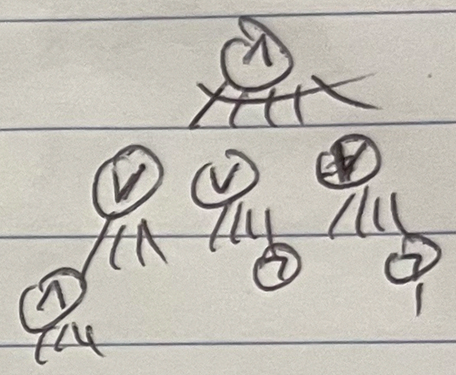
QAC^0 and parity.

[with Daniel Grier and Jackson Morris; OpenAI released proofs]

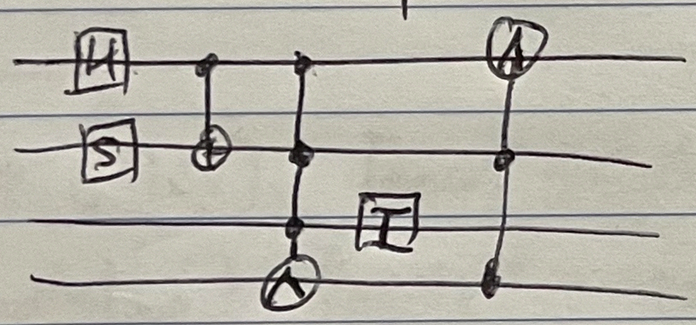
Background: low-depth circuit power (quantum vs classical)

- physical implementation
- classical lower bounds (random restriction, polynomial method, Fourier)
- Quantum advantage provable in search, sampling
- Quantum primitives.

AC^0: AND, OR, negation. with unbounded fanin.
Constant depth.



QAC^0: single-qubit gates + generalized Toffoli.
Constant depth.
$|x\rangle|b\rangle \to |x\rangle|b \oplus AND(x)\rangle$.



Thm [Håstad '86]: Parity not in AC^0

Question [Moore '99]: Is parity in QAC^0?

Thm [Moore '99]: Parity $\Leftrightarrow$ cat/GHZ state $\Leftrightarrow$ fanout in QAC^0.

$\frac{1}{\sqrt{2}}(|0^n\rangle + |1^n\rangle)$. $\quad |b\rangle|0^n\rangle \to |b\rangle|b^n\rangle$.

Pf: Fanout $\Rightarrow$ CAT:

$|0\rangle \xrightarrow{H} |0\rangle+|1\rangle \xrightarrow{\text{Fanout}} |0^n\rangle + |1^n\rangle$.

CAT $\Rightarrow$ Parity:

$|x\rangle|0\rangle \xrightarrow{\text{state prep}} |x\rangle(|0^n\rangle+|1^n\rangle) \xrightarrow{\text{control-phase}} |x\rangle(|0^n\rangle + (-1)^{|x|}|1^n\rangle)$

$\xrightarrow{\text{state unprep}} |x\rangle\begin{cases} |0^n\rangle+|1^n\rangle \to |0^n\rangle & |x| \text{ is even} \\ |0^n\rangle - |1^n\rangle \to |\perp\rangle & |x| \text{ is odd.} \end{cases}$

$\xrightarrow{OR_n} |x\rangle|\varphi_x\rangle|\text{parity}(x)\rangle$.

Parity $\Rightarrow$ Fanout: $|b\rangle \xrightarrow{H^{\otimes n}} |b\rangle\sum|x\rangle \xrightarrow{\text{parity}} |b\rangle\sum|x_1, x_2, \ldots, x_n\rangle|x_1 \oplus x_2 \oplus \cdots \oplus x_n \oplus b\rangle$

$= |b\rangle\begin{cases} \sum|\text{even string}\rangle & b=0 \\ \sum|\text{odd strings}\rangle & b=1. \end{cases}$

$\xrightarrow{H^{\otimes(n+1)}} |b\rangle\begin{cases} |0^{n+1}\rangle + |1^{n+1}\rangle & b=0 \\ |0^{n+1}\rangle - |1^{n+1}\rangle & b=1. \end{cases}$

$= |b\rangle(|0^{n+1}\rangle + (-1)^b|1^{n+1}\rangle)$.

$|0\rangle \to |0\rangle+|1\rangle \xrightarrow{\text{above}} |0\rangle|0^{n+1}\rangle$

$|1\rangle \to |0\rangle-|1\rangle \xrightarrow{\text{above}} |1\rangle|1^{n+1}\rangle$.

