QAC^0 contains TC^0 (with many copies of the input)

w/ Daniel Grier & Jackson Morris (UCSD)

① Background.

Low-depth circuit (Quantum vs classical).

- physical implementation.
- classical lower bounds (random restriction, polynomial method, Fourier, etc)
- Quantum advantage provable in search, sampling. [BGK'17, BKST'19, GKMOW'26]
- Quantum primitives

QAC^0 vs AC^0

QAC^0: single-qubit gates + Generalized Toffoli

$|x\rangle|b\rangle \to |x\rangle|b \oplus AND(x)\rangle$.

AC^0: AND, OR, $\neg$ with unbounded fanin.

[Moore'99]

Question: Can QAC^0 compute parity?

Thm [Moore'99] Parity $\Leftrightarrow$ Cat (GHZ) state $\Leftrightarrow$ Fanout in QAC^0.

Cat (GHZ) state: $\frac{1}{\sqrt{2}}(|0^n\rangle + |1^n\rangle)$.

Fanout: $|b\rangle|0^n\rangle \to |b\rangle|b^n\rangle$.

Proof. Fanout $\Rightarrow$ CAT: $|0\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle) \xrightarrow{\text{Fanout}} \frac{1}{\sqrt{2}}(|0^n\rangle+|1^n\rangle)$

CAT $\Rightarrow$ Parity: $|x\rangle \xrightarrow[\text{prep}]{\text{state}} |x\rangle(|0^n\rangle+|1^n\rangle) \to |x\rangle(|0^n\rangle + (-1)^{\Sigma x_i}|1^n\rangle)$

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

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

Parity $\Rightarrow$ Fanout: $|b\rangle \to |b\rangle\sum|x\rangle. \to |b\rangle\sum|x_1\oplus x_2, x_2\oplus x_3, \ldots, x_n\rangle|x_1\oplus b\rangle.$

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

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

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

Thm [HŠ'05, GM'25]. Fanout $\Leftrightarrow$ Maj $\Leftrightarrow$ Mod_p $\forall p$. $\Leftrightarrow$ QFT over $\mathbb{Z}_p$.

Thm [Rosenthal '20]. Parity is apx computable in exponential-size QAC^0.

Thm [FFGHZ'03, B'11, PFGT'20, R'20, NPVY'23, ADOY'24, JTVW'25]

Depth-3 QAC^0 can't compute parity [JTVW'25]

Depth-d QAC^0 with $n^{1+3^{-d}}$ ancilla cannot compute parity [ADOY'24]

Thm [Our]. There exists a decision problem L in QAC^0 but not in $AC^0[p]$. $QAC^0 \not\subseteq AC^0[p]$.

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

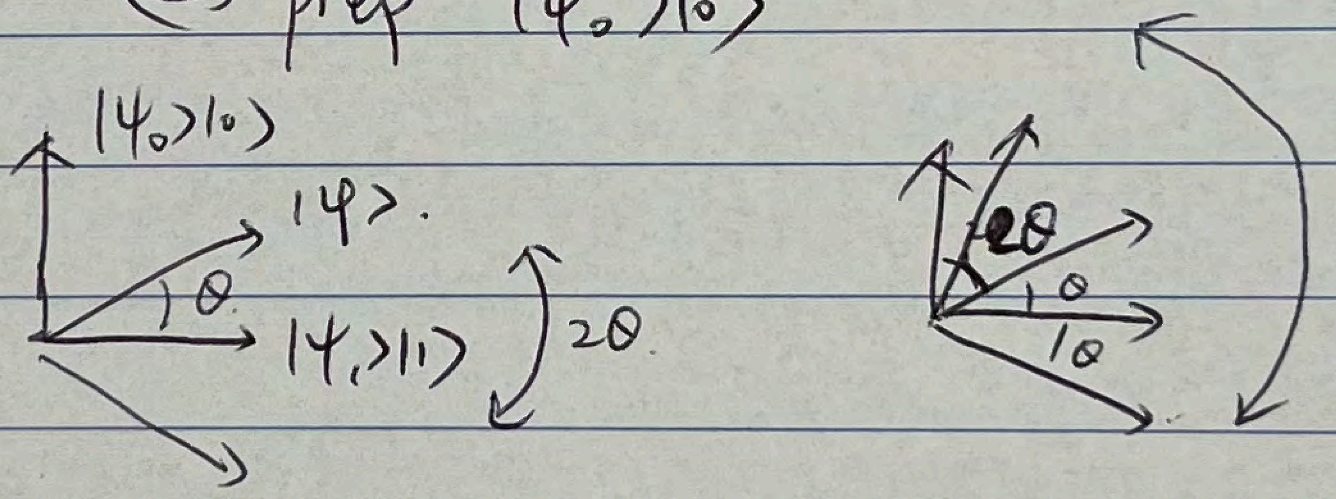
---

① Fanout of log-size [Rosenthal '20].

