Title: Matchgates and the classical simulation of associated quantum circuits

Date: Apr 28, 2008 02:50 PM

URL: http://pirsa.org/08040048

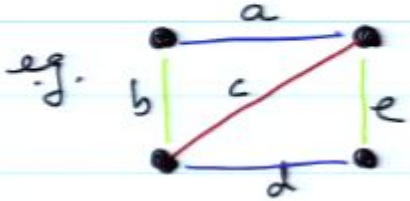
Abstract: Some years ago Valiant introduced a notion of \'matchgate\' and \'holographic algorithm\', based on properties of counting perfect matchings in graphs. This provided some new poly-time classical algorithms and embedded in this formalism, he recognised a remarkable class of quantum circuits (arising when matchgates happen to be unitary) that can be classically efficiently simulated. Subsequently various workers (including Knill, Terhal and DiVincenzo, Bravyi) showed that these results can be naturally interpreted in terms of the formalism of fermionic quantum computation. In this talk I will outline how unitary matchgates and their simulability arise from considering a Clifford algebra of anticommuting symbols, and then I\'ll discuss some avenues for further generalisation and interesting properties of matchgate circuits. In collaboration with Akimasa Miyake, University of Innsbruck.

# Matchgates and Classical Simulation of associated quantum circuits

Richard Jozsa
&
Akimasa Miyake

# Valiant's theory of matchgates & holographic algorithms

## Perfect matchings in graphs




e.g. (weighted) (planar) graph

count perfect matchings } #P-hard in general (bipartite)
polytime for planar graphs!

existence of perfect matching is in P

More generally:

weighted graph: $\mathrm{PerfM}(G) = \sum_{\substack{M \\ \text{perf matching}}} \prod_{(i,j)\in M} w_{ij}$

(all $w$'s $= 1$ $\rightsquigarrow$ counting)

Planar $G$: FKT algorithm computes $\mathrm{PerfM}(G)$ in poly time.

(~ Pfaffian of an antisym incidence matrix)

Idea of matchgate (planar):

Weighted graph $G$ with "input" $(1,\dots,n)$ and "output" $(1,\dots,m)$ nodes

$$M^{i_1\dots i_n}_{j_1\dots j_m} = \mathrm{Perf}M\left(G - \begin{matrix}\text{omitted nodes}\\ \text{i.e. indices} = 1\end{matrix}\right) \qquad i,j = 0,1$$

Circuits of these tensors $\rightsquigarrow$ contraction of terms corresponds to same problem on larger "concatenated" graph

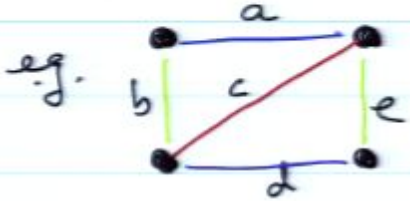
So contraction is poly-time computable too.

Matchgate identities: set of (quadratic) equations on arbitrary matrix's entries guaranteeing that it is a matchgate for some $G$.

$\longrightarrow$ get some unitary matchgates...

# Valiant's theory of matchgates & holographic algorithms

## Perfect matchings in graphs




e.g. (weighted) (planar) graph

count perfect matchings } #P-hard in general (bipartite)
polytime for planar graphs!

existence of perfect matching is in P

More generally:

weighted graph: $\mathrm{PerfM}(G) = \sum_{\substack{M \\ \text{perf matching}}} \prod_{(i,j)\in M} w_{ij}$

(all $w$'s $= 1$ $\rightsquigarrow$ counting)

Planar $G$: FKT algorithm computes $\mathrm{PerfM}(G)$ in poly time.

(~ Pfaffian of an antisym incidence matrix)

Idea of matchgate (planar):

Weighted graph $G$ with "input" $(1,\dots,n)$ and "output" $(1,\dots,m)$ nodes

$$M^{i_1\dots i_n}_{j_1\dots j_m} = \mathrm{Perf}M\left(G - \begin{matrix}\text{omitted nodes}\\ \text{i.e. indices} = 1\end{matrix}\right) \qquad i,j = 0,1$$

Circuits of these tensors $\rightsquigarrow$ contraction of terms corresponds to same problem on larger "concatenated" graph

So contraction is poly-time computable too.

Matchgate identities: set of (quadratic) equations on arbitrary matrix's entries guaranteeing that it is a matchgate for some $G$.

$\longrightarrow$ get some unitary matchgates...

