Quantum Majority is Powerful

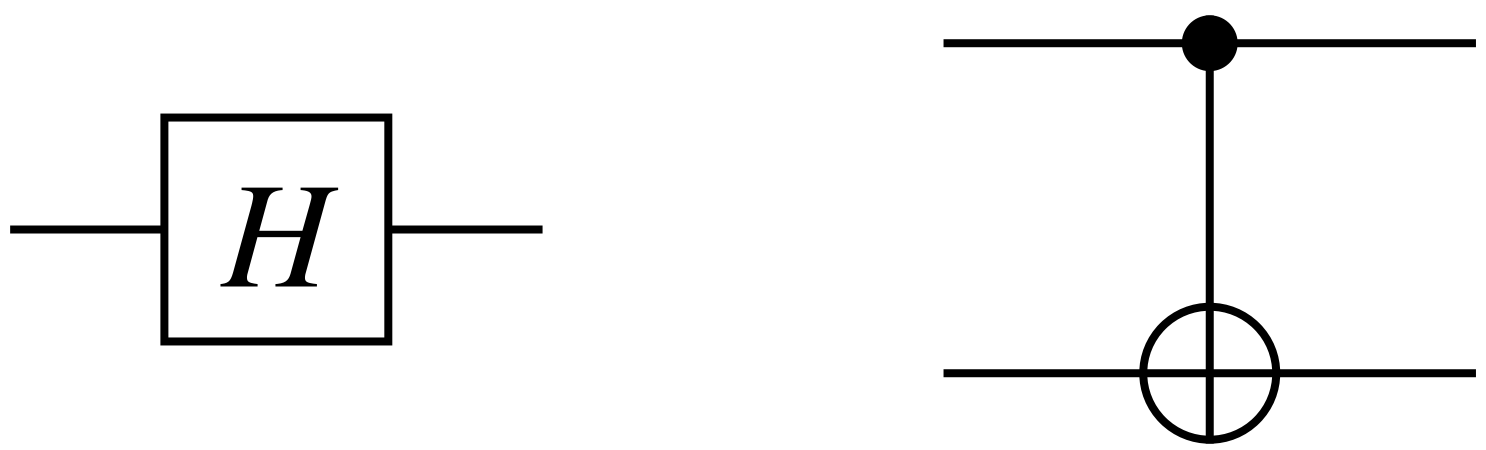
Daniel Grier
UC San Diego

Jackson Morris
UC San Diego

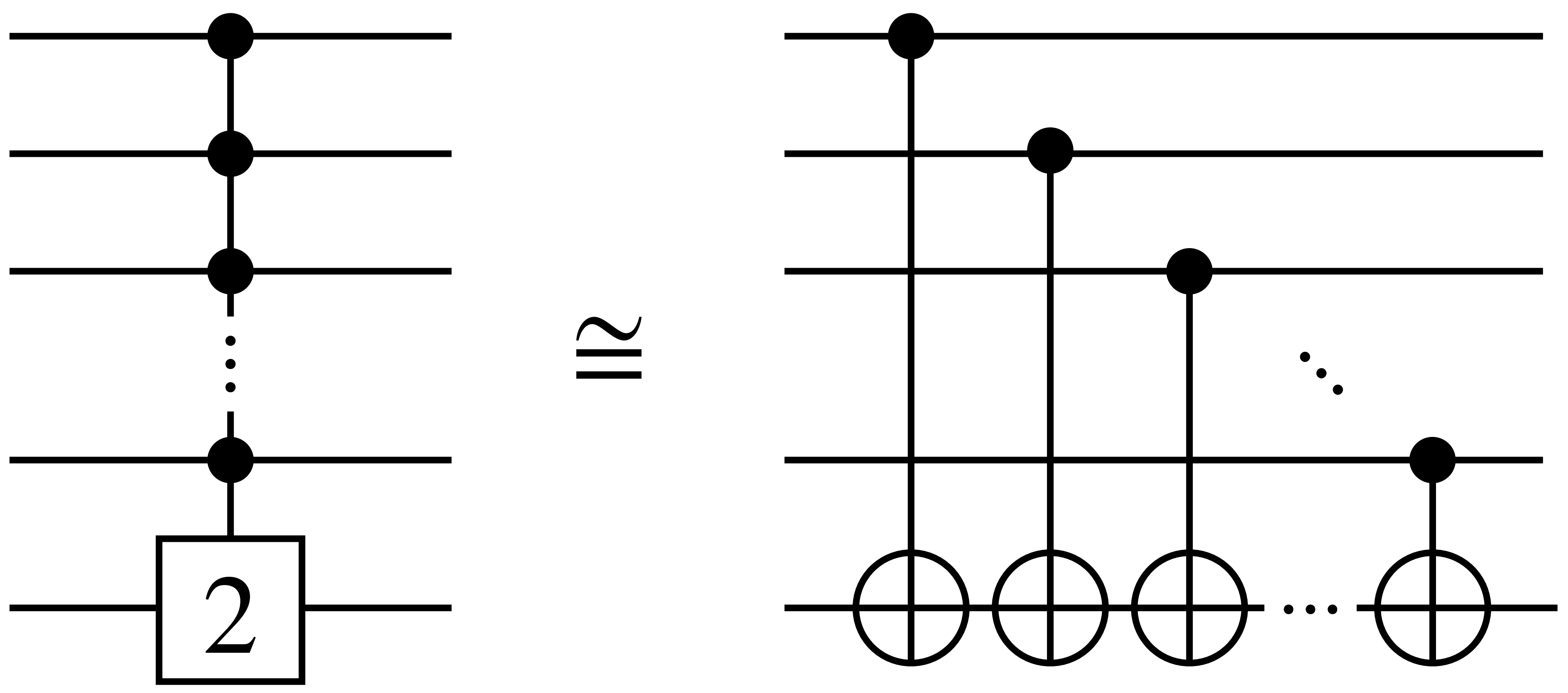
Large quantum gates

Question: What is the power of large multi-qubit gates?

Setting: Circuits with arbitrary 1- and 2-qubit gates and some restricted set of multi-qubit gates



1- and 2-qubit gates



multi-qubit gate

Large gates might be experimentally feasible

Rydberg atoms:

- Efficient multiparticle entanglement via asymmetric Rydberg blockade [Saffman, Mølmer 2009]
- Parallel implementation of high-fidelity multiqubit gates with neutral atoms [Levine et al. 2019]

⋮

Ion Traps:

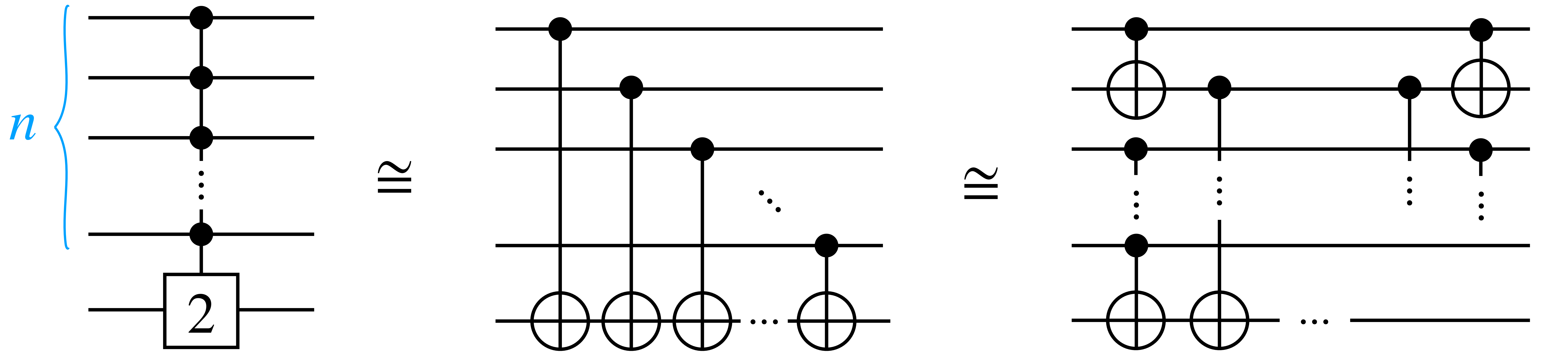
- Quantum computations with cold trapped ions [Cirac, Zoller 1995]
- Multi-particle entanglement of hot trapped ions [Mølmer, Sørensen 1999]

⋮

Large gates often have efficient small-gate decompositions

Question: What is the power of large multi-qubit gates?

Observation: Large entangling gates can be efficiently decomposed into circuits of 1- and 2-qubit gates



Gates: n

Depth: n

Gates: $O(n)$

Depth: $O(\log(n))$

Large gates in constant depth

Question: What is the power of large multi-qubit gates in constant depth?

- **Experiments:** Possibility for less decoherence

  Large gate fidelity might be better than the fidelity of the circuit composed of smaller gates

- **Quantum Advantage:**

  Constant-depth quantum circuits can solve problems that constant-depth classical circuits cannot [Bravyi, Gosset, König 17]

  Exact sampling is hard unless polynomial hierarchy collapses [Terhal, DiVincenzo 02]

- **Deep knowledge in classical setting**

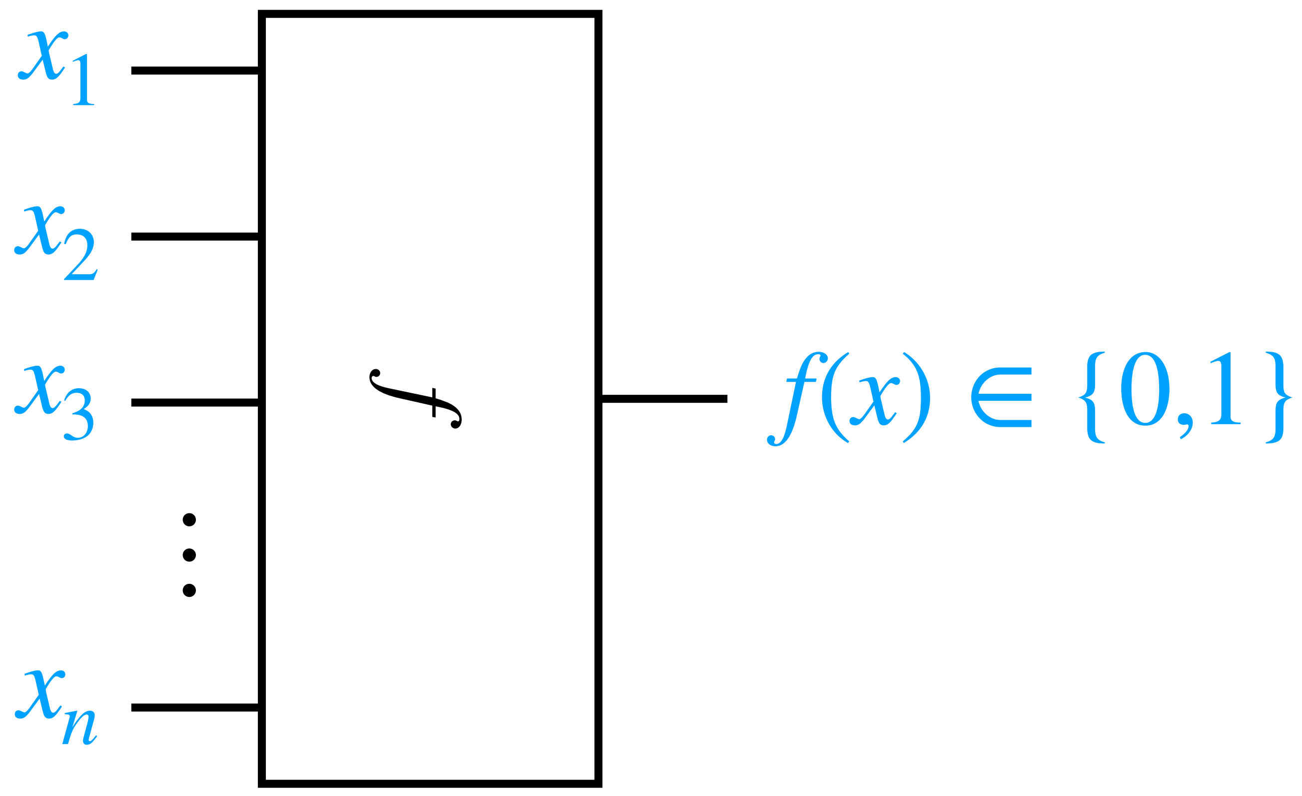
Quantum vs. classical circuits in constant depth

Question: What results hold for classical circuits but not quantum ones?

Correspondence between classical and quantum gate classes:

Classical circuit classes

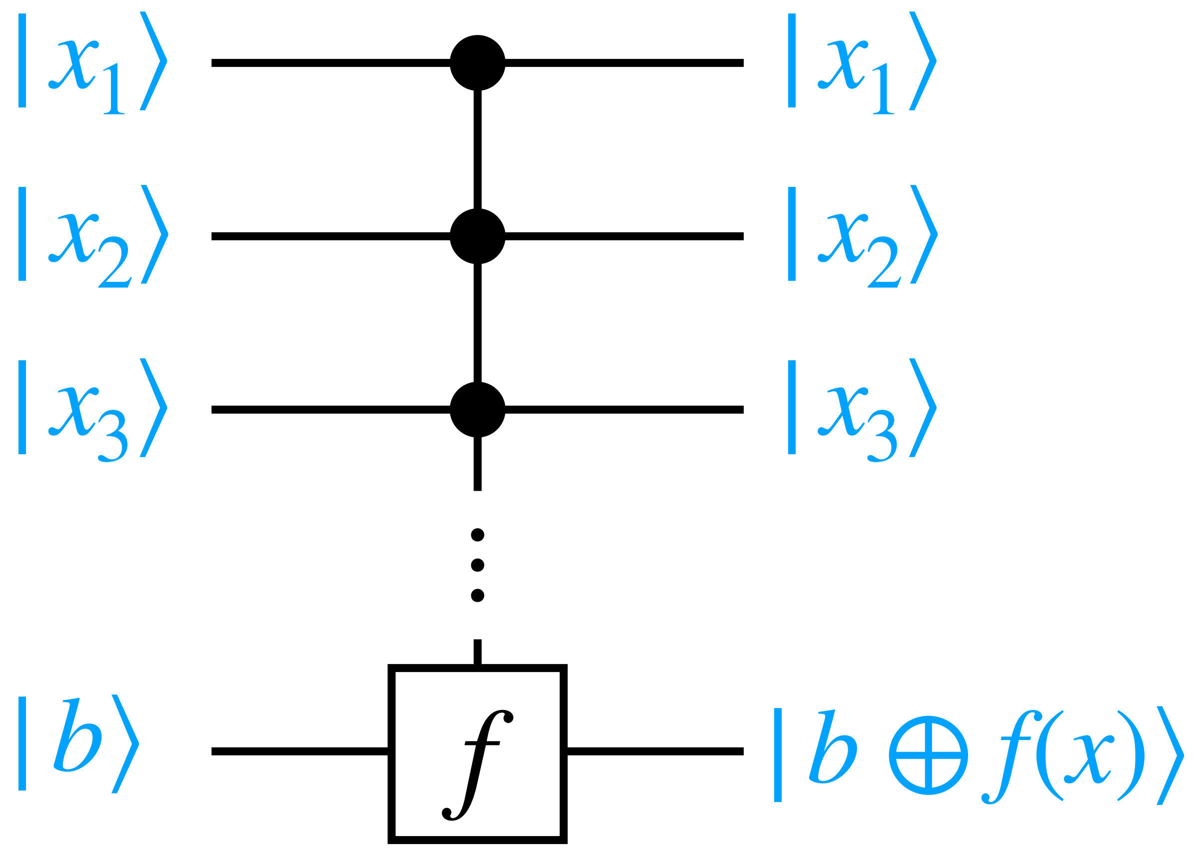
1- and 2-input gates



$\Longleftrightarrow$

Quantum circuit classes

1- and 2-qubit gates



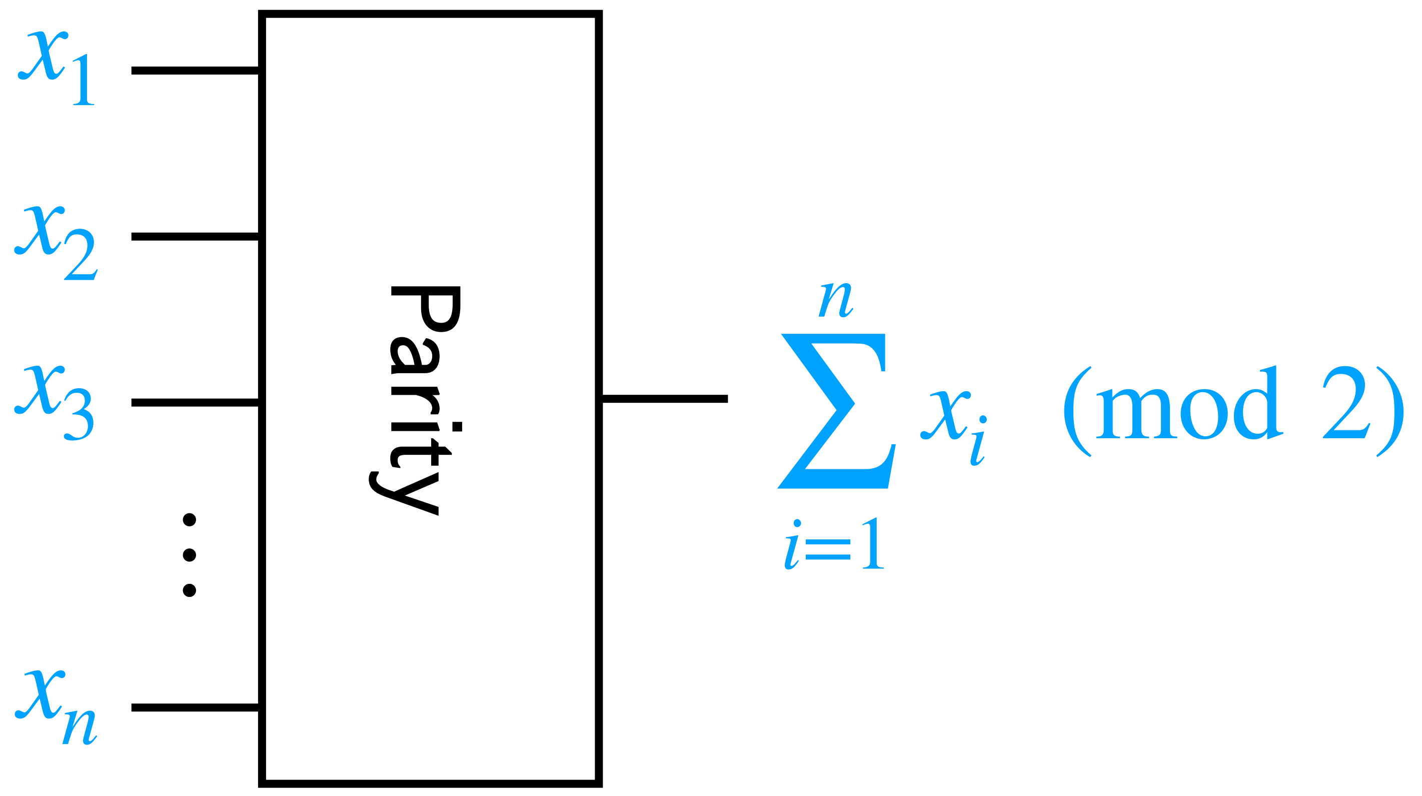
Quantum vs. classical circuits in constant depth

Question: What results hold for classical circuits but not quantum ones?

