

Magic states for matchgate computations

Richard Jozsa
DAMTP, University of Cambridge UK

with

Martin Hebenstreit, Barbara Kraus (Innsbruck),
Sergii Strelchuk, Mithuna Yoganathan (Cambridge)

arXiv:1905.08584

Phys. Rev. Lett. **123**, 080503 (Aug 2019)

Main result:

All pure non-Gaussian fermionic states
are magic states for matchgate computations.

Magic states (Bravyi & Kitaev 2004)

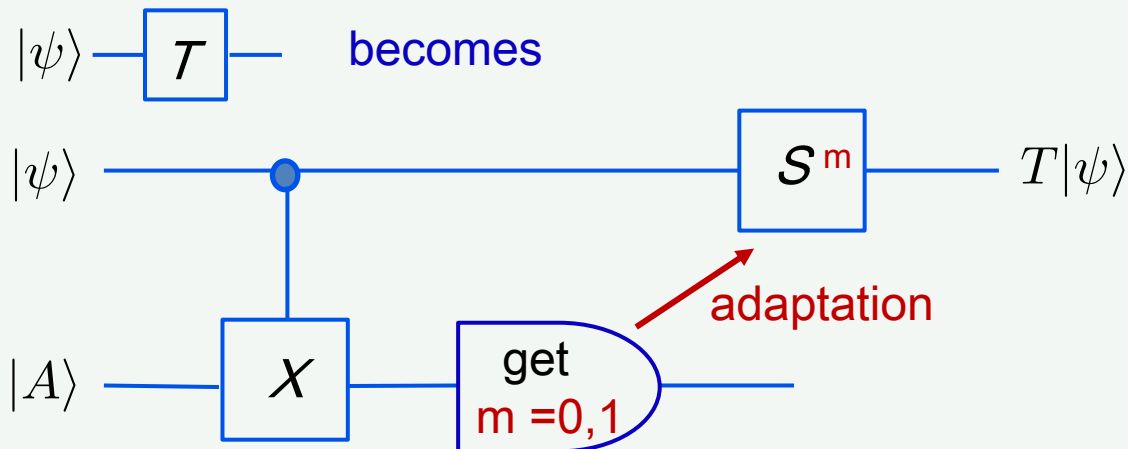
Special input states that extend classically simulatable circuits to full universal QC power (UQC) while retaining same gate set, and allowing intermediate measurements with adaptive choices.

Gate gadgets (for Clifford circuits)

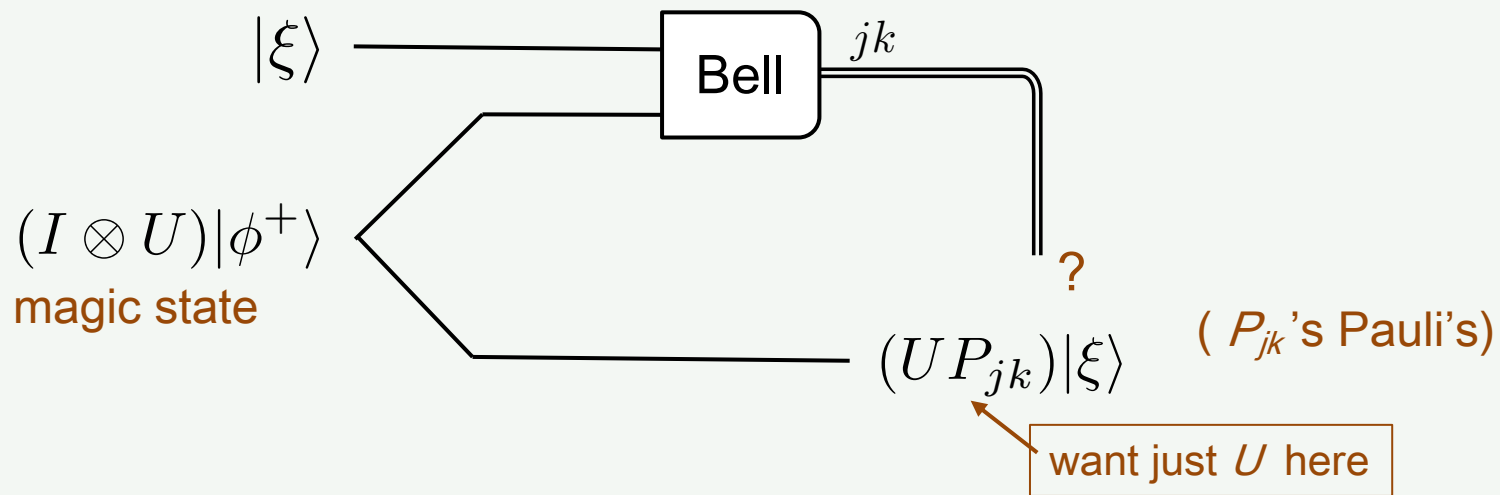
Example 1: Clifford gates with $T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$ is UQC