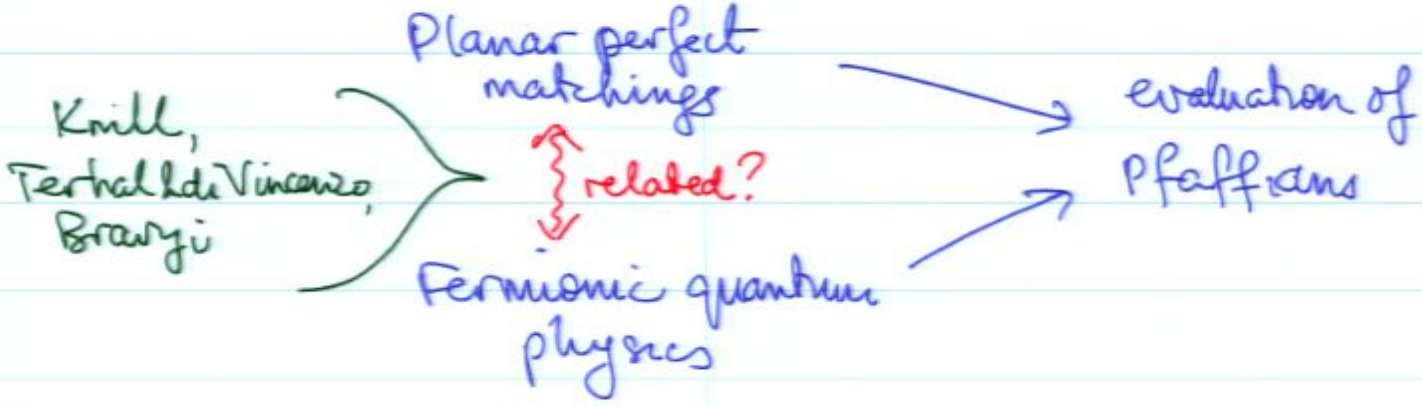
"Holographic" Algorithms:

reduce other problems to such matchgate contractions.

Potentially expon. large sums (Pfaffians/Det's) but get "expon many" cancellations ~ "interferences".

like quantum computing but have all classical poly-time.

Enter: some physics! –



## Valiant's theorem (classical simulation of unitary matchgate circuits)

Consider 2-qubit gates $G(A,B) = \begin{bmatrix} p & 0 & 0 & q \\ 0 & w & x & 0 \\ 0 & y & z & 0 \\ r & 0 & 0 & s \end{bmatrix}$ $A = \begin{bmatrix} p & q \\ r & s \end{bmatrix}$ $B = \begin{bmatrix} w & x \\ y & z \end{bmatrix}$

with $A, B$ both in $su(2)$ (or $U(2)$ with same determinant)

ie. $A$ acts in 00/11 and $B$ acts in 01/10 subspaces.

Consider any (polysized) circuit of $G(A,B)$ gates with:

- $G(A,B)$ acts on nearest-neighbour (nn) lines only
- input is any product state
- final measurement is in $Z_k$ basis on any single line $k$

Then output can be classically efficiently simulated.

More precisely: can compute $\langle \psi_{out} | Z_k | \psi_{out} \rangle = P_0 - P_1$ to $k$ digits in poly$(n,k)$ time. □

will give proof & further significance of n.n. condition & further generalisations.

Warning: non-n.n. use of $G(A,B)$ gates not allowed !!

SWAP = $G(I,X)$ not included (fails by just a minus sign--)

But $S = G(Z,X) = G(Z,I)\,G(I,X) = CZ \cdot SWAP$
is allowed.

Theorem:

(a) n.n. $G(A,B)$ gates with SWAP is universal for quantum computing.

More strongly (limited use of SWAP suffices):

(b) $G(A,B)$ gates acting on n.n. and next-n.n. is efficiently universal for quantum computing.

Proof: (nice..) do at end if time ...

# Valiant's theorem (classical simulation of unitary matchgate circuits)

Consider 2-qubit gates $G(A,B) = \begin{bmatrix} p & 0 & 0 & q \\ 0 & w & x & 0 \\ 0 & y & z & 0 \\ r & 0 & 0 & s \end{bmatrix}$ $A = \begin{bmatrix} p & q \\ r & s \end{bmatrix}$ $B = \begin{bmatrix} w & x \\ y & z \end{bmatrix}$

with $A, B$ both in $su(2)$ (or $U(2)$ with same determinant)

ie. $A$ acts in 00/11 and $B$ acts in 01/10 subspaces.

Consider any (polynomial) circuit of $G(A,B)$ gates with:

- $G(A,B)$ acts on nearest-neighbour (nn) lines only
- input is any product state
- final measurement is in $Z_k$ basis on any single line $k$

Then output can be classically efficiently simulated.

More precisely: can compute $\langle \psi_{out} | Z_k | \psi_{out} \rangle = P_0 - P_1$ to $k$ digits in poly$(n,k)$ time. □

will give proof & further significance of n.n. condition & further generalisations.

Warning: non-n.n. use of $G(A,B)$ gates not allowed !!

SWAP = $G(I,X)$ not included (fails by just a minus sign--)

But $S = G(Z,X) = G(Z,I)\,G(I,X) = CZ.\,SWAP$
is allowed.

Theorem:

(a) n.n. $G(A,B)$ gates with SWAP is universal for quantum computing.

More strongly (limited use of SWAP suffices):

(b) $G(A,B)$ gates acting on n.n. and next-n.n. is efficiently universal for quantum computing.

Proof: (nice..) do at end if time ...

Back to proof of Valiant's theorem:

For n qubit lines start with operators

$a_1, \ldots, a_n$ : $\{a_i, a_j\} \equiv a_i a_j + a_j a_i = 0 = \{a_i^+, a_j^+\}$

and $\{a_i, a_j^+\} = \delta_{ij}$

Introduce $c_{2k-1} = a_k + a_k^+$

$c_{2k} = (a_k - a_k^+)/i$

} 2n Hermitian operators.