Thm [HS05, GM25]. Fanout $\Leftrightarrow$ Majority $\Leftrightarrow$ MOD_p $\forall p$ $\Leftrightarrow$ QFT over $\mathbb{Z}_p$.

Thm [Rosenthal '20] Parity is (approximately) in exponential-size QAC^0.

Thm [FFGHZ '03, B '11, PFGT '20, R '20, NPVY '23, ADOT '25, JTVW '26, GGJ '26]

Depth-3 QAC^0 cannot compute parity [JTVW '26]

Depth-d QAC^0 with $n^{1+3^{-d}}$ ancilla cannot compute parity [ADOT '25].

if depth-d QAC^0 can compute parity, then $n^{1+c^{-d}}$ ancilla suffice for some $c>0$.

Parity not in QAC^0 [OpenAI].

Thm [Our]. Parity is in QAC^0 if the input is duplicated poly(n) times.

$$\text{CopyParity}(x^{(1)}, x^{(2)}, \dots, x^{(m)}) := \begin{cases} \text{parity}(x^{(1)}) & \text{if } x^{(1)} = x^{(2)} = \cdots = x^{(m)} \\ 0 & \text{o/w} \end{cases}$$

$x^{(1)}, x^{(2)}, \dots, x^{(m)} \in \{0,1\}^n$. $m = n^2$.

Thm [Our] $TC^0 \subseteq QAC^0 \circ NC^0$.

Cor [Our] There is a decision problem L in QAC^0 but not in $AC^0[p]$.

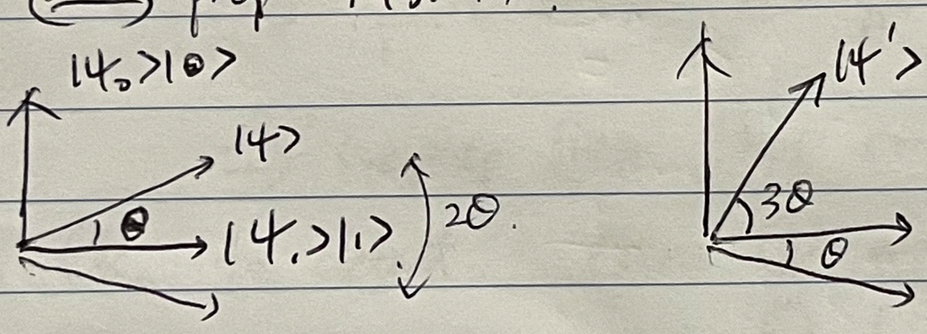
$QAC^0 \not\subseteq AC^0[p]$.

D. Fanout of log-size. [Rosenthal '20]

Thm [Grover] prep $c \cdot |\psi_0\rangle|0\rangle + \sqrt{1-c^2}\,|\psi_1\rangle|1\rangle$ for $c = \sin\frac{\pi}{4k+2}$ $k = \Theta(1)$ integer

$\overset{QAC^0}{\Longrightarrow}$ prep $|\psi_0\rangle|0\rangle$.

Proof



Lem prep $c \cdot |\psi_0\rangle|0\rangle + \sqrt{1-c^2}\,|\psi_1\rangle|1\rangle$ for $c = \Theta(1)$

$\overset{QAC^0}{\Longleftarrow}$ prep $|\psi_0\rangle|0\rangle$.

Proof $|00\rangle \to a|00\rangle + ?|01\rangle$ such that $\alpha \cdot c = \sin\frac{\pi}{4k+2}$.

$|10\rangle \to ?|10\rangle + ?|11\rangle$.

then we can prep $\sin\frac{\pi}{4k+2}|\psi_0\rangle|0\rangle + ?|\psi_1'\rangle|\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\rangle$.

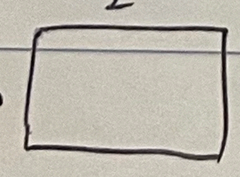
Thm [Rosenthal '20]. CAT state is approximately in exp(n)-size QAC^0.

Prof. $|0^n\rangle \to \Sigma|x\rangle \to \Sigma|x\rangle|AND(x)\rangle$

$\to -|1^n\rangle + \sum_{x \neq 1^n}|x\rangle \xrightarrow{H^{\otimes n}} (1-2\cdot 2^{-n})|0^n\rangle + 2\cdot 2^{-n}\sum|1^n\rangle + 2^{-n}\sum_{x \neq \{0^n,1^n\}}|x\rangle$.