Correspondence between classical and quantum gate classes:

Classical circuit classes*

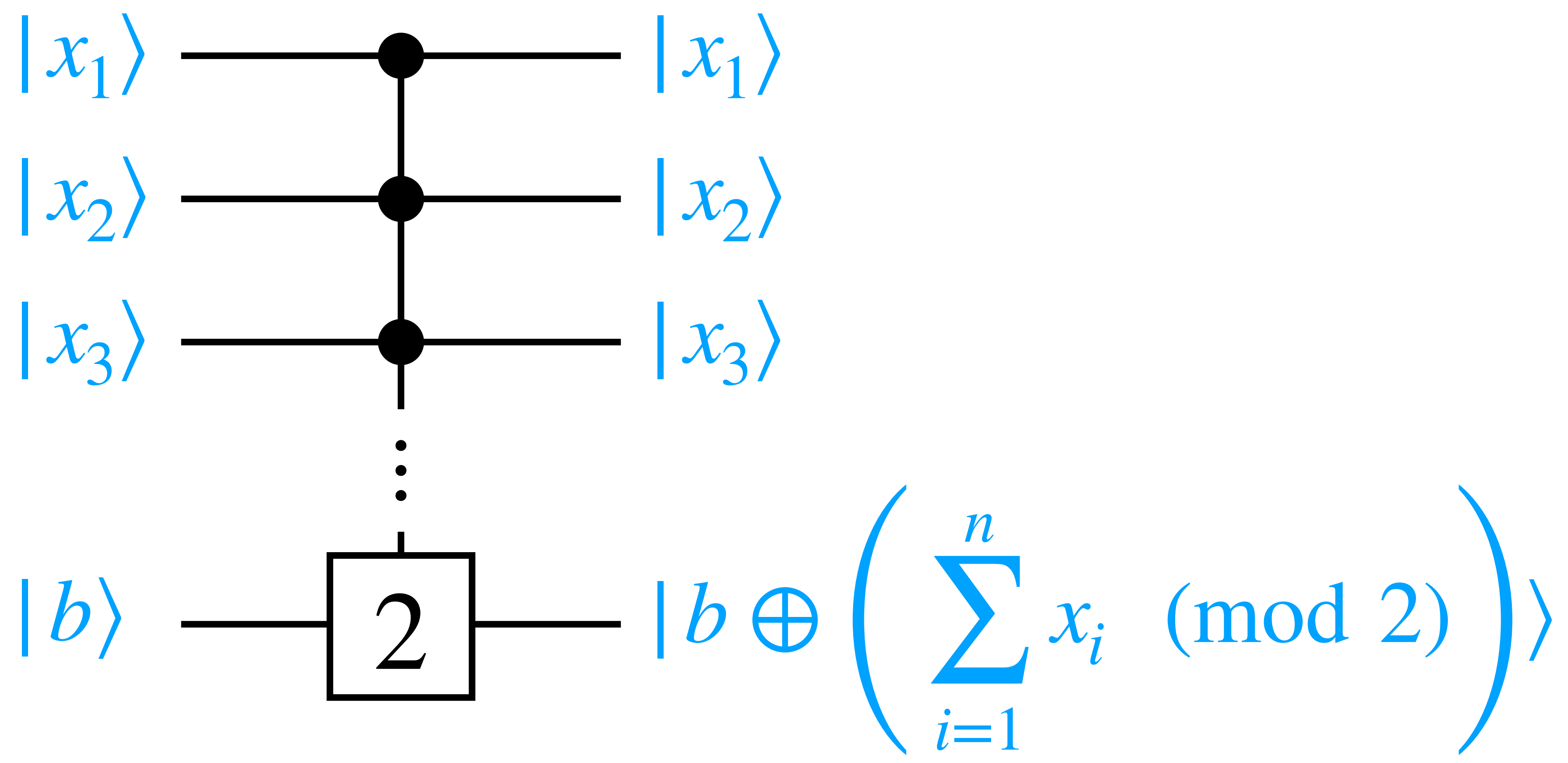
1- and 2-input gates



$\Longleftrightarrow$

Quantum circuit classes

1- and 2-qubit gates



Constant depth classical circuits can't compute parity

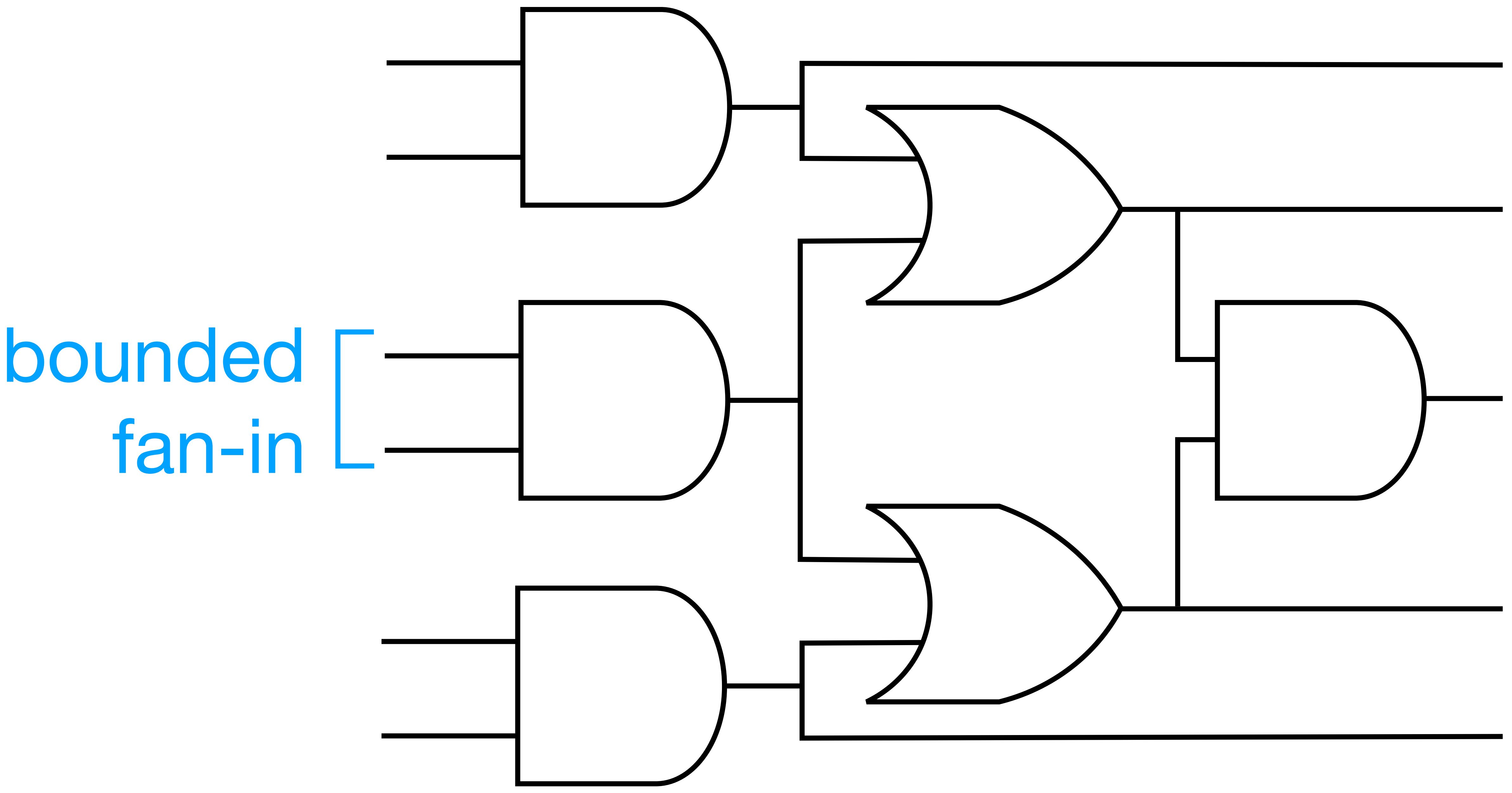
Question: Let $\mathscr{C}_1$ and $\mathscr{C}_2$ be classical circuit complexity classes.

$$\mathscr{C}_1 \subsetneq \mathscr{C}_2 \quad \overset{?}{\Longrightarrow} \quad \text{Q-}\mathscr{C}_1 \subsetneq \text{Q-}\mathscr{C}_2$$

Example: $\mathrm{NC}^0 \subsetneq \mathrm{NC}^0[2]$

NC

No large gates



Constant depth classical circuits can't compute parity

Question: Let $\mathscr{C}_1$ and $\mathscr{C}_2$ be classical circuit complexity classes.

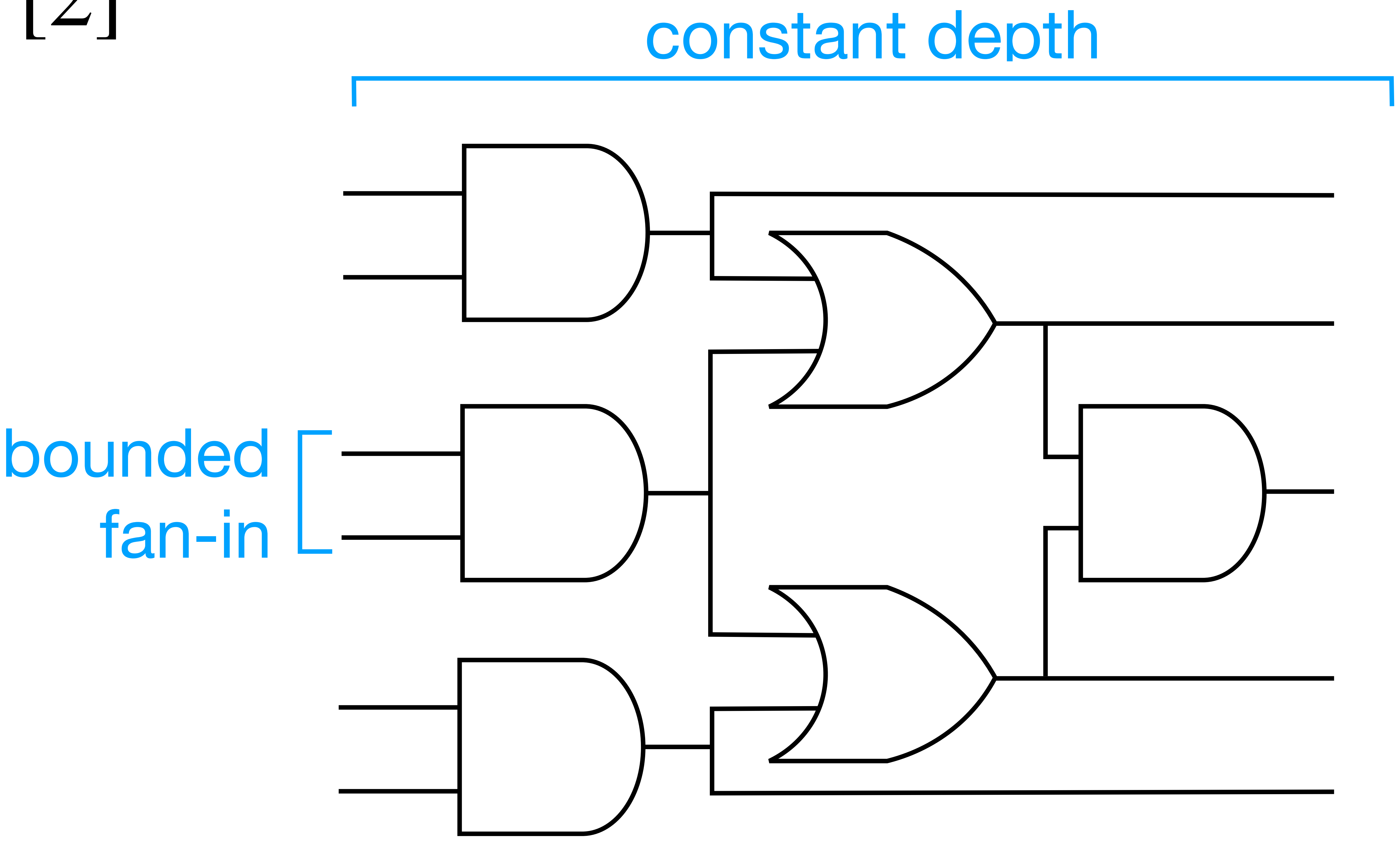
$$\mathscr{C}_1 \subsetneq \mathscr{C}_2 \quad \overset{?}{\Longrightarrow} \quad \text{Q-}\mathscr{C}_1 \subsetneq \text{Q-}\mathscr{C}_2$$

Example: $\mathrm{NC}^0 \subsetneq \mathrm{NC}^0[2]$

Constant depth

NC^0

No large gates



Constant depth classical circuits can't compute parity

Question: Let $\mathscr{C}_1$ and $\mathscr{C}_2$ be classical circuit complexity classes.

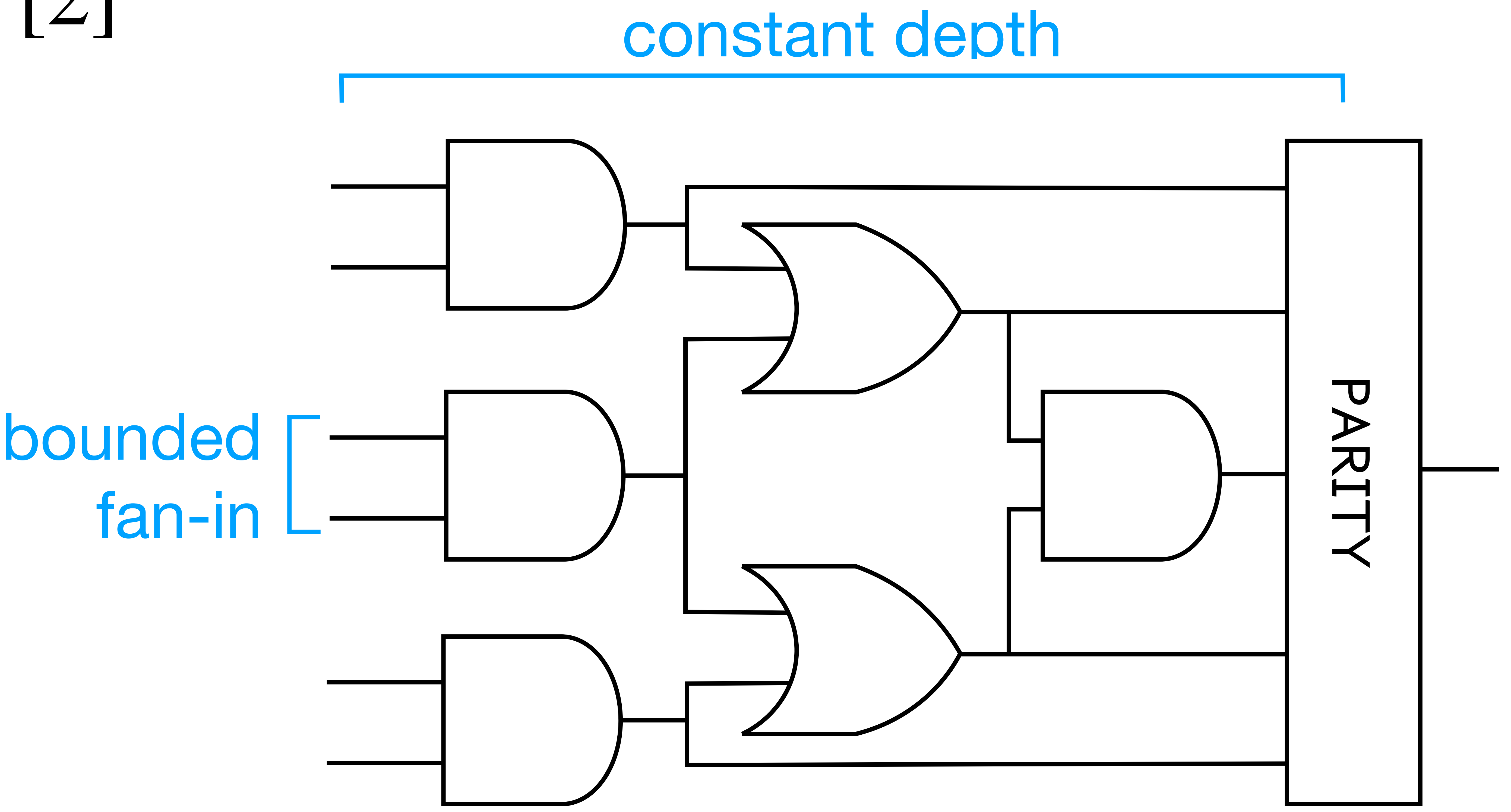
$$\mathscr{C}_1 \subsetneq \mathscr{C}_2 \quad \stackrel{?}{\Longrightarrow} \quad \text{Q-}\mathscr{C}_1 \subsetneq \text{Q-}\mathscr{C}_2$$

Example: $\mathrm{NC}^0 \subsetneq \mathrm{NC}^0[2]$

Constant depth

$\mathrm{NC}^0[2]$ ← Large parity gates

No large gates

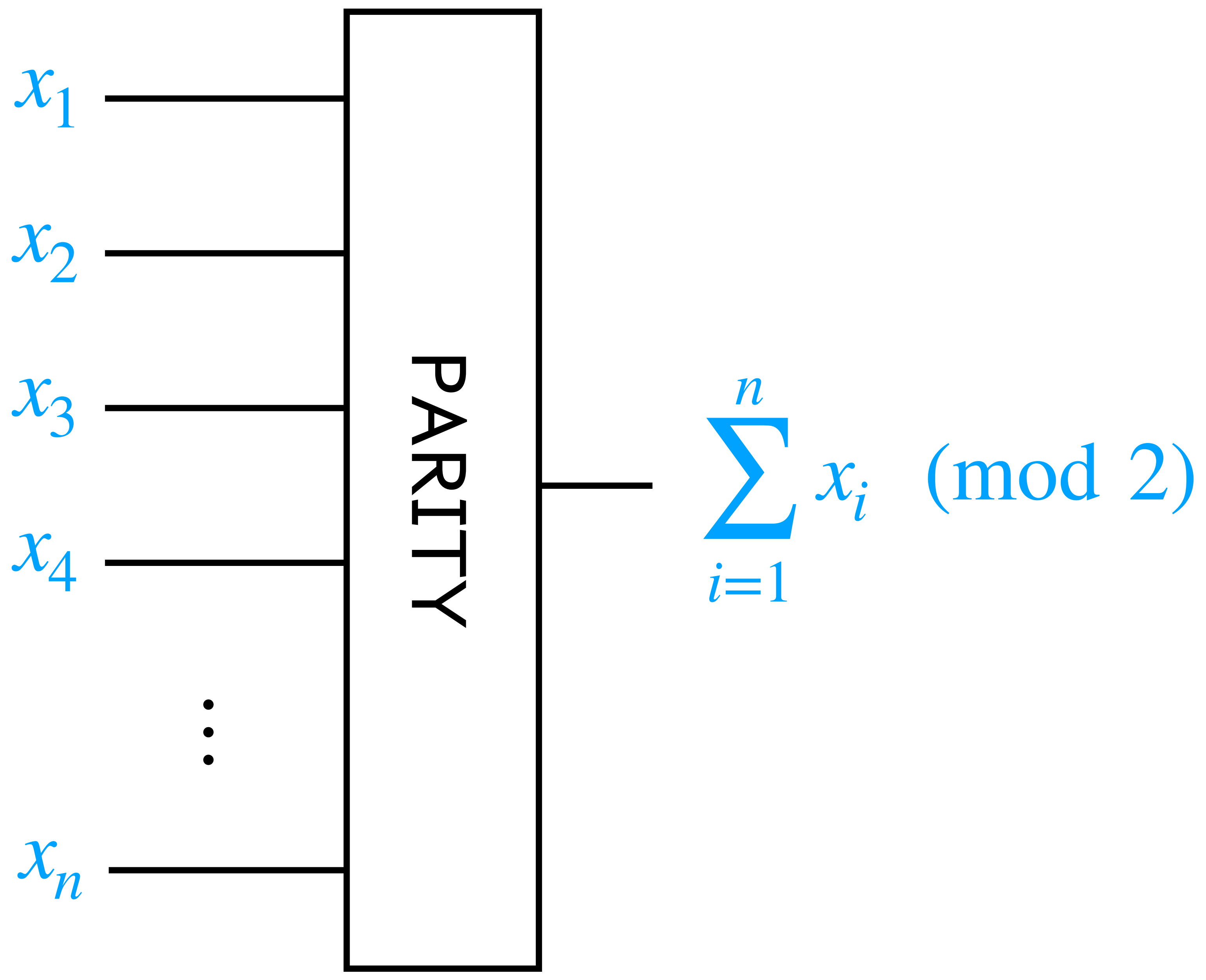


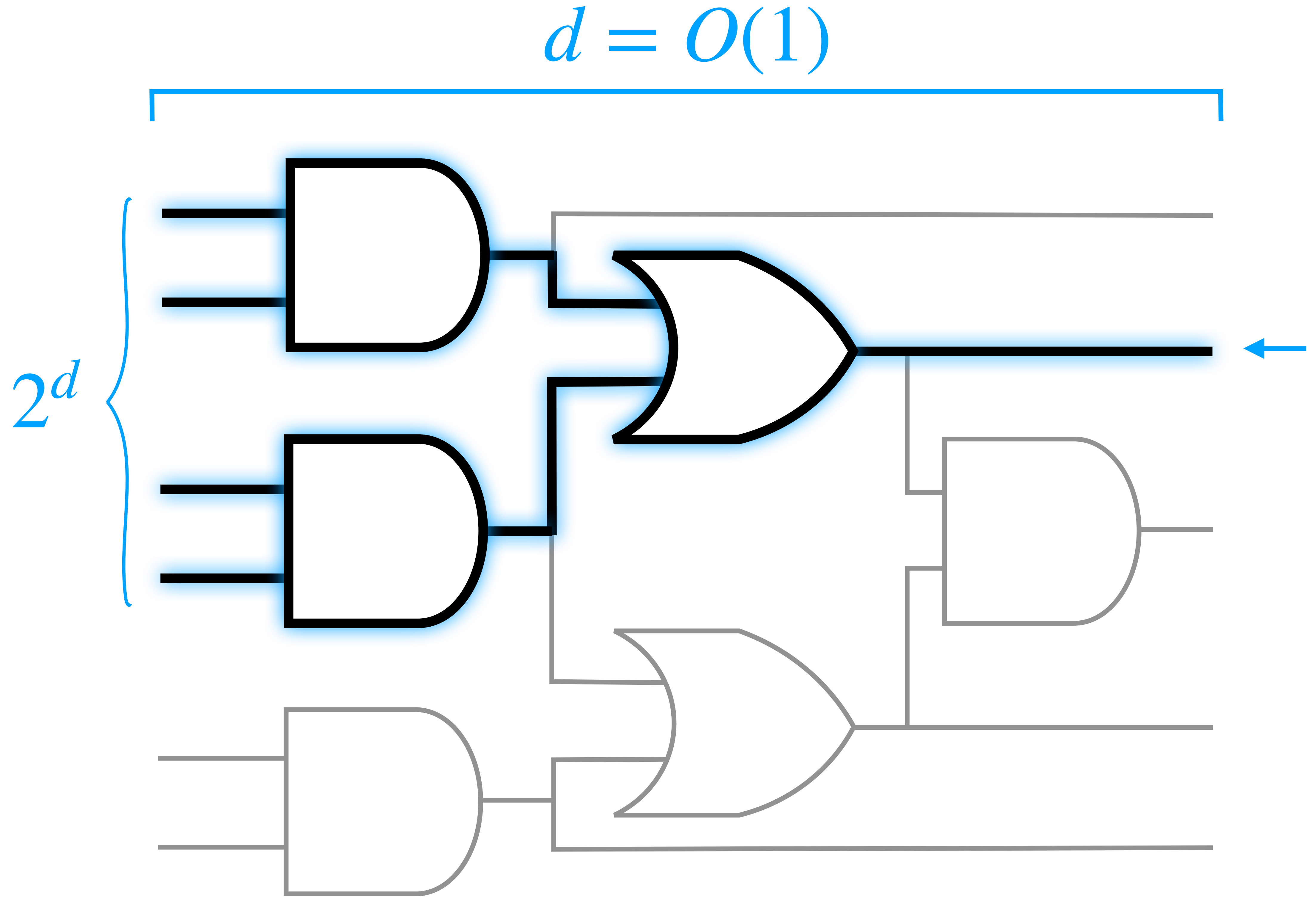
Lightcone of output bit is constant size

Question: Let $\mathscr{C}_1$ and $\mathscr{C}_2$ be classical circuit complexity classes.

$$\mathscr{C}_1 \subsetneq \mathscr{C}_2 \quad \overset{?}{\Longrightarrow} \quad \text{Q-}\mathscr{C}_1 \subsetneq \text{Q-}\mathscr{C}_2$$