So $\{c_\mu, c_\nu\} = 2\delta_{\mu\nu} I \quad \mu, \nu = 1, \ldots, 2n$ } Clifford Algebra $C_{2n}$

General vector in this algebra is

$$\sum_{i_1 < \ldots < i_k} a_{i_1 \ldots i_k} c_{i_1} \ldots c_{i_k}$$

maybe empty

Hence $2^{(2n)} = (2^n)^2$ dimensional as a vector space

Matrix representations ~ $(2^n \times 2^n)$-matrices.

Warning: non-n.n. use of $G(A,B)$ gates not allowed !!

SWAP = $G(I,X)$ not included (fails by just a minus sign--)

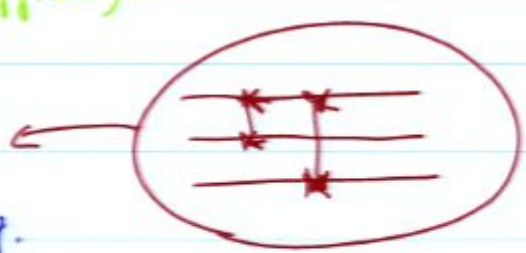
But $S = G(Z,X) = G(Z,I)\,G(I,X) = CZ.\,SWAP$
is allowed.

Theorem:

(a) n.n. $G(A,B)$ gates with SWAP is universal for quantum computing.

More strongly (limited use of SWAP suffices):

(b) $G(A,B)$ gates acting on n.n. and next-n.n. is efficiently universal for quantum computing.



Proof: (nice..) do at end if time ...

## Valiant's theorem (classical simulation of unitary matchgate circuits)

Consider 2-qubit gates $G(A,B) = \begin{bmatrix} p & 0 & 0 & q \\ 0 & w & x & 0 \\ 0 & y & z & 0 \\ r & 0 & 0 & s \end{bmatrix}$ $A = \begin{bmatrix} p & q \\ r & s \end{bmatrix}$ $B = \begin{bmatrix} w & x \\ y & z \end{bmatrix}$

with $A, B$ both in $su(2)$ (or $U(2)$ with same determinant)

ie. $A$ acts in 00/11 and $B$ acts in 01/10 subspaces.

Consider any (polynomial) circuit of $G(A,B)$ gates with:

- $G(A,B)$ acts on nearest-neighbour (nn) lines only
- input is any product state
- final measurement is in $Z_k$ basis on any single line $k$

Then output can be classically efficiently simulated.

More precisely: can compute $\langle \psi_{out} | Z_k | \psi_{out} \rangle = P_0 - P_1$ to $k$ digits in poly$(n,k)$ time. □

will give proof & further significance of n.n. condition & further generalisations.

Warning: non-n.n. use of $G(A,B)$ gates not allowed !!

SWAP = $G(I,X)$ not included (fails by just a minus sign--)

But $S = G(Z,X) = G(Z,I)\,G(I,X) = CZ \cdot SWAP$
is allowed.

Theorem:

(a) n.n. $G(A,B)$ gates with SWAP is universal for quantum computing.

More strongly (limited use of SWAP suffices):

(b) $G(A,B)$ gates acting on n.n. and next-n.n. is efficiently universal for quantum computing.

Proof: (nice..) do at end if time ...

Back to proof of Valiant's theorem:

For n qubit lines start with operators

$a_1, \ldots, a_n$ : $\{a_i, a_j\} \equiv a_i a_j + a_j a_i = 0 = \{a_i^+, a_j^+\}$

and $\{a_i, a_j^+\} = \delta_{ij}$

Introduce $c_{2k-1} = a_k + a_k^+$

$c_{2k} = (a_k - a_k^+)/i$

} 2n Hermitian operators.

So $\{c_\mu, c_\nu\} = 2\delta_{\mu\nu} I \quad \mu, \nu = 1, \ldots, 2n$ } Clifford Algebra $C_{2n}$

General vector in this algebra is

$$\sum_{i_1 < \ldots < i_k} a_{i_1 \ldots i_k} c_{i_1} \ldots c_{i_k}$$

maybe empty

Hence $2^{(2n)} = (2^n)^2$ dimensional as a vector space

Matrix representations ~ $(2^n \times 2^n)$-matrices.

Now do some pure algebra (no actual matrices yet..)

Quadratic Hamiltonians $H = i \sum_{\mu \neq 0=1}^{2n} h_{\mu\nu} c_\mu c_\nu$

Note $c_\mu c_\nu = -c_\nu c_\mu$ so wlog $h_{\mu\nu} = -h_{\nu\mu}$

and then hermitian $\Rightarrow$ $h_{\mu\nu}$ real

i.e. $h_{\mu\nu}$ is real antisymmetric $(2n \times 2n)$ matrix

Basic theorem: H as above. $U = e^{iH}$ unitary operation.

Then $U^\dagger c_\mu U = \sum_{\nu=1}^{2n} R_{\mu\nu} c_\nu$

with $R \in SO(2n)$ [In fact $R = e^{2h}$]

(and get all $SO(2n)$ in this way).

