Interactive quantum advantage with noisy, shallow Clifford circuits

Nathan Ju (University of Illinois)

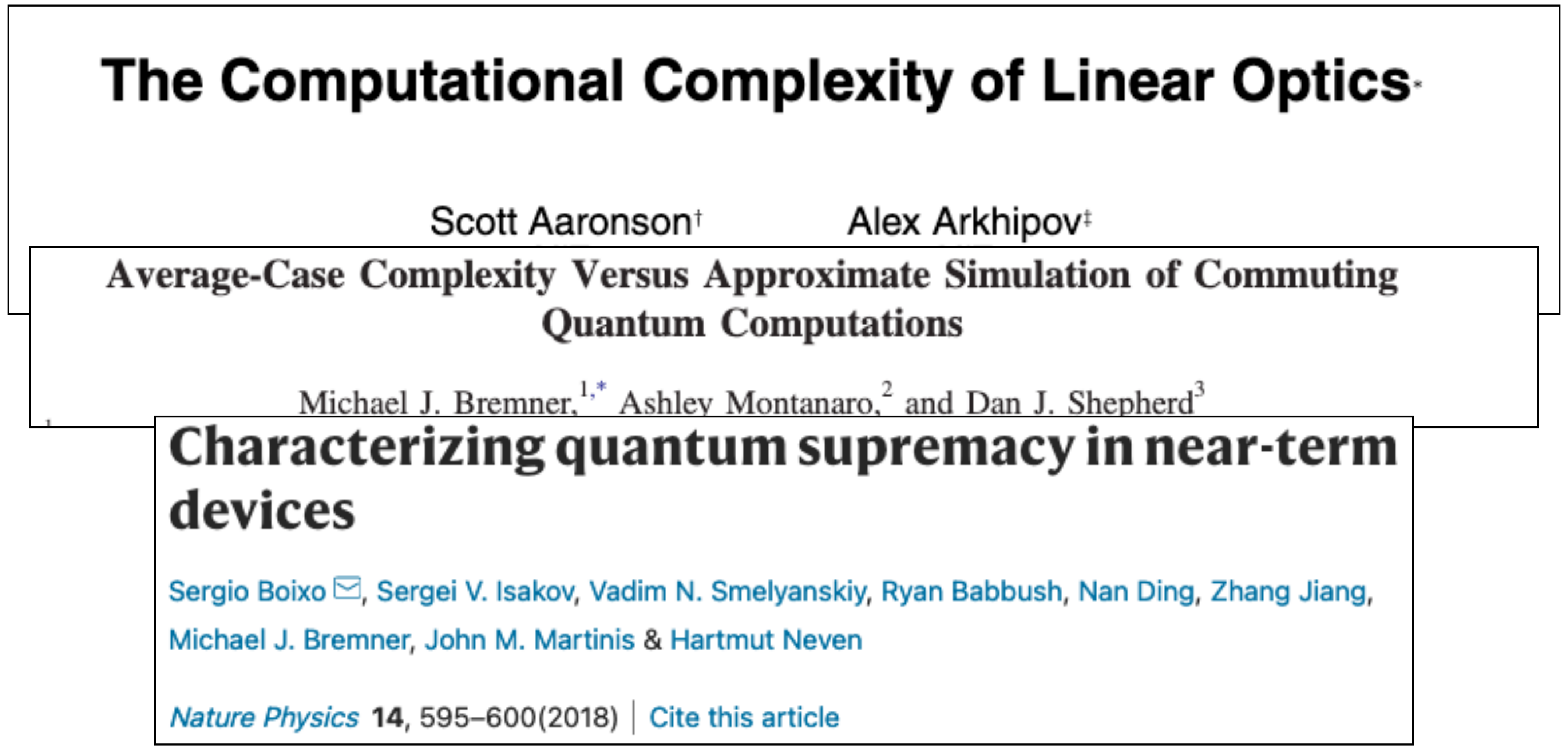
joint work with

Daniel Grier (University of Waterloo) Luke Schaeffer (University of Waterloo)

IQC Institute for Quantum Computing

Motivation: Quantum advantage?

Near-term, noisy quantum computers solve sampling tasks that are classically intractable, **assuming some conjectures**


The Computational Complexity of Linear Optics

Scott Aaronson† Alex Arkhipov‡

Average-Case Complexity Versus Approximate Simulation of Commuting Quantum Computations

Michael J. Bremner,[1,*] Ashley Montanaro,[2] and Dan J. Shepherd[3]

Characterizing quantum supremacy in near-term devices

Sergio Boixo, Sergei V. Isakov, Vadim N. Smelyanskiy, Ryan Babbush, Nan Ding, Zhang Jiang, Michael J. Bremner, John M. Martinis & Hartmut Neven

Nature Physics **14**, 595–600(2018) | Cite this article

Compare noisy and shallow quantum computers against <u>shallow/weak</u> classical computers instead, **with fewer or no conjectures**?

Noisy quantum advantage against weak circuits

Improving on this breakthrough result from 2018…

Quantum advantage with shallow circuits

Sergey Bravyi[1], David Gosset[1,*], Robert König[2,†]

+ See all authors and affiliations

Science 19 Oct 2018:
Vol. 362, Issue 6412, pp. 308-311
DOI: 10.1126/science.aar3106

Noisy quantum advantage against weak circuits

Bravyi, Gosset, König, Tomamichel [BGKT19]:

There is a relation task solved by a noisy constant-depth quantum circuit (QNC^0) with probability $1 - o(1)$ on all inputs.

A classical probabilistic circuit with bounded fan-in gates and constant-depth (NC^0) solves the task with probability at most $9/10$ over a uniform input.

Improving on this breakthrough result from 2018…

Quantum advantage with shallow circuits

Sergey Bravyi[1], David Gosset[1,*], Robert König[2,†]

+ See all authors and affiliations

Science 19 Oct 2018:
Vol. 362, Issue 6412, pp. 308-311
DOI: 10.1126/science.aar3106

Noisy quantum advantage against weak circuits

Bravyi, Gosset, König, Tomamichel [BGKT19]:

There is a relation task solved by a noisy constant-depth quantum circuit (QNC^0) with probability $1 - o(1)$ on all inputs.