Example: $\mathrm{NC}^0 \subsetneq \mathrm{NC}^0[2]$



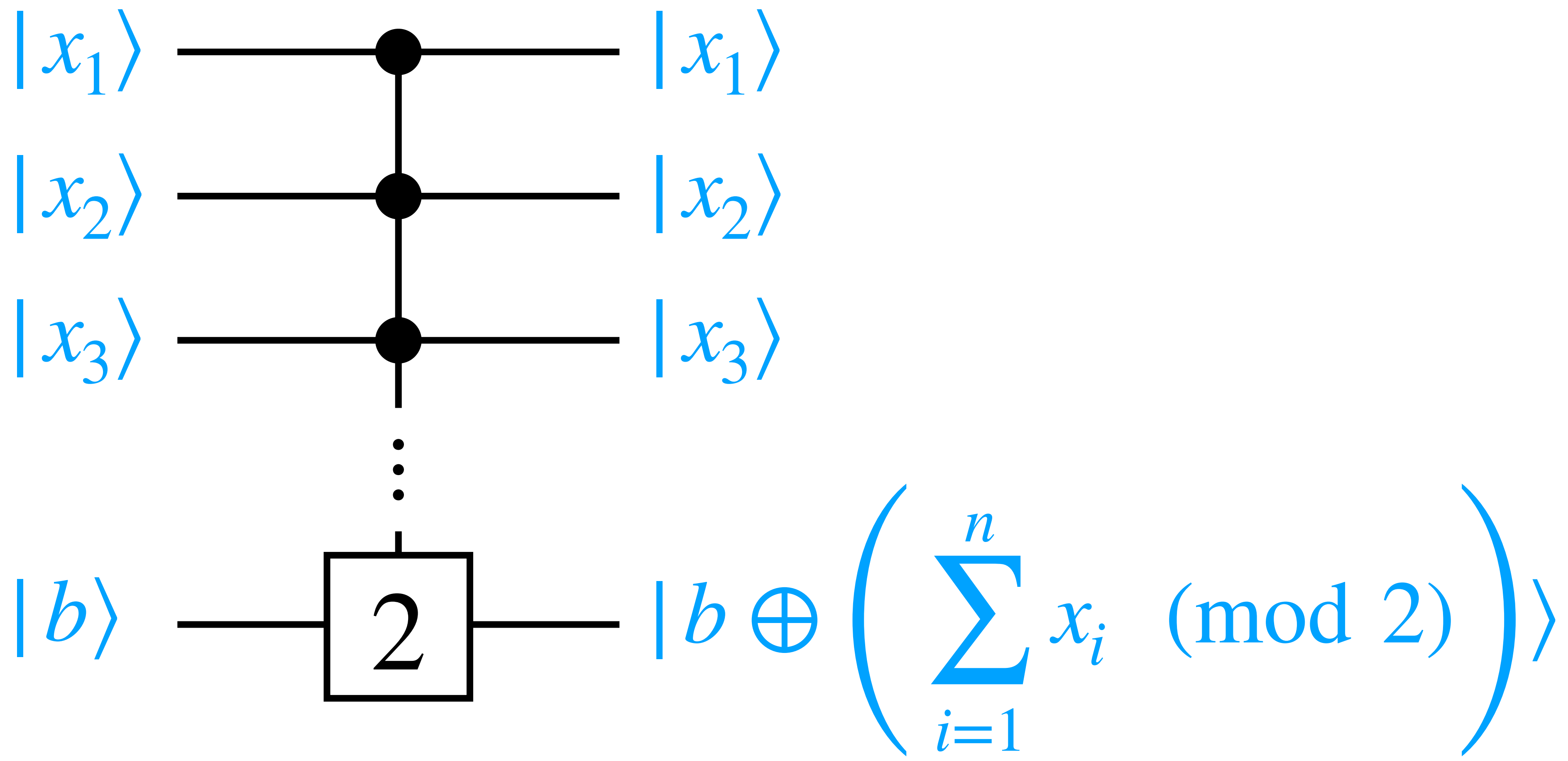


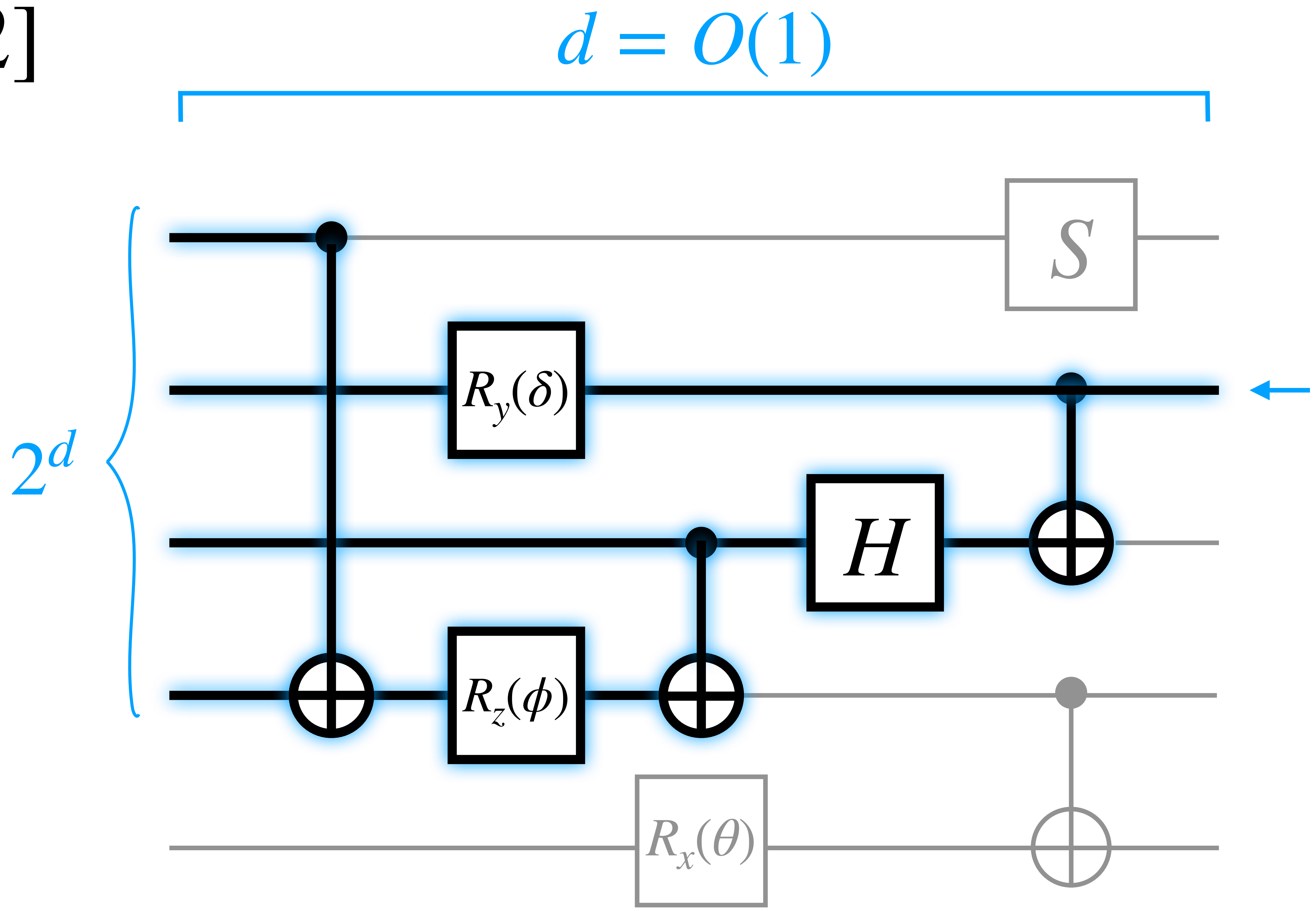
Quantum circuits are also constrained by lightcones

Question: Let $\mathscr{C}_1$ and $\mathscr{C}_2$ be classical circuit complexity classes.

$$\mathscr{C}_1 \subsetneq \mathscr{C}_2 \quad \overset{?}{\Longrightarrow} \quad \text{Q-}\mathscr{C}_1 \subsetneq \text{Q-}\mathscr{C}_2$$

Example: $\mathrm{QNC}^0 \subsetneq \mathrm{QNC}^0[2]$





AND gates cannot simulate Parity gates

Question: Let $\mathscr{C}_1$ and $\mathscr{C}_2$ be classical circuit complexity classes.

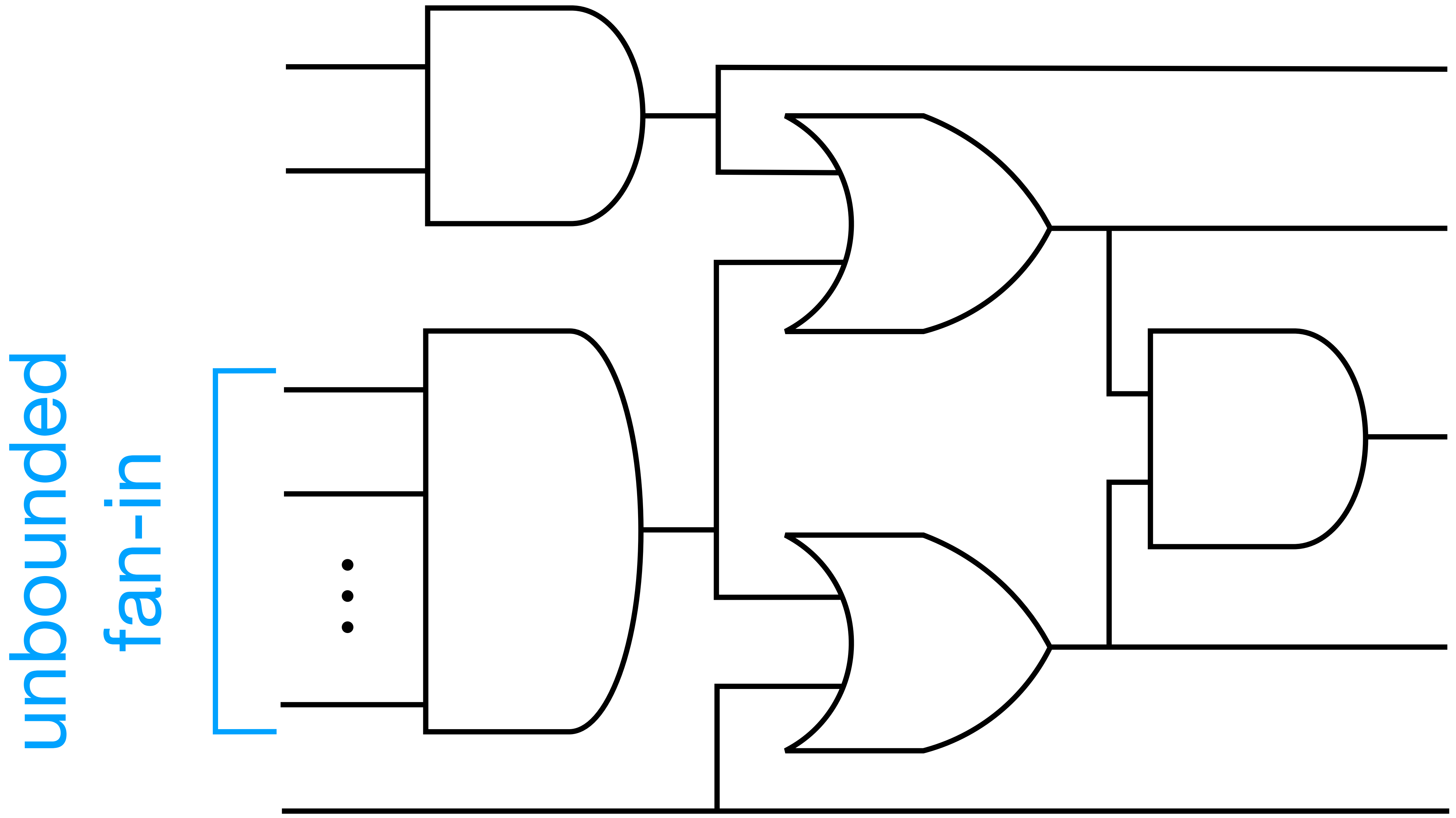
$$\mathscr{C}_1 \subsetneq \mathscr{C}_2 \quad \overset{?}{\Longrightarrow} \quad \text{Q-}\mathscr{C}_1 \subsetneq \text{Q-}\mathscr{C}_2$$

Example: $\mathrm{AC}^0 \subsetneq \mathrm{AC}^0[2]$

[Ajtai / Furst, Saxe, Sipser 83]

AC

Large And gates



AND gates cannot simulate Parity gates

Question: Let $\mathscr{C}_1$ and $\mathscr{C}_2$ be classical circuit complexity classes.

$$\mathscr{C}_1 \subsetneq \mathscr{C}_2 \quad \overset{?}{\Longrightarrow} \quad \text{Q-}\mathscr{C}_1 \subsetneq \text{Q-}\mathscr{C}_2$$

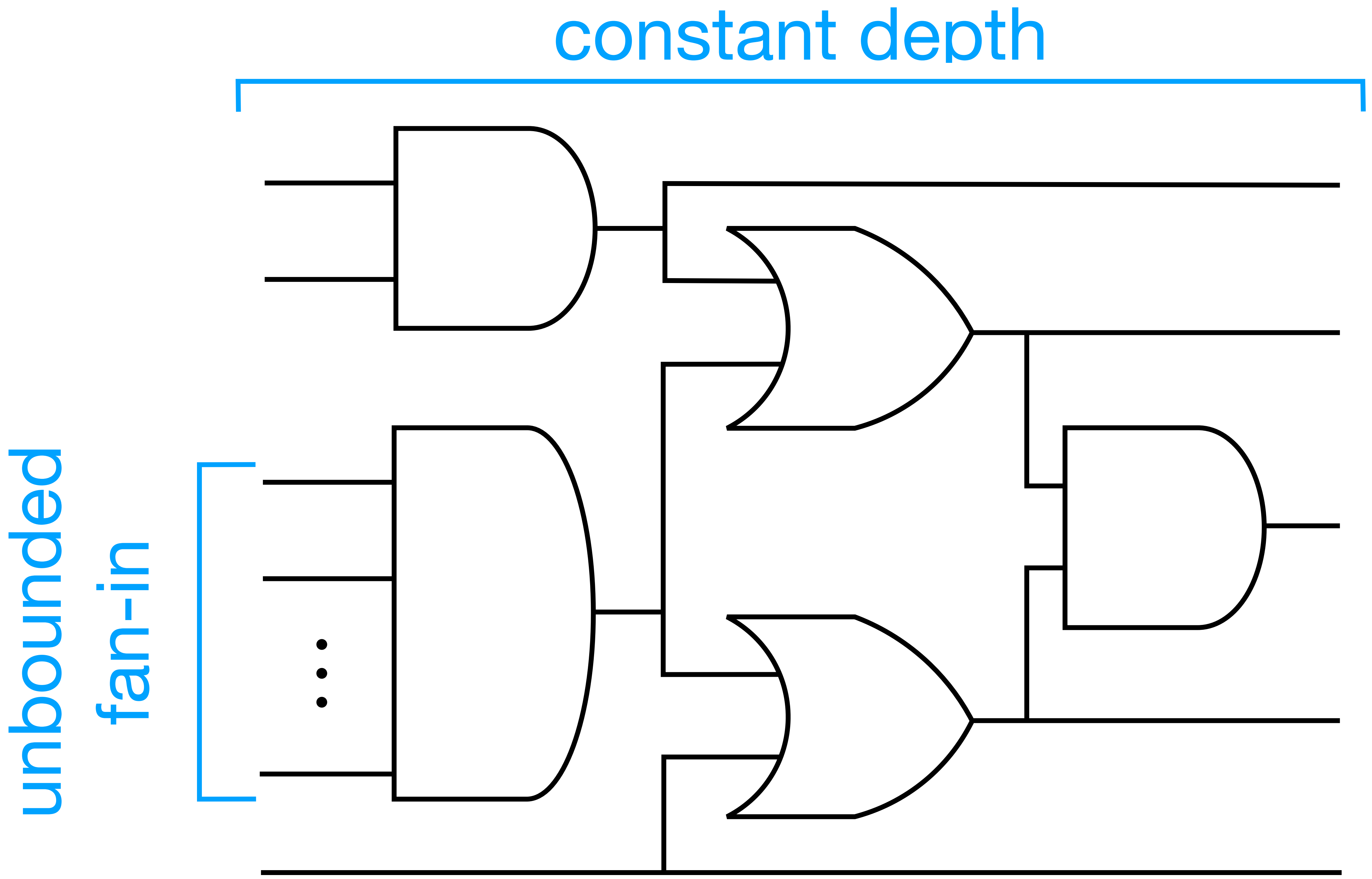
Example: $\mathrm{AC}^0 \subsetneq \mathrm{AC}^0[2]$

[Ajtai / Furst, Saxe, Sipser 83]

Constant depth

AC^0

Large And gates



AND gates cannot simulate Parity gates

Question: Let $\mathscr{C}_1$ and $\mathscr{C}_2$ be classical circuit complexity classes.

$$\mathscr{C}_1 \subsetneq \mathscr{C}_2 \quad \overset{?}{\Longrightarrow} \quad \text{Q-}\mathscr{C}_1 \subsetneq \text{Q-}\mathscr{C}_2$$

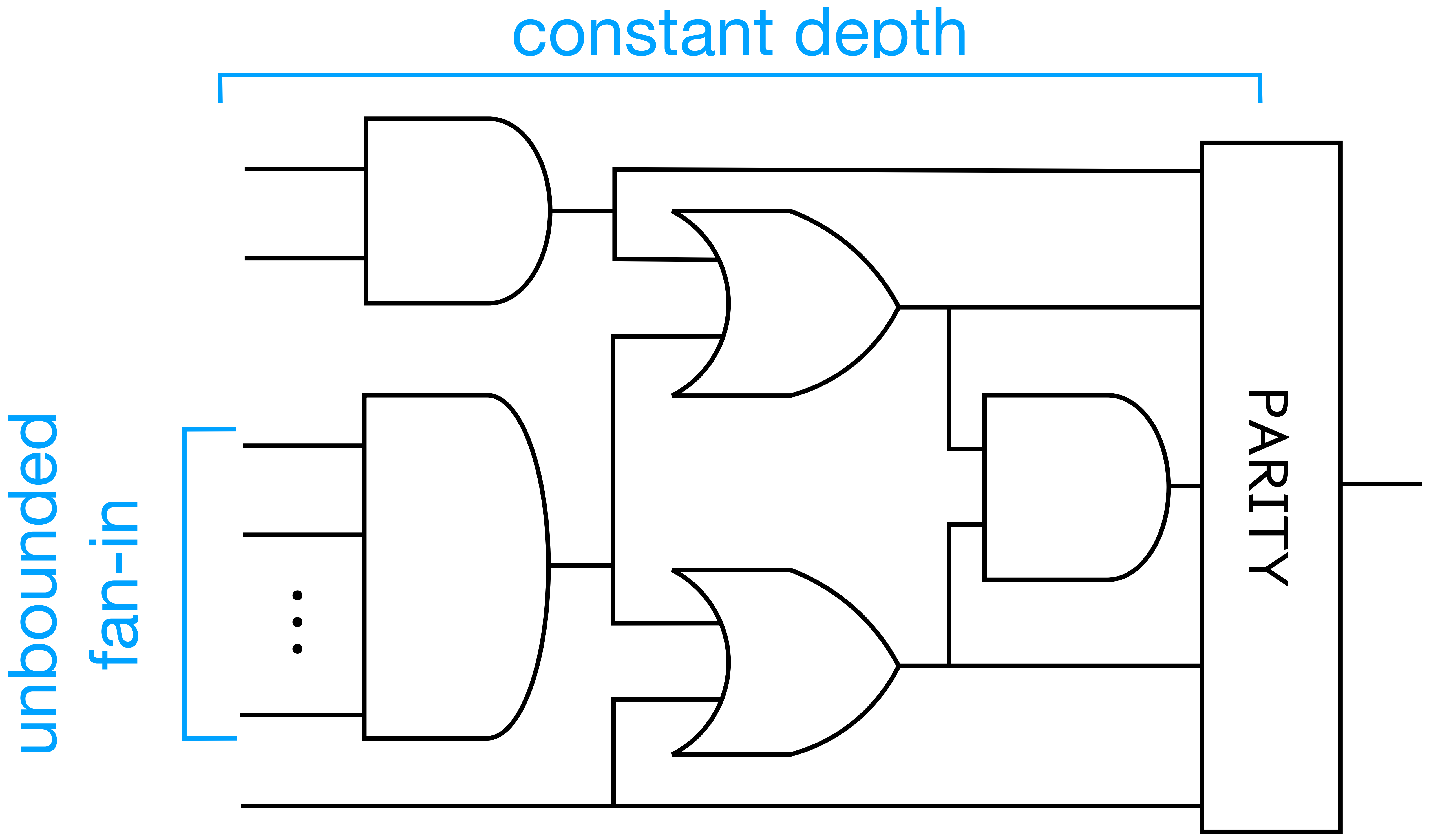
Example: $\mathsf{AC}^0 \subsetneq \mathsf{AC}^0[2]$

[Ajtai / Furst, Saxe, Sipser 83]

Constant depth

$\mathsf{AC}^0[2]$ ← Large parity gates

Large And gates



AND gates cannot simulate Parity gates

Question: Let $\mathscr{C}_1$ and $\mathscr{C}_2$ be classical circuit complexity classes.

$$\mathscr{C}_1 \subsetneq \mathscr{C}_2 \quad \overset{?}{\Longrightarrow} \quad \text{Q-}\mathscr{C}_1 \subsetneq \text{Q-}\mathscr{C}_2$$