Significance. $U^\dagger c_\mu U$ could finish up anywhere in expon-big $2^{2n}$-dimensional linear space $\mathcal{C}_{2n}$ (cf $e^{iH}$ ~ powers of all $c_\nu$'s etc..)

but happens to stay in $2n$ (poly sized!) dimensions!!

**Proof idea:**

Consider $U(t) = e^{iHt}$ !

$$c_\mu(t) = U(t)\, c_\mu\, U(t)^\dagger$$

Then $$\frac{dc_\mu}{dt} = [H, c_\mu]$$

But: $[c_\mu, c_{\nu_1} c_{\nu_2}] = c_\mu c_{\nu_1} c_{\nu_2} - c_{\nu_1} c_{\nu_2} c_\mu = 0$ if $\mu \neq \nu_1, \nu_2$

$[c_\mu, c_\mu c_\nu] =$ -- $= 2c_\nu$

So $$\frac{dc_\mu}{dt} = 2h_{\mu\nu} c_\nu$$ and result follows immediately at $t=1$

(recalling: infinitesimal rotations $\equiv$ antisym matrices) //

Strategy for Valiant's classical simulation result:

Find a Hermitian rep. of $\mathfrak{so}_{2n}$ on n-qubit operators ($2^n \times 2^n$ matrices)

So quadratic Hamiltonian $\rightsquigarrow$ a class of n-qubit gates

Let M be any circuit of these; $|\psi_{out}\rangle = M|\psi_{in}\rangle$

Then for each $\mu$

$$\langle c_\mu \rangle_{out} = \langle \psi_{in}|M^\dagger c_\mu M|\psi_{in}\rangle = \sum_{\mu=1}^{2n} a_{\mu\nu}\langle \psi_{in}|c_\nu|\psi_{in}\rangle$$

where $a_{\mu\nu}$ = product of all $so(2n)$ matrices coming from M.

so this is poly-time computable.

Then if $|\psi_{in}\rangle$ is product state and

$c_\mu$ are product operators on n-qubits

we get: $\langle \psi_{in}|c_\mu|\psi_{in}\rangle$ & hence $\langle c_\mu \rangle_{out}$

are poly-time computable.

Now do some pure algebra (no actual matrices yet..)

Quadratic Hamiltonians $H = i \sum_{\mu \neq \nu = 1}^{2n} h_{\mu\nu} c_\mu c_\nu$

Note $c_\mu c_\nu = -c_\nu c_\mu$ so wlog $h_{\mu\nu} = -h_{\nu\mu}$

and then hermitian $\Rightarrow$ $h_{\mu\nu}$ real

i.e. $h_{\mu\nu}$ is real antisymmetric $(2n \times 2n)$ matrix

Basic theorem: H as above. $U = e^{iH}$ unitary operation.

Then $U^\dagger c_\mu U = \sum_{\nu=1}^{2n} R_{\mu\nu} c_\nu$

with $R \in SO(2n)$ [In fact $R = e^{2h}$]

(and get all $SO(2n)$ in this way).

Significance. $U^\dagger c_\mu U$ could finish up anywhere in exponentially big $2^{2n}$-dimensional linear space $\mathcal{C}_{2n}$ (cf $e^{iH}$ ~ powers of all $c_\nu$'s etc..)

but happens to stay in $2n$ (poly sized!) dimensions!!

**Proof idea:**

Consider $U(t) = e^{iHt}$ !

$$C_\mu(t) = U(t)\, C_\mu\, U(t)^\dagger$$

Then $$\frac{dC_\mu}{dt} = [H, C_\mu]$$

But: $[C_\mu, C_{\nu_1} C_{\nu_2}] = C_\mu C_{\nu_1} C_{\nu_2} - C_{\nu_1} C_{\nu_2} C_\mu = 0$ if $\mu \neq \nu_1, \nu_2$

$[C_\mu, C_\mu C_\nu] =$ -- $= 2C_\nu$

So $$\frac{dC_\mu}{dt} = 2h_{\mu\nu} C_\nu$$ and result follows immediately at $t = 1$

(recalling: infinitesimal rotations $\equiv$ antisym matrices) //

Strategy for Valiant's classical simulation result:

Find a Hermitian rep. of $\mathfrak{so}_{2n}$ on n-qubit operators ($2^n \times 2^n$ matrices)

So quadratic Hamiltonian $\rightsquigarrow$ a class of n-qubit gates

Let M be any circuit of these; $|\psi_{out}\rangle = M|\psi_{in}\rangle$

Then for each $\mu$

$$\langle c_\mu \rangle_{out} = \langle \psi_{in}|M^\dagger c_\mu M|\psi_{in}\rangle = \sum_{\mu=1}^{2n} a_{\mu\nu}\langle \psi_{in}|c_\nu|\psi_{in}\rangle$$

where $a_{\mu\nu}$ = product of all $so(2n)$ matrices coming from M.

so this is poly-time computable.

Then if $|\psi_{in}\rangle$ is product state and

$c_\mu$ are product operators on n-qubits

we get: $\langle \psi_{in}|c_\mu|\psi_{in}\rangle$ & hence $\langle c_\mu \rangle_{out}$

are poly-time computable.