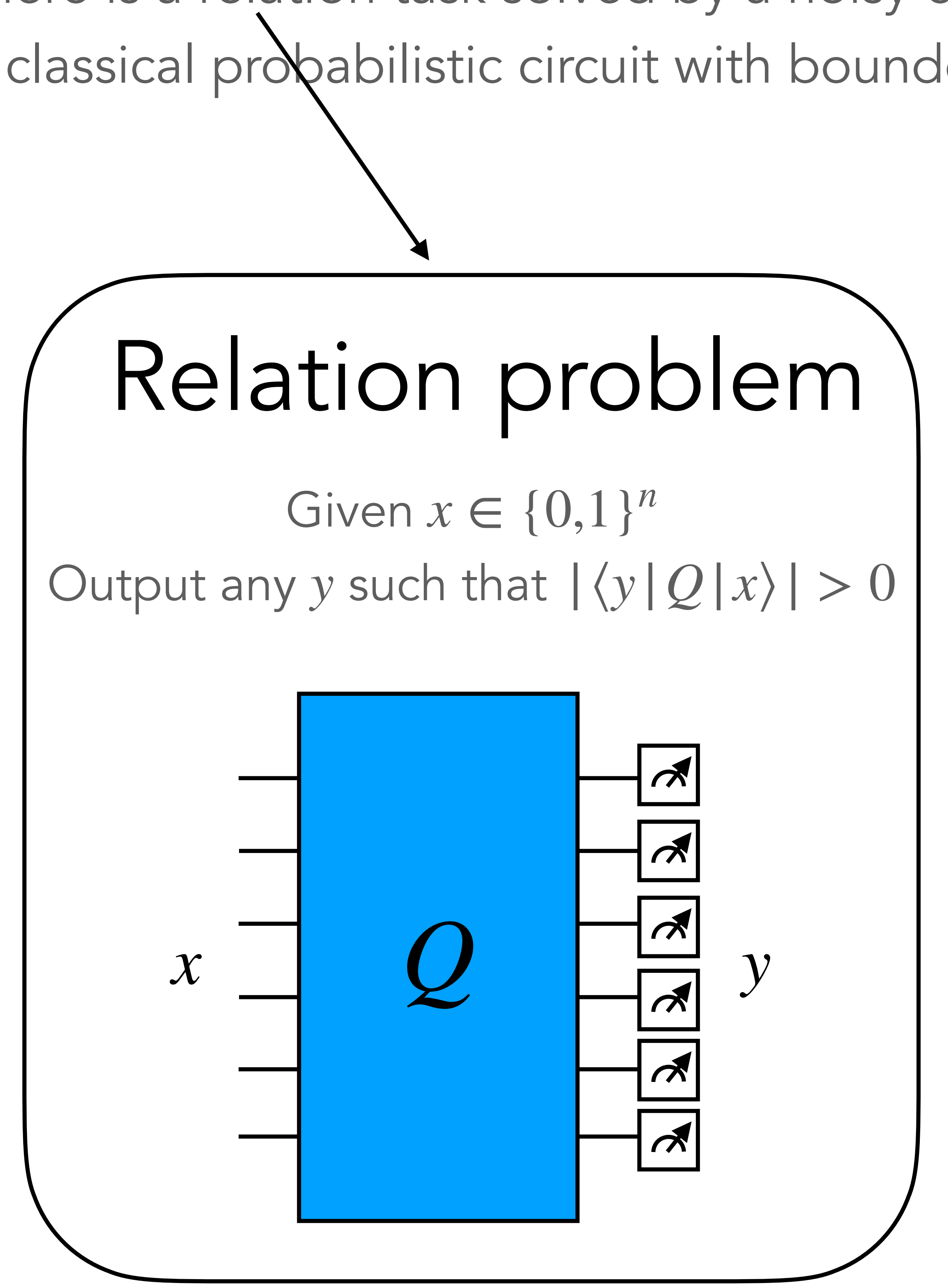
A classical probabilistic circuit with bounded fan-in gates and constant-depth (NC^0) solves the task with probability at most $9/10$ over a uniform input.

Noisy quantum advantage against weak circuits

Bravyi, Gosset, König, Tomamichel [BGKT19]:

There is a relation task solved by a noisy constant-depth quantum circuit (QNC^0) with probability $1 - o(1)$ on all inputs.

A classical probabilistic circuit with bounded fan-in gates and constant-depth (NC^0) solves the task with probability at most $9/10$ over a uniform input.



Noisy quantum advantage against weak circuits

Bravyi, Gosset, König, Tomamichel [BGKT19]:

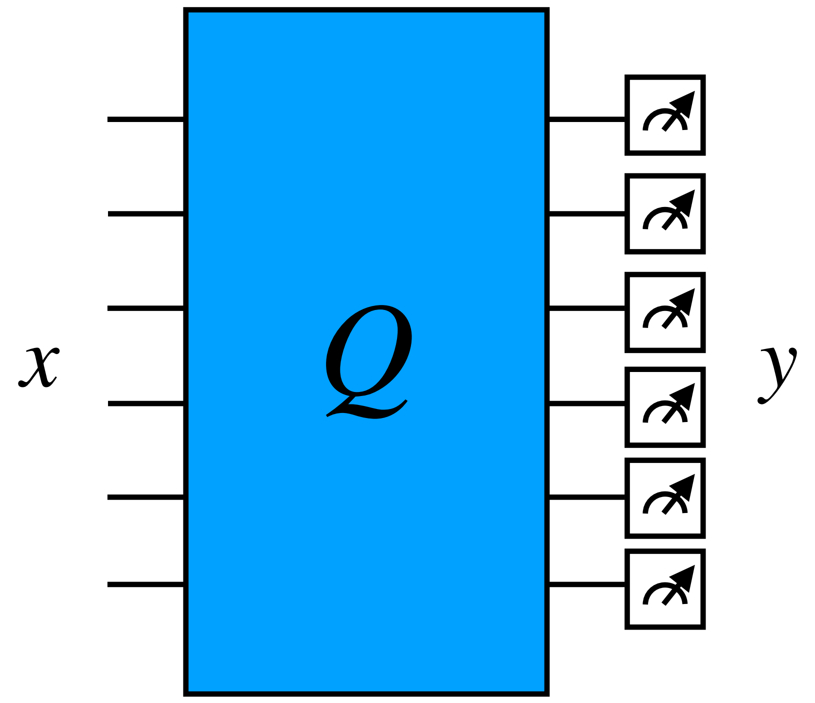
There is a relation task solved by a noisy constant-depth quantum circuit (QNC^0) with probability $1 - o(1)$ on all inputs.

A classical probabilistic circuit with bounded fan-in gates and constant-depth (NC^0) solves the task with probability at most $9/10$ over a uniform input.

Relation problem

Given $x \in \{0,1\}^n$

Output any y such that $|\langle y|Q|x\rangle| > 0$

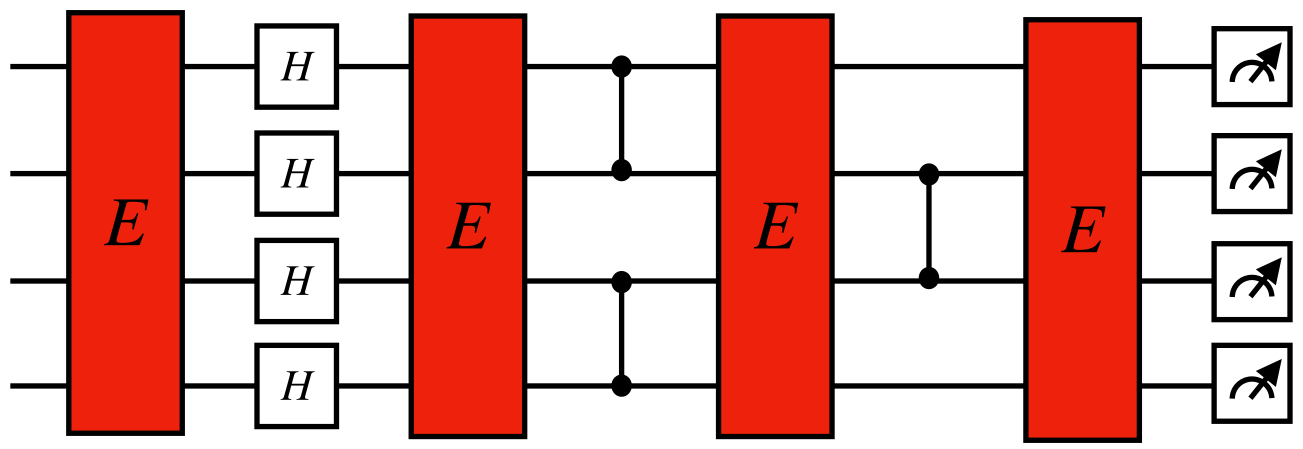


Local stochastic noise model

[Aliferis, Gottesman, Preskill 2007]

Random n-qubit Pauli E is *local stochastic with noise rate* p

if it acts non-trivially on qubits $F \subseteq [n]$ with probability $\leq p^{|F|}$



Noisy quantum advantage against weak circuits

Bravyi, Gosset, König, Tomamichel [BGKT19]:

There is a relation task solved by a noisy constant-depth quantum circuit (QNC^0) with probability $1 - o(1)$ on all inputs.