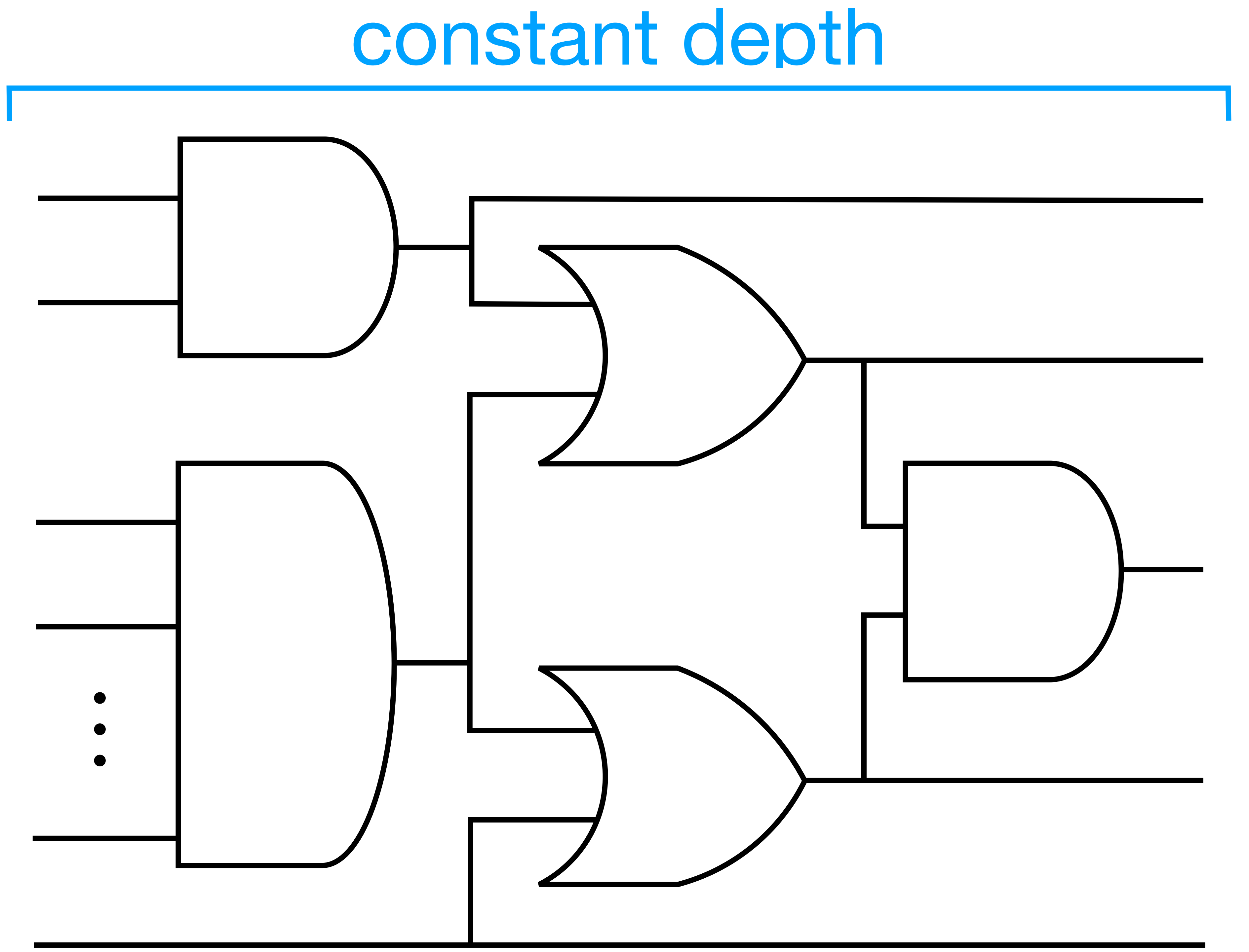
Example: $\mathrm{AC}^0 \subsetneq \mathrm{AC}^0[2]$

[Ajtai / Furst, Saxe, Sipser 83]

Constant depth

$\mathrm{AC}^0[2]$ ← Large parity gates

Large And gates



AND gates cannot simulate Parity gates

Question: Let $\mathscr{C}_1$ and $\mathscr{C}_2$ be classical circuit complexity classes.

$$\mathscr{C}_1 \subsetneq \mathscr{C}_2 \quad \overset{?}{\Longrightarrow} \quad \text{Q-}\mathscr{C}_1 \subsetneq \text{Q-}\mathscr{C}_2$$

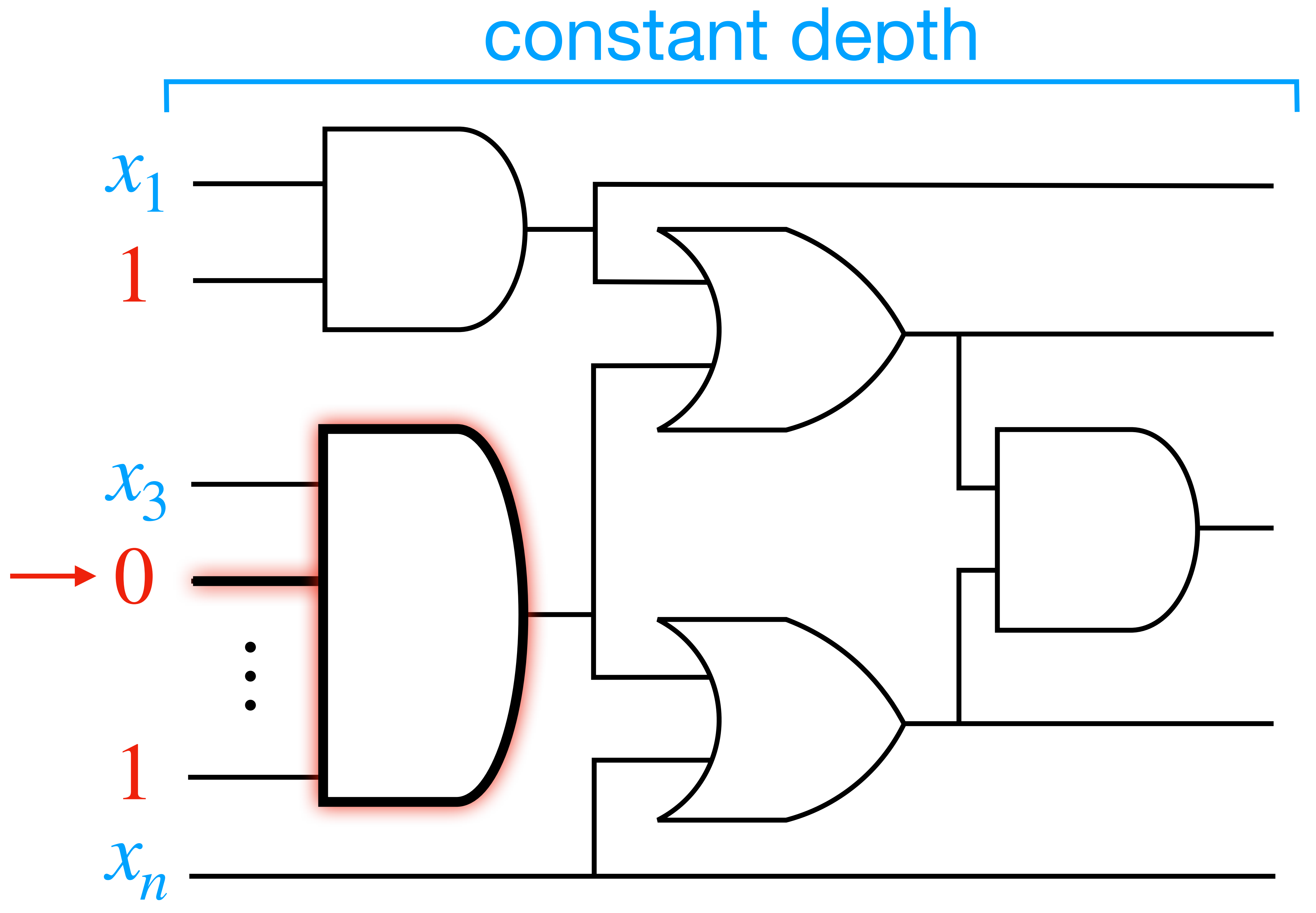
Example: $\mathrm{AC}^0 \subsetneq \mathrm{AC}^0[2]$

[Ajtai / Furst, Saxe, Sipser 83]

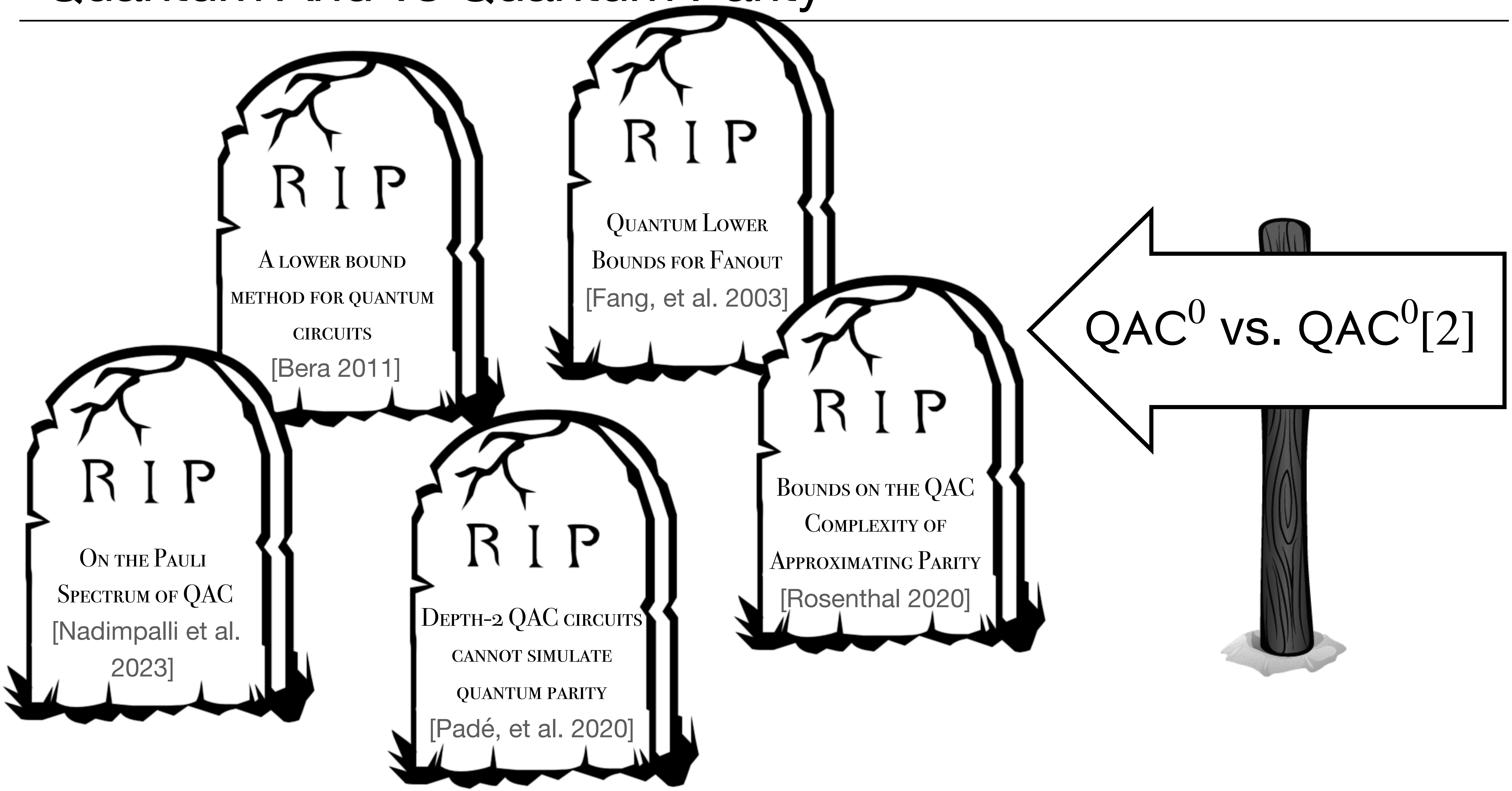
Constant depth

$\mathrm{AC}^0[2]$ ← Large parity gates

Large And gates



Quantum And vs Quantum Parity

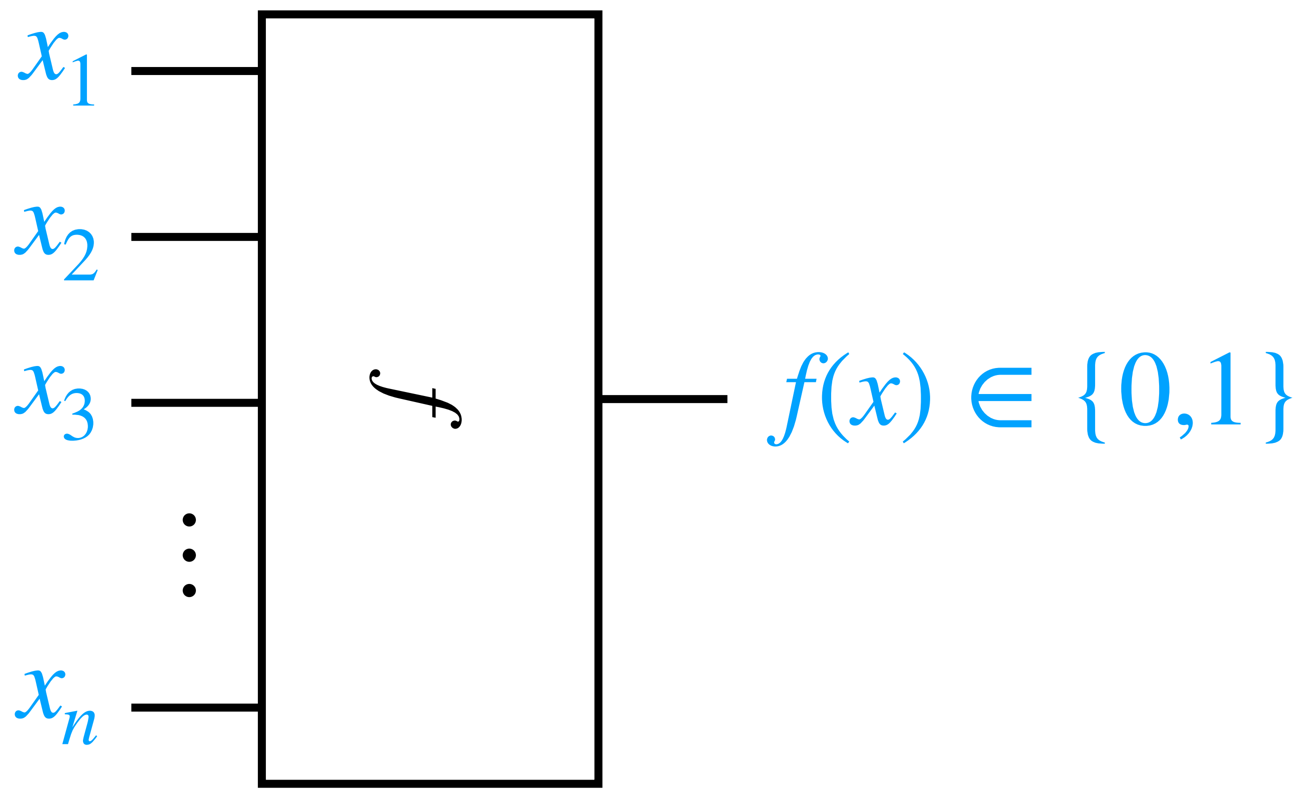


Outline

- Barrier to separations
    - Quantum constant-depth circuits are powerful
    - The surprising relevance of Fanout and Parity
- Maybe we should look for other powerful gates…
- Quantum Majority is powerful

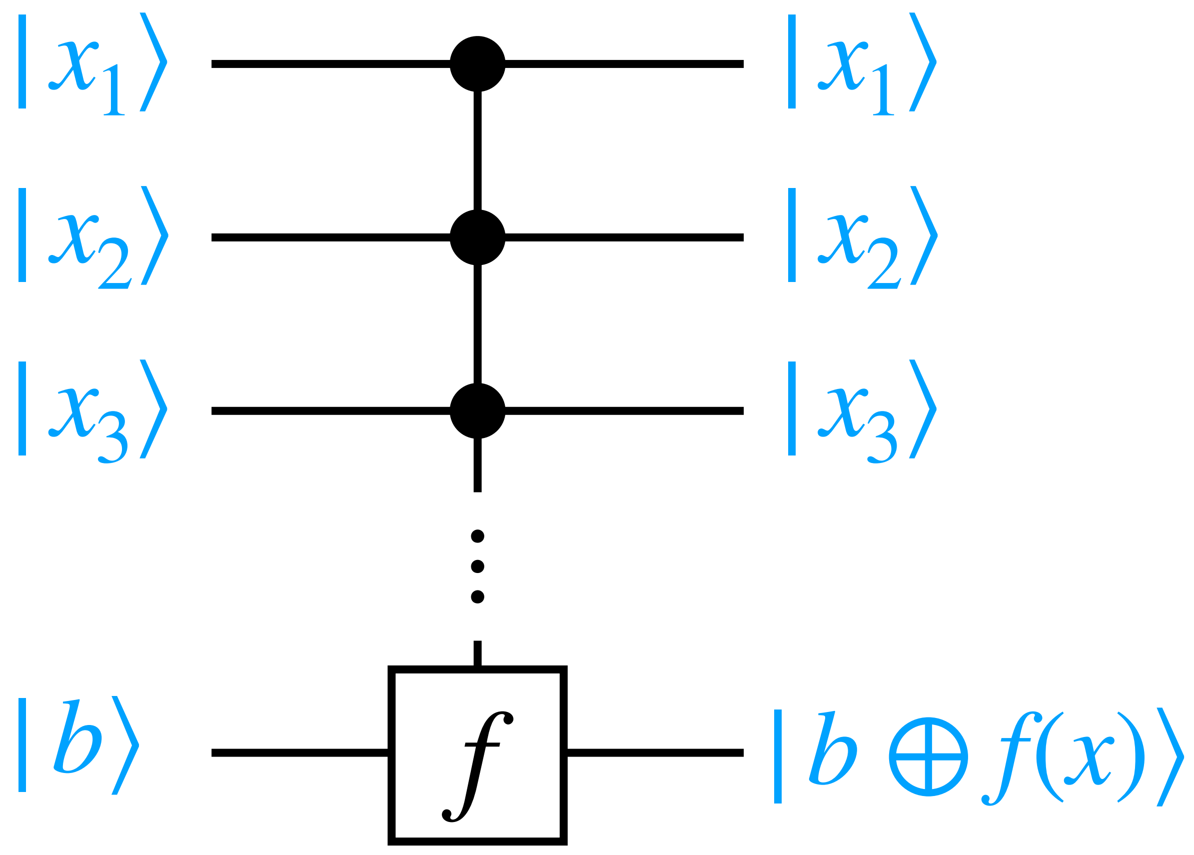
Correspondence between classical and quantum gate classes

Classical circuit classes *
1- and 2-input gates

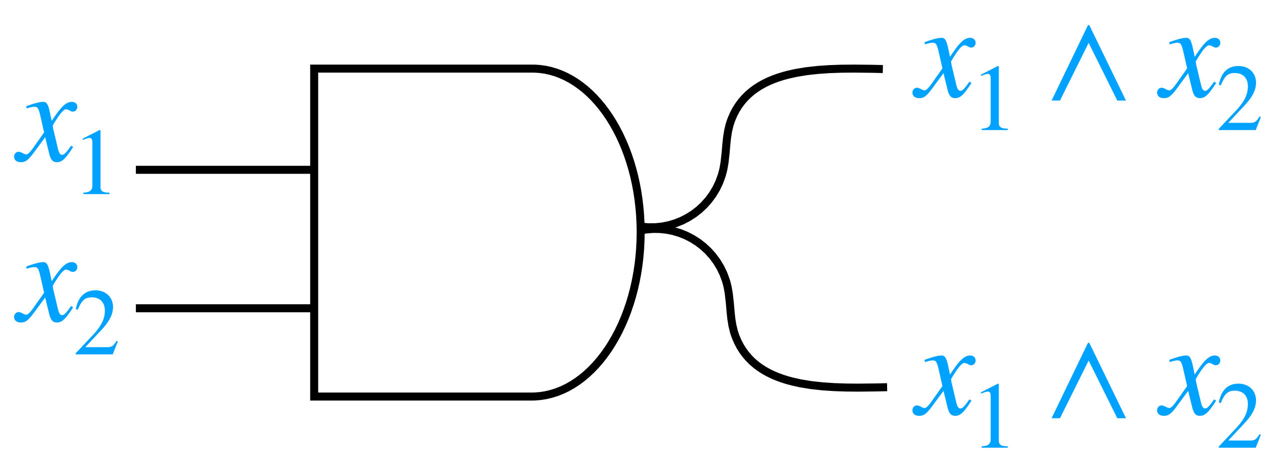


$\iff$

Quantum circuit classes
1- and 2-qubit gates

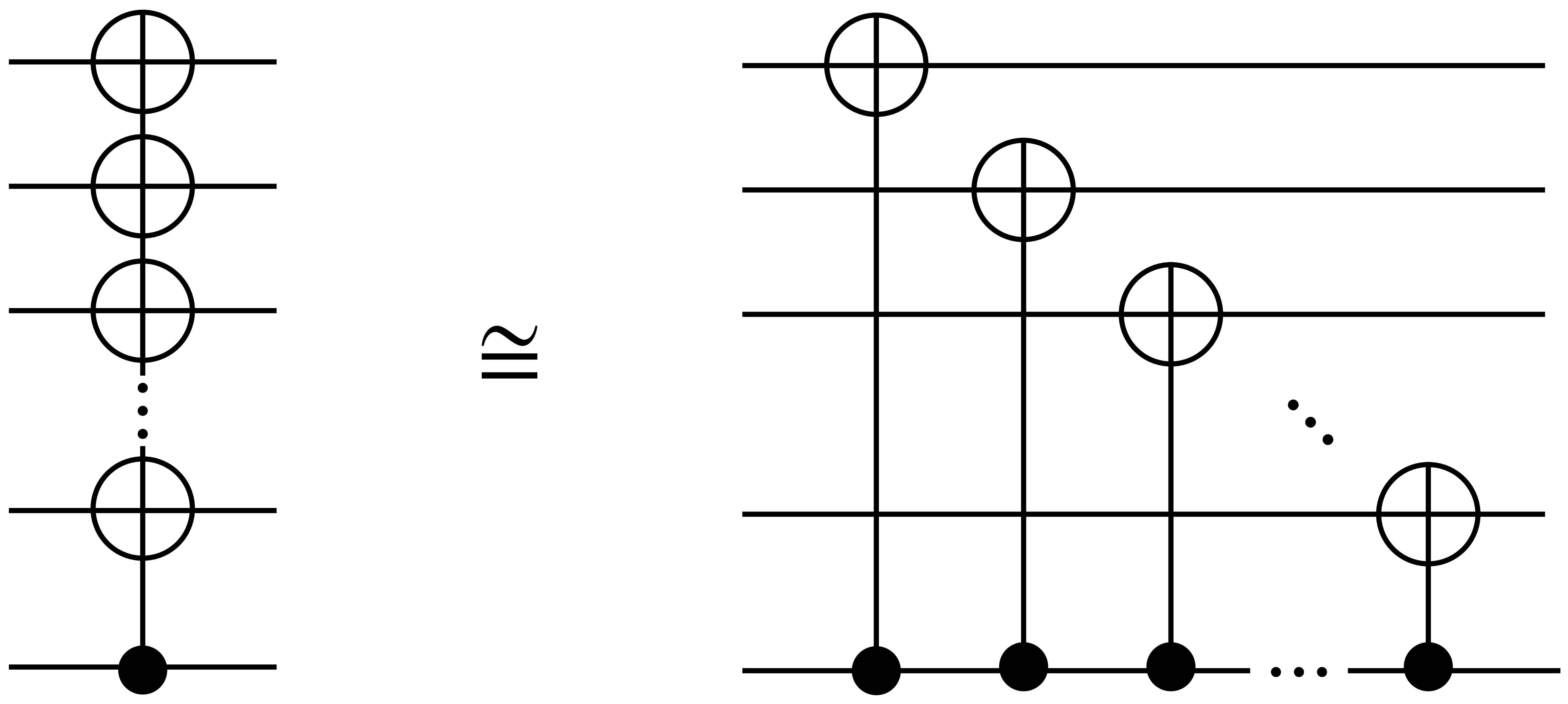


Fanout: Classical gate classes allowed to copy gate outputs



Quantum Fanout

$$\text{Fanout}\,|b, x_1, x_2, \ldots, x_n\rangle = |b, x_1 \oplus b, \ldots, x_n \oplus b\rangle$$