But really want $\langle Z_k \rangle_{out}$ ($k^{th}$ line) e.g. $Z_1$

Note: $\mathcal{C}_{2n}$ spans all $2^n \times 2^n$ matrices (recall $\dim(\mathcal{C}_{2n}) = 2^n 2^n$)

so $Z_k$ = some poly in $C_\mu$'s

If degree of this poly is bounded (indep of $n$) then $\langle Z_k \rangle_{out}$ still poly-time computable:

e.g. if $Z_1 = C_1 C_2$

$MM^+$

then $\langle Z_1 \rangle_{out} = \langle \psi_{in} | M^+ C_1 C_2 M | \psi_{in} \rangle$

$$= \langle \psi_{in} | \sum_{\nu_1, \nu_2} a_{1\nu_1} a_{2\nu_2} C_{\nu_1} C_{\nu_2} | \psi_{in} \rangle$$

$O(n^2)$ product operators

product state

Strategy for Valiant's classical simulation result:

Find a Hermitian rep. of $\mathfrak{so}_{2n}$ on n-qubit operators ($2^n \times 2^n$ matrices)

So quadratic Hamiltonian $\rightsquigarrow$ a class of n-qubit gates

Let M be any circuit of these; $|\psi_{out}\rangle = M|\psi_{in}\rangle$

Then for each $\mu$

$$\langle c_\mu \rangle_{out} = \langle \psi_{in}|M^\dagger c_\mu M|\psi_{in}\rangle = \sum_{\mu=1}^{2n} a_{\mu\nu}\langle \psi_{in}|c_\nu|\psi_{in}\rangle$$

where $a_{\mu\nu}$ = product of all $so(2n)$ matrices coming from M.

so this is poly-time computable.

Then if $|\psi_{in}\rangle$ is product state and

$c_\mu$ are product operators on n-qubits

we get: $\langle \psi_{in}|c_\mu|\psi_{in}\rangle$ & hence $\langle c_\mu \rangle_{out}$

are poly-time computable.

**Proof idea:**

Consider $U(t) = e^{iHt}$ !

$$C_\mu(t) = U(t)\, C_\mu\, U(t)^\dagger$$

Then $$\frac{dC_\mu}{dt} = [H, C_\mu]$$

But: $[C_\mu, C_{\nu_1} C_{\nu_2}] = C_\mu C_{\nu_1} C_{\nu_2} - C_{\nu_1} C_{\nu_2} C_\mu = 0$ if $\mu \neq \nu_1, \nu_2$

$[C_\mu, C_\mu C_\nu] =$ -- $= 2C_\nu$

So $$\frac{dC_\mu}{dt} = 2h_{\mu\nu} C_\nu$$ and result follows immediately at $t = 1$

(recalling: infinitesimal rotations $\equiv$ antisym matrices) //

Now do some pure algebra (no actual matrices yet..)

Quadratic Hamiltonians $H = i \sum_{\mu \neq \nu = 1}^{2n} h_{\mu\nu} c_\mu c_\nu$

Note $c_\mu c_\nu = -c_\nu c_\mu$ so wlog $h_{\mu\nu} = -h_{\nu\mu}$

and then hermitian $\Rightarrow$ $h_{\mu\nu}$ real

i.e. $h_{\mu\nu}$ is real antisymmetric $(2n \times 2n)$ matrix

Basic theorem: H as above. $U = e^{iH}$ unitary operation.

Then $U^\dagger c_\mu U = \sum_{\nu=1}^{2n} R_{\mu\nu} c_\nu$

with $R \in SO(2n)$ [In fact $R = e^{2h}$]

(and get all $SO(2n)$ in this way).

Significance. $U^\dagger c_\mu U$ could finish up anywhere in expon-big $2^{2n}$-dimensional linear space $\mathcal{C}_{2n}$ (cf $e^{iH}$ ~ powers of all $c_i$'s etc..)

but happens to stay in $2n$ (poly sized!) dimensions!!

But really want $\langle Z_k \rangle_{out}$ ($k^{th}$ line) e.g. $Z_1$

Note: $\mathcal{C}_{2n}$ spans all $2^n \times 2^n$ matrices (recall $\dim(\mathcal{C}_{2n}) = 2^n 2^n$)

so $Z_k$ = some poly in $C_\mu$'s

If degree of this poly is bounded (indep of $n$) then $\langle Z_k \rangle_{out}$ still poly-time computable:

e.g. if $Z_1 = C_1 C_2$

then $\langle Z_1 \rangle_{out} = \langle \psi_{in} | M^\dagger C_1 C_2 M | \psi_{in} \rangle$ ($M M^\dagger$)

$$= \langle \psi_{in} | \sum_{\nu_1, \nu_2} a_{1\nu_1} a_{2\nu_2} C_{\nu_1} C_{\nu_2} | \psi_{in} \rangle$$

$O(n^2)$ product operators; product state

Jordan-Wigner rep. of $C_{2n}$ on $n$ qubits

(product operators and Pauli's too!)

$C_1 = X I \cdots I$

$C_2 = Y I \cdots I$

$C_3 = Z X I \cdots I$

$C_4 = Z Y I \cdots I$

$C_{2k-1} = Z \cdots Z X I \cdots I$

$C_{2k} = Z \cdots Z Y \underset{\uparrow k^{th} \text{ slot}}{I} \cdots I$

$[a_k = Z \cdots Z (X+iY) I \cdots I]$

Easy to check $C_\mu C_\nu + C_\nu C_\mu = 2\delta_{\mu\nu} I$

Also $Z_k = i C_{2k-1} C_{2k}$

Hence: $\langle Z_k \rangle_{out}$ is poly time computable for any product state input & any circuit of $U = e^{iH}$'s with $H \sim$ quadratic ham.