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

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

Proof.



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

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

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

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

then we can prep $\sin\frac{\pi}{4k+2}|\psi_0\rangle|00\rangle + ?|\psi_1'\rangle|\begin{smallmatrix}01\\10\\11\end{smallmatrix}\rangle$.

Thm [Rosenthal '20 / Nekomata]. CAT state in exp(n) size QAC^0.

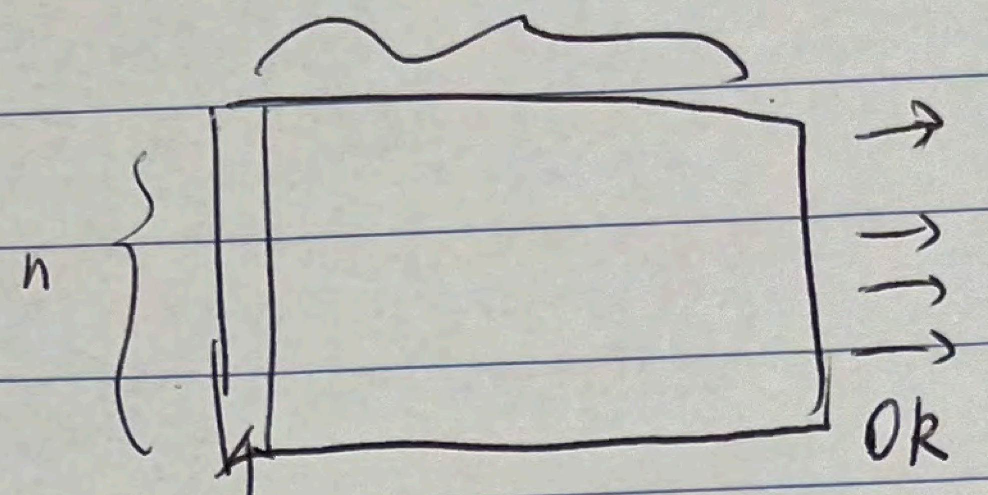
Pf. $|0^n\rangle \to \sum|x\rangle \to \sum|x\rangle|AND(x)\rangle \to -|1^n\rangle + \sum_{x\neq 1^n}|x\rangle$.

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

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

$$(1-2^{-n})|0^n\rangle + 2^{-n}|1^n\rangle \to \left((1-2^{-n})|0^n\rangle + 2^{-n}|1^n\rangle\right)^{\otimes 2^n}$$ Tribes

$\cancel{2^n \to (1-2^{-n})^{2^n}(|0^n\rangle)^{2^n} + \ldots}$



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

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

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

$(1-2^{-n})|0^n\rangle + 2^{-n}|1^n\rangle.$

<u>Cor</u>. Fanout of polylog size is in QAC^0.

---

②. W-test.

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

Then we can <u>weakly decide</u> ~~Exactly~~ Mid Function

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

<u>Pf</u>.

$|x\rangle \xrightarrow{\text{state prep}} |x\rangle|W\rangle = |x\rangle \sum |e_i\rangle \to |x\rangle \sum (-1)^{x_i} |e_i\rangle$

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

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

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

$|x\rangle \xrightarrow{\text{state unprep}} |x\rangle\left(\underset{\frac{n-2|x|}{n}}{|0^n\rangle} + \underset{\sqrt{1-\left(\frac{n-2|x|}{n}\right)^2}}{|\perp\rangle}\right) \xrightarrow{OR} \begin{cases} 0 & \text{if } |x| = n/2 \\ 1 \text{ wp} \geq \frac{1}{n^2} & \text{if } |x| \neq n/2 \end{cases}$

<u>Cor</u> $\mathrm{Mid}^{\uparrow n^2} \in QAC^0$ ~~iff~~ if we can prep W-state

<u>Pf</u>. apply above n^2 times.

then take OR ~~AND~~ of all result.

if $|x| = n/2 \Rightarrow$ 0.