Quantum Fanout is scary

Theorem [Moore 1999]**:** $\mathrm{QNC}^0[2] = \mathrm{QNC}^0_{wf}$

→ Constant-depth quantum circuits with Fanout can compute Parity

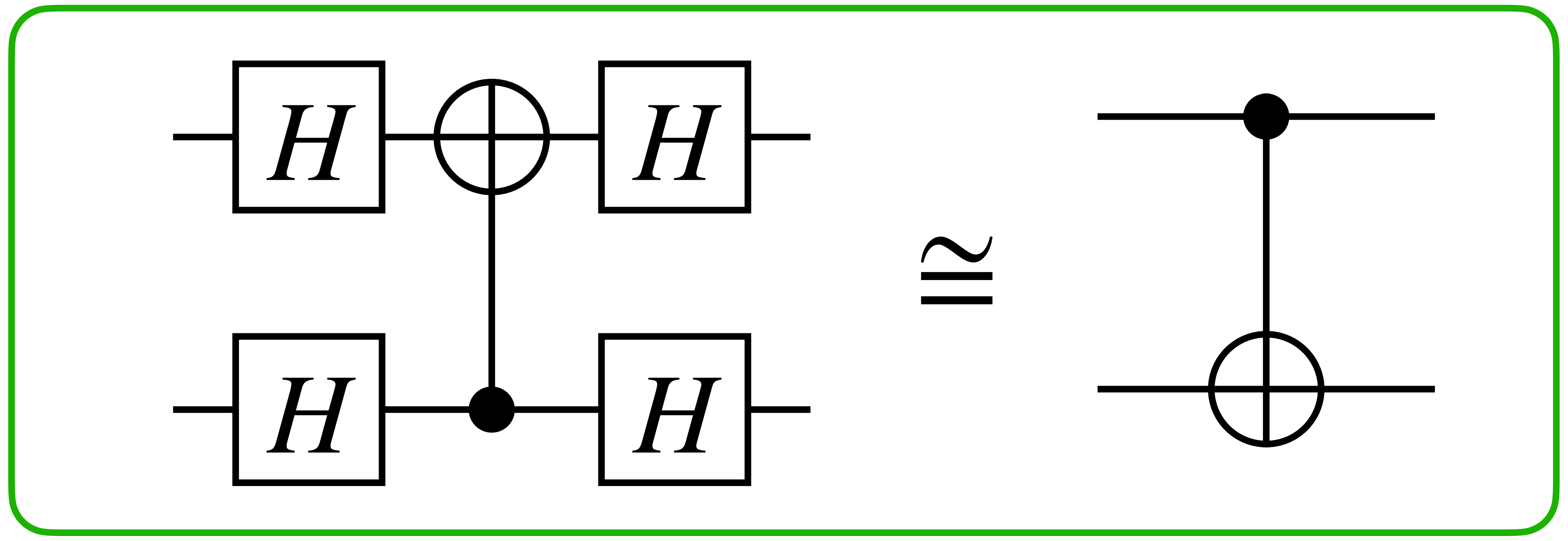
→ $(H^{\otimes n})$ · Fanout · $(H^{\otimes n})$ = Parity

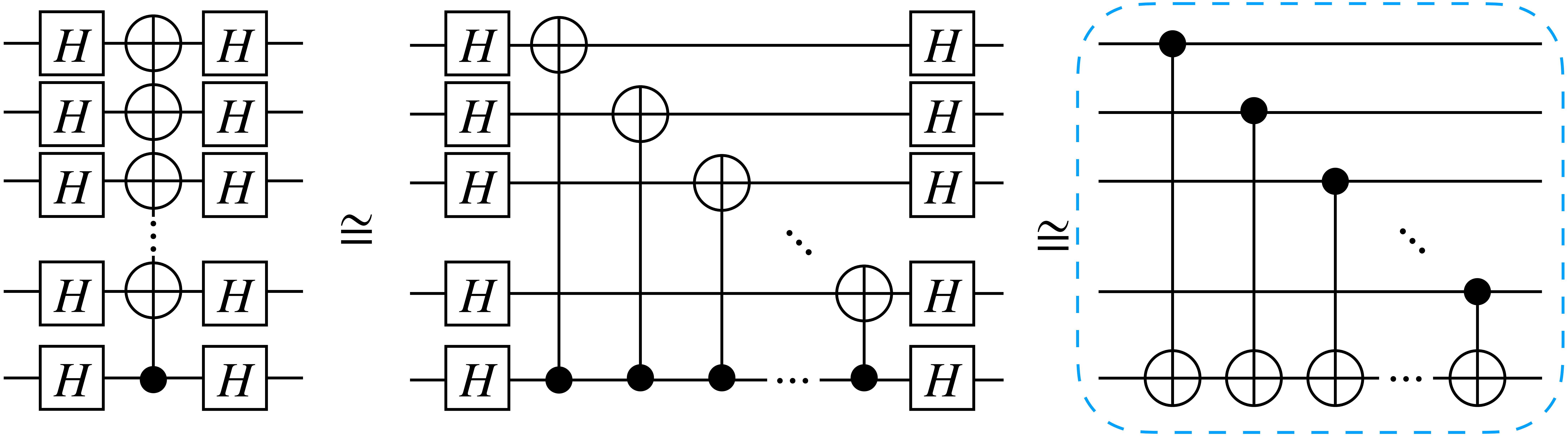
Recall: $\mathrm{AC}^0 \subsetneq \mathrm{AC}[2]$

→ Classical fanout does not imply Parity

Quantum Fanout implies Quantum Parity

Theorem [Moore 1999]**:**
$\mathrm{QNC}^0[2] = \mathrm{QNC}^0_{wf}$





Parity!

Let's try another separation…

Question: Let $\mathscr{C}_1$ and $\mathscr{C}_2$ be classical circuit complexity classes.

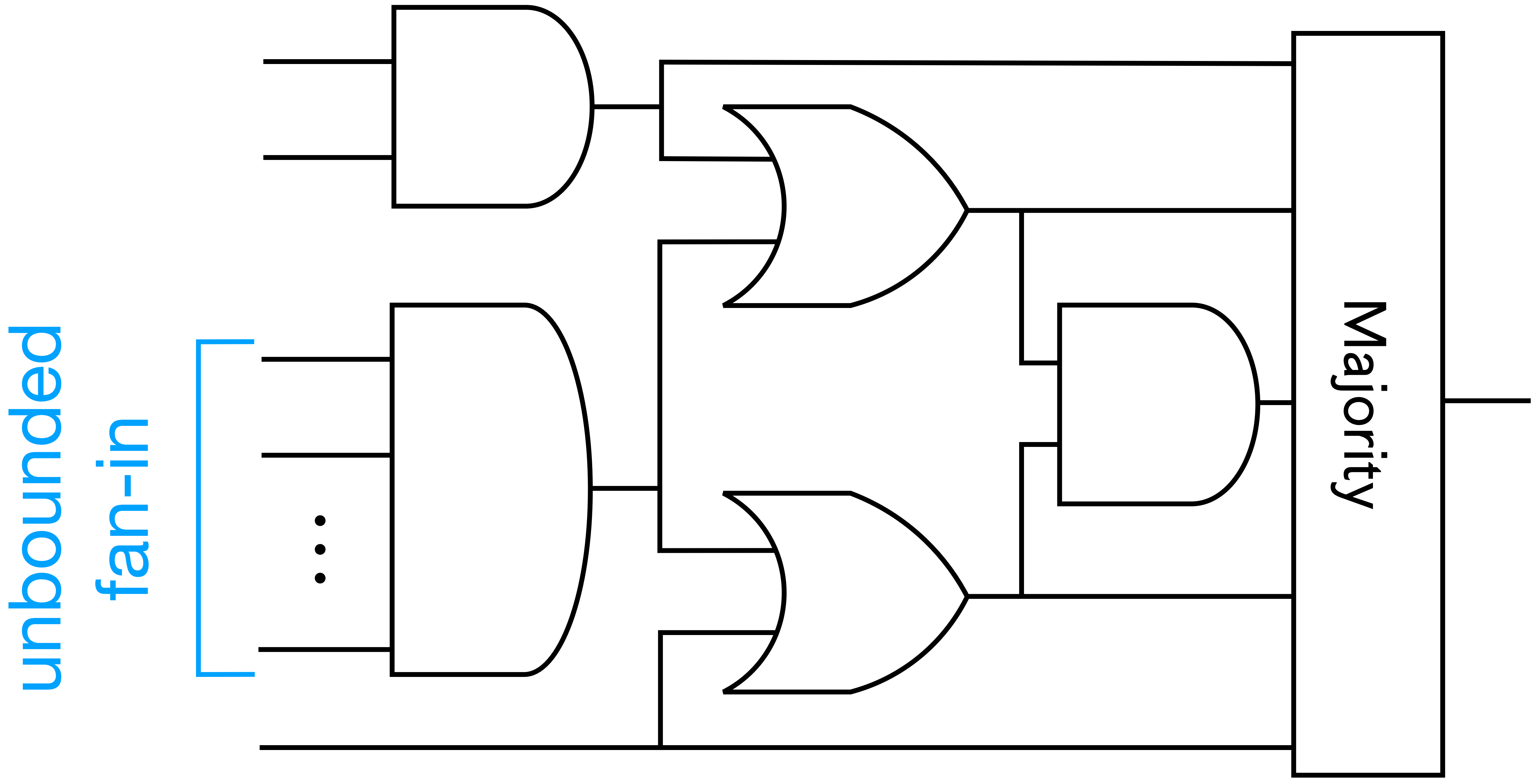
$$\mathscr{C}_1 \subsetneq \mathscr{C}_2 \quad \overset{?}{\Longrightarrow} \quad \text{Q-}\mathscr{C}_1 \subsetneq \text{Q-}\mathscr{C}_2$$

Example: $\mathrm{AC}^0[2] \subsetneq \mathrm{TC}^0$

[Razborov, Smolensky 87]

TC

Large Threshold gates



Let's try another separation…

Question: Let $\mathscr{C}_1$ and $\mathscr{C}_2$ be classical circuit complexity classes.

$$\mathscr{C}_1 \subsetneq \mathscr{C}_2 \quad \overset{?}{\Longrightarrow} \quad \text{Q-}\mathscr{C}_1 \subsetneq \text{Q-}\mathscr{C}_2$$

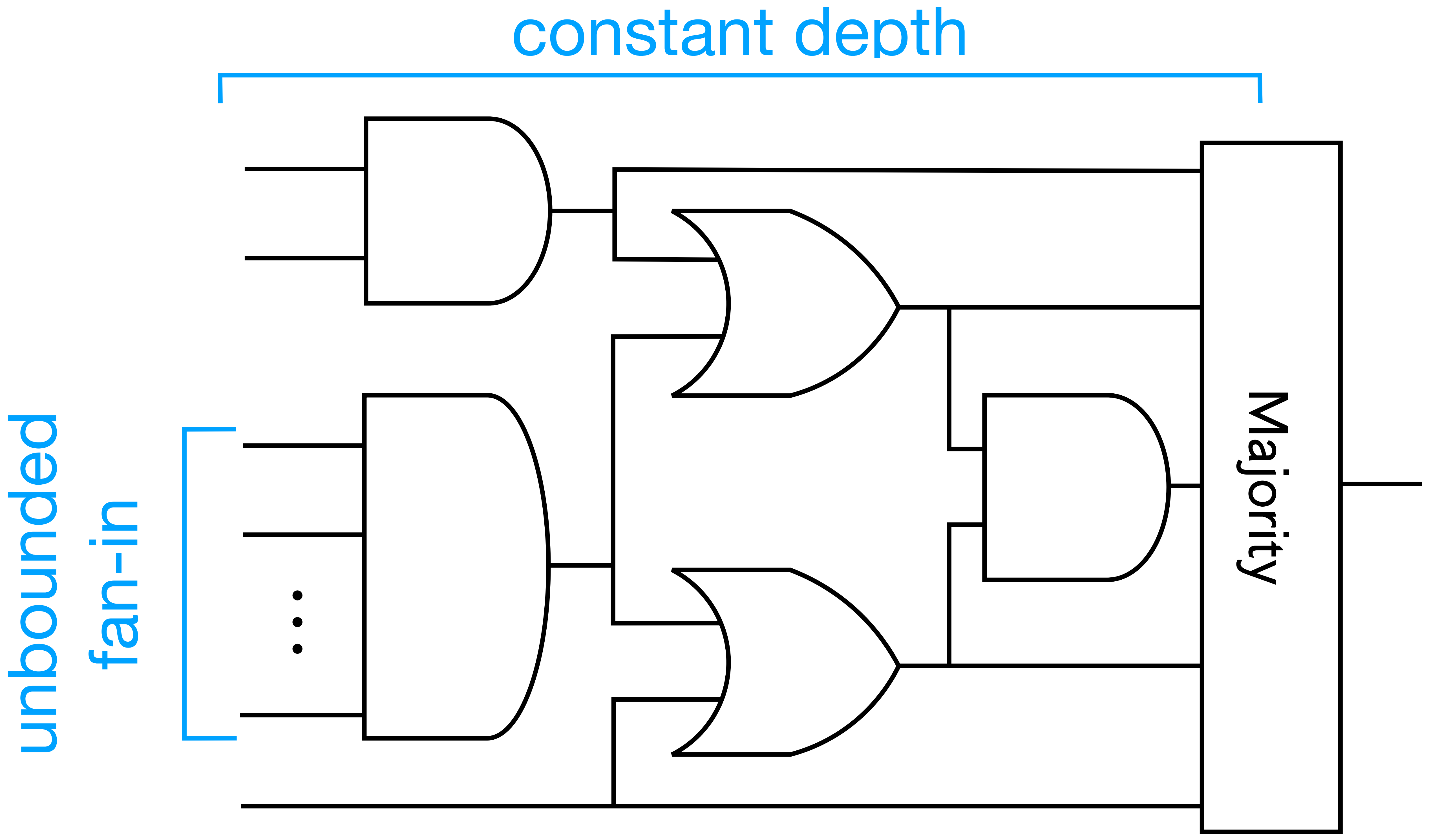
Example: $\mathrm{AC}^0[2] \subsetneq \mathrm{TC}^0$

[Razborov, Smolensky 87]

Constant depth

TC^0

Large Threshold gates



Fanout is powerful…

Question: Let $\mathscr{C}_1$ and $\mathscr{C}_2$ be classical circuit complexity classes.

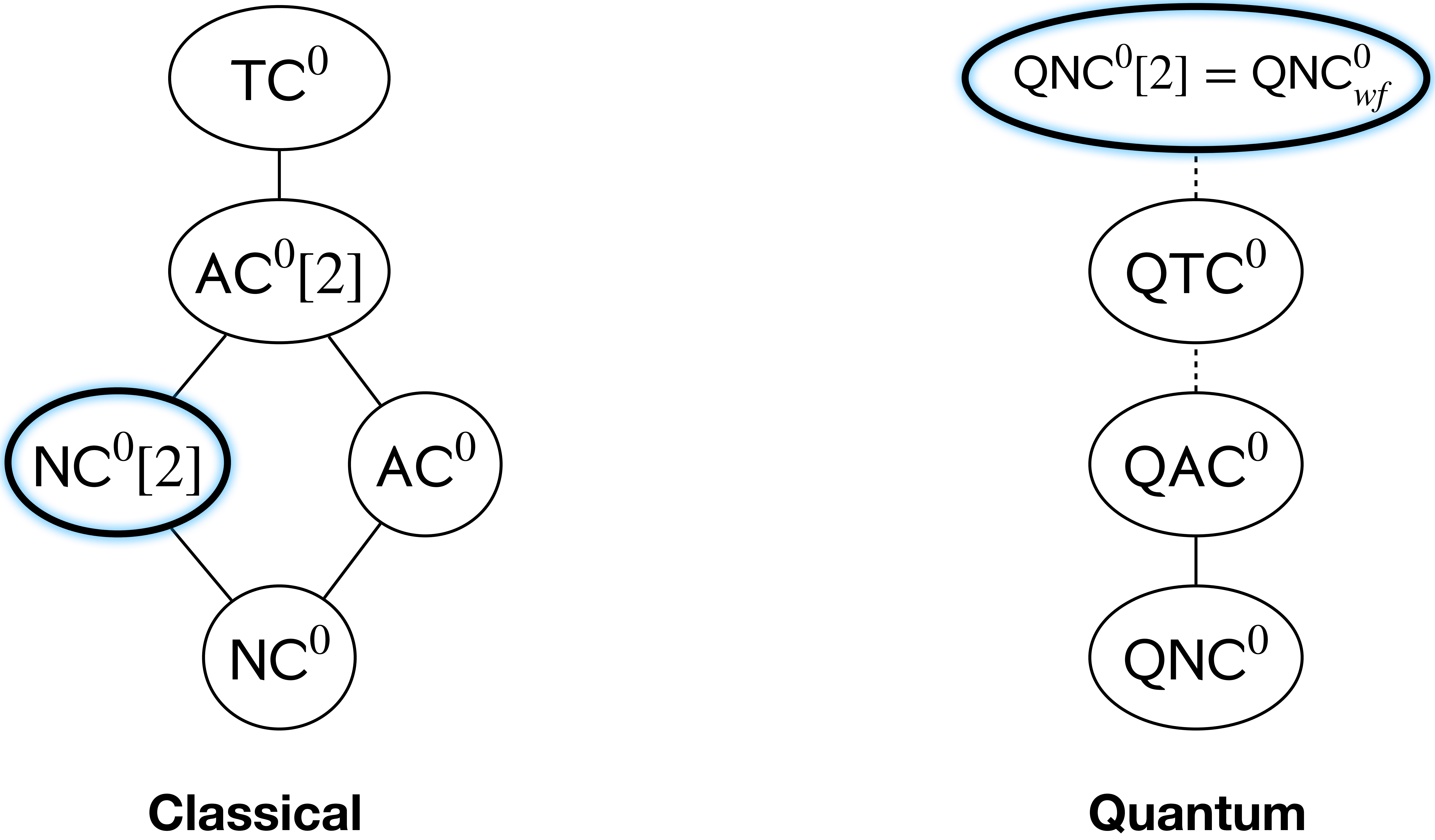
$$\mathscr{C}_1 \subsetneq \mathscr{C}_2 \qquad \overset{?}{\Longrightarrow} \qquad \text{Q-}\mathscr{C}_1 \subsetneq \text{Q-}\mathscr{C}_2$$

Example: $\mathrm{QAC}^0[2] \subsetneq \mathrm{QTC}^0$?