But: what do these unitary $n$-qubit gates look like?

First look at just qubit lines 1 & 2:

Quadratic terms from $c_1, c_2, c_3, c_4$ (equiv: quadratic hermitian combinations of $a_1, a_2, a_1^\dagger, a_2^\dagger$)

Get:

| | |
|---|---|
| $i c_1 c_2$ | $ZI$ |
| $i c_1 c_3$ | $YX$ |
| $i c_1 c_4$ | $YY$ |
| $i c_2 c_3$ | $XX$ |
| $i c_2 c_4$ | $XY$ |
| $i c_3 c_4$ | $IZ$ |

- all preserve 00/11 & 01/10 subspaces
- all trace free; six parameters' worth.

So get $su(2) \oplus su(2)$ in the subspaces

e.g. can make $X, Y, Z$ in each subspace

(eg $\frac{1}{2}(XX+YY)$ is $X$ acting in 01/10, maps 00/11 to zero.)

Hence: get precisely Valiant's $G(A,B)$'s on lines 1 & 2.

But: what about all other general quadratic $H$'s, using distant lines & more $c_\mu$'s?

i.e. Valiant nn gates are just part of a larger set of gates that can act on more distant lines, but $G(A,B)$'s themselves on distant line pairs are <u>not</u> in the set!

Warning: if a nn hamiltonian term e.g. $a_1 a_2$ is replaced by non-nn, $a_1 a_3$ say, we still have a quadratic hamiltonian, but <u>do not</u> get same 2-qubit gate $U_{12}$ acting on lines 1 & 3!

$(k=1)\ (k=2)$

e.g. $C_2 C_4 \approx X_1 Y_2$

but $C_2 C_6 \approx X_1 Z_2 Y_3$ !

$(k=1)\ (k=3)$

**Theorem:** For any $H = i \sum_{\mu,\nu=1}^{2n} h_{\mu\nu} c_\mu c_\nu$ we have that

$U = e^{iH}$ (on n qubits) is a circuit of n.n. $G(A,B)$ gates.

i.e. $U = U_m U_{m-1} \cdots U_1$ with each $U_j = e^{iH_j}$ having

$H_j = i \sum h_{\nu_1,\nu_2} c_{\nu_1} c_{\nu_2}$ summed over only 2 n.n. lines $(2k-1, 2k, 2k+1, 2k+2)$

i.e. get nothing extra new from non-n.n. quadratic hamiltonians.

Proof idea

Had $U^\dagger c_\mu U = \sum R_{\mu\nu} c_\nu$

$R \in SO(2n) \rightsquigarrow$ decompose into Euler angles

$R = R_1 \cdots R_K \quad K \sim O(n^2)$

each $R_j$ is rotation in 2-dim plane only.

So $R_j \rightsquigarrow U_j = e^{iH_j}$ $H_j = i k c_{\nu_1} c_{\nu_2}$ involving only two $c_\nu$'s

and then get $U = U_1 \cdots U_K$ too.

i.e. Valiant nn gates are just part of a larger set of gates that can act on more distant lines, but $G(A,B)$'s themselves on distant line pairs are <u>not</u> in the set!

Warning: if a nn hamiltonian term e.g. $q_1 q_2$ is replaced by non-nn, $q_1 q_3$ say, we still have a quadratic hamiltonian, but <u>do not</u> get same 2-qubit gate $U_{12}$ acting on lines 1 & 3!

$(k=1)\ (k=2)$

e.g. $C_2 C_4 \approx X_1 V_2$

but $C_2 C_6 \approx X_1 Z_2 V_3$ !

$(k=1)\ (k=3)$

**Theorem:** For any $H = i \sum_{\mu,\nu=1}^{2n} h_{\mu\nu} c_\mu c_\nu$ we have that

$U = e^{iH}$ (on n qubits) is a circuit of n.n. $G(A,B)$ gates.

i.e. $U = U_m U_{m-1} \cdots U_1$ with each $U_j = e^{iH_j}$ having

$H_j = i \sum h_{\nu_1,\nu_2} c_{\nu_1} c_{\nu_2}$ summed over only 2 n.n. lines $(2k-1, 2k, 2k+1, 2k+2)$

i.e. get nothing extra new from non-n.n. quadratic hamiltonians.

Proof idea

Had $U^\dagger c_\mu U = \sum R_{\mu\nu} c_\nu$

$R \in SO(2n) \rightsquigarrow$ decompose into Euler angles

$R = R_1 \cdots R_K \quad K \sim O(n^2)$

each $R_j$ is rotation in 2-dim plane only.

So $R_j \rightsquigarrow U_j = e^{iH_j}$ $H_j = i k c_{\nu_1} c_{\nu_2}$ involving only two $c_\nu$'s

and then get $U = U_1 \cdots U_K$ too.