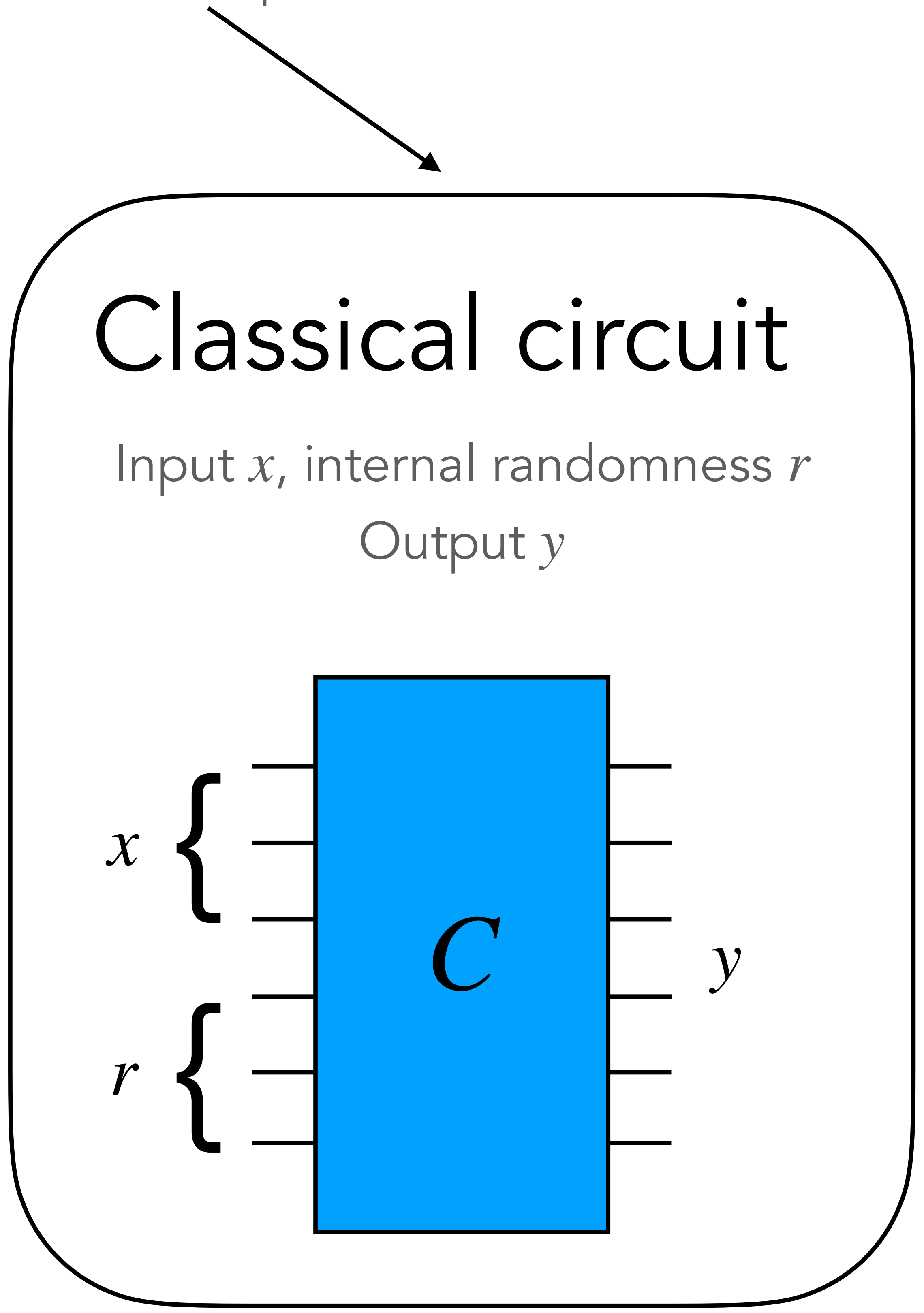
A classical probabilistic circuit with bounded fan-in gates and constant-depth (NC^0) solves the task with probability at most $9/10$ over a uniform input.

Noisy quantum advantage against weak circuits

Bravyi, Gosset, König, Tomamichel [BGKT19]:

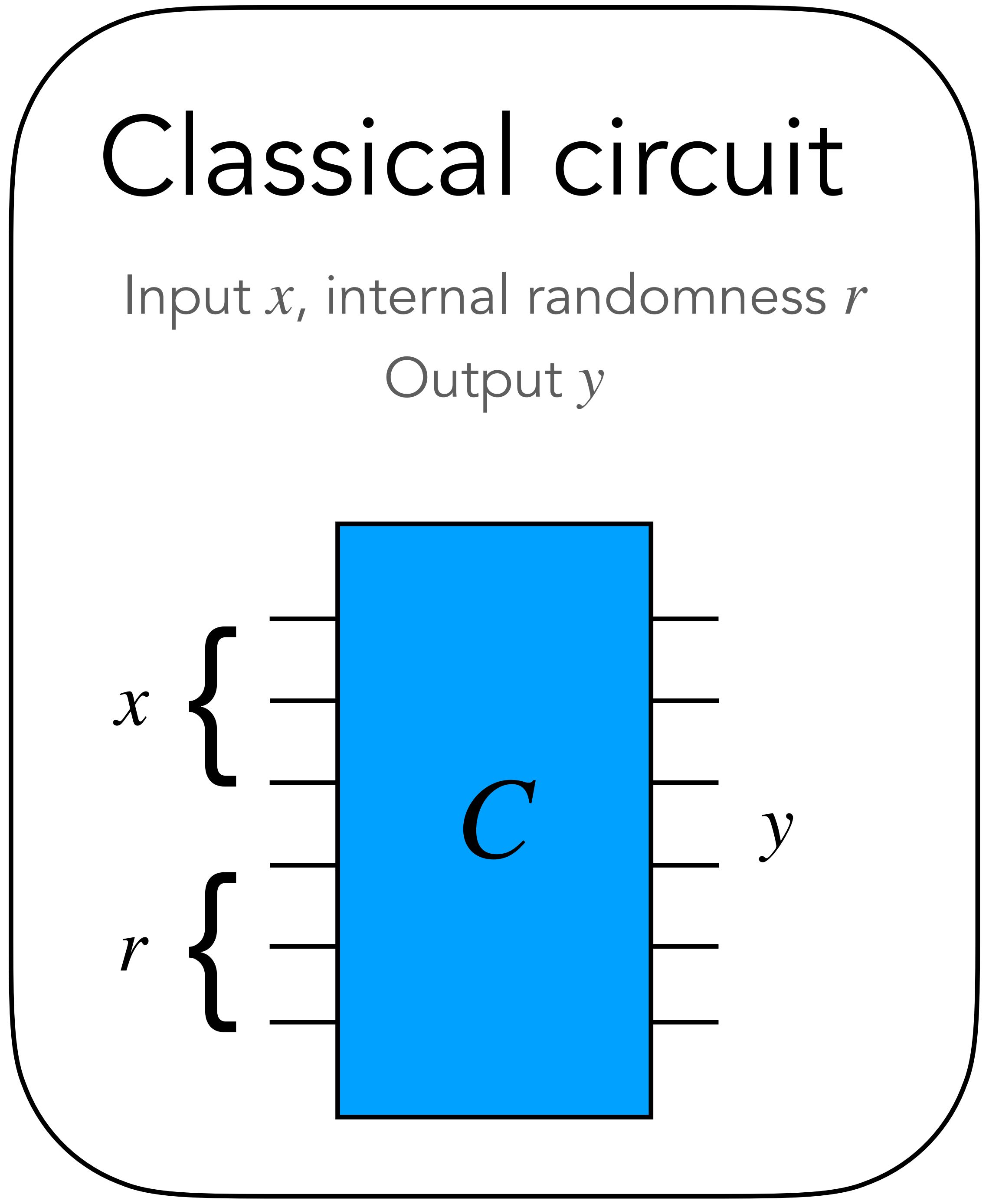
There is a relation task solved by a noisy constant-depth quantum circuit (QNC^0) with probability $1 - o(1)$ on all inputs.

