underline{B}(t) \quad \text{with} \quad M_i^k = \sum_j \xi_j c_{ji}^k$$

and so $\underline{B}(t) = e^{Mt}\underline{B}(0)$. Finally setting $t = 1$ we obtain the matrix of values $[a_{ij}]$ as $[a_{ij}] = e^M = I + M + M^2/2! + \ldots$. The exponential series converges rapidly and the result (involving $d \times d$ matrix algebra) can be computed to $m$ digits with $O(m)$ terms, so the whole calculation takes poly$(m, d)$ time. $\square$

Now with the above in view, we can make a connection to our desired features (S1) – (S4). For each $n$, to $n$ qubit lines we associate a matrix Lie algebra $\mathcal{A}_n$ of dimension $d =$poly$(n)$, comprising matrices of size $2^n \times 2^n$. If furthermore, $\mathcal{A}_n$ has a basis of matrices that are tensor products of 1-qubit matrices (hence having poly$(n)$ sized descriptions) then (S1) will be satisfied. If $A \in \mathcal{A}_n$ is skew-hermitian then $e^A$ will be unitary and we take $\mathcal{U}_n$ to be the corresponding set of unitary operations. Lemma 1 then guarantees that (S2) will be satisfied. (Note that Lemma 1 applies for all $A \in \mathcal{A}$, even if $e^A$ is not unitary, and this leads to a classical simulation result for circuits of gates that are not necessarily unitary.) For (S3) and (S4) we just choose suitably well behaved classes; for example (as will apply in our case below), if $\mathcal{A}_n$ has a basis of product matrices we can take input states to be product states, and require also that $\mathcal{A}_n$ contains say $I \otimes \ldots \otimes I \otimes Z \otimes I \ldots \otimes I$ (having $Z$ on the $k^{\text{th}}$ line), for some or all $1 \leq k \leq n$.

Finally let us return to the JW simulation of matchgate circuits, to see it as an example of the above formalism. Consider again $2n$ generators $c_\mu$, $\mu = 1, \ldots, 2n$ that satisfy the Clifford algebra anti-commutation relations eq. (6) and we may concretely regard them as being the Jordan-Wigner operators eq. (5). The linear span $\mathcal{L}_1$ of the $c_\mu$'s is not closed under commutators e.g. if $\mu \neq \nu$ then $[c_\mu, c_\nu] = c_\mu c_\nu - c_\nu c_\mu = 2c_\mu c_\nu$ which is not generally expressible as a linear sum. However the linear span $\mathcal{L}_2$ of all quadratic products $c_\mu c_\nu$ *does* form a Lie algebra, being closed under commutators by virtue of the Clifford *anti*-commutation relations; indeed we have $[c_\mu c_\nu\,,\, c_\alpha c_\beta] = c_\mu c_\nu c_\alpha c_\beta - c_\alpha c_\beta c_\mu c_\nu$ which is zero if all indices are distinct, or it reduces to a quadratic expression again if two indices are equal. If we omit the identity matrix from $\mathcal{L}_2$ (i.e. the case of $\mu = \nu$ in quadratic terms) then the remaining Lie algebra has dimension $d = \binom{2n}{2} = n(2n-1) = O(n^2)$. This algebra is in fact isomorphic to the (complexified) Lie algebra of the special orthogonal group SO$(2n)$ in $2n$ dimensions, as for example, they have the same structure constants for suitable choices of bases. (The quadratic terms with $\mu = \nu$ then just contribute an extra single dimension to the Lie group as an overall scalar multiple for the matrices $e^A$). Thus taking $\mathcal{A}_n$ for $n$ qubit lines to be the Lie algebra $\mathcal{L}_2$ (and using the JW operators for the $c_\mu$'s) we have (S1) – (S4) all holding and we obtain our efficient classical simulation of fermionic matchgate circuits viz. circuits of gates that are exponentials of quadratic expressions in the JW operators.