Magic state $|A\rangle = \frac{1}{\sqrt{2}} (|0\rangle + e^{i\pi/4}|1\rangle)$

Replace each T gate by the “ T -gadget”:



Example 2: More generally – gate teleportation (relevant for later)



If $UP = (\text{Clifford})U$ then can correct P_{jk} with (allowed) Clifford gate (depending adaptively on outcome jk).
 i.e. need $UPU^\dagger = \text{Clifford}$
 i.e. U in 3rd level of Clifford hierarchy e.g. T gate is there.
 (Level n conjugates Paulis into level $n-1$).

Matchgates (MGs) - any 2-qubit gate of the form

$$G(A, B) = \begin{bmatrix} p & 0 & 0 & q \\ 0 & a & b & 0 \\ 0 & c & d & 0 \\ r & 0 & 0 & s \end{bmatrix}$$

$$A = \begin{bmatrix} p & q \\ r & s \end{bmatrix} \quad B = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

acts in even $\{ |00\rangle, |11\rangle \}$ *and odd* $\{ |01\rangle, |10\rangle \}$ *subspaces respectively.*

with A and B in $U(2)$ both with **same determinant**,
and acting only on **nearest neighbour** (n.n.) qubit lines.

Note: $SWAP = G(I, X)$ is **not** a MG!
but $fSWAP = G(Z, X)$ is a MG.

maps

$ 00\rangle$ to $ 00\rangle$	$ 11\rangle$ to $- 11\rangle$
$ 01\rangle$ to $ 10\rangle$	$ 10\rangle$ to $ 01\rangle$

Physical significance

Introduce n fermionic modes: a_1, \dots, a_n with

$$\text{(CCRs)} \quad \{a_i, a_j\} = \{a_i^\dagger, a_j^\dagger\} = 0 \quad \{a_i, a_j^\dagger\} = \delta_{ij} \quad i, j = 1, \dots, n$$

Quadratic hamiltonians: quadratic in a_i 's and a_i^\dagger 's

Map n fermionic modes to n qubits:

introduce vacuum state $|\Omega\rangle$ and define n -qubit basis by

$$|k_1 \dots k_n\rangle = (a_1^\dagger)^{k_1} \dots (a_n^\dagger)^{k_n} |\Omega\rangle \quad k_i \text{'s} = 0, 1$$

Then (CCRs) \implies

these states are orthonormal and matrix of a_j 's and a_j^\dagger 's are the standard Jordan-Wigner representation:

$$\tilde{c}_{2j-1} = (a_j + a_j^\dagger) \quad \tilde{c}_{2j} = -i(a_j - a_j^\dagger)$$

$$\begin{aligned} c_{2j-1} &= Z \otimes Z \otimes \dots \otimes Z \otimes X_j \otimes I \otimes \dots \otimes I \\ c_{2j} &= Z \otimes Z \otimes \dots \otimes Z \otimes Y_j \otimes I \otimes \dots \otimes I \end{aligned}$$

Fact: for any U on n qubits -

U corresponds to an evolution of fermionic modes under a quadratic Hamiltonian *if and only if*

U is a circuit of (n.n.) matchgates.

