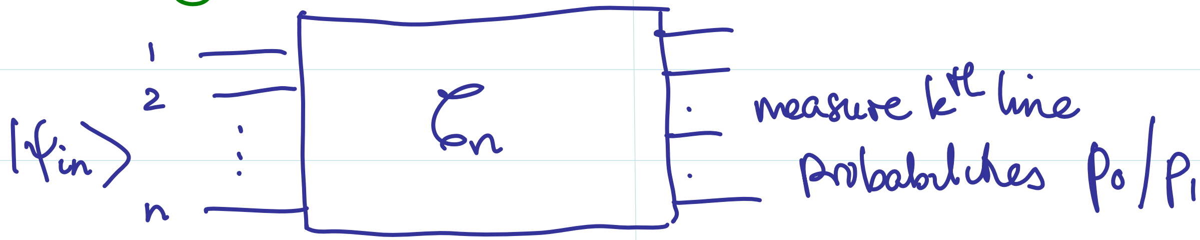
Lie algebras and classical simulation of quantum circuits

Richard Jozsa
DAMTP University of Cambridge UK.

Strong classical simulation



quantum circuit, size $N = \text{poly}(n)$

Given description of C_n & $|\psi_{in}\rangle$ want to classically compute p_0/p_1 (to m digits of accuracy) in poly(n,m) time.

We'll take $|\psi_{in}\rangle$ = any product state $|\alpha_1\rangle|\alpha_2\rangle \ldots |\alpha_n\rangle$

Key example: Clifford circuits (of H, $S = \text{diag}(1\ i)$ & CZ gates)

Key property - C Clifford $\Rightarrow C^\dagger (P_1 \otimes \ldots \otimes P_n) C = P_1' \otimes \ldots \otimes P_n'$ for any Pauli's P_i, & update computable in $O(n)$ time.

Gottesman-Knill theorem (variant)

As above. $\mathcal{C}_n$ = Clifford circuit.
Then strongly classically simulatable.

Easy proof: (not the stabiliser formalism!)

$$|\psi_{out}\rangle = \mathcal{C}_n |\psi_{in}\rangle$$ (and measure e.g. first line)

$$p_0 - p_1 = \langle Z_1 \rangle_{out} = \langle \psi_{in} | \mathcal{C}_n^\dagger (Z \otimes I \otimes \ldots \otimes I) \mathcal{C}_n | \psi_{in} \rangle$$

Now $\mathcal{C}_n = C_N \ldots C_3 C_2 C_1$

So successively conjugate by C_i's to get

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

computable in $O(n)$ time

(and P_i''s computable in $O(N)$-time). $\square$

Now want to generalise this simple formalism ...

Key features: $C^{\dagger}(P_1 \otimes \dots \otimes P_n) C = P_1' \otimes \dots \otimes P_n'$

1. have restricted class of U's that preserve a poly-describable structure $\mathcal{S}$ (here Pauli group) under conjugation and conjugation-update of $\mathcal{S}$ is computable in poly(n) time.

2. for $A \in \mathcal{S}$, $\langle \psi_{in} | A | \psi_{in} \rangle$ computable in poly(n) time.

3. $\mathcal{S}$ contains observables of interest e.g. Z_k.

- don't need $\mathcal{S}$ to be a group.
- seek other mathematical occurrences of these features!
- Lie algebras: Somma, Barnum, Ortiz, Knill quant-ph/060103.

Finite dimensional matrix Lie algebra $\mathcal{A}$ is:

- a vector space of matrices (dimension d) ← d not to be confused with size of matrices!
- closed under bracket $[X,Y] \stackrel{\text{def}}{=} XY - YX$
- If $B_1, \dots B_d$ is basis of matrices for A then have structure constants $[B_i, B_j] = \sum_k c_{ij}^k B_k$
- Associated Lie group $\mathcal{G} = \{ e^X : X \in A \}$

($\mathcal{G}$ will be a group if vector space A is closed under $[\cdot,\cdot]$
cf. BCH formula for Z: $e^X e^Y = e^Z$)

Basic theorem (adjoint representation of Lie group $\mathcal{G}$ on its Lie algebra A)

If $X \in A$ then $e^X \in \mathcal{G}$ has
$$e^{-X} Y e^X \in A \quad \text{for all } Y \in A$$

i.e. A preserved under conjugation by $\mathcal{G}$.

(and this gives a representation of $\mathcal{G}$ on A)

Conjugation update rule

Lemma: adjoint action of e^X on A can be computed (to m digits) in poly(d,m) time (d = dimension of A).

Proof: Basis B_i $i=1,\ldots,d$ $\quad X = \sum_j \xi_j B_j$

Want a_{ij} : $\quad e^X B_i e^{-X} = \sum_j a_{ij} B_j$

Introduce $B_i(t) = e^{tX} B_i e^{-tX}$ $\quad$ so $B_i(0) = B_i$

Then $\dfrac{dB_i}{dt} = [X, B_i(t)] = \sum_{jk} \xi_j c_{ji}^{k} B_k(t)$.

So if $\underline{B}(t) = \begin{pmatrix} B_1(t) \\ \vdots \\ B_d(t) \end{pmatrix}$ $\quad \dfrac{d\underline{B}}{dt} = M\underline{B}$ $\quad M_i^k = \sum_j \xi_j c_{ji}^{k}$

and $\underline{B}(t) = e^{Mt}\,\underline{B}(0)$ & set $t=1$.