In the same way, from the Lie algebra formalism we can also easily obtain the classical simulation result for hamiltonians that involve both quadratic and linear terms i.e. gates $e^A$ with exponents $A \in \mathcal{L}_{1\oplus 2}$. For this we simply notice that (despite that fact that $\mathcal{L}_1$ is not a Lie algebra), $\mathcal{L}_{1\oplus 2} = \mathcal{L}_1 \oplus \mathcal{L}_2$ is a Lie algebra, again closed under commutators by virtue of the Clifford algebra anti-commutation relations. If we again omit the case of $\mu = \nu$ in the quadratic terms then the resulting Lie algebra has dimension $d = \binom{2n}{2} + 2n = n(2n+1) = O(n^2)$, and it is isomorphic to the (complexified) Lie algebra of the orthogonal group SO$(2n+1)$.

It would be interesting to seek further natural occurrences of the conditions in (S1) – (S4), perhaps using other Lie algebras, or indeed further unrelated constructions, recalling that our original motivating example of Clifford circuits does not itself seem to arise from

any underlying Lie algebra (as Clifford operations form only a discrete set of gates).

# 5 Appendix: proof of Theorem 1

Before proving this theorem we introduce some further terminology. Note first that for each $ij$, $B_{ij}$ occurs in exactly five of the matchgate identities. Let $\mathcal{M}(ij)$ be the corresponding set of five identities and let $\mathcal{N}(ij)$ be the remaining five. It was noted in [9] that the set of matchgate identities possesses a high degree of symmetry. This leads to associated dependencies and in fact, for any non-zero matrix, only five of the ten matchgate identities are significant, in the following sense.

**Lemma 2.** *Let $ij$ be given. Suppose that a matrix $B$ has $B_{ij} \neq 0$ and $B$ satisfies the identities in $\mathcal{M}(ij)$. Then $B$ satisfies the identities in $\mathcal{N}(ij)$ too, so $B \in \mathcal{MG}$.*

**Proof.** Consider the illustrative case of $ij = 44$, which has $\mathcal{M}(44) = \{M_1, M_2, M_3, M_4, M_5\}$ and $\mathcal{N}(44) = \{M_6, M_7, M_8, M_9, M_{10}\}$. Now consider each element of $\mathcal{N}(44)$ in turn, multiplied by $B_{44}$. For $M_6$ we have:

$$B_{44}M_6 = (B_{11}B_{44})B_{24} - (B_{12}B_{44})B_{23} + (B_{13}B_{44})B_{22} - (B_{21}B_{44})B_{14}.$$

Each bracketed term is the $B_{44}$-term of an identity $M_k$ in the set $\mathcal{M}(44)$ viz. respectively $M_1, M_5, M_4$ and $M_2$. Replacing the brackets by these full expressions we find that all the extra terms cancel and we get:

$$B_{44}M_6 = (M_1)B_{24} - (M_5)B_{23} + (M_4)B_{22} - (M_2)B_{14}.$$

So if $B_{44} \neq 0$ then $M_1 = \ldots = M_5 = 0$ implies that $M_6 = 0$. The same procedure works for all other $M_i$'s in $\mathcal{N}(44)$ too. Furthermore it also works for any $\mathcal{M}(ij)$ and $\mathcal{N}(ij)$ (for all initial choices of $ij$). The mind-numbingly long list of (eighty) claimed algebraic relations can be readily verified, for example by computer algebra. □

**Proof of Theorem 1(a).** We need to show that any non-invertible matchgate $B$ is the limit of invertible matchgates. If $B$ is the all-zero matrix, let $\tilde{B}$ be any invertible matchgate and setting $\tilde{B}_k = \tilde{B}/k$ we have $B = \lim_{k\to\infty} \tilde{B}_k$. Thus suppose that $B$ contains some non-zero entry $B_{i_0j_0} = c \neq 0$, which will remain constant in the following constructions. Let $B_{i_1j_1}, \ldots, B_{i_5j_5}$ be the multipliers of $B_{i_0j_0}$ in the five matchgate identities of $\mathcal{M}(i_0j_0)$. Dividing these identities by $c$ we obtain $B_{i_1j_1}, \ldots, B_{i_5j_5}$ expressed in terms of $c$ and the ten entries $B_{kl}$ with $kl \neq i_0j_0, i_1j_1, \ldots, i_5j_5$.