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

~~Cor QAC^0 ...~~

Fact [Razborov-Smolensky '87] $\mathrm{Mid} \notin AC^0[p] \Rightarrow \mathrm{Mid}^{\uparrow n^2} \notin AC^0[p]$.

~~Fact~~

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

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

---

③. W state prep.

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

$$\overset{\uparrow}{\mathrm{Ex}}1(x) = \mathbb{1}[|x|=1].$$

pf. ~~$|x|=1 \Leftrightarrow$~~

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

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

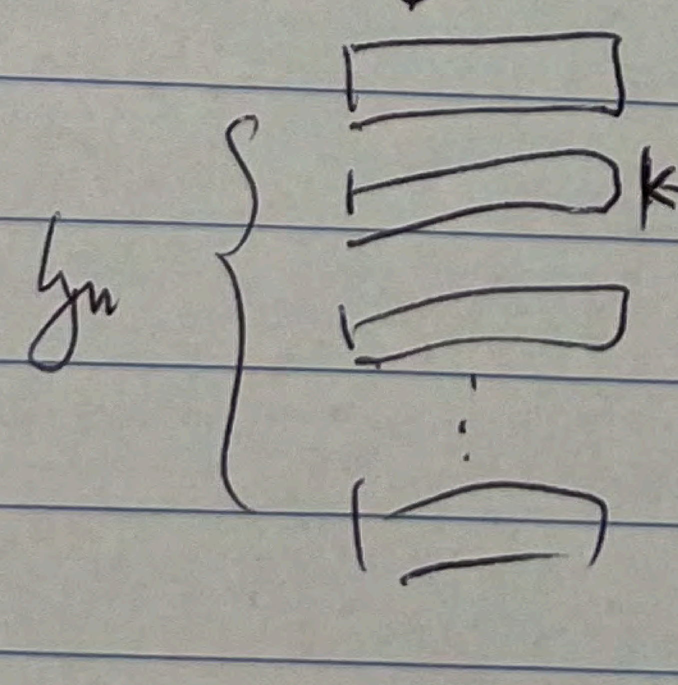
~~$\mathrm{Exact}_1(x) \Leftrightarrow$ exactly one of $S_0^{(t)}$ $S_1^{(t)}$~~

$$\begin{matrix} S_0^{(1)} & S_1^{(1)} \\ S_0^{(2)} & S_1^{(2)} \\ \vdots & \\ S_0^{(\log n)} & S_1^{(\log n)} \end{matrix} \xrightarrow{\ x\ } \begin{matrix} z_0^{(1)} & z_1^{(1)} \\ z_0^{(2)} & z_1^{(2)} \\ \vdots & \\ z_0^{(\log n)} & z_1^{(\log n)} \end{matrix} \qquad z_b^{(t)} = \mathbb{1}[x_{S_b^{(t)}} \text{ containing } 1].$$

$$\mathrm{Exact}_1(x) = \mathrm{Exact}_1(z_0^{(1)}, z_1^{(1)}, \ldots, z_0^{(\log n)}, z_1^{(\log n)}).$$

~~$\Leftarrow$ [HWWY '94].~~

in QAC^0



$\longleftarrow$ $\mathrm{Exact}_1(z)$. at the k-th bit.

Thm W-state prep in QAC^0.

Pf.

$$|0^n\rangle \longrightarrow \left(\left(1-\tfrac{1}{n}\right)|0\rangle + \tfrac{1}{\sqrt{n}}|1\rangle\right)^{\otimes n}$$

$$\longrightarrow \frac{1}{\sqrt{n}}\cdot\left(1-\frac{1}{n}\right)^{n-1}\sum_i |e_i\rangle + |\perp\rangle \longleftarrow \text{not Exact-1}$$

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

Exact-1

$$\longrightarrow \Theta(1)|W\rangle|1\rangle + |\perp\rangle|0\rangle.$$

$\square$

Open:

1. gate set: $U(1)$ + Toff $\longrightarrow$ finite + Toff ?

2. Error. Mid$^{\uparrow n^3}$: Completeness 1

   Soundness $2^{-\mathrm{poly}(n)} \Rightarrow 0$?

3. Copy complexity Mid$^{\uparrow n^2}$

   $\searrow$ Mid$^{\uparrow n}$ possible $\longrightarrow$ much lower ?

4. $AC^0 \subseteq QAC^0$?