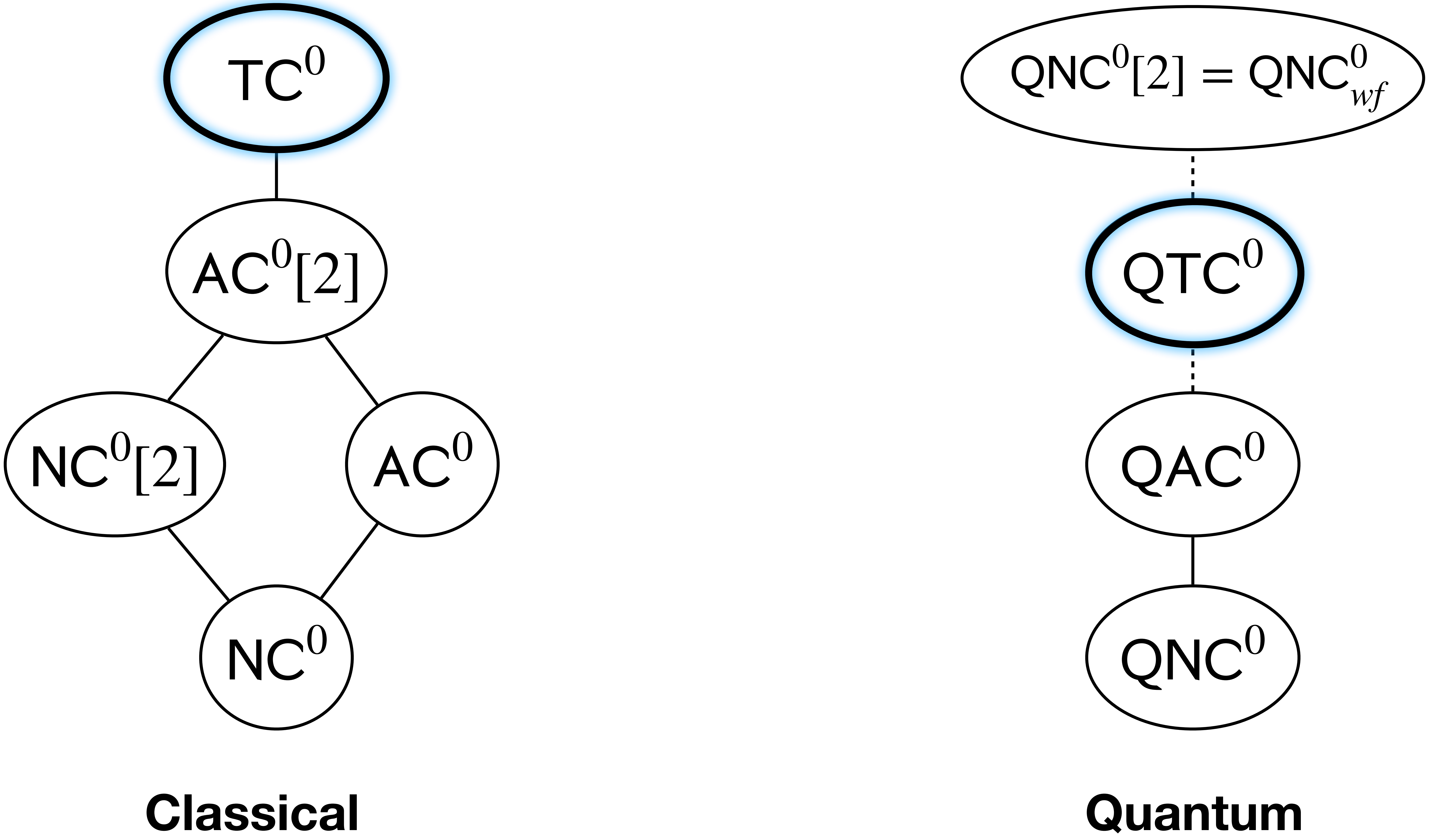
Theorem [Høyer, Špalek 02]**:** $\mathrm{QTC}^0 \subseteq \mathrm{QNC}^0[2] = \mathrm{QAC}^0[2]$

Constant-depth quantum circuits with Fanout can compute Threshold

Low-depth complexity classes recap



Low-depth complexity classes recap



Quantum Majority is powerful

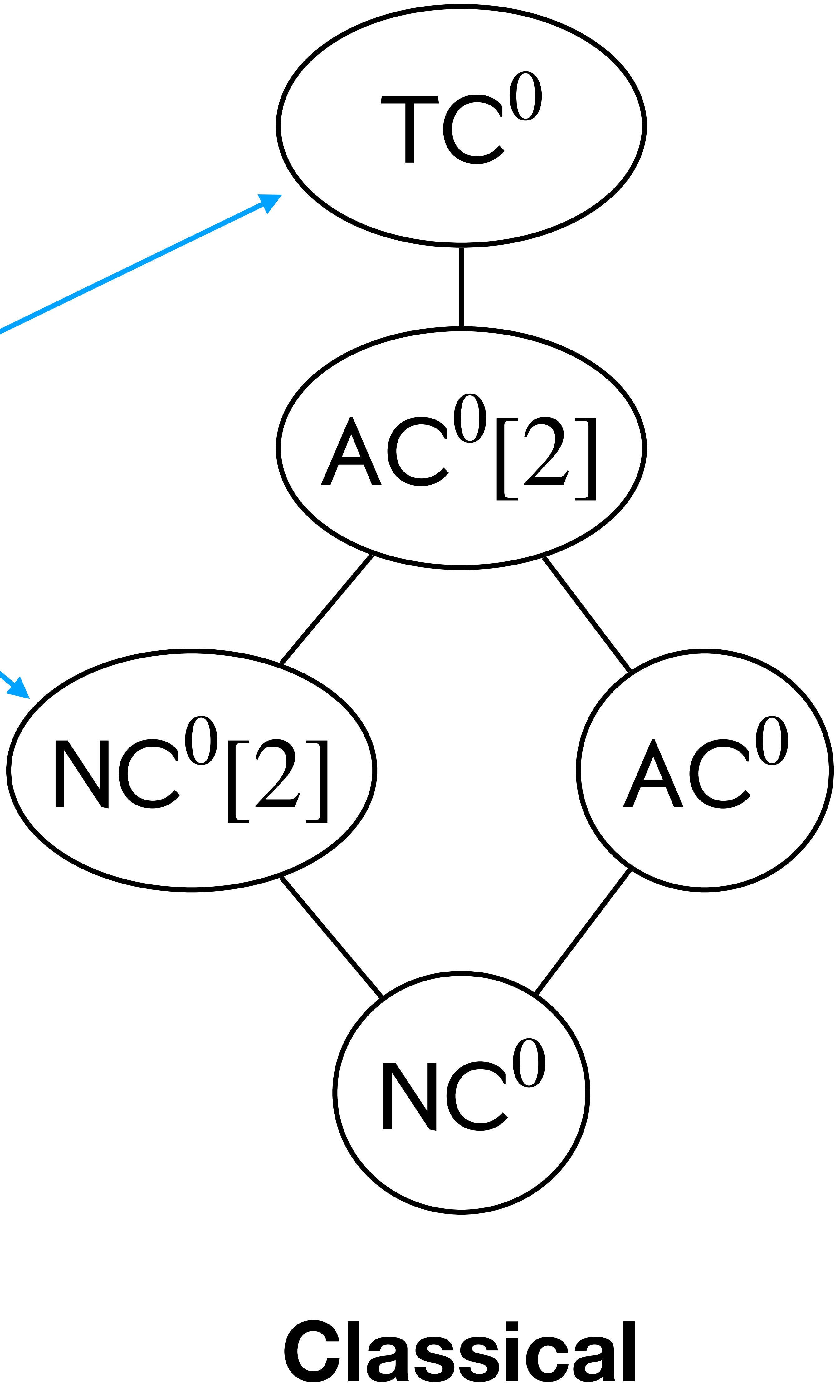
Theorem [G, Morris]**:** $\mathrm{QNC}^0[2] \subseteq \mathrm{QTC}^0$

- Constant-depth quantum circuits with Majority can compute Parity
- *Caveat:* construction is approximate (inverse-poly precision)
  - [Høyer, Špalek 2002] construction *also* approximate
  - Made exact by [Takahashi, Tani 2011]
- *Anti-Caveat:* construction applies to a generalization of Majority
  - Seem useless in the classical setting, but computes Parity in the quantum setting

Classical Threshold gates can compute Parity

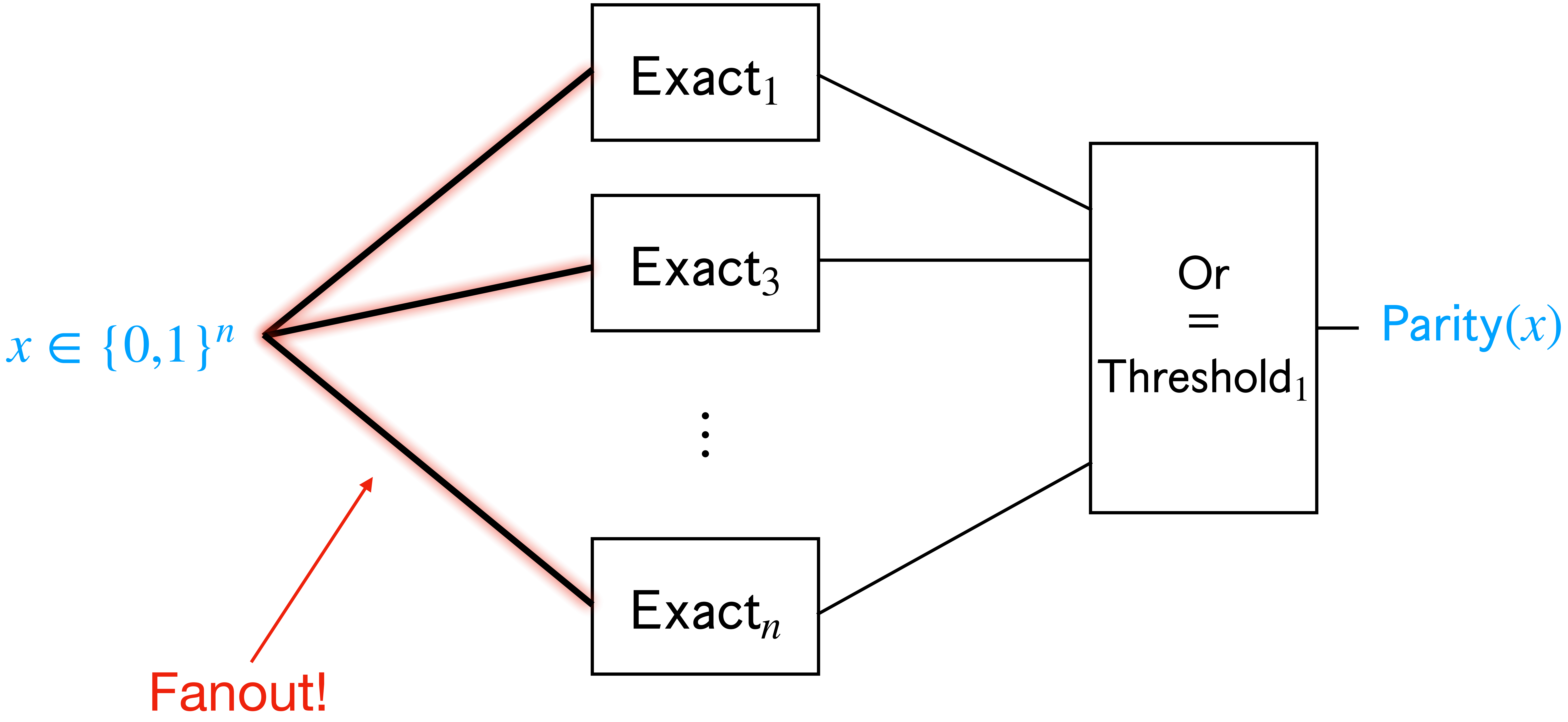
Question: Why isn't this result trivial?

Classical Threshold gates
can compute Parity



Classical Threshold gates can compute Parity

Idea: $\text{Exact}_k(x) = \text{Threshold}_k(x) \wedge \overline{\text{Threshold}_{k+1}(x)}$



Quantum Majority implies Parity — Proof Outline

Theorem [G, Morris]**:** $\mathrm{QNC}^0[2] \subseteq \mathrm{QTC}^0$

→ Constant-depth quantum circuits with Majority can compute Parity

Proof Outline: (following [Rosenthal 20])

1) Cat state generation implies Fanout

2) Give a construction for a Cat state

Ingredient 1: Cat state creation implies Parity

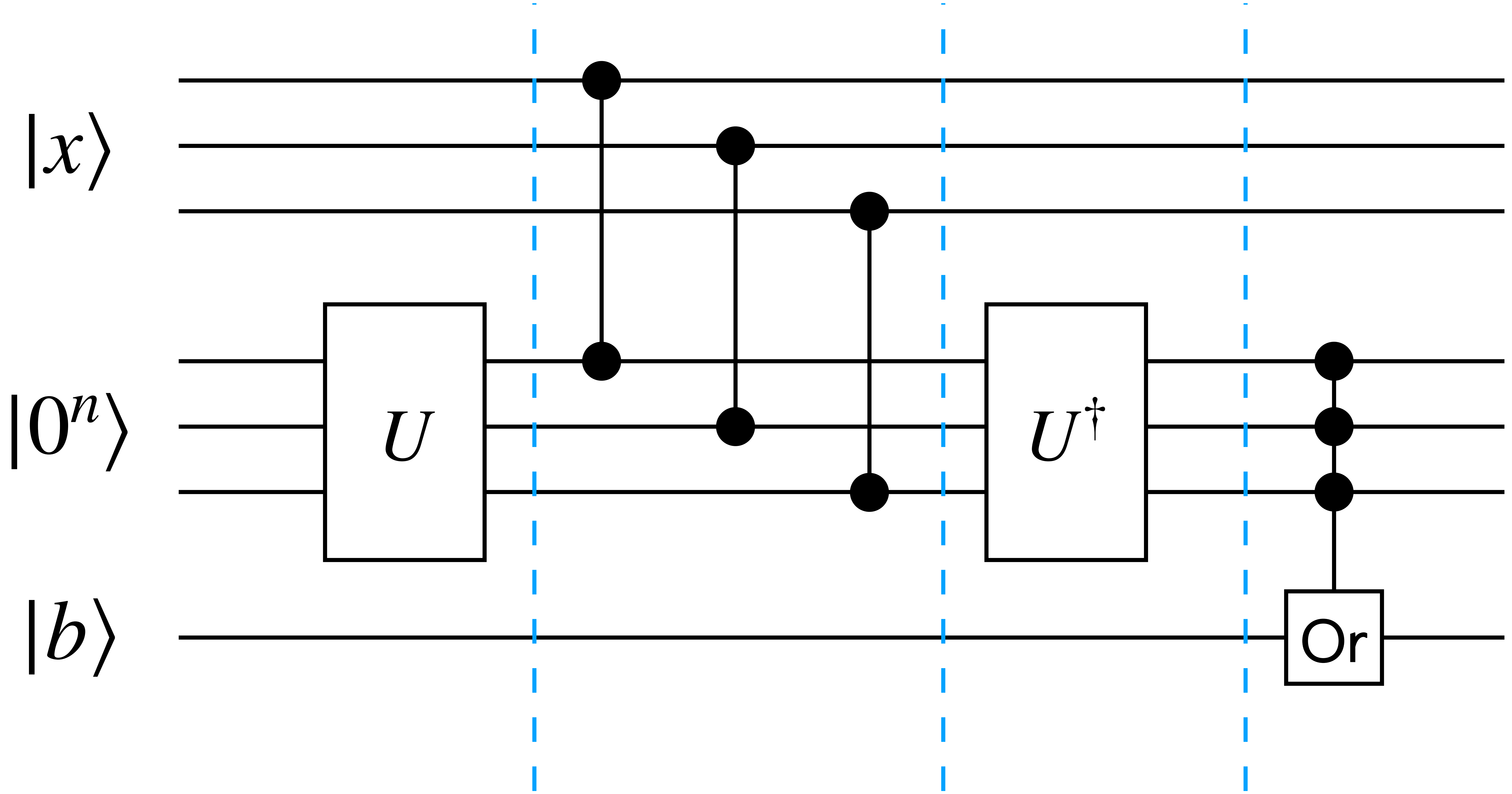
Theorem [Moore 1999]**:** Suppose you can implement unitaries U and $U^\dagger$ such that

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

in constant depth. Then, using Quantum Or gates and $U, U^\dagger$ gates you can implement Parity in constant depth.

Ingredient 1: Cat state creation implies Parity

$$\frac{|x, 0^n, b\rangle + (-1)^{|x|}\,|x, 1^n, b\rangle}{\sqrt{2}}$$



$$\frac{|x, 0^n, b\rangle + |x, 1^n, b\rangle}{\sqrt{2}}$$

$$\begin{cases} |x, 0^n, b\rangle & \text{if } |x| \equiv 0 \pmod 2 \\ |x, \phi, b\rangle & \text{if } |x| \equiv 1 \pmod 2 \end{cases}$$

Ingredient 1: Cat state creation implies Parity

Theorem [Moore 1999]**:** Suppose you can implement unitaries U and $U^\dagger$ such that

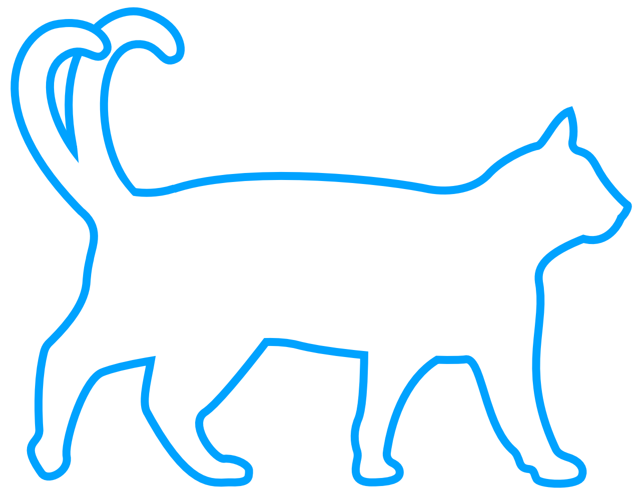
$$U|0^n\rangle = \frac{|0^n\rangle + |1^n\rangle}{\sqrt{2}}$$

in constant depth. Then, using Quantum Or gates and $U, U^\dagger$ gates you can implement Parity in constant depth.

Also works when $U|0^n\rangle = \dfrac{|0^n\rangle \otimes |\psi_0\rangle + |1^n\rangle \otimes |\psi_1\rangle}{\sqrt{2}}$

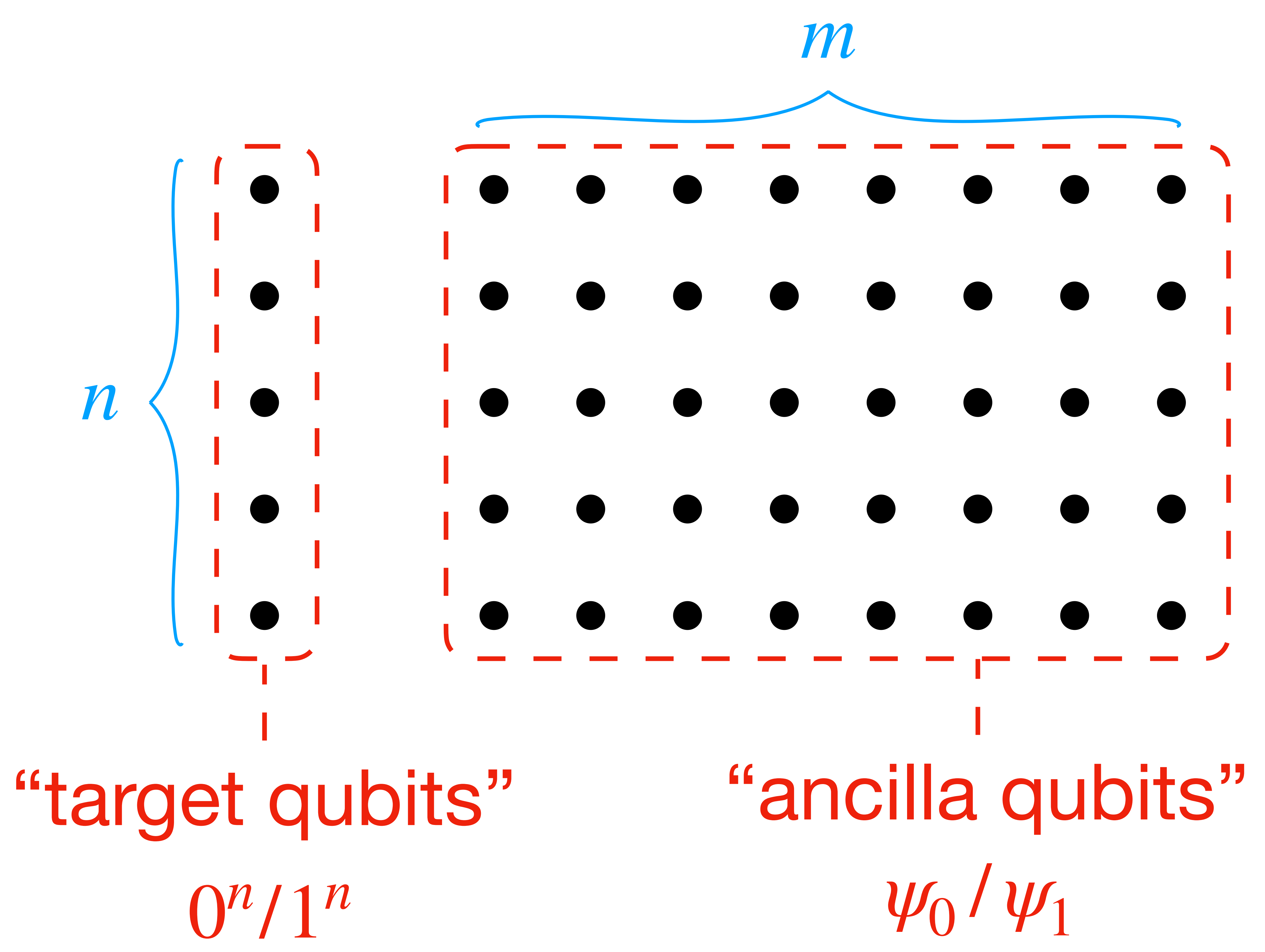
"nekomata"
[Rosenthal 2020]

Corollary: If you can approximately construct a nekomata, then you can approximate Parity

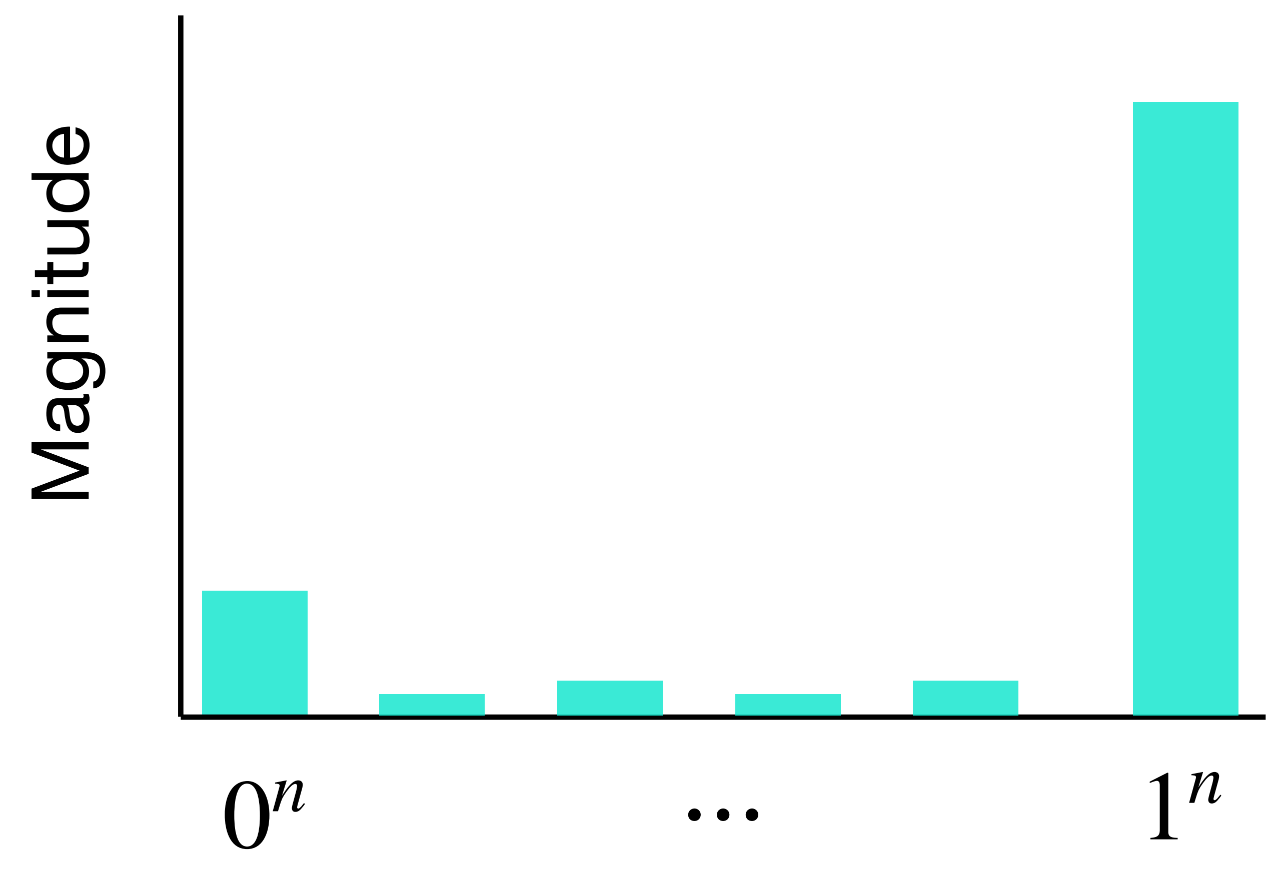


Ingredient 2: Construct approximate nekomata

Goal: $\dfrac{|0^n\rangle \otimes |\psi_0\rangle + |1^n\rangle \otimes |\psi_1\rangle}{\sqrt{2}}$



i. For each ancilla column, construct state with most mass on $|0^n\rangle$ and $|1^n\rangle$.