We substitute these into $B$ and for fixed $B_{i_0j_0} = c$ we obtain a matrix $\tilde{B}$ that is freely parameterised by ten complex variables (viz. the $B_{kl}$ above) and which satisfies $\mathcal{M}(i_0j_0)$ with $B_{i_0j_0} = c \neq 0$. Thus by Lemma 2, $\tilde{B} \in \mathcal{MG}$.

Then $\det \tilde{B}$ is a polynomial in the ten variables. Now for any $i_0j_0$ there is an invertible matchgate whose $i_0j_0^{\text{th}}$ entry is $c$ so $\det \tilde{B}$ cannot be identically zero. Thus its zero set must have empty interior so $\{\tilde{B} : \det \tilde{B} \neq 0\}$ is dense in the set of all matchgates $\tilde{B}$ with $\tilde{B}_{i_0j_0} = c$. Hence $B$ is the limit of such invertible matchgates. □

To facilitate the proof of Theorem 1(b) we first establish a geometrical interpretation of the ten matchgate identities, which will also provide a connection to the Jordan-Wigner

operators. It is an extension of a construction in [4], given there for a setting of five matchgate identities.

We begin by introducing the four-qubit vector

$$|\Upsilon\rangle = \sum_{j=1}^{4} |j\rangle\,|j\rangle$$

(where the labels $j = 1, 2, 3, 4$ correspond to qubit labels $00, 01, 10, 11$ respectively). Then (up to an overall factor of $i$) we introduce the so-called Choi-Jamiolkowski state for the 2-qubit operation $XY$ (writing $I$ for the identity on the first two qubits):

$$|F_0\rangle = I \otimes (XY)\,|\Upsilon\rangle = |1\rangle\,|4\rangle - |2\rangle\,|3\rangle + |3\rangle\,|2\rangle - |4\rangle\,|1\rangle$$

which is an *anti-symmetric* vector in $\mathbb{C}^4 \otimes \mathbb{C}^4$. We extend $|F_0\rangle$ to a full orthogonal basis of the 6-dimensional anti-symmetric subspace with the following vectors:

$$\begin{aligned}
|F_0\rangle &= |1\rangle|4\rangle - |4\rangle|1\rangle - |2\rangle|3\rangle + |3\rangle|2\rangle \\
|F_1\rangle &= |1\rangle|4\rangle - |4\rangle|1\rangle + |2\rangle|3\rangle - |3\rangle|2\rangle \\
|F_2\rangle &= |1\rangle|2\rangle - |2\rangle|1\rangle \\
|F_3\rangle &= |1\rangle|3\rangle - |3\rangle|1\rangle \\
|F_4\rangle &= |2\rangle|4\rangle - |4\rangle|2\rangle \\
|F_5\rangle &= |3\rangle|4\rangle - |4\rangle|3\rangle.
\end{aligned}$$

Since all these vectors are real we have $\langle F_i| = |F_i\rangle^\dagger = |F_i\rangle^T$ (where $T$ denotes transpose and $\dagger$ the conjugate transpose). Now for any $4\times 4$ matrix $B$, $B\otimes B$ preserves the anti-symmetric subspace. Introduce

$$\begin{aligned}
D_i &= \langle F_i|\,(B \otimes B)\,|F_0\rangle \\
D_i^T &= \langle F_0|\,(B \otimes B)\,|F_i\rangle = \langle F_i|\,B^T \otimes B^T\,|F_0\rangle
\end{aligned}$$

By direct calculation it is easy to verify the following relations:

$$\begin{aligned}
D_1 + D_1^T &= 4M_1 \\
D_4 &= 2M_2 \\
D_5 &= 2M_3 \\
D_5^T &= 2M_4 \\
D_4^T &= 2M_5 \\
D_2 &= 2M_6 \\
D_2^T &= 2M_7 \\
D_1 - D_1^T &= 4M_8 \\
D_3 &= 2M_9 \\
D_3^T &= 2M_{10}
\end{aligned}$$

Thus $B$ is a matchgate if and only if $D_i = 0$ and $D_i^T = 0$ for $i = 1, \ldots, 5$. Now since $\{|F_i\rangle : i = 0, 1, \ldots, 5\}$ is an orthogonal basis for the anti-symmetric subspace we see that $D_i = 0$ for $i = 1, \ldots, 5$ iff $|F_0\rangle$ is an eigenvector of $B \otimes B$. Similarly $D_i^T = 0$ for $i = 1, \ldots, 5$ iff $|F_0\rangle$ is an eigenvector of $B^T \otimes B^T$ and we have proved:

**Theorem 6.** *A $4 \times 4$ matrix $B$ is a matchgate iff $|F_0\rangle$ is an eigenvector of both $B \otimes B$ and $B^T \otimes B^T$.*

We remark that Theorem 6 immediately implies that the set of invertible matchgates forms a group, which was proven by other means in [9].