# Clifford Algebras and Clifford Operations

Recall Clifford operation $C(P_1 \otimes .. \otimes P_n)C^+ = P_1' \otimes .. \otimes P_n'$

Recall Clifford algebra relations $c_\mu c_\nu + c_\nu c_\mu = 2\delta_{\mu\nu} I$ ⊛

Recall Jordan-Wigner rep. $c_\mu$'s are Pauli products.

Fact: if $c_\mu$'s satisfy ⊛ then so do $\tilde{c}_\mu = U c_\mu U^+$ for any unitary $U$.

Recall:
Classical simulation result relied on Clifford algebra quadratic hamiltonian property plus
Product structure of J-W rep (related to product state inputs)
Clifford operations $U = C$ preserve both aspects!

So: play same game with new rep. $\tilde{c}_\mu = T_n c_\mu T_n^+$
where $T_n$ is any n-qubit Clifford operation.

Quadratic hamiltonians & exponentials →
$\tilde{U}_{new} = T U_{old} T^+$ too.

Also want:

- $Z_1$ (and $Z_k$'s) should be bounded-degree polys in $\tilde{C}_\mu$'s
  (previously had quadratic; poly simulation cost depends on this degree.)
- We want to identify suitably local (K-local) new gates $\tilde{U}_{new}$ (not just big global n-qubit gates) for new basic gates.
  e.g. might require Valiant's n.n. $G(A,B)$'s on lines $i, i+1$ to conjugate into a local gate of K lines around $i$.

Note: Clifford $T_n$'s need not be "translationally symmetric" across the n lines and may vary with n.
So can get classically simulatable circuits that have different gates allowed on different sets of lines.

Since new gates are $T(\text{old})T^\dagger$'s we can think of new simulated circuits as same as old ones but input states are now $T|\psi_{in,old}\rangle$ (entangled, not products now) and final measurement is now $TZ_kT^\dagger$ (not just $Z_k$)
i.e. we can simulate Valiant's original circuits but now on certain entangled inputs too with corresponding enlargement of output observables to certain (multi-line) observables.
Examples: explicit choices of Clifford $T_n$'s
— not nice so far...

Thm: G(A,B) gates acting n.n., next-n.n. and next-next-n.n. are universal for quantum computation.

↖ consider first..

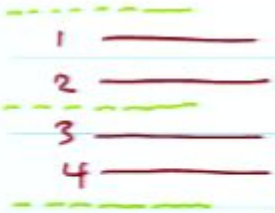
Proof: Given any polysized quantum circuit assume wlog it comprises n.n. CZ's and 1-qubit gates A.

Re-code input 0's & 1's as 00's & 11's (doubling number of lines)
Then whole computation (with suitably coded gate operations) stays in 00/11 subspaces of line pairs (12), (34), (56)...

On any such pair can do 1-qubit gate A as n.n. G(A,A).

Hence it suffices to show how to do CZ encoded on n.n. pairs eg (12) (34)

CZ acting on 00/11 subspaces of n.n. line pairs:




$$CZ_{23} = G(Z,I)_{23} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

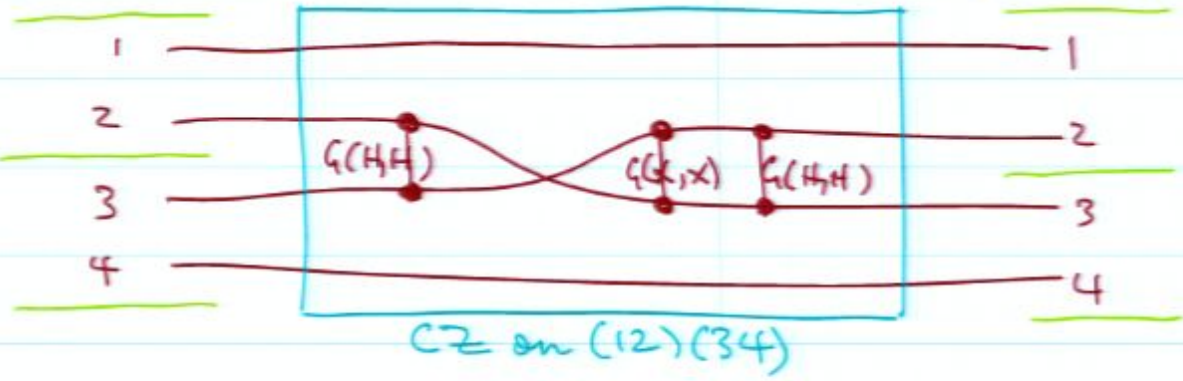
acts as $x11y \to -x11y$

$$x\begin{matrix}01\\10\\00\end{matrix}y \to x\begin{matrix}01\\10\\00\end{matrix}y$$

Hence works as encoded CZ on all $xx/yy$ quadruples.