$\to |\psi_0\rangle|0\rangle + |\psi_1\rangle|1\rangle$. where $|\psi_0\rangle = (1-2\cdot 2^{-n})|0^n\rangle + 2\cdot 2^{-n}|1^n\rangle$

$|\psi_0\rangle^{\otimes 2^n} = \left((1-2^{-n})|0^n\rangle + 2^{-n}|1^n\rangle\right)^{\otimes 2^n}$ tribes.



$|0^n\rangle + |1^n\rangle$

$(1-2^{-n})^{2^n} = \Theta(1)$

$\Pr[\text{some col is } 1^n] \approx 2^n \cdot 2^{-n} = \Theta(1)$.

Cor: Fanout/parity of polylog size is in QAC^0.

---

② W-test.

Thm If we can prep W-state $|W\rangle = \frac{1}{\sqrt{n}} \sum_{i=1}^{n} |e_i\rangle$. $e_i = 0^{i-1}10^{n-i}$

then we can weakly decide Mid function

$$Mid(x) = \mathbb{1}[|x| = n/2]$$

Pf: $|x\rangle|0^n\rangle \to |x\rangle|W\rangle \to |x\rangle \sum_i (-1)^{x_i}|e_i\rangle$.

① $|x| = n/2$. $\sum_i (-1)^{x_i}|e_i\rangle$ is orthogonal to $|W\rangle$.

$\Rightarrow$ unprep $|W\rangle$ gives something $\perp$ to $|0^n\rangle$.

② $|x| \neq n/2$. $\langle W| \sum_i (-1)^{x_i}|e_i\rangle = \frac{1}{n}\sum (-1)^{x_i} = \frac{n-2|x|}{n}$.

$\Rightarrow \sum_i (-1)^{x_i}|e_i\rangle$ is $\frac{1}{n^2}$-far from $|W\rangle$.

$\Rightarrow$ unprep $|W\rangle$ gives something with $\geq \frac{1}{n^2}$ overlap of $|0^n\rangle$

Use QR_n to detect. Case ① always zero

case ② has $\geq \frac{1}{n^2}$ being one.

Cor: copyMid $\in QAC^0$. if we can prep W state.

Pf. apply above n^2 times, then take OR of all results. (also check input consistency) — use AND/OR

if $|x| = n/2$, then 0. wp 1

if $|x| \neq n/2$, then 0 wp $\leq (1-\frac{1}{n^2})^{n^2} = 0.1$.

Fact [Razborov-Smolensky '87] Mid $\notin AC^0[p]$. $\Rightarrow$ copyMid $\notin AC^0[p]$

Cor $TC^0 \subseteq QAC^0 \cdot NC^0$.

pf Use NC^0 to make copies. & TC^0 consists of {Mid, AND, OR}

③. $|W\rangle$ state prep.

Thm. We can compute Exact-1 function in QAC^0.

$$EX1(x) = \mathbb{1}[|x|=1].$$

Pf. Define $S_0^{(t)} = \{i \in [w] : \text{the } t\text{-th bit of } i \text{ is } 0\}$

$S_1^{(t)} = \{i \in [w] : \text{the } t\text{-th bit of } i \text{ is } 1\}$

$S_0^{(1)}$ $S_1^{(1)}$ $\quad$ $z_0^{(1)}$ $z_1^{(1)}$

$S_0^{(2)}$ $S_1^{(2)}$ $\xrightarrow{X}$ $z_0^{(2)}$ $z_1^{(2)}$ $\quad$ $z_b^{(t)} = \mathbb{1}[X_{S_b^{(t)}} \text{ contains } 1]$.

$S_0^{(w)}$ $S_1^{(w)}$ $\quad$ $z_0^{(w)}$ $z_1^{(w)}$

~~$EX1(x) = \mathbb{1}(z_0^{(1)}, z_1^{(1)}, \ldots, z_0^{(w)}, z_1^{(w)})$~~

~~$|x|=1 \iff z_0^{(t)}$ and $z_1^{(t)}$~~

if $|x|>1$, then for some t, we have $z_0^{(t)} = z_1^{(t)} = 1$.

Thm $|W\rangle$ state prep is in QAC^0.