**Proof of Theorem 1(b).** We show that $\mathcal{G} \subseteq \mathcal{M}\mathcal{G}^*$ and $\mathcal{M}\mathcal{G}^* \subseteq \mathcal{G}$. For the first inclusion consider again the 11 generators of the Lie algebra $\mathcal{L}$ given in eq. (4), which we now label as $A_0 = II$ and $A_i$ with $i = 1, \ldots, 10$ for the others. It is easy to check that

$$A_i(XY) + (XY)A_i^T = 0 \quad \text{for } i = 1, \ldots, 10. \tag{11}$$

Next we recall that $|F_0\rangle = I \otimes (XY)\,|\Upsilon\rangle$ and note the following facts: (i) for any 2-qubit operator $W$ we have $I \otimes W\,|\Upsilon\rangle = W^T \otimes I\,|\Upsilon\rangle$ and (ii) $I \otimes W\,|\Upsilon\rangle = 0$ iff $W = 0$. Using these facts we can see that eq. (11) is equivalent to

$$(A_i \otimes I + I \otimes A_i)\,|F_0\rangle = 0 \quad \text{for } i = 1, \ldots, 10. \tag{12}$$

Now if $A = \sum_{i=0}^{10} \alpha_i A_i$ is any element of the Lie algebra $\mathcal{L}$ we have

$$e^{(A\otimes I + I \otimes A)} = e^{A \otimes I} e^{I \otimes A} = B \otimes B \quad \text{where } B = e^A.$$

Then eq. (12) (and the fact that $A_0$ is the identity operation) implies that $|F_0\rangle$ is an eigenvector of $e^{(A\otimes I + I\otimes A)}$ i.e. of $B \otimes B$. Since $\mathcal{L}$ is closed under taking transposes and $B^T = e^{(A^T)}$, we similarly have $|F_0\rangle$ being an eigenvector of $B^T \otimes B^T$, so by Theorem 3, $B \in \mathcal{M}\mathcal{G}^*$ and $\mathcal{G} \subseteq \mathcal{M}\mathcal{G}^*$.

For the reverse inclusion, let $B \in \mathcal{M}\mathcal{G}^*$ be any invertible matchgate. Then (since $B$ is invertible) $B = e^A$ for some $4 \times 4$ matrix $A$ and $B \otimes B = e^A \otimes e^A$ so Theorem 3 gives

$$e^A \otimes e^A\,|F_0\rangle = \lambda\,|F_0\rangle$$

for some $\lambda \neq 0$. Thus $e^{tA} \otimes e^{tA}\,|F_0\rangle = \lambda^t\,|F_0\rangle$ for $t \in \mathbb{R}$ and taking $\frac{d}{dt}|_{t=0}$ we get

$$(A \otimes I + I \otimes A)\,|F_0\rangle = \lambda'\,|F_0\rangle$$

for some $\lambda'$. So

$$\langle F_i|\,A \otimes I + I \otimes A)\,|F_0\rangle = 0 \quad \text{for } i = 1, \ldots, 5. \tag{13}$$

This gives five linear equations on the sixteen entries of $A$. Since $|F_i\rangle$ are orthogonal, the equations are independent, and we must have an 11-dimensional linear space of solutions. Now any $4 \times 4$ matrix $A$ can be written as

$$A = \sum_{i,j=0}^{3} \alpha_{ij} P_i \otimes P_j$$

where $P_0 = I$, $P_1 = X$, $P_2 = Y$ and $P_3 = Z$ are the Pauli matrices. We know from eq. (12) (and $I \otimes I\,|F_0\rangle = |F_0\rangle$) that all 11 generators $A_0, A_1, \ldots, A_{10}$ of the Lie algebra $\mathcal{L}$ satisfy eq. (13) so $\mathcal{L}$ itself must be the 11-dimensional linear space of solutions of eq. (13) i.e. $A \in \mathcal{L}$ so $B = e^A \in \mathcal{G}$, completing the proof of Theorem 1(b). $\square$