A classical probabilistic circuit with bounded fan-in gates and constant-depth (NC^0) solves the task with probability at most $9/10$ over a uniform input.



Noisy quantum advantage against weak circuits

Bravyi, Gosset, König, Tomamichel [BGKT19]:
There is a relation task solved by a noisy constant-depth quantum circuit (QNC^0) with probability $1 - o(1)$ on all inputs.
A classical probabilistic circuit with bounded fan-in gates and constant-depth (NC^0) solves the task with probability at most $9/10$ over a uniform input.



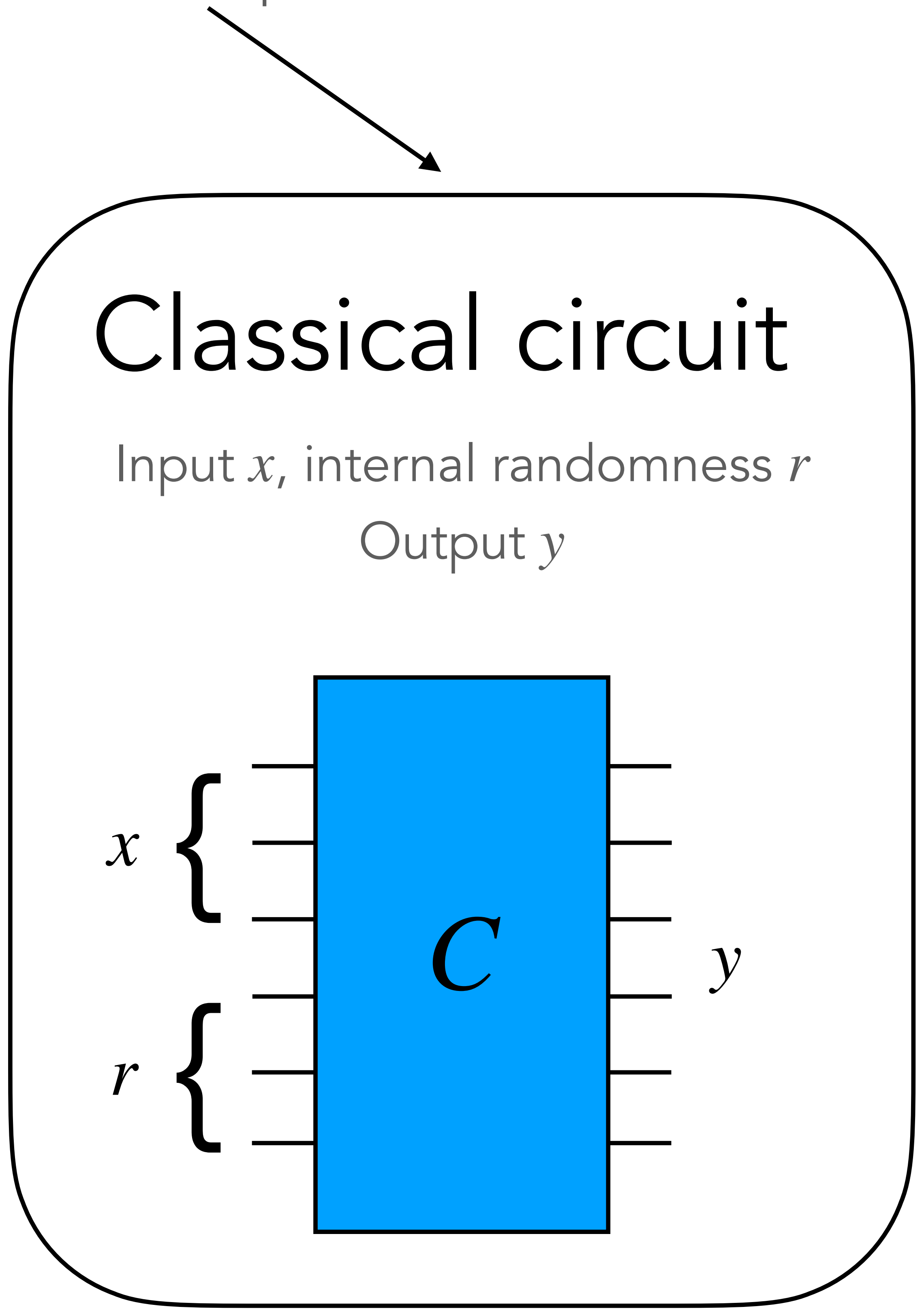
Bounded fan-in, constant-depth classical circuits (NC^0) are fairly weak.
Can we increase the separation to compare against more powerful classical circuits?

Noisy quantum advantage against weak circuits

Bravyi, Gosset, König, Tomamichel [BGKT19]:

There is a relation task solved by a noisy constant-depth quantum circuit (QNC^0) with probability $1 - o(1)$ on all inputs.

A classical probabilistic circuit with bounded fan-in gates and constant-depth (NC^0) solves the task with probability at most $9/10$ over a uniform input.



Bounded fan-in, constant-depth classical circuits (NC^0) are fairly weak.

Can we increase the separation to compare against more powerful classical circuits?

