Every NAND formula can be evaluated in time $O(N^{\frac{1}{2}+\varepsilon})$

1

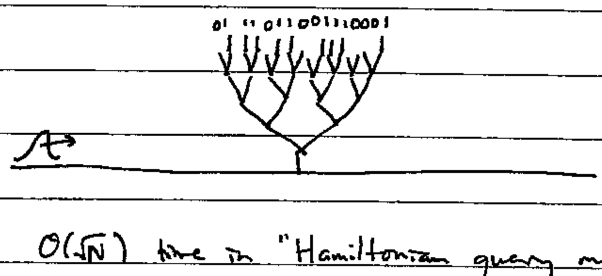
quant-ph/0703015, with Reichardt / Špalek / Zhang

Background

Main question: Given a Boolean formula on N variables, how many variables must we query to evaluate the formula?

- Simple example: OR. Classical, $\Theta(N)$. Quantum, $\Theta(\sqrt{N})$ (Grover, BBBV).
- Harder example: AND-OR trees = game trees
  - Constant depth: $O(\sqrt{N}\ \mathrm{poly}(\log N))$ (BCW 98)
    in fact, $O(\sqrt{N} \cdot c^d)$ by controlling the error at each level (HMdW 03)
  - Balanced binary: $\Theta(N^{0.753})$ classical (Snir 85, SW86, Santha 95)
    $\Omega(\sqrt{N})$ quantum (BS04, read-once formulas)
    for a long time, no better-than-classical quantum algorithm was known!

Idea of Farhi, Goldstone, Gutmann 07: scattering on trees



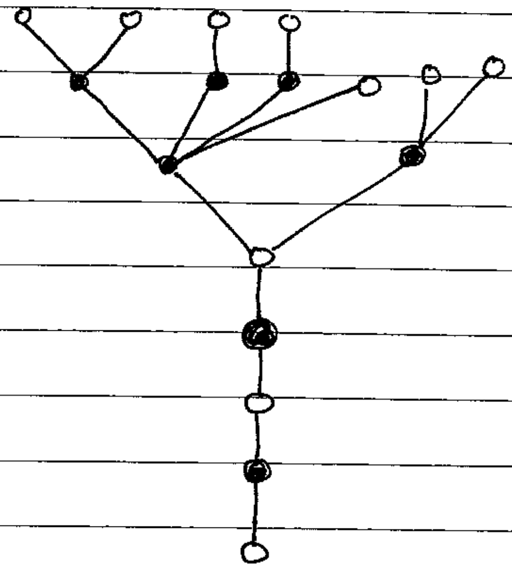
NAND = 0 : reflect
NAND = 1 : ~~reflect~~ transmit

$O(\sqrt{N})$ time in "Hamiltonian query model"
$O(N^{\frac{1}{2}+\varepsilon})$ time & queries with discrete simulation (CCJY)

- This talk: $O(N^{\frac{1}{2}+\varepsilon})$ time algorithm for arbitrary NAND formulas

Idea of algorithm

formula $\longleftrightarrow$ tree



- leaves evaluate to 0
- internal vertices are NAND gates on children
- construct quantum walk on this graph
  (weights on edges; cts or discrete time walk)
- tail of $\approx \sqrt{N}$ vertices, even length
- starting state: unif. sup. over even vertices in tail
  (alternating phases)

Claim:

- if NAND = 0, this ~~is~~ ~~has constant overlap with~~ an eigenvector of the weighted graph with eigenvalue 0
- if NAND = 1, it lives in a subspace with eigenvalues $\gtrsim \frac{1}{\sqrt{N}}$

- thus phase estimation can decide the NAND in time $\approx \sqrt{N}$

[Note: Can assume formula is $\approx$ balanced (depth $O(\log N)$) with at worst
$N \to N^{1+\varepsilon}$ (Bshouty - Cleve - Eberly 91)]

Outline of proof

Energy 0:

- If NAND = 1, any 0-energy eigenstate has no overlap on even tail vertices (Lemma 3)
- If NAND = 0, the initial state has constant overlap with a 0-energy eigenstate (Lemma 4)

Small energy ($O(\frac{1}{\sqrt{N}})$):