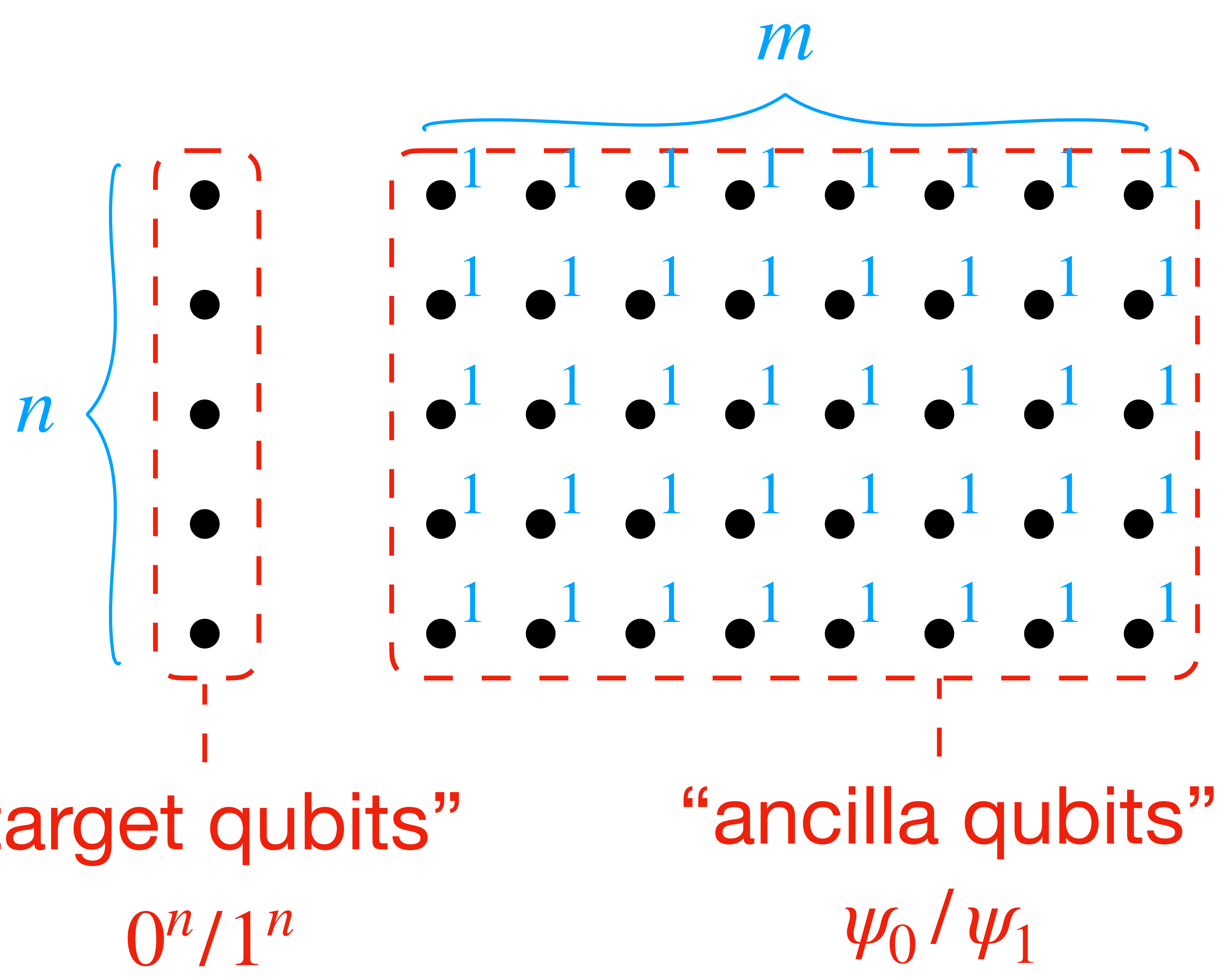
ii. Set m so that measuring all ones in the ancillas with probability $1/2$.

$\implies$ some column is zeros $\approx 1/2$

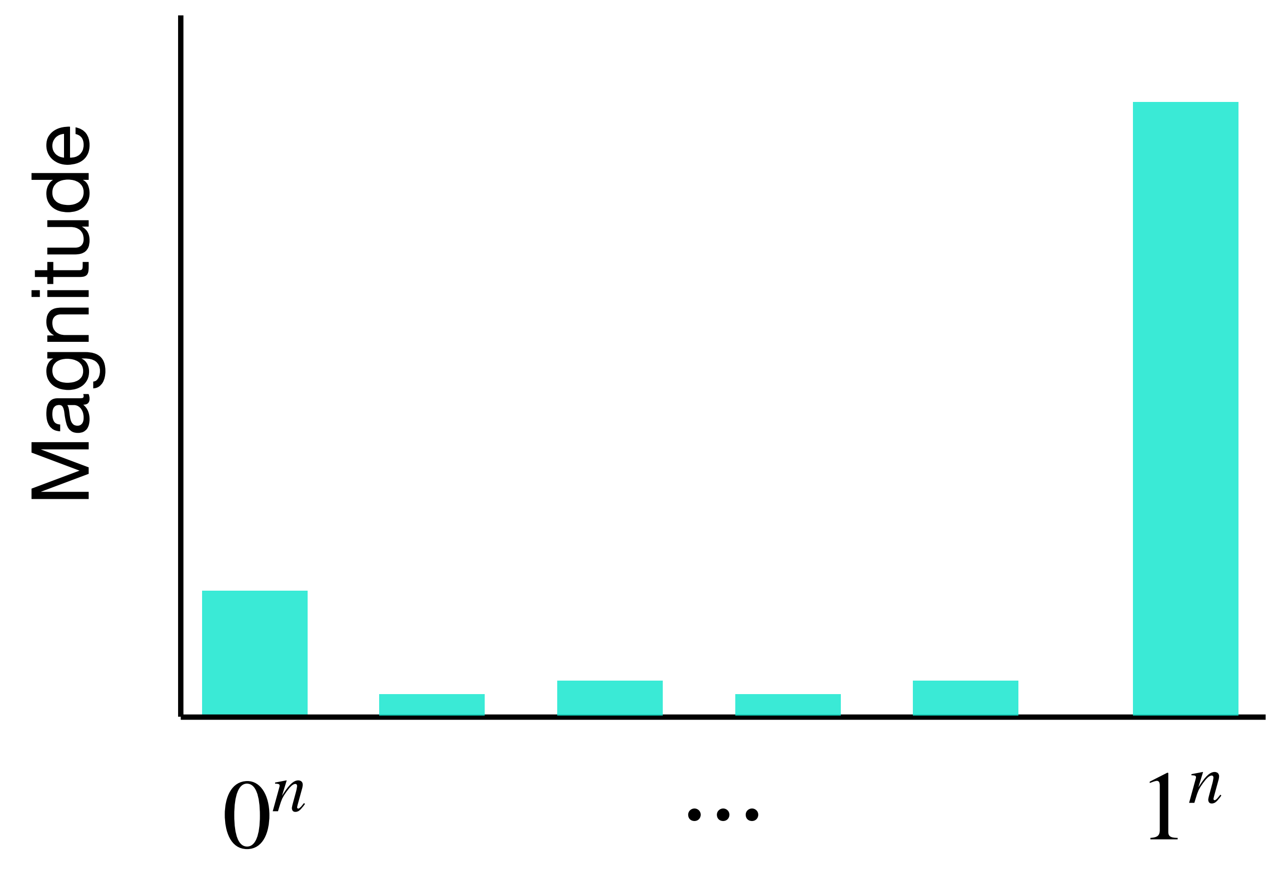
iii. For each row, apply And gate from ancillas to target

Ingredient 2: Construct approximate nekomata

Goal: $\dfrac{|0^n\rangle \otimes |\psi_0\rangle + |1^n\rangle \otimes |\psi_1\rangle}{\sqrt{2}}$



i. For each ancilla column, construct state with most mass on $|0^n\rangle$ and $|1^n\rangle$.



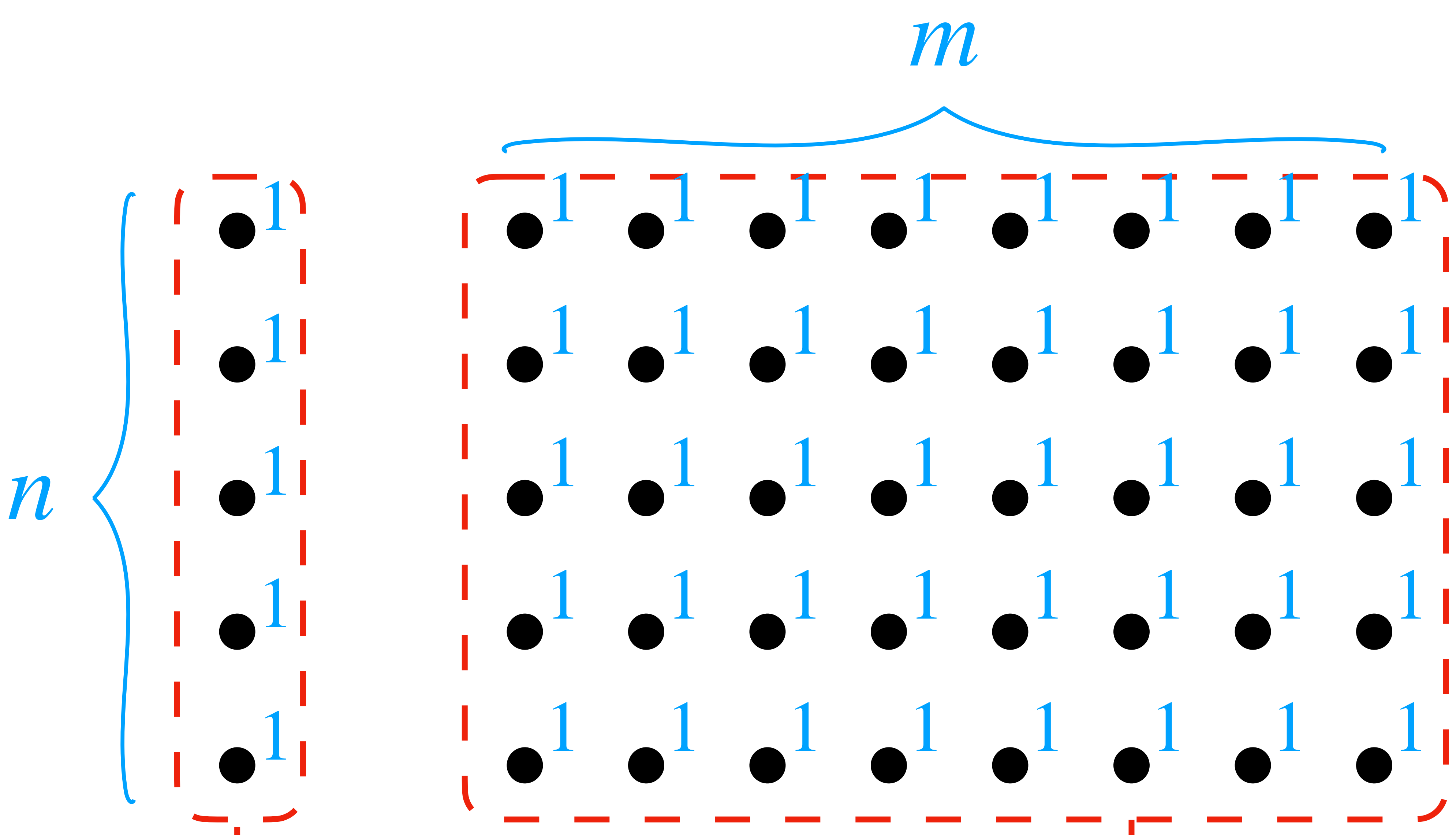
ii. Set m so that measuring all ones in the ancillas with probability $1/2$.

$\implies$ some column is zeros $\approx 1/2$

iii. For each row, apply And gate from ancillas to target

Ingredient 2: Construct approximate nekomata

Goal: $$\frac{|0^n\rangle \otimes |\psi_0\rangle + |1^n\rangle \otimes |\psi_1\rangle}{\sqrt{2}}$$



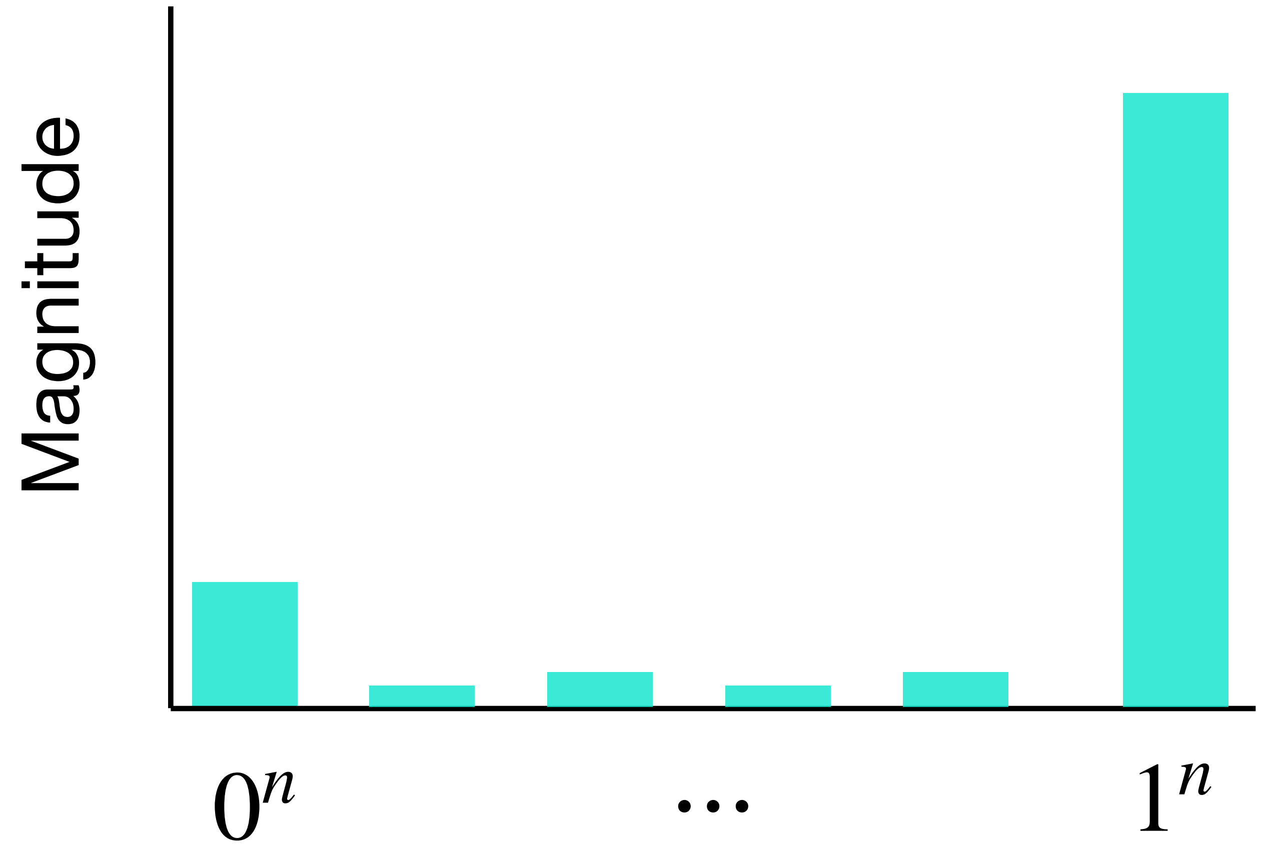
“target qubits”

$0^n / 1^n$

“ancilla qubits”

ψ_0 / ψ_1

i. For each ancilla column, construct state with most mass on $|0^n\rangle$ and $|1^n\rangle$.



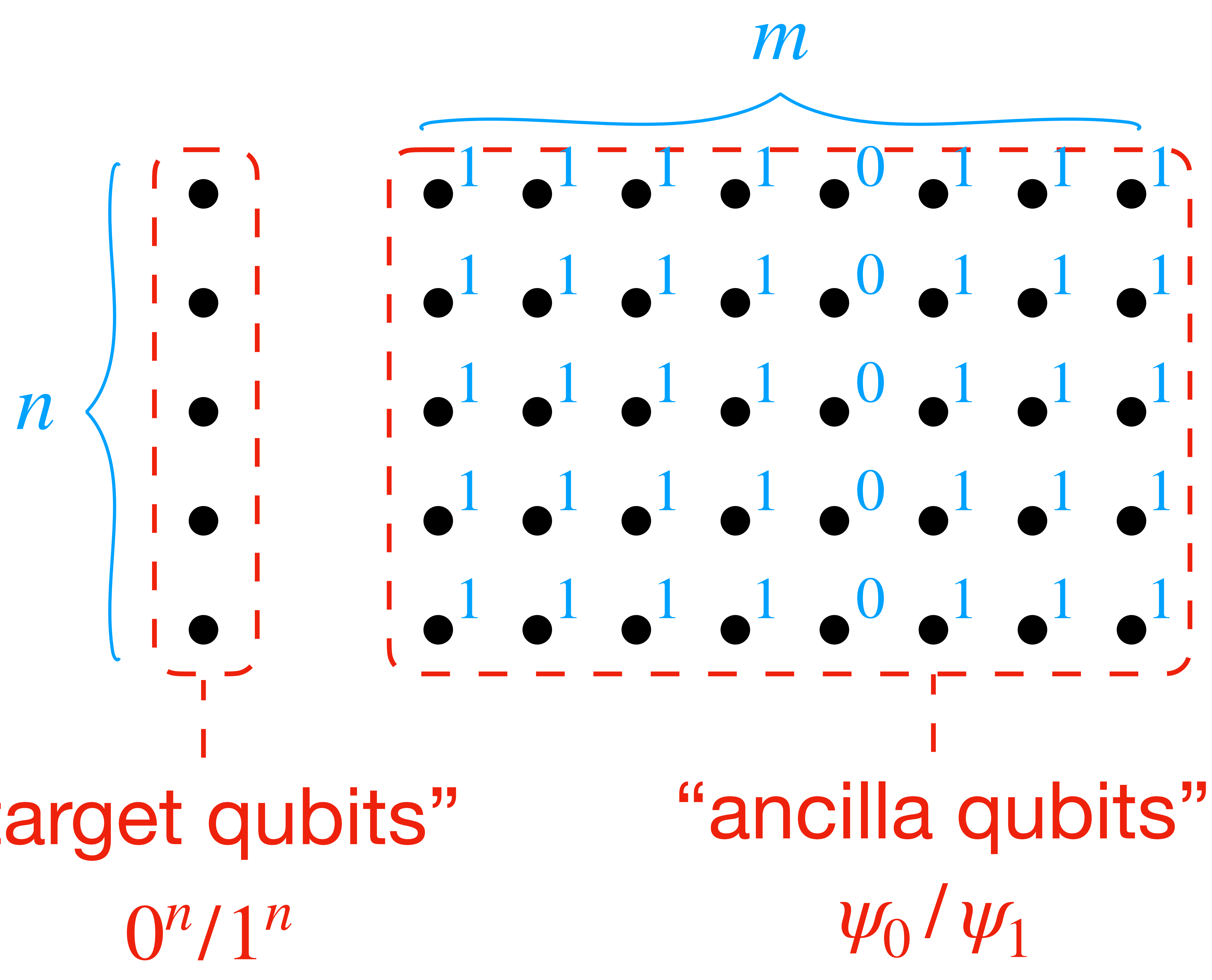
ii. Set m so that measuring all ones in the ancillas with probability $1/2$.