Classical simulation properties of MG computations

Poly-sized circuit of MGs on n qubit lines.

Measurements (final or intermediate) are always in comp basis.

Scenarios:

Comp-in: only computational basis inputs $|i_1 \dots i_n\rangle$ allowed.

Prod-in: general product state inputs $|\alpha_1\rangle \dots |\alpha_n\rangle$ allowed.

1-out: single line output (1 bit).

Many-out: multi-line output ($k \leq n$ bits).

Ad-Mmt: intermediate mmts allowed and later MGs can be chosen adaptively to depend on earlier mmt outcomes.

Theorem 1 (Valiant, Terhal&DiVincenzo, Knill ~2000)

Comp-in and **Many-out**: any output probability or marginal can be classically efficiently computed, so can efficiently sample too.

Theorem 2 (Terhal&DiVincenzo 2000)

Comp-in with **Ad-Mmt** and **Many-out**: output distribution can be classically efficiently sampled.

Theorem 3 (RJ and A. Miyake 2008)

Prod-in and **1-out**: output probabilities can be classically efficiently computed (so sampled too).

(!)Theorem 4 (D. Brod 2016)

Prod-in with **Ad-Mmt** and **Many-out**: output distribution can be classically efficiently sampled.

Theorem 1 (Valiant, Terhal&DiVincenzo, Knill ~2000)

Comp-in and **Many-out**: any output probability or marginal can be classically efficiently computed, so can efficiently sample too.

Theorem 2 (Terhal&DiVincenzo 2000)

Comp-in with **Ad-Mmt** and **Many-out**: output distribution can be classically efficiently sampled.

Theorem 3 (RJ and A. Miyake 2008)

Prod-in and **1-out**: output probabilities can be classically efficiently computed (so sampled too).

(!)Theorem 4 (D. Brod 2016)

Prod-in with **Ad-Mmt** and **Many-out**: output distribution can be classically efficiently sampled.

Compare(!): Clifford circuits have wide range of classical simulation complexities (including quantum universal) in analogous scenarios! MG circuits appear “*more classically simulatable*” yet Clifford gates/circuits have representation as classical stochastic maps on a phase space (viz. the discrete Wigner function formalism).

Brod's method: reduce Prod-in to Comp-in

(will be relevant for magic states, in a moment)

We'll use the following simple facts about MGs:

(A1): $G(Z,X)$ acts as usual *SWAP* if one of the lines is $|0\rangle$.

(A2): For any 1-qubit phase gate $P(\phi)$, $I \otimes P(\phi)$ and $P(\phi) \otimes I$ are MGs.

(A3): $G(H,H) |\phi\rangle|+\rangle = (H|\phi\rangle) |+\rangle$ so if we have an extra ancilla $|+\rangle$ next to a line, we can implement H on that line.

Also know **(A4):** $\{H, P(\phi)\}$ is universal for all 1-qubit gates.

So:

Start with $|0\rangle \dots |0\rangle|0\rangle|+\rangle$ and make $|0\rangle \dots |0\rangle |\alpha_1\rangle|+\rangle$ (by (A2),(A3),(A4))

Next swap $|\alpha_1\rangle$ to left end giving $|\alpha_1\rangle|0\rangle \dots |0\rangle |+\rangle$ (by (A1))

Continue in same way, making $|\alpha_2\rangle$ in rightmost $|0\rangle$ and swap it to the left over all $|0\rangle$'s etc, to **finally get**

$$|0\rangle \dots |0\rangle|+\rangle \xrightarrow{\text{MG circuit}} |\alpha_1\rangle \dots |\alpha_n\rangle|+\rangle$$

Thus for Prod-in, any MG circuit

C on $|\alpha_1\rangle \dots |\alpha_n\rangle$

can be reduced to a (slightly larger) MG circuit

C* now on $|0\rangle \dots |0\rangle |+\rangle$.