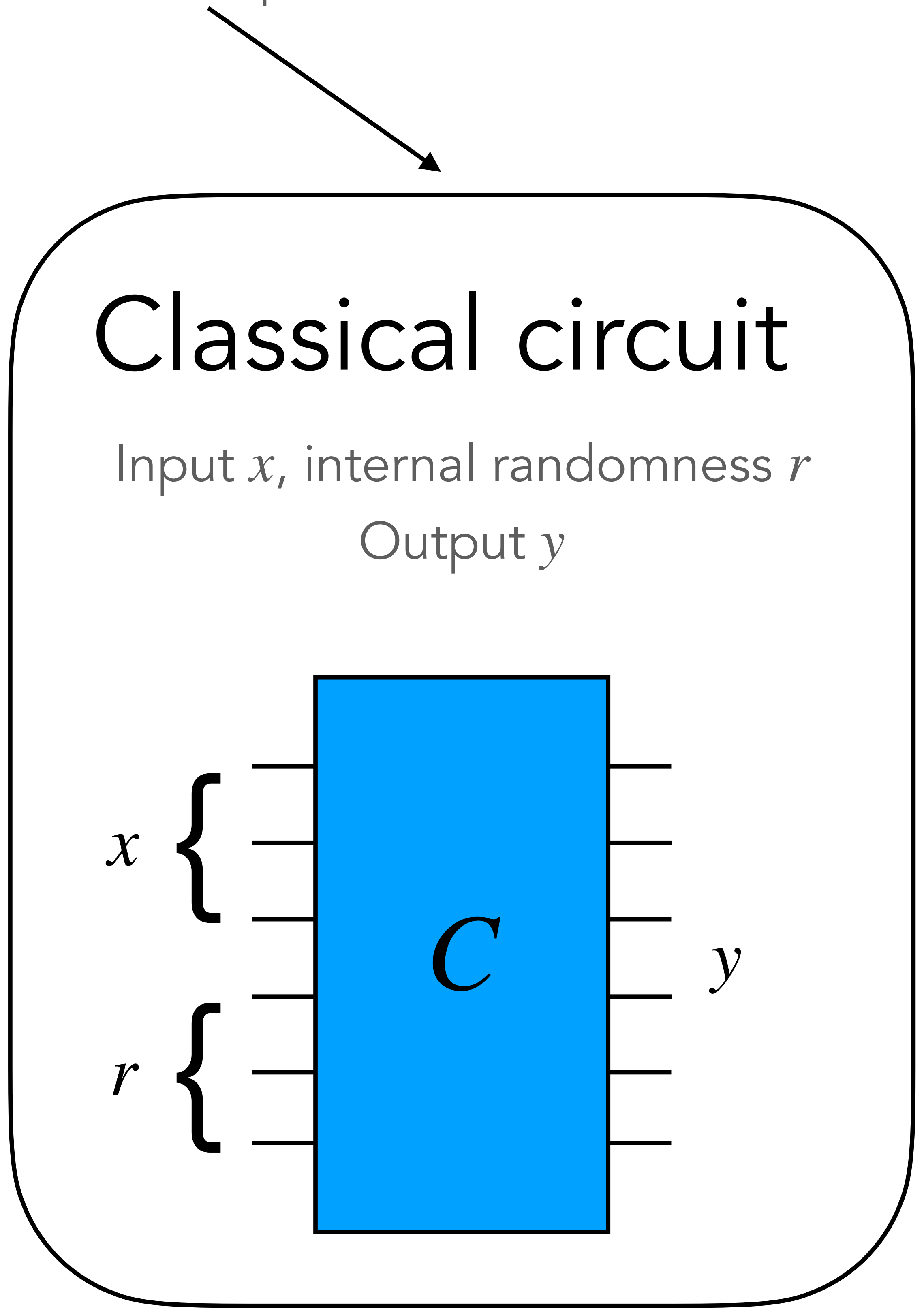
Without noise, yes: [BGK18], [CSV18], [Le19], [BKST19], [GS20]

Noisy quantum advantage against weak circuits

Bravyi, Gosset, König, Tomamichel [BGKT19]:

There is a relation task solved by a noisy constant-depth quantum circuit (QNC^0) with probability $1 - o(1)$ on all inputs.

A classical probabilistic circuit with bounded fan-in gates and constant-depth (NC^0) solves the task with probability at most $9/10$ over a uniform input.



Bounded fan-in, constant-depth classical circuits (NC^0) are fairly weak.

Can we increase the separation to compare against more powerful classical circuits?

Without noise, yes: [BGK18], [CSV18], [Le19], [BKST19], [GS20]

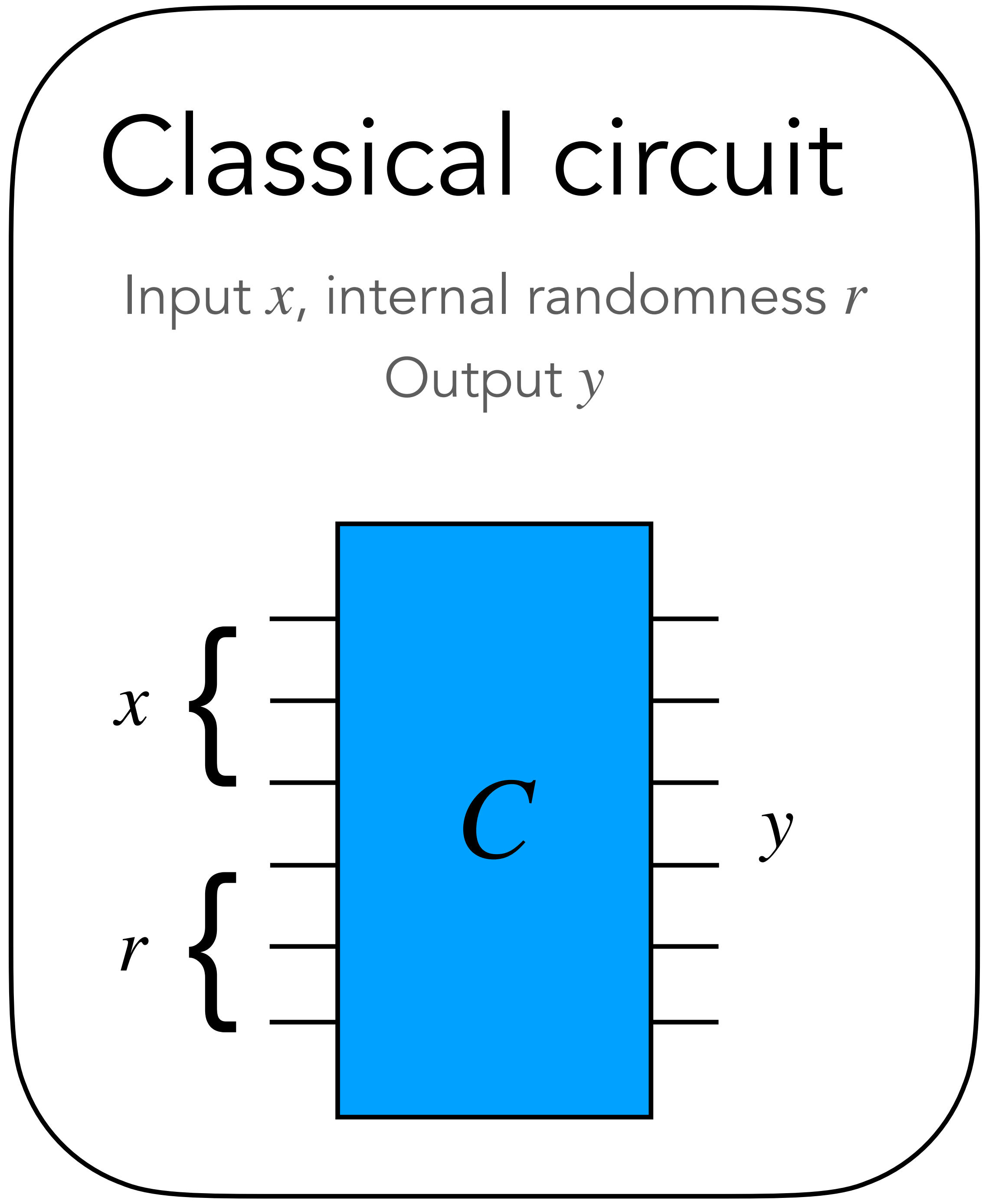
With noise?