$\Longrightarrow$ some column is zeros $\approx 1/2$

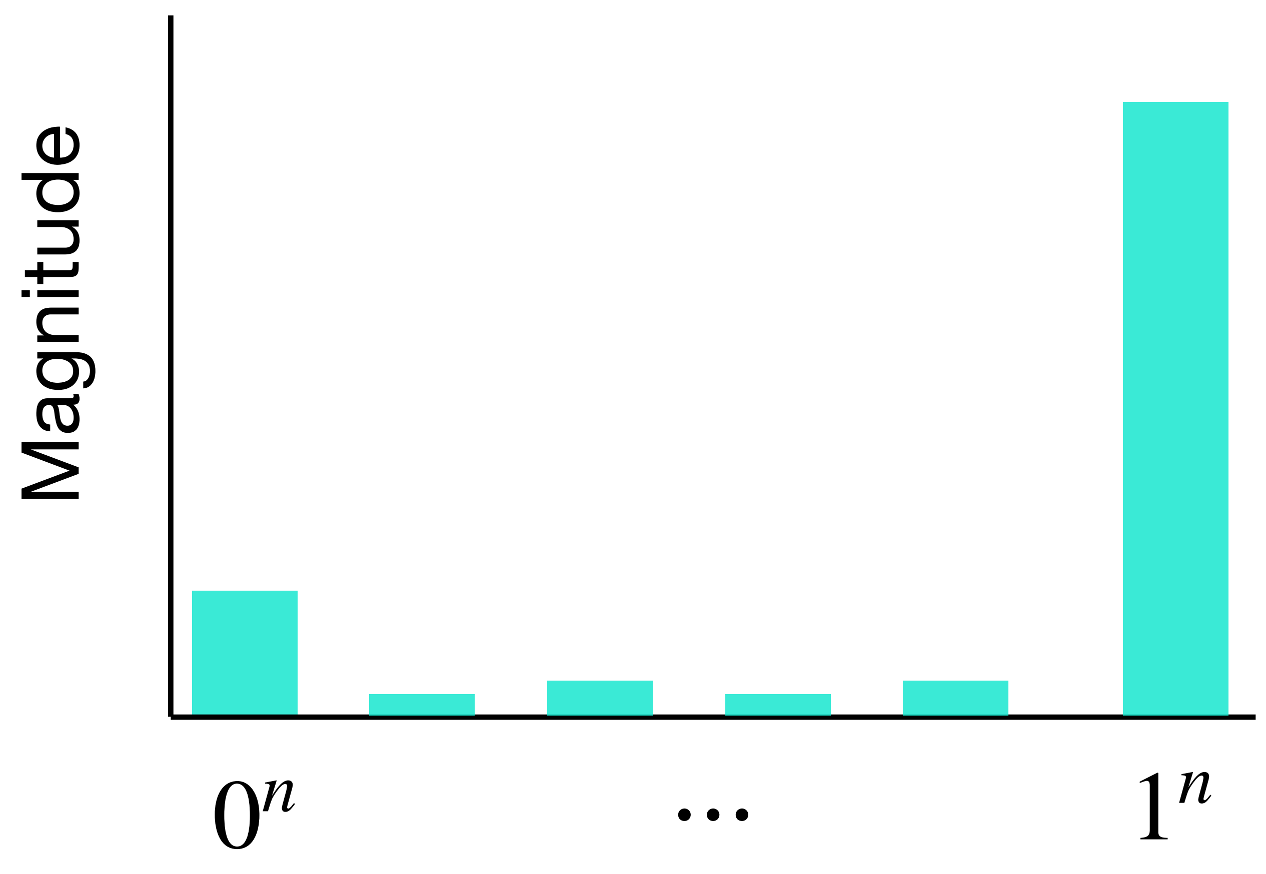
iii. For each row, apply And gate from ancillas to target

Ingredient 2: Construct approximate nekomata

Goal: $\dfrac{|0^n\rangle \otimes |\psi_0\rangle + |1^n\rangle \otimes |\psi_1\rangle}{\sqrt{2}}$



i. For each ancilla column, construct state with most mass on $|0^n\rangle$ and $|1^n\rangle$.



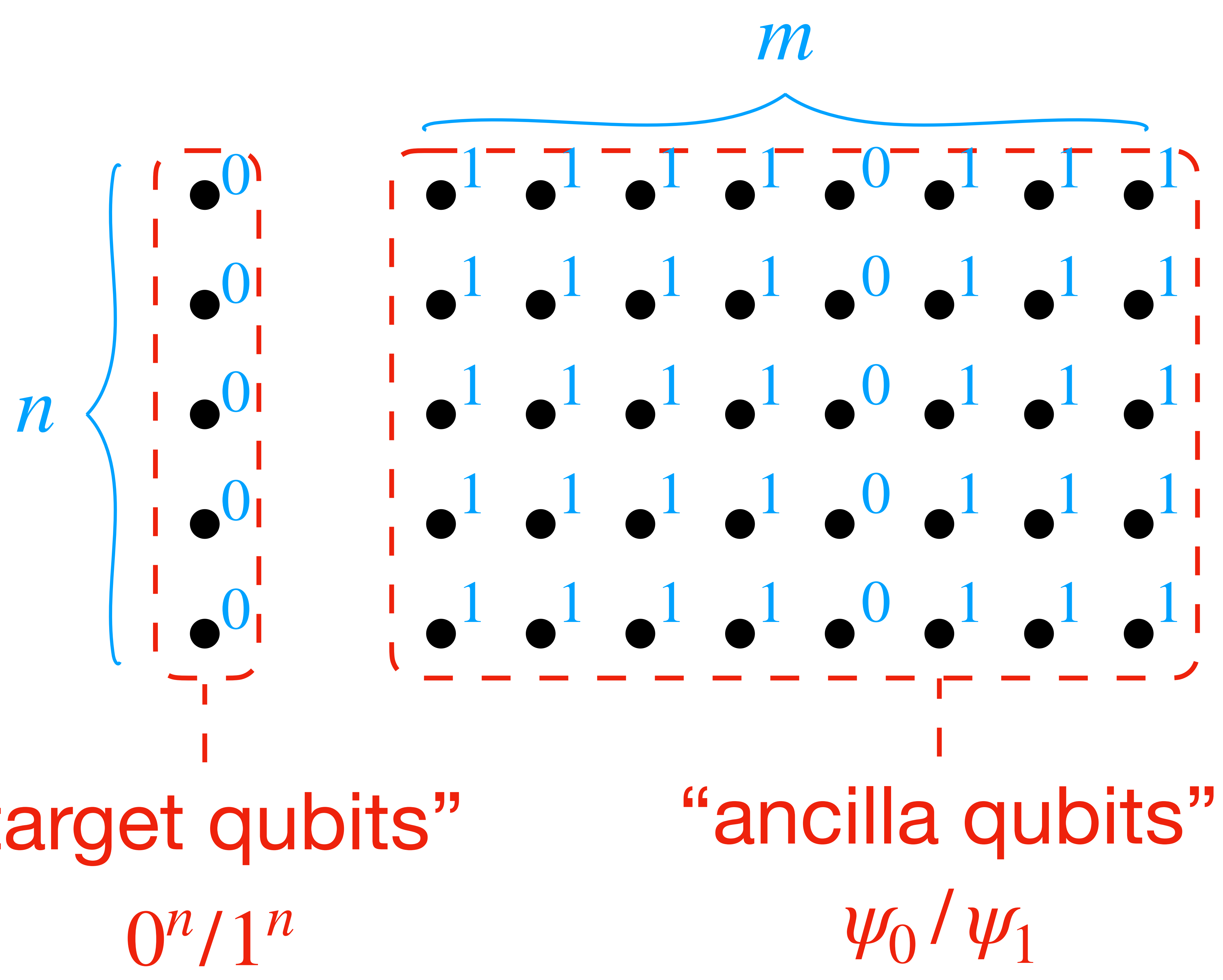
ii. Set m so that measuring all ones in the ancillas with probability $1/2$.

$\Longrightarrow$ some column is zeros $\approx 1/2$

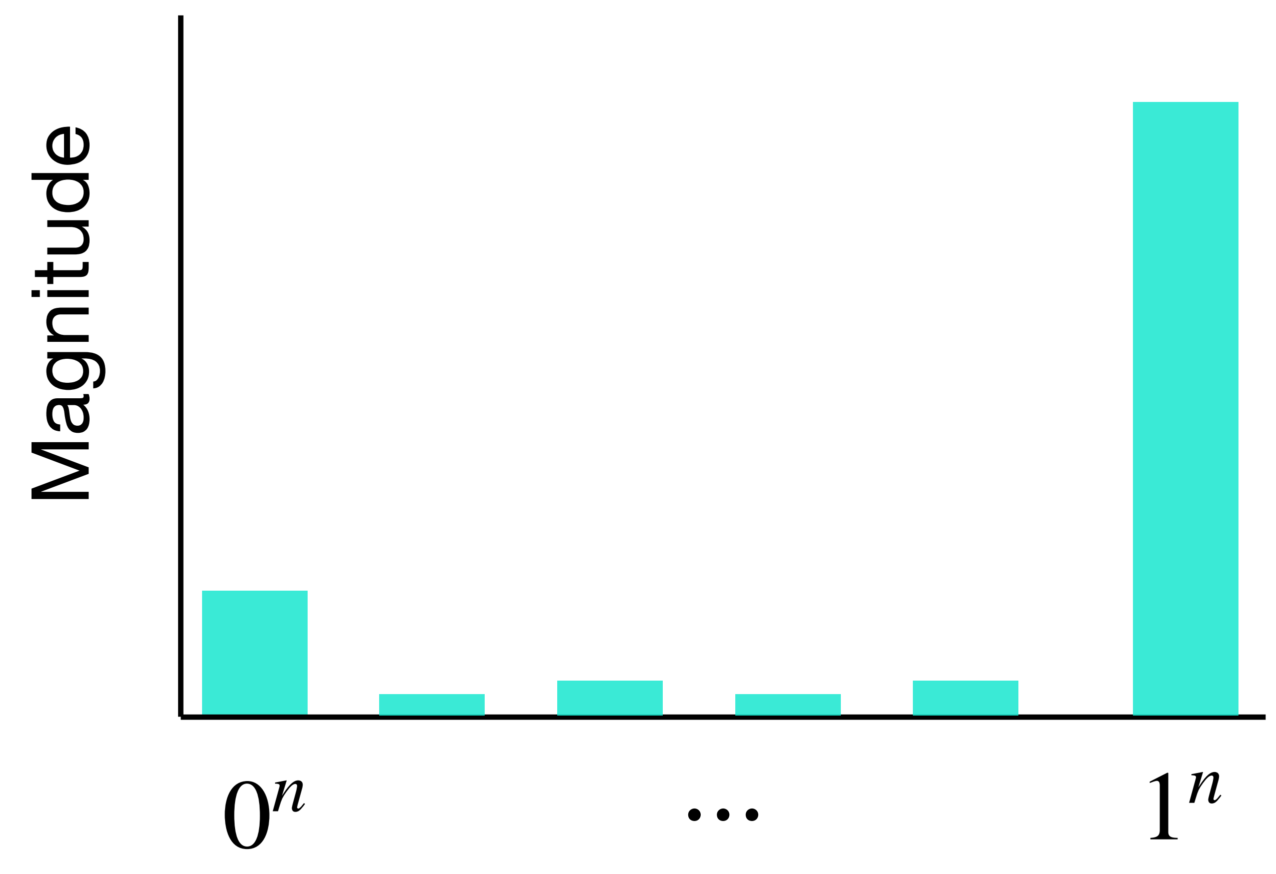
iii. For each row, apply And gate from ancillas to target

Ingredient 2: Construct approximate nekomata

Goal: $\dfrac{|0^n\rangle \otimes |\psi_0\rangle + |1^n\rangle \otimes |\psi_1\rangle}{\sqrt{2}}$



i. For each ancilla column, construct state with most mass on $|0^n\rangle$ and $|1^n\rangle$.



ii. Set m so that measuring all ones in the ancillas with probability $1/2$.

$\implies$ some column is zeros $\approx 1/2$

iii. For each row, apply And gate from ancillas to target

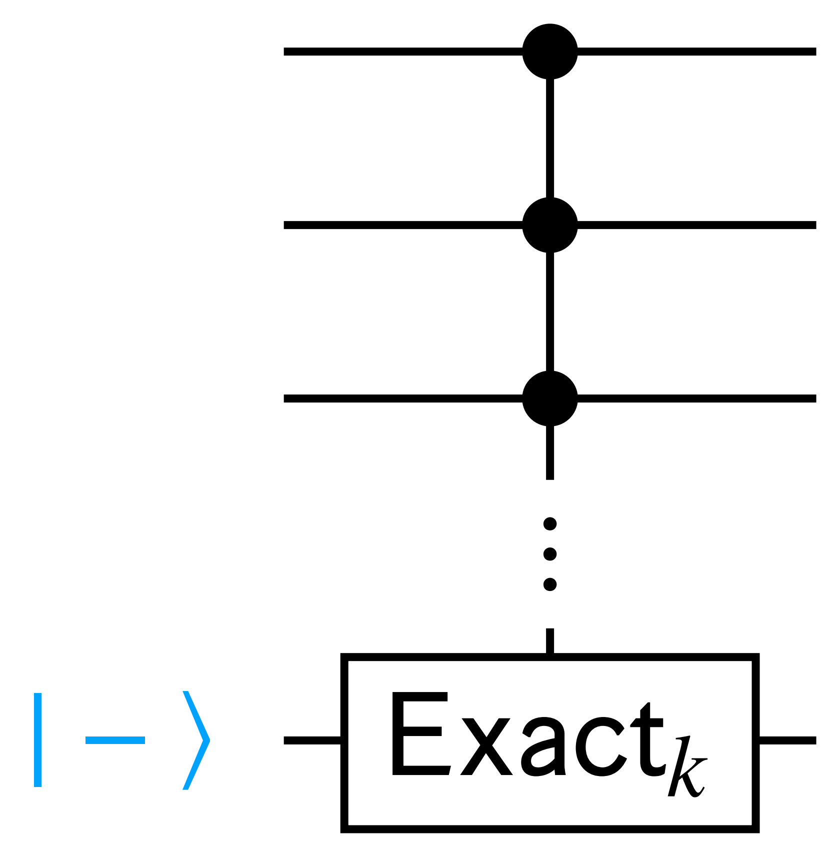
Ingredient 2i: Constructing weighted column

Parity-restricted gate: Let $S \subseteq \{0,1\}^n$ be strings with same parity

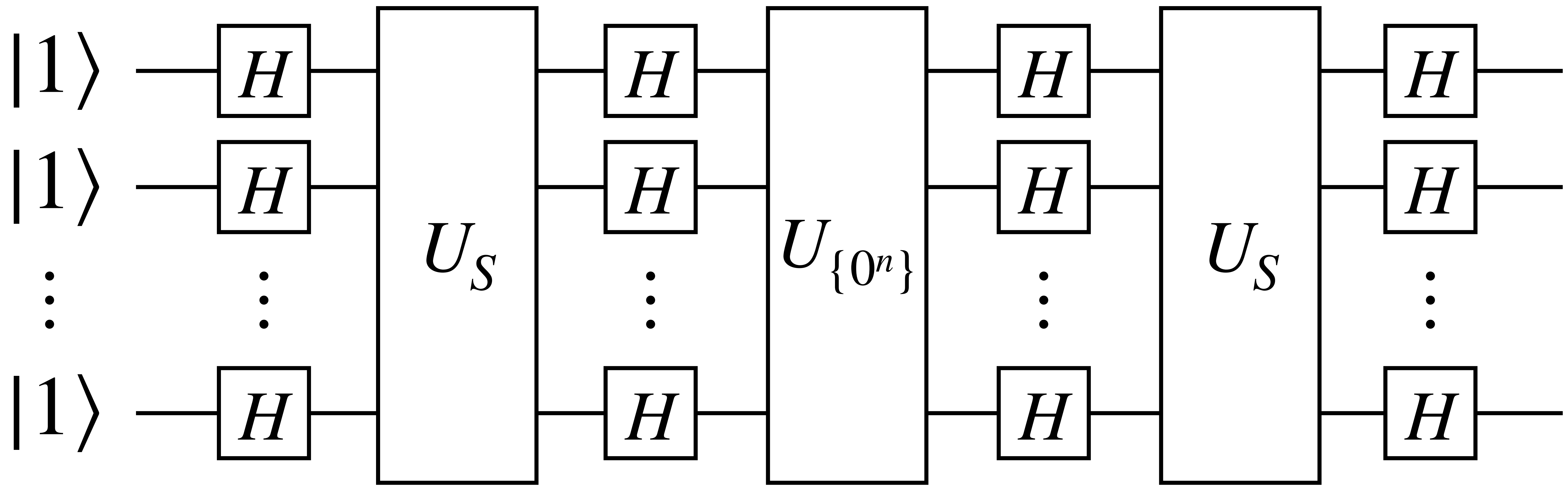
$$U_S|x\rangle = (-1)^{x \in S}|x\rangle$$

Recall: Threshold gates can be used to generate Exact gates

Exact$_k$ is a parity-restricted gate with $|S| = \binom{n}{k}$



Ingredient 2i: Constructing weighted column

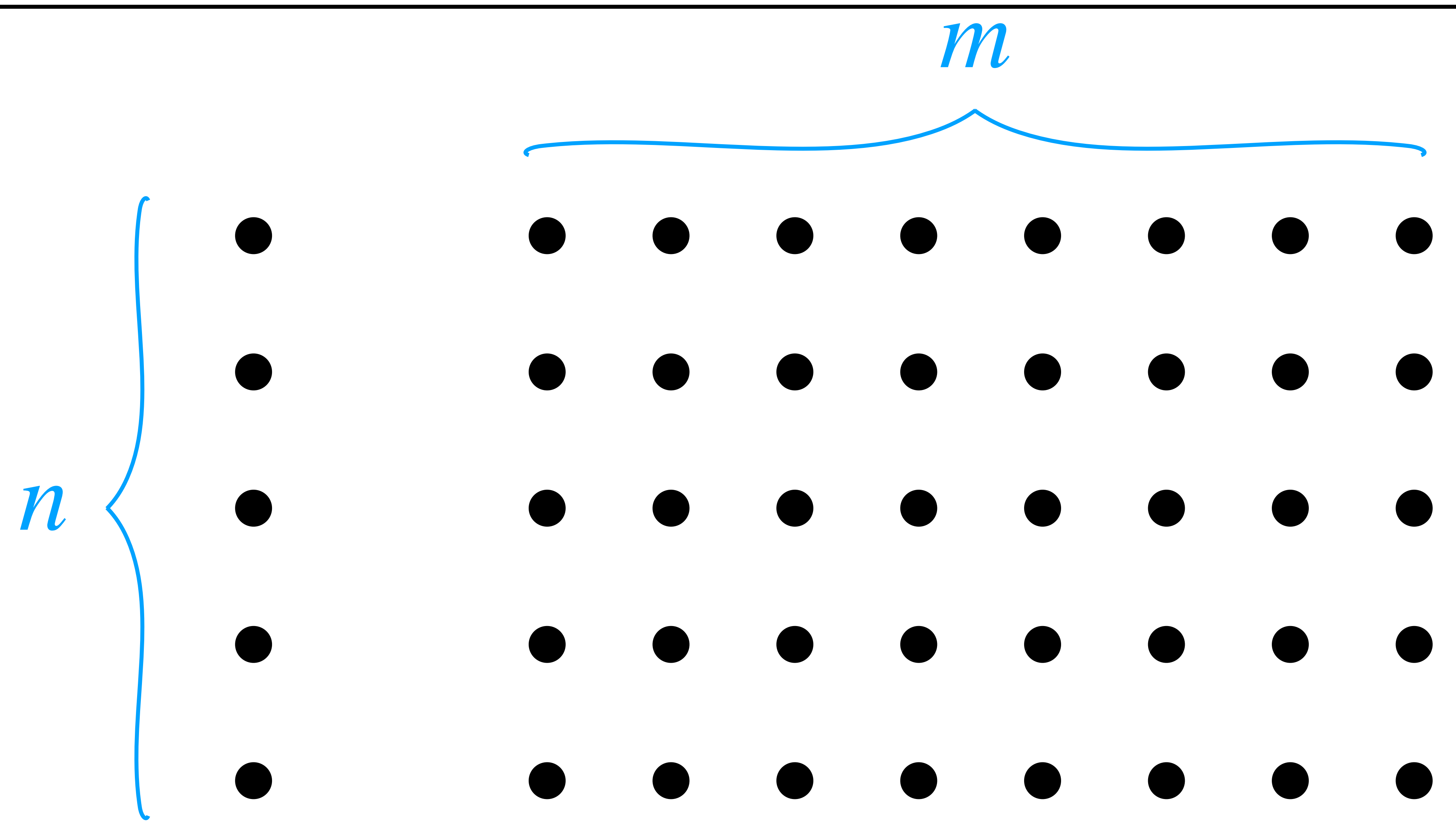


Don't read this:

$$\Pr[\text{measure } |0^n\rangle] = 4\left(1 - \frac{|S|}{2^{n-1}}\right)^2 \frac{|S|^2}{2^{2n-2}}$$

$$\Pr[\text{measure } |1^n\rangle] = \left(1 - \frac{|S|^2}{2^{2n-3}}\right)^2$$

Ingredient 2: Construct approximate nekomata



i. For each ancilla column, construct this biased state

ii. Set number of columns m

iii. For each row, apply And from ancillas to target

Theorem: Exists $m \approx \dfrac{4^n}{|S|^2}$

such that probability all columns are $|1^n\rangle$

$$> \frac{1}{2} - \frac{|S|^2}{4^{n-1}}$$

exists $|0^n\rangle$ column with probability

$$> \frac{1}{2} - \frac{|S|}{2^{n-2}}$$

Consider $\text{Exact}_{n/2}$ gate

$$|S| = \binom{n}{n/2} \approx \frac{2^n}{\sqrt{n\pi/2}}$$

Putting everything together again

Theorem: There is a constant-depth quantum circuit constructed from U_S and And gates that approximates Parity with a number of gates

$$\text{poly}\left(n, \frac{4^n}{|S|^2}\right)$$

- Poly-size threshold circuits for Parity $\implies$ $\text{QNC}^0_{wf} \subseteq \text{QTC}^0$
- And gate is a U_S gate with $|S| = 1$

$\implies$ Exponential size QAC^0 for Parity [Rosenthal 20]

Open questions

- Is there an exact quantum circuit for Parity using Majority?
- Are the And gates necessary in our Parity construction?
- Does $\mathsf{QAC}^0 = \mathsf{QAC}^0[2]$?
- Is there a complete characterization of the power of Boolean gates in constant depth?