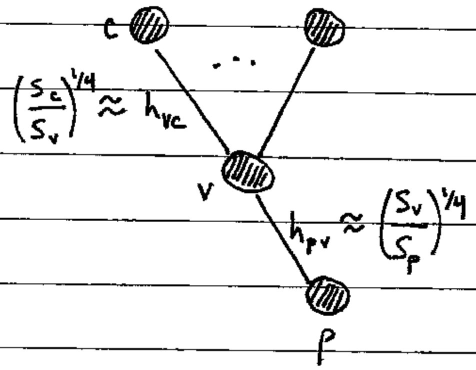
- If NAND = 1, any such eigenstate has no overlap on the tail (Lemma 5)

To prove this, show that low-energy eigenstates implement the NAND gates as follows: (Theorem 7)

$\bar{\Lambda}(v) = 0 \Rightarrow$ $\frac{\text{parent}}{\text{vertex}}$ amplitude small and positive

$\bar{\Lambda}(v) = 1 \Rightarrow$ $\frac{\text{parent}}{\text{vertex}}$ amplitude negative, large magnitude

The Hamiltonian (leave up for reference)



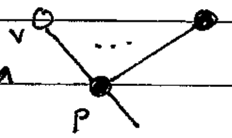
$$H|v\rangle = h_{pv}|p\rangle + \sum_c h_{vc}|c\rangle$$

for $H|E\rangle = E|E\rangle$, $\quad E\langle v|E\rangle = h_{pv}\langle p|E\rangle + \sum_c h_{vc}\langle c|E\rangle$

Lemma 3: If $\bar{\Lambda}(p) = 1$ and $\Pi_{T_p} H|\psi\rangle = 0$,
then $\langle p|\psi\rangle = 0$.

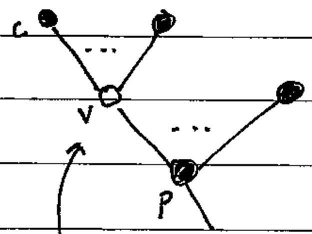
Proof by induction.

- Base case: some child of p is a leaf



$h_{pv}\langle p|\psi\rangle = 0$

- Induction step: some child v of p has $\bar{\Lambda}(v) = 0$; all its children c have $\bar{\Lambda}(c) = 1$



by induction hyp., $\langle c|\psi\rangle = 0 \ \forall c$
$\Rightarrow h_{pv}\langle p|\psi\rangle = 0$ $\square$

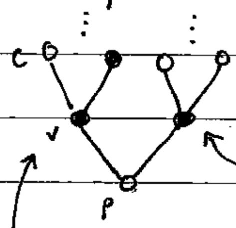
E=0, NAND = 0

Lemma 4: If $\bar{\Lambda}(p)=0$ then $\exists\ |\psi\rangle$ satisfying

$$\Pi_{T_p}|\psi\rangle = |\psi\rangle, \qquad \| |\psi\rangle \| = 1$$

with $\Pi_{T_p} H |\psi\rangle = 0$ and $\langle p|\psi\rangle \geq \frac{1}{s_p^{1/4}}$

Balanced binary case with all $h_{pv} = 1$:



pick one child to have a nonzero weight

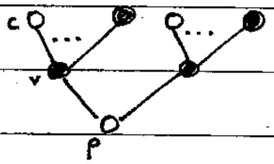
$\langle p|\psi\rangle + \langle c|\psi\rangle = 0$

→ equal weights, alternating phases

$|\psi\rangle$ is a superposition over a certificate for $\bar{\Lambda}(p)=0$

certificate size $= \sqrt{N}$, so $\langle p|\psi\rangle = \frac{1}{N^{1/4}}$

Proof by induction:



Define an unnormalized state $|\phi\rangle$ and let $|\psi\rangle = \frac{|\phi\rangle}{\| |\phi\rangle \|}$.

$$\langle p|\phi\rangle = 1 \quad \text{and} \quad \Pi_{T_c}|\phi\rangle = -\frac{h_{pv}}{h_{vc}} \frac{|\psi_c\rangle}{\langle c|\psi_c\rangle}$$

child of v in the certificate

$$\text{Then } \| |\phi\rangle \|^2 = 1 + \sum_v \frac{h_{pv}^2}{h_{vc}^2 \langle c|\psi_c\rangle^2}$$