MG circuits preserve parity of any input Comp-in string
so for input $|0\rangle \dots |0\rangle |+\rangle$ the two branches from

$\frac{1}{\sqrt{2}} |0\rangle \dots |0\rangle |0\rangle$ and $\frac{1}{\sqrt{2}} |0\rangle \dots |0\rangle |1\rangle$ never interfere

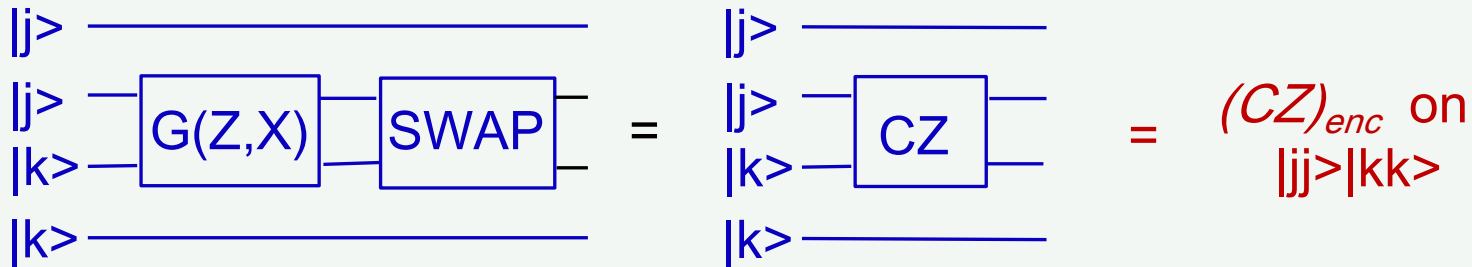
and output probabilities are averages
of the two Comp-in processes with input
 $|0\rangle \dots |0\rangle |0\rangle$ and $|0\rangle \dots |0\rangle |1\rangle$ respectively.

Matchgates with (n.n.) *SWAP* is UQC

Encode 0 and 1 as $|00\rangle$ and $|11\rangle$ *i.e. use the even subspace.*

Then any 1-qubit gate U encodes as $U_{enc} = G(U, U)$

and can get $(CZ)_{enc}$ (which then suffices for UQC) using *SWAP*:



Definitions for n qubit states

Fermionic state: superposition of only even parity or only odd parity bit strings.

Gaussian state: any state obtainable via action of a MG circuit on a computational basis input.

(so Gaussian is special case of fermionic)

(MG analogue of stabiliser state)

Magic states for matchgate circuits

more subtle than the Clifford case

An m qubit state $|M\rangle$ is a magic state for a k qubit gate R if

(M1): there is a MG circuit C with adaptive measurements (“the R -gate gadget”) such that

$$|\alpha\rangle|M\rangle \xrightarrow{C} (R|\alpha\rangle)|\tilde{M}\rangle \quad \text{for any } |\alpha\rangle \text{ on } k \text{ qubits}$$

(and $|\tilde{M}\rangle$ may depend on measurement outcomes but not on $|\alpha\rangle$) .

More generally (inexact implementation of R):

For any $\epsilon > 0$ there is an adaptive MG circuit of size $\text{poly}(1/\epsilon)$ with

$$|\alpha\rangle|M\rangle^{\otimes p} \xrightarrow{C} (R|\alpha\rangle)|\tilde{M}\rangle \quad \text{with } p = \text{poly}(1/\epsilon)$$

with probability $> 1 - \epsilon$ (over intermediate measurement outcomes).

This suffices to represent R in bounded error computations like BQP.

However we will need more conditions on $|M\rangle$ to be a magic state...

Example

MGs with $R = H$ is known to be UQC.

H can be implemented with MGs if $|+\rangle$ ancilla available (Brod)

i.e. $|+\rangle$ functions as a 'magic state' for H

(and $|+\rangle$ is even preserved in the gadget!)

(!) But also: MG circuits with Comp-in and input $|+\rangle$'s is classically simulatable (even with Ad-mmt and Many-out).

So conclude $BQP = BPP!$?

Example

MGs with $R = H$ is known to be UQC.