Noisy quantum advantage against weak circuits

Bravyi, Gosset, König, Tomamichel [BGKT19]:

There is a relation task solved by a noisy constant-depth quantum circuit (QNC^0) with probability $1 - o(1)$ on all inputs.

A classical probabilistic circuit with bounded fan-in gates and constant-depth (NC^0) solves the task with probability at most $9/10$ over a uniform input.



Bounded fan-in, constant-depth classical circuits (NC^0) are fairly weak.

Can we increase the separation to compare against more powerful classical circuits?

Without noise, yes: [BGK18], [CSV18], [Le19], [BKST19], [GS20]

With noise? This work: yes!

Can we get a best-of-both-worlds situation?

Separation between:

	Noiseless quantum circuit	Noisy quantum circuit
Weaker classical circuit (Below NC^0)		
Stronger classical circuit (Above NC^0)		

Can we get a best-of-both-worlds situation?

Separation between:

	Noiseless quantum circuit	Noisy quantum circuit
Weaker classical circuit (Below NC^0)		
Stronger classical circuit (Above NC^0)		

NC^0

Can we get a best-of-both-worlds situation?

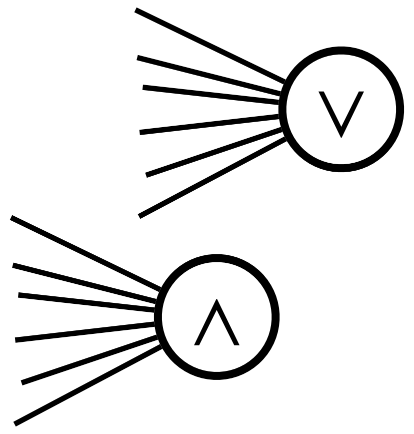
Separation between:

	Noiseless quantum circuit	Noisy quantum circuit
Weaker classical circuit (Below NC^0)		
Stronger classical circuit (Above NC^0)		

$\mathsf{NC}^0 \subsetneq \mathsf{AC}^0$

Can we get a best-of-both-worlds situation?

Separation between:	Noiseless quantum circuit	Noisy quantum circuit
Weaker classical circuit (Below NC^0)		
Stronger classical circuit (Above NC^0)		



Constant depth, **unbounded** fan-in classical circuits

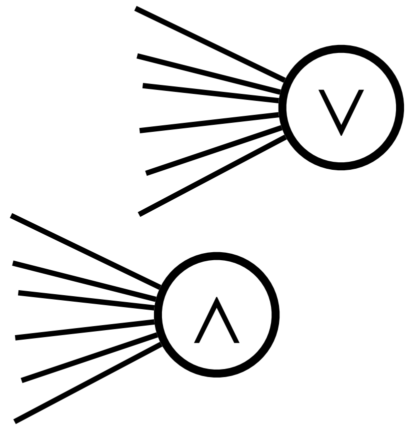
↑

$\mathsf{NC}^0 \subsetneq \mathsf{AC}^0$

Can we get a best-of-both-worlds situation?

Separation between:

	Noiseless quantum circuit	Noisy quantum circuit
Weaker classical circuit (Below NC^0)		
Stronger classical circuit (Above NC^0)		



Constant depth, **unbounded** fan-in classical circuits

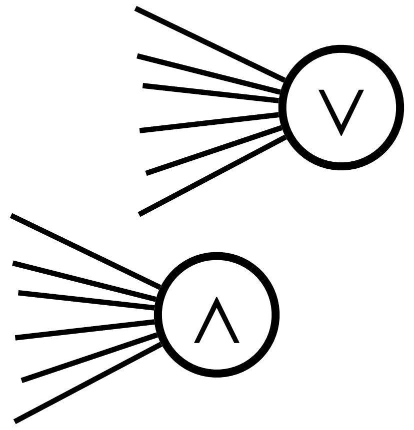
↑

$\mathsf{NC}^0 \subsetneq \mathsf{AC}^0 \subsetneq \mathsf{AC}^0[p]$

Can we get a best-of-both-worlds situation?

Separation between:

	Noiseless quantum circuit	Noisy quantum circuit
Weaker classical circuit (Below NC^0)		
Stronger classical circuit (Above NC^0)		



Constant depth, **unbounded** fan-in classical circuits

↑

$\mathsf{NC}^0 \subsetneq \mathsf{AC}^0 \subsetneq \mathsf{AC}^0[p]$

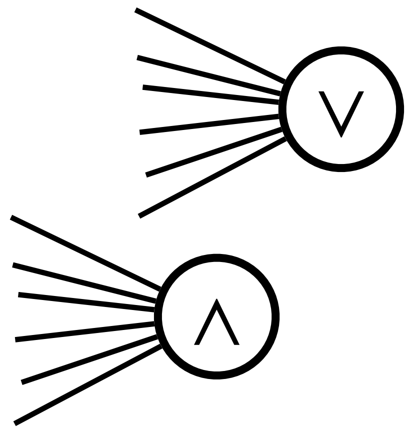
↓

AC^0 circuits with MOD_p gates

Can we get a best-of-both-worlds situation?

Separation between:

	Noiseless quantum circuit	Noisy quantum circuit
Weaker classical circuit (Below NC^0)		
Stronger classical circuit (Above NC^0)		



Constant depth, **unbounded** fan-in classical circuits

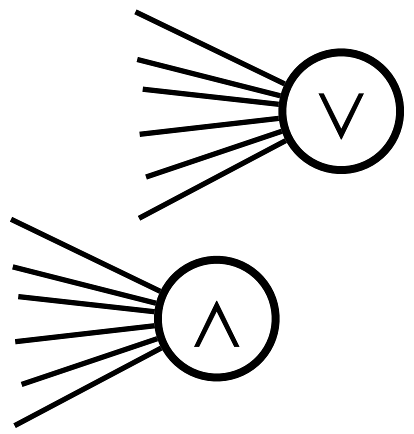
$$\mathsf{NC}^0 \subsetneq \mathsf{AC}^0 \subsetneq \mathsf{AC}^0[p] \subsetneq \mathsf{L}$$

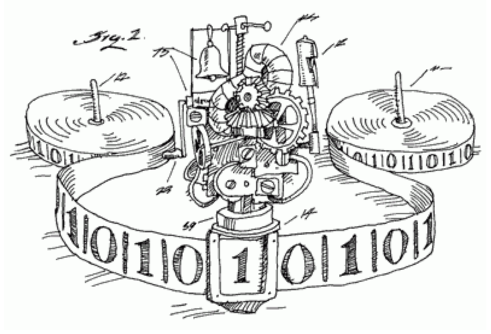
AC^0 circuits with MOD_p gates

Can we get a best-of-both-worlds situation?