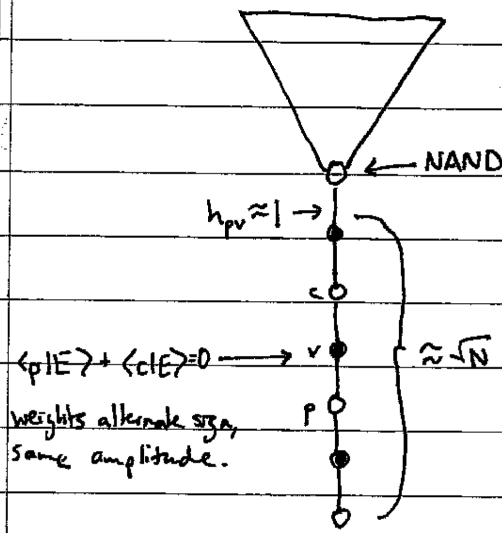
$$\leq 1 + \sum_v \sqrt{\frac{s_v/s_p}{s_c/s_v}}\ \sqrt{s_c} = 1 + \sum_v \frac{s_v}{\sqrt{s_p}} = 1 + \sqrt{s_p}$$

$$\approx \sqrt{s_p}$$

□

Boosting the overlap

Lemma 4 only gives overlap$^2 \approx \frac{1}{\sqrt{N}}$ at the root.
We want constant overlap, so we append a tail of even length $\approx \sqrt{N}$.



Now we have constant overlap with the starting state.

Low-energy eigenstates implement NAND

Lemma 5: If NAND $=1$, then no eigenvector $|E\rangle$ of H with $E \in (0, \frac{1}{\sqrt{N}}]$ is nonzero on any tail vertex.

Theorem 7: Let $H|E\rangle = E|E\rangle$ with $E \in (0, \frac{1}{\sqrt{N}}]$.

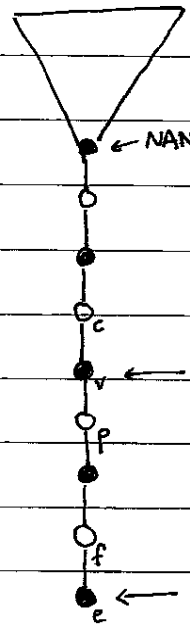
Then $\forall\, v \in T$, either $\langle v|E\rangle = \langle p|E\rangle = 0$ or

$$\bar{\Lambda}(v) = 0 \;\Rightarrow\; 0 \le \frac{\langle p|E\rangle}{\langle v|E\rangle} \le (s_v s_p)^{1/4} E$$

$$\bar{\Lambda}(v) = 1 \;\Rightarrow\; 0 \ge \frac{\langle v|E\rangle}{\langle p|E\rangle} \ge -\left(\frac{s_v^3}{s_p}\right)^{1/4} E.$$

Proof of Lemma 5: by contradiction.

Let $|E\rangle$ have $E \in (0, \frac{1}{\sqrt{N}}]$ and $\langle c|E\rangle \neq 0$ for some $c \in$ tail.



$E\langle v|E\rangle = h_{vc}\langle c|E\rangle + h_{pv}\langle p|E\rangle$

so either $\langle v|E\rangle \neq 0$ or $\langle p|E\rangle \neq 0$.

iterating, either $\langle e|E\rangle \neq 0$ or $\langle f|E\rangle \neq 0$.

$E\langle e|E\rangle = h_{ef}\langle f|E\rangle$, so in fact both are nonzero.

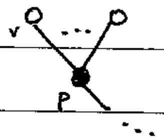
$$\frac{\langle e|E\rangle}{\langle f|E\rangle} \approx \frac{1}{E}.$$

Now by Thm 7, $\frac{\langle e|E\rangle}{\langle f|E\rangle} \le \sqrt{N}\, E \;\Rightarrow\; E \ge \frac{1}{N^{1/4}}$, contradiction. $\square$

Proof of Theorem 7

By induction.