H can be implemented with MGs if $|+\rangle$ ancilla available (Brod)

i.e. $|+\rangle$ functions as a 'magic state' for H

(and $|+\rangle$ is even preserved in the gadget!)

(!) But also: MG circuits with Comp-in and input $|+\rangle$'s is classically simulatable (even with Ad-mmt and Many-out).

So conclude $BQP = BPP$!?

(!) But $|+\rangle$ needs to be adjacent to the line of H action!

For UQC we generally want to implement many R 's in a n.n. MG circuit

But (unlike Clifford case):

(a) generally cannot swap $|M\rangle$ next to $|\alpha\rangle$ line to implement a gadget by n.n. MGs;

(b) cannot initially place $|M\rangle$'s between input lines (where later needed) as this partitions the circuit into independent sectors for n.n. MGs!

Use of $|+\rangle$ is debilitatingly constrained by (a) and (b) above!

So impose a second condition on $|M\rangle$ to be a magic state:

(M2): $|M\rangle$ can be swapped through arbitrary states using n.n. MGs only.

Example.

$|0\rangle$ can be swapped anywhere using $G(Z, X)$

$|1\rangle$ can be swapped anywhere using $G(-Z, X)$

$|1\rangle|1\rangle$ maps to $-|1\rangle|1\rangle$
but never get $|1\rangle|1\rangle$
to swap.
Similarly for $|0\rangle|0\rangle$.

$|+\rangle$ cannot be swapped around (unless BQP=BPP)

Theorem:

$|M\rangle$ satisfies (M2) if and only if $|M\rangle$ is a fermionic state.

Thus any magic state must be a fermionic state.

Not a priori clear that *any* state satisfies both (M1) and (M2)?..

Magic state for SWAP gate in MG circuits

Remark

Smallest number of qubits for any magic state is *four* since:

- (i) for one qubit, any adaptive MG circuit is classically simulatable;
- (ii) all 2- and 3-qubit fermionic states are Gaussian.

Introduce:

$$|M\rangle_{1234} = |\phi^+\rangle_{13}|\phi^+\rangle_{24} = \frac{1}{2} [|0000\rangle + |0101\rangle + |1010\rangle + |1111\rangle]$$

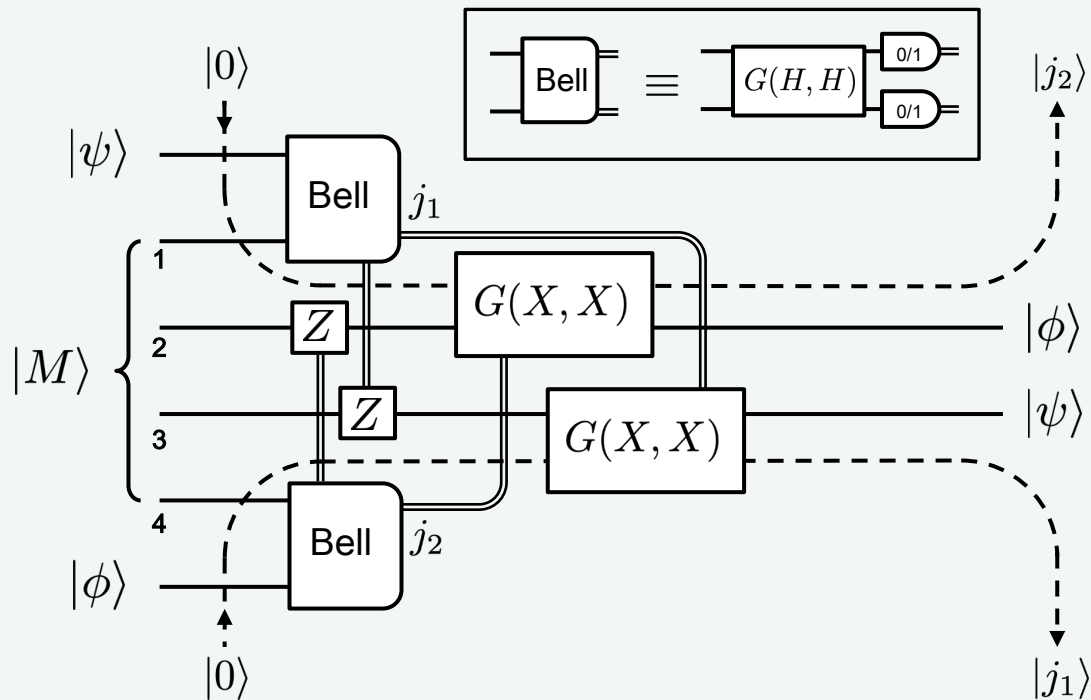
$|M\rangle$ is fermionic so satisfies (M2).