Separation between:

	Noiseless quantum circuit	Noisy quantum circuit
Weaker classical circuit (Below NC^0)		
Stronger classical circuit (Above NC^0)		





Constant depth, **unbounded** fan-in classical circuits

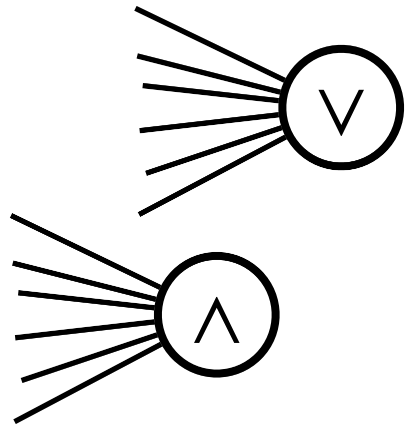
Log-space Turing Machines

$$\mathsf{NC}^0 \subsetneq \mathsf{AC}^0 \subsetneq \mathsf{AC}^0[p] \subsetneq \mathsf{L}$$

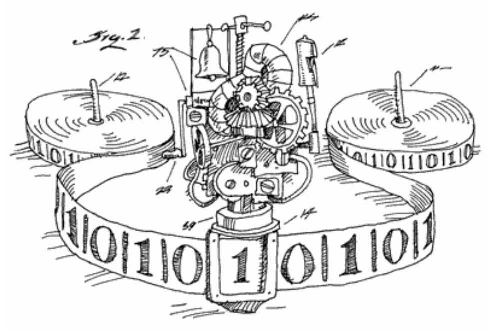
AC^0 circuits with MOD_p gates

Can we get a best-of-both-worlds situation?

Separation between:	Noiseless quantum circuit	Noisy quantum circuit
Weaker classical circuit (Below NC^0)		
Stronger classical circuit (Above NC^0)		



Constant depth, **unbounded** fan-in classical circuits



Log-space Turing Machines

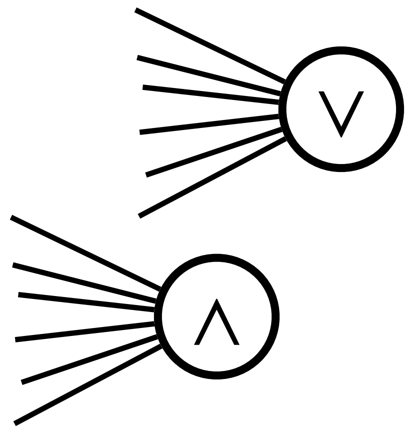
$$\mathsf{NC}^0 \subsetneq \mathsf{AC}^0 \subsetneq \mathsf{AC}^0[p] \subsetneq \mathsf{L} \subseteq \oplus\mathsf{L}$$

AC^0 circuits with MOD_p gates

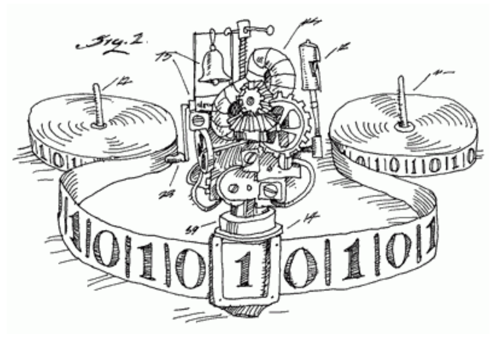
Can we get a best-of-both-worlds situation?

Separation between:

	Noiseless quantum circuit	Noisy quantum circuit
Weaker classical circuit (Below NC^0)		
Stronger classical circuit (Above NC^0)		



Constant depth, **unbounded** fan-in classical circuits



Log-space Turing Machines

$$\mathsf{NC}^0 \subsetneq \mathsf{AC}^0 \subsetneq \mathsf{AC}^0[p] \subsetneq \mathsf{L} \subseteq \oplus\mathsf{L}$$

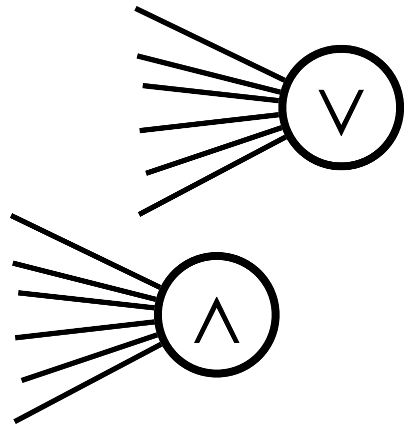
AC^0 circuits with MOD_p gates

Complete problem: Parity of $s \to t$ paths in a DAG

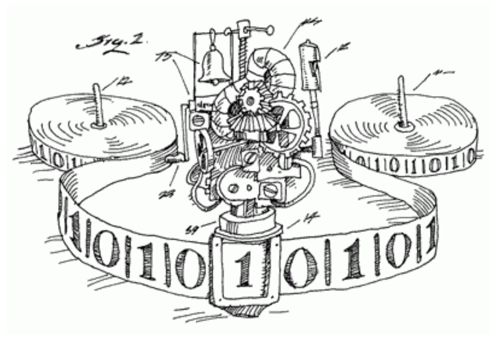
Can we get a best-of-both-worlds situation?

Separation between:

	Noiseless quantum circuit	Noisy quantum circuit
Weaker classical circuit (Below NC^0)	[BGK18] [CSV18] [Le19]	
Stronger classical circuit (Above NC^0)		



Constant depth, **unbounded** fan-in classical circuits



Log-space Turing Machines

$$\mathsf{NC}^0 \subsetneq \mathsf{AC}^0 \subsetneq \mathsf{AC}^0[p] \subsetneq \mathsf{L} \subseteq \oplus\mathsf{L}$$

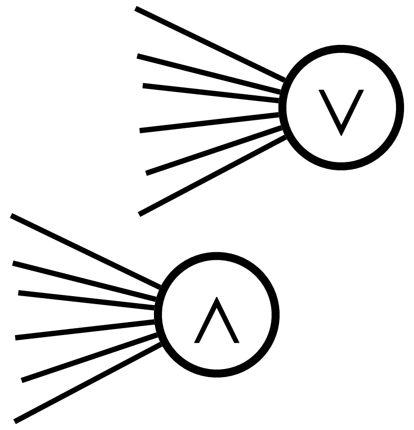
AC^0 circuits with MOD_p gates

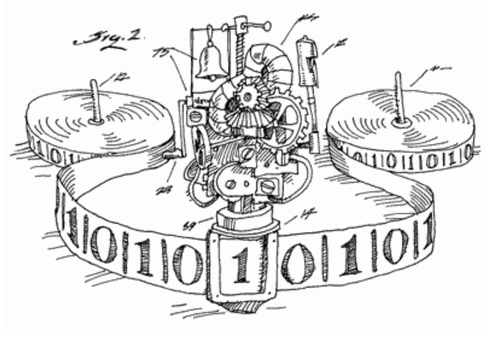
Complete problem: Parity of $s \to t$ paths in a DAG

Can we get a best-of-both-worlds situation?