So $[a_{ij}] = e^M = I + M + M^2/2! + \cdots$

computable to m digits with $O(m)$ terms

so all in poly(d,m) time. $\square$

Our strategy:

For n qubit lines: associate matrix Lie algebra A_n of dim $d = \text{poly}(n)$
& $X \in A_n$ are $2^n \times 2^n$ sized matrices.

Then have ① for operations $U \in \mathcal{G}$.

If $X \in A_n$ skew-hermitian then e^X unitary.

For ② and ③ need suitably nice choice of matrices in A_n, and $|\psi_{in}\rangle$.

For $|\psi_{in}\rangle$ = any product state

if $X \in A_n$ is tensor product matrix $X = X_1 \otimes \ldots \otimes X_n$ (X_i's 2×2 matrices)

then get ②, and get ③ if A_n contains say Z_k's.

Using this formalism, get Valiant's classically simulatable matchgate circuits

(with $A_n \cong so(2n)$ or $so(2n+1)$ represented by product matrices.)

How it works:

Start with abstract Clifford algebra on $2n$ generators

$c_\mu \quad \mu = 1, \dots, 2n$

$\{c_\mu, c_\nu\} \equiv c_\mu c_\nu + c_\nu c_\mu = 2\delta_{\mu\nu}$ (ACG) anti-commutators!

then

linear span $\{c_\mu\text{'s}\}$ not closed under commutators

$[c_\mu, c_\nu] = c_\mu c_\nu - c_\nu c_\mu = 2 c_\mu c_\nu \quad (\mu \neq \nu) \dots$

But

! linear span $\{c_\mu c_\nu\text{'s} : \mu \neq \nu\}$ is a Lie algebra

closed under $[c_\mu c_\nu, c_\alpha c_\beta] \overset{\text{def}}{=} c_\mu c_\nu c_\alpha c_\beta - c_\alpha c_\beta c_\mu c_\nu$

by virtue of anti-commutation relations!

[Fact: this Lie algebra, dim $d = 2n(2n-1)/2 = O(n^2)$

is isomorphic to $so(2n)$ – same structure constants.]

So take $A_n = \text{span}\{c_\mu c_\nu\text{'s} : \mu \neq \nu\}$ seek

representation by tensor product matrices.

Jordan-Wigner representation

k^{th} slot

$$\begin{cases} c_1 = XI..I & c_3 = ZXI..I & \cdots & c_{2k-1} = Z..ZXI.I \\ c_2 = YI..I & c_4 = ZYI..I & & c_{2k} = Z..ZYI..I & \cdots \end{cases}$$

'line 1' 'line 2' 'line k'

c_μ's all Hermitian and anti-commute

So $c_\mu c_\nu$ anti-Hermitian so

$$U = e^{\sum_{\mu,\nu} a_{\mu\nu} c_\mu c_\nu} \quad \underline{\text{unitary}}$$

for real (antisymmetric) $a_{\mu\nu}$'s.

Also have $Z_k = -i\, c_{2k-1} c_{2k} \in \mathcal{A}_n$

So immediately get

Theorem: any circuit of gates $U = e^{\sum_{\mu\nu} a_{\mu\nu} c_\mu c_\nu}$ with $|\psi_{in}\rangle$ = any product state is strongly classically simulatable. $\square$

What are these gates U?

- If $c_\mu c_\nu$ has μ from line k and ν from line l then $c_\mu c_\nu$ acts across all lines $k \leftrightarrow l$.
- If μ, ν are indices from nearest-neighbour lines $k, k+1$ then get 2-qubit gates of the form:

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

in $SU(2)$

in physics this gives classical simulation of non-interacting fermions.

[Fact: general $U = e^{\sum a_{\mu\nu} c_\mu c_\nu}$ is always $O(n^3)$ sized circuit of nearest-neighbour $G(A,B)$'s.

$\sim$ Euler angle representation of $SO(2n)$ rotations in terms of 2-dim rotations.]

A further bonus:

span(c_μ's) not a Lie algebra, span($c_\mu c_\nu$'s) is a Lie algebra

and! span(c_μ's, $c_\mu c_\nu$'s) is a Lie algebra too ($\cong so(2n+1)$)

closed under [,] by virtue of anti-commutation relations again.

So with JW formalism, can strongly classically simulate U's of the form

$$U = e^{[\sum k_\alpha c_\alpha + \sum a_{\mu\nu} c_\mu c_\nu]}$$

In particular for first line have

$$c_1 = X_1 \quad c_2 = Y_1 \quad i c_1 c_2 = Z_1$$

So have arbitrary $aX_1 + bY_1 + cZ_1$ exponents

i.e. arbitrary 1-qubit gates on first line anywhere

in a n.n. $G(A,B)$ circuit.

given also by Valiant in his matchgate formalism.

[Linear terms for other (k^{th}) lines give gates

acting across all lines $1 \leftrightarrow k$.]

Further issues?

- other Lie algebras / groups?

- other mathematical formalisms for generating examples of 1 2 3?
  (discrete examples like Clifford circuits?..)

- generalisation of JW formalism to dimensions $d \geq 3$?