Pf. $|0\rangle^n \longrightarrow$ ~~$\cdots$~~ $\left(\left(1-\frac{1}{n}\right)|0\rangle + \frac{1}{\sqrt{n}}|1\rangle\right)^{\otimes n}$.

$$= \frac{1}{\sqrt{n}}\left(1-\frac{1}{n}\right)^{n-1} \sum_i |e_i\rangle + |\perp\rangle.$$

$$= \Theta(1)|W\rangle + |\perp\rangle.$$

$\longrightarrow |W\rangle$ exact-1 + exact Grover.

OpenAI's lower bound. Parity is not in QAC^0.

Key lemma. Let D and M be mismatch projections

$$M = \sum_{i \in S} (I - |v_i\rangle\langle v_i|)_{\bar{v}_i} \quad \text{checks if the } i\text{-th qubit mismatches } |v_i\rangle.$$

$$D = \sum_{i \in T} (I - |w_i\rangle\langle w_i|)_{\bar{w}_i}$$

then $\| [M \geq N^\beta] U [D=0] U^\dagger [M \leq N^\alpha] \| \leq e^{-N^\gamma}$ for every $\beta > \max\{\alpha, \gamma\}$.

U: QAC^0 ckt

projection

Intuition. You start with some state "close" to $|v_1\rangle \otimes |v_2\rangle \otimes \cdots \otimes |v_n\rangle$ $[M \leq N^\alpha]$.

Pass through a QAC^0-conjugated product projection $U[D=0]U^\dagger$

Cannot obtain a state "far" from $|v_1\rangle \otimes |v_2\rangle \otimes \cdots \otimes |v_n\rangle$. $[M \geq N^\beta]$.

Example. $U = I$.

then it is $[M \geq N^\beta]\,[D=0]\,[M \leq N^\alpha] = \left[\sum_i (I - |v_i\rangle\langle v_i|) \leq N^\alpha\right]$.

$[\sum_i (I - |v_i\rangle\langle v_i|) \geq N^\beta]$. $\prod_i |w_i\rangle\langle w_i|$

- if $|w_i\rangle \approx |v_i\rangle$, then $(I - |v_i\rangle\langle v_i|)\,|w_i\rangle\langle w_i| \approx 0$.
- if $|w_i\rangle \perp |v_i\rangle$, then $|w_i\rangle\langle w_i|v_i\rangle\langle v_i| \approx 0$.

either way, small contribution.

Cor Parity / GHZ state not in QAC^0.

Pf if $GHZ \in QAC^0$.

then $U|0^n\rangle = \frac{1}{\sqrt{2}}(|0^n\rangle + |1^n\rangle)$.

Let $\Phi(W_i\rangle = |V_i\rangle = |0^n\rangle$. $N^\alpha = 0$. $N^\beta = N$.

then $[D=0] = |0^n\rangle\langle 0^n|$ $[M \le N^\alpha] = |0^n\rangle\langle 0^n|$

~~$[M \le N^\alpha] = |0^n\rangle\langle 0^n|$.~~

~~$[M \ge N^\beta]$~~ ~~$|0^n\rangle\langle 0^n|$~~.

$U[D=0]U^\dagger = U|0^n\rangle\langle 0^n|U^\dagger = \frac{1}{2}(|0^n\rangle + |1^n\rangle)(\langle 0^n| + \langle 1^n|)$.

$U[D=0]U^\dagger[M \le N^\alpha] = \frac{1}{2}(|0^n\rangle + |1^n\rangle)(\langle 0^n|)$.

$[M \ge N^\beta]U[D=0]U^\dagger[M \le N^\alpha] = \frac{1}{2}|1^n\rangle\langle 0^n|$ has operator norm $\frac{1}{2}$

Pf of key lemma induction on QAC^0 depth.

~~depth 1~~ $U = VR$. R is a layer of generalized Toffolis.

$U = VR$. R is a layer of single-qubit gate. ✓

$[M \ge N^\beta]U[D=0]U^\dagger[M \le N^\alpha]$ $D = \prod |w_i\rangle\langle w_i|$ $I - 2|1^n\rangle\langle 1^n|$.

$= [M \ge N^\beta]VR[D=0]R^\dagger V^\dagger[M \le N^\alpha]$.

$\Pi(I - 2|1^c\rangle\langle 1^c|)$ $\Pi(I - 2|1^c\rangle\langle 1^c|)$.