$|M\rangle$ is Choi state for SWAP with the reordering and partition 14|23

$$|M\rangle_{1234} = I_{14} \otimes \text{SWAP}_{23} \sum_{i,j=0}^1 |ij\rangle_{14} |ij\rangle_{23} \quad (\text{up to factor of a half})$$

We'll use $|M\rangle_{1234}$ to teleport from 14 over to 23
i.e. do gate teleportation for $U = \text{SWAP}$

The SWAP gadget for matchgates



Note:

$$(SWAP)(P_2 \otimes P_3) = (P_3 \otimes P_2) \otimes (SWAP)$$

For Z correction: $G(Z, Z) = Z \otimes I$ is a matchgate.

For X correction: bring in ancilla $|0\rangle$ with $G(Z, X)$'s, apply $G(X, X) = X \otimes X$, and then remove ancilla $|1\rangle$ with $G(-Z, X)$'s.

Main theorem


All fermionic states that are not Gaussian are magic states for matchgate computations.

Outline of approach to proof

Introduce the (even fermionic) state

$$|M_\phi\rangle = \frac{1}{2} [|0000\rangle + |0011\rangle + |1100\rangle + e^{i\phi} |1111\rangle]$$

Choi state for
C-phase(ϕ) gate



Then have three lemmas

Lemma 1: any 4-qubit fermionic state $|\xi\rangle$ which is non-Gaussian is MG-equivalent to $|M_\phi\rangle$ for some $\phi \in (0, 2\pi)$.

In fact we give an explicit depth-3 MG circuit transforming $|\xi\rangle$ into an $|M_\phi\rangle$ for suitable ϕ in $(0, 2\pi)$.

Not also that $|M_\phi\rangle$ is Gaussian iff $\phi = 0$ or 2π .

Lemma 2: for $k \geq 4$ let $|\psi_{k+1}\rangle$ be any $(k+1)$ -qubit fermionic **non**-Gaussian state. Then using MGs and measurements, $|\psi_{k+1}\rangle$ can be transformed with probability > 0 into a k -qubit fermionic **non**-Gaussian state, and hence to $k = 4$ and hence to $|M_\phi\rangle$.

Useful technical ingredient in this proof (and in other proofs)

Fact (Bravyi 2005)

$$\text{Let } \Lambda_n = \sum_{i=1}^{2n} c_i \otimes c_i$$

Then

(a) Any fermionic state $|\xi\rangle$ is a Gaussian state **iff** $\Lambda_n (|\xi\rangle \otimes |\xi\rangle) = 0$

(b) Any even operator R is Gaussian **iff** $[\Lambda_n, R \otimes R] = 0$

(No such neat exact algebraic characterization for stabilizer states and Clifford operations?)

Lemma 3: $|M_\phi\rangle$ can be used to realise the 2-qubit C-phase(ϕ) gate.

And known (Brod & Galvao 2011):

MGs with C-phase(ϕ) for any ϕ in $(0, 2\pi)$ is UQC.

Proof idea

$|M_\phi\rangle$ is Choi state for C-phase(ϕ).

Use it in the SWAP gadget construction to implement C-phase(ϕ) or C-phase($-\phi$) with probabilities half.

Then show how this can be rectified to get C-phase(ϕ) with probability $(1-\varepsilon)$ using $O(\text{poly}(1/\varepsilon))$ copies of $|M_\phi\rangle$.

Finally putting together lemmas 1,2,3 gives the main result.