Finally note: $G(Z,I) = G(H,H)\,G(X,I)\,G(H,H)$

$\to = G(X,X)G(I,X) = G(XX)SWAP$



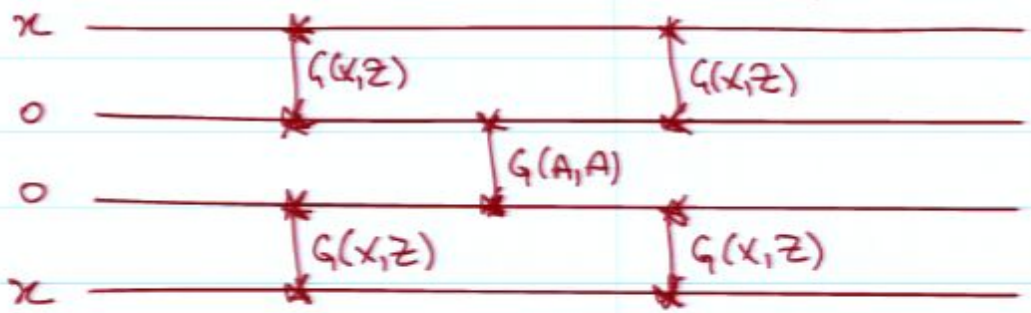
Note that SWAP used only on "cross-over" pairs
of encoding pairs 12|34|56|.. i.e. on (23), (45), (6,7) etc.
Hence never get SWAP ladders moving any line more
than one place distant.
So: straightening out all $\times$ crossings will move
$G(A,B)_{n.n.}$'s lines at most one further apart at each end
i.e. get $G(A,B)$ on n.n, next-n.n. or next-next-n.n.
but never any further.

Better Encoding:

$0 \longrightarrow$ quadruple $|0000\rangle$

$1 \longrightarrow$ $|1001\rangle$

CZ as above but now A done by:




Now never move both ends so get universality of n.n. & next-n.n. gates.

Can we extend cl. simulatability from n.n. to next-n.n.?

Recall BQP ~ output probs $\geq 3/4$ or $\leq \frac{1}{4}$ (bounded away from $\frac{1}{2}$)

Introduce PQP ~ output probs $\geq \frac{1}{2}+\frac{1}{2^n}$ or $\leq \frac{1}{2}-\frac{1}{2^n}$ (input size $=n$)

Can easily see $NP \subseteq PP \subseteq PQP$

Introduce $V_{n.n.}$ = PQP languages with n.n. $G(A,B)$ PQP-circuits.

Then Valiant thm $\Rightarrow$ $V_{n.n.} \subseteq P$

Universality thm $\Rightarrow$ all PQP $\approx$ n.n & nextn.n. $G(A,B)$ circuits

So <u>if</u> n.n/nextn.n. $G(A,B)$ PQP-circuits are cl. sim'ble

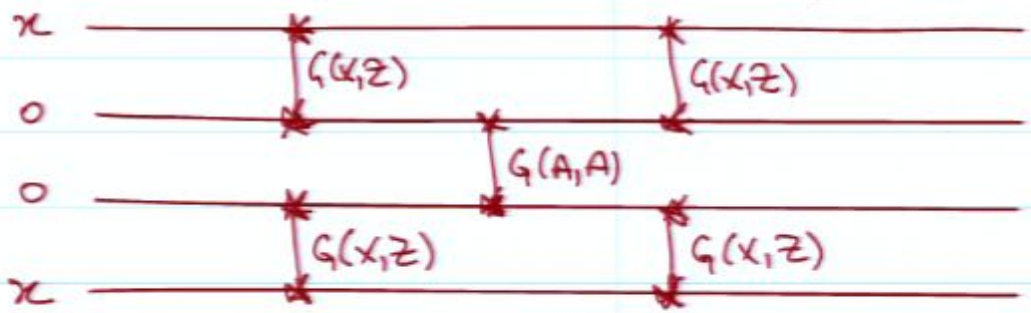
<u>then</u> $P = NP = PP$ implausible! ---

Better Encoding:

$0 \longrightarrow$ quadruple $|0000\rangle$

$1 \longrightarrow$ $|1001\rangle$

CZ as above but now A done by:




Now never move both ends so get universality of n.n. & next-n.n. gates.

Can we extend cl. simulatability from n.n. to next-n.n.?

Recall BQP ~ output probs $\geq 3/4$ or $\leq \frac{1}{4}$ (bounded away from $\frac{1}{2}$)

Introduce PQP ~ output probs $\geq \frac{1}{2}+\frac{1}{2^n}$ or $\leq \frac{1}{2}-\frac{1}{2^n}$ (input size $=n$)

Can easily see $NP \subseteq PP \subseteq PQP$

Introduce $V_{n.n.}$ = PQP languages with n.n. $G(A,B)$ PQP-circuits.

Then Valiant thm $\Rightarrow$ $V_{n.n.} \subseteq P$

Universality thm $\Rightarrow$ all PQP $\approx$ n.n & nextn.n. $G(A,B)$ circuits

So <u>if</u> n.n/nextn.n. $G(A,B)$ PQP-circuits are cl. sim'ble

<u>then</u> $P = NP = PP$ implausible! ---

But same argument for BQP is less compelling:

Generally believed that NP, PP not in BQP

So cl. sims. of nn./next-n.n. $G(A,B)$ BQP-circuits would not imply P=NP=PP  hence "less implausible..."

But then would get P=BQP.

Note: for latter conclusion, suffices to use for weaker notion of classical simulability:

* ability to efficiently sample output distribution once

in contrast to

* ability to efficiently classically compute output probs to exponential accuracy (as in Valiant thm.)