① If R projection is small. (R is small) then we expand $R[D=0]R^\dagger$ as 4^r terms of → at most r relevant Toffolis.

and apply induction hypothesis.

product projection

② If r is big. then we use approximation theory / Chebyshev poly.

~~$[D=0] \approx p(|w_1\rangle\langle w_1| - |w_2\rangle\langle w_2|, \dots, |w_r\rangle\langle w_r|)$~~

~~- deg N^δ - error ε $N^\delta \le \beta$.~~

~~- At most N^δ terms~~

$[D=0] \approx p(|w_1 \times w_1|, (w_2 \times w_2|, \dots, (w_p \times w_{r-1})$

- approximate up to $D \le N^{\alpha+\varepsilon_1} = N^{\beta^+}$
- error up to $e^{-N^{\gamma+\varepsilon_2}} = e^{-N^{\beta^-}}$
- (degree/terms) / total L_1 weight. up to $e^{N^{\frac{\alpha+\gamma+\varepsilon_1+\varepsilon_2}{2}}} = e^{N^{\beta^-}}$

$\| [M \ge N^\beta] V R [D=0] R^\dagger V^\dagger [M \le N^\alpha] \|$

$= \| [M \ge N^\beta] V R\, p(|w_1 \times w_1|, \dots, |w_r \times w_{r-1}) R^\dagger V^\dagger [M \le N^\alpha] \| \le e^{N^{\frac{\alpha+\gamma+\varepsilon_1+\varepsilon_2}{2}}} \cdot e^{-N^{\alpha+\varepsilon_1}} \approx e^{-N^\beta}$

$+ \| [M \ge N^\beta] V R \left([D=0] - p(|w_1 \times w_1|, \dots, (w_n \times w_{n-1}) \right) R^\dagger V^\dagger [M \le N^\alpha] \| \le \| [D=0] - p(w_1 \times w_1) \dots \|$

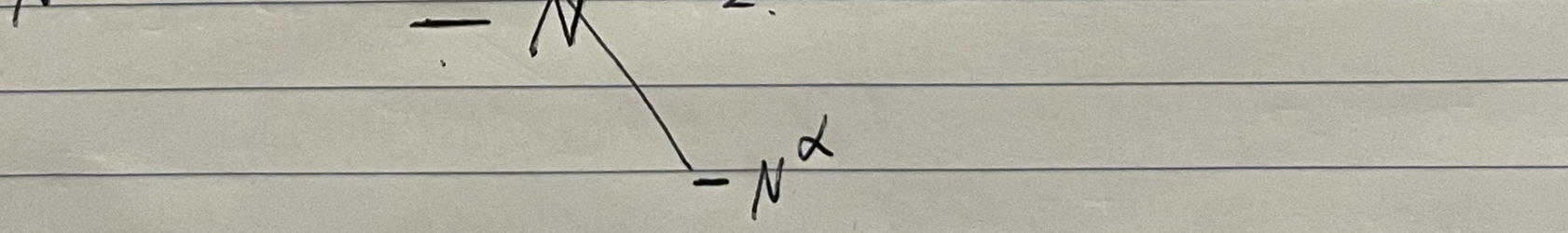
$\le e^{-N^{\gamma+\varepsilon_2}}$.

need $\alpha+\varepsilon_1 > \frac{\alpha+\gamma+\varepsilon_1+\varepsilon_2}{2}$

$\alpha+\varepsilon_1 > \beta$.

$\varepsilon_1 = \beta - \alpha$

$\varepsilon_2 = \beta - \gamma$.



$[D=0] \approx p(|w_1 \times w_1|, |w_2 \times w_2|, \ldots, |w_r \times w_n|)$.

$\beta > \alpha$.

$\gamma = \beta^-$

- approximate up to $D \leq N^{\beta^+}$
- error up to $e^{-N^{\beta^-}}$
- terms / total L_1 weight up to e^{N^β}

$\| [M \geq N^\beta] V R [D=0] R^\dagger V^\dagger [M \leq N^\alpha] \|$

$\leq \| [M \geq N^\beta] V R_p R^\dagger V^\dagger [M \leq N^\alpha] \| \leq e^{N^{\beta^-}} \cdot e^{-N^\gamma} \approx e^{-N^\gamma}$.

$+ \| [M \geq N^\beta] V R ([D=0] - p) R^\dagger V^\dagger [M \leq N^\alpha] \| \leq e^{-N^{\beta^+ - }} \leq e^{-N^\gamma}$.