Finally we mention a possible alternative "brute force" approach to proving the inclusion $\mathcal{G} \subseteq \mathcal{M}\mathcal{G}^*$. Any element of $\mathcal{G}$ has the form $e^A$ where $A$ is a (complex) linear combination of the eleven $4 \times 4$ matrices given explicitly in eq. (4). Thus we could envisage using computer algebra to explicitly compute $e^A$ symbolically as a function of eleven variables and then check each of the matchgate identities on the resulting matrix elements. A significant issue here is the complexity of the symbolic manipulations needed to simplify the very long multivariate algebraic expressions obtained. Using straightforward programming in Mathematica implemented on a standard modern laptop, it took eight hours to compute and simplify all sixteen entries of $e^A$ and many of the matchgate identities required several more hours each, for their explicit symbolic verification on the resulting matrix entry expressions. We would expect that these timings could probably be significantly reduced by more perspicacious programming.

### Acknowledgments

Thanks to Niel de Beaudrap and Dan Browne for helpful discussions and to Leslie Valiant for raising the question of the full equivalence of matchgates and the JW formalism. RJ was supported in part by the EC network Q-ALGO. AM was supported in part by National Science Foundation grants PHY-1212445 and PHY-1314955.

## References

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

[2] L. Valiant, Holographic algorithms. *SIAM J. Computing* **37:5** 1565-1594 (2007).

[3] B. Terhal and D. DiVincenzo, Classical simulation of noninteracting-fermion quantum circuits. *Phys. Rev. A* **65**, 032325/1-10 (2002).

[4] E. Knill, Fermionic linear optics and matchgates. Preprint available at arXiv:quant-ph/0108033 (2001).

[5] S. Bravyi and A. Kitaev, Fermionic quantum computation. *Annals of Physics* **298**, Iss. 1 pp.210-226 (2002)

[6] R. Jozsa and A. Miyake, Matchgates and classical simulation of quantum circuits. *Proc. R. Soc. (Lond) A* **464**, p3089-3106 (2008).

[7] R. Somma, H. Barnum, G. Ortiz and E. Knill, 2006 Efficient solvability of hamiltonians and limits on the power of some quantum computational models. *Phys. Rev. Lett.* **97**, 190501.

[8] P. Jordan and E. Wigner, Über das Paulische Äquivalenzverbot. *Zeitschrift für Physik* **47**, 631-651 (1928).

[9] J-Y. Cai, V. Choudhary, P. Lu, On the Theory of Matchgate Computations, ccc, pp.305-318, *Twenty-Second Annual IEEE Conference on Computational Complexity (CCC'07)* (2007).

[10] M. Nielsen and I. Chuang, Quantum Computation and Quantum Information. Cambridge University Press (2000).

[11] D. Gottesman, Stabilizer Codes and Quantum Error Correction, PhD thesis, California Institute of Technology, Pasadena, CA (1997).

[12] R. Jozsa and M. Van den Nest, Classical simulation complexity of extended Clifford circuits, *Quant. Inform. Comp.* **14** p633-648 (2014).

[13] S. Clark, R. Jozsa and N. Linden, Generalised Clifford groups and simulation of associated quantum circuits, *Quant. Inform. Comp.* **8** p106-126 (2008)

[14] R. Jozsa, Embedding classical into quantum computation, *Springer LNCS* **5393** Beth Festschrift, J. Calmet, W. Geiselmann, J. Mueller-Quade (eds.), p43-49 (2008).

[15] W. Fulton and J. Harris, Representation theory: a first course. Graduate Texts in Mathematics 129, Springer-Verlag New York (1991).

[16] R. Jozsa, B. Kraus, A. Miyake and J. Watrous, Matchgate and space-bounded quantum computations are equivalent. *Proc. R. Soc. (Lond) A* **466**, p809-830 (2010).

[17] M. Van den Nest, Quantum matchgate computations and linear threshold gates. *Proc. R. Soc. (Lond) A* **467**, p821-840 (2011).