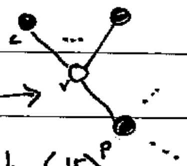
Base case: $\bar{\Lambda}(\text{leaf}) = 0$.



$$E\langle v|E\rangle = h_{pv}\langle p|E\rangle$$

$$\text{so} \quad \frac{\langle p|E\rangle}{\langle v|E\rangle} = \frac{E}{h_{pv}} = s_p^{1/4} E \qquad (s_v = 1)$$

Induction step, $\bar{\Lambda}(v) = D$:



$$E\langle v|E\rangle = h_{pv}\langle p|E\rangle + \sum_c h_{vc}\langle c|E\rangle$$

$$\text{so} \quad \frac{\langle p|E\rangle}{\langle v|E\rangle} = \frac{1}{h_{pv}}\left(E - \sum_c h_{vc}\frac{\langle c|E\rangle}{\langle v|E\rangle}\right)$$

$$\leq \frac{E}{h_{pv}} + \frac{1}{h_{pv}}\sum_c h_{vc}\left(\frac{s_c^3}{s_v}\right)^{1/4} E$$

$$= \left[\left(\frac{s_p}{s_v}\right)^{1/4} + \left(\frac{s_p}{s_v}\right)^{1/4}\sum_c\left(\frac{s_c}{s_v}\right)^{1/4}\left(\frac{s_c^3}{s_v}\right)^{1/4}\right]E$$

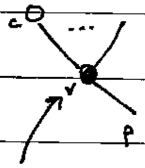
$$= \left[\left(\frac{s_p}{s_v}\right)^{1/4} + \left(\frac{s_p}{s_v^3}\right)^{1/4}\sum_c s_c\right]E$$

$$= \left[\underbrace{\left(\frac{s_p}{s_v}\right)^{1/4}}_{O(1)\text{ for }\approx\text{ balanced formulas}} + \underbrace{(s_p s_v)^{1/4}}_{\text{typically }\sim\sqrt{N}}\right]E$$

$$\approx (s_p s_v)^{1/4} E$$

Proof of Theorem 7, continued

Induction step, $\bar{\Lambda}(v) = 1$:



$$E\langle v|E\rangle = h_{pv}\langle p|E\rangle + \sum_c h_{vc}\langle c|E\rangle$$

so $$\frac{\langle v|E\rangle}{\langle p|E\rangle} = h_{pv}\left(E - \sum_c h_{vc}\frac{\langle c|E\rangle}{\langle v|E\rangle}\right)^{-1}$$

$$\geq h_{pv}\left(E - \underbrace{\sum_{c:\bar{\Lambda}(c)=0}}_{\text{at least 1 term}} h_{vc}\frac{1}{(S_v S_c)^{1/4}E} + \underbrace{\sum_{c:\bar{\Lambda}(c)=1}}_{\text{upper bound by sum over all } c} h_{vc}\left(\frac{S_c^3}{S_v}\right)^{1/4} E\right)^{-1}$$

$$\geq \left(\frac{S_v}{S_p}\right)^{1/4}\left(E - \left(\frac{S_c}{S_v}\right)^{1/4}\frac{1}{(S_v S_c)^{1/4}E} + E\sum_c\left(\frac{S_c}{S_v}\right)^{1/4}\left(\frac{S_c^3}{S_v}\right)^{1/4}\right)^{-1}$$

$$= \left(\frac{S_v}{S_p}\right)^{1/4}\left(E - \underbrace{\frac{1}{\sqrt{S_v}\,E}}_{O(1/\sqrt{N})} + \sqrt{S_v}\,E\right)^{-1}$$

actually, have to ~~include~~ ~~a term~~ modify things slightly so that this is smaller; here, neglect it

$$\approx -\left(\frac{S_v^3}{S_p}\right)^{1/4} E$$

$\square$

The quantum walk

Two approaches:

- Continuous-time quantum walk e^{-iHt}.

  For a constant-degree graph with edge weights upper bounded by h, can simulate with $O((ht)^{1+\varepsilon})$ steps. ($\varepsilon > 0$ arbitrary)
  (high-order Lie product decomposition)

  $\Rightarrow$ running time $O(N^{\frac{1}{2}+\varepsilon})$

- Discrete-time quantum walk a la Szegedy.

  Spectrum of H is exactly what we need to understand this walk. No simulation overhead!

  $\Rightarrow$ running time $O(\sqrt{N})$, assuming formula starts out $\approx$ balanced.

  Note: Ambainis gave another algorithm with this running time for $\approx$ balanced formulas using a different approach

Still open: $O(\sqrt{N})$ algorithm for general formulas?