Separation between:

	Noiseless quantum circuit	Noisy quantum circuit
Weaker classical circuit (Below NC^0)	[BGK18] [CSV18] [Le19]	
Stronger classical circuit (Above NC^0)	[BKST19] [GS20] : Interactive problem	





Constant depth, **unbounded** fan-in classical circuits

Log-space Turing Machines

$$\mathsf{NC}^0 \subsetneq \mathsf{AC}^0 \subsetneq \mathsf{AC}^0[p] \subsetneq \mathsf{L} \subseteq \oplus\mathsf{L}$$

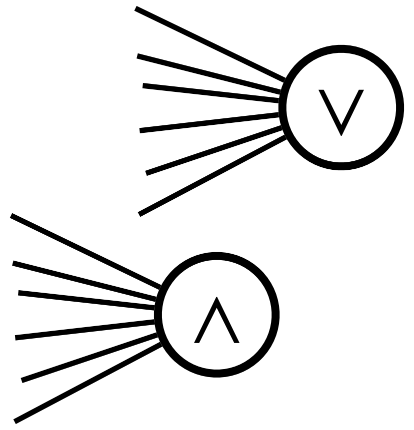
AC^0 circuits with MOD_p gates

Complete problem: Parity of $s \to t$ paths in a DAG

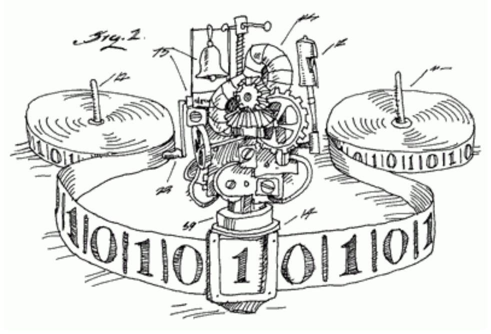
Can we get a best-of-both-worlds situation?

Separation between:

	Noiseless quantum circuit	Noisy quantum circuit
Weaker classical circuit (Below NC^0)	[BGK18] [CSV18] [Le19]	[BGKT19]
Stronger classical circuit (Above NC^0)	[BKST19] [GS20] : Interactive problem	



Constant depth, **unbounded** fan-in classical circuits



Log-space Turing Machines

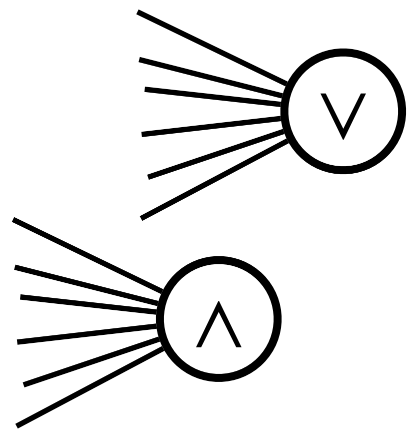
$$\mathsf{NC}^0 \subsetneq \mathsf{AC}^0 \subsetneq \mathsf{AC}^0[p] \subsetneq \mathsf{L} \subseteq \oplus\mathsf{L}$$

AC^0 circuits with MOD_p gates

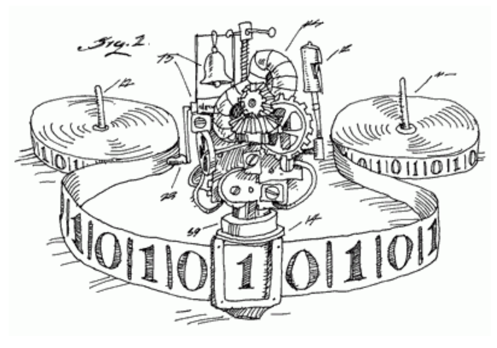
Complete problem: Parity of $s \to t$ paths in a DAG

Can we get a best-of-both-worlds situation?

Separation between:	Noiseless quantum circuit	Noisy quantum circuit
Weaker classical circuit (Below NC^0)	[BGK18] [CSV18] [Le19]	[BGKT19]
Stronger classical circuit (Above NC^0)	[BKST19] [GS20] : Interactive problem	This work: Make these results **noisy** separations



Constant depth, **unbounded** fan-in classical circuits



Log-space Turing Machines

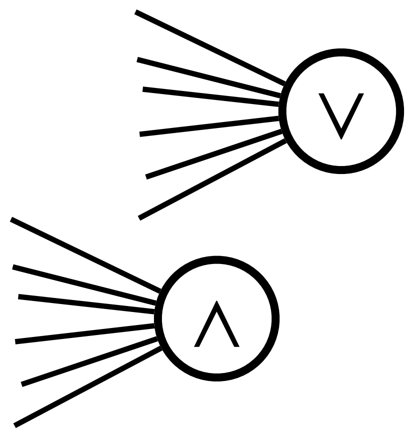
$$\mathsf{NC}^0 \subsetneq \mathsf{AC}^0 \subsetneq \mathsf{AC}^0[p] \subsetneq \mathsf{L} \subseteq \oplus\mathsf{L}$$

AC^0 circuits with MOD_p gates

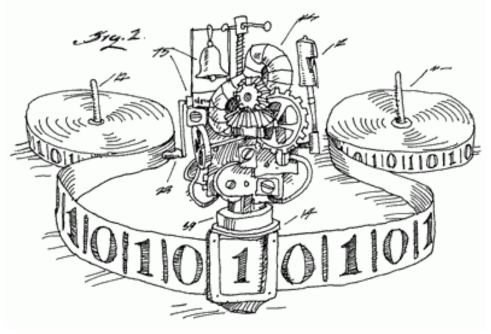
Complete problem: Parity of $s \to t$ paths in a DAG

Can we get a best-of-both-worlds situation?

Separation between:	Noiseless quantum circuit	Noisy quantum circuit
Weaker classical circuit (Below NC^0)	[BGK18] [CSV18] [Le19]	[BGKT19]
Stronger classical circuit (Above NC^0)	[BKST19] [GS20] : Interactive problem	This work: Make these results **noisy** separations



Constant depth, **unbounded** fan-in classical circuits



Log-space Turing Machines

$$\mathsf{NC}^0 \subsetneq \mathsf{AC}^0 \subsetneq \mathsf{AC}^0[p] \subsetneq \mathsf{L} \subseteq \oplus\mathsf{L}$$

AC^0 circuits with MOD_p gates

Complete problem: Parity of $s \to t$ paths in a DAG

Outline: Three steps to prove a noisy separation

Noiseless average-case separation:
Let $\mathscr{I}$ be a task solved by a **noiseless** QNC^0 circuit on all inputs with certainty.
Prove that a classical probabilistic machine solves $\mathscr{I}$ with probability at most $1 - \delta$ on a uniformly random input.

Outline: Three steps to prove a noisy separation

Noiseless average-case separation:
Let $\mathscr{I}$ be a task solved by a **noiseless** QNC^0 circuit on all inputs with certainty.
Prove that a classical probabilistic machine solves $\mathscr{I}$ with probability at most $1 - \delta$ on a uniformly random input.

This step will require new ideas!

Outline: Three steps to prove a noisy separation

Noiseless average-case separation:
Let $\mathcal{I}$ be a task solved by a **noiseless** QNC^0 circuit on all inputs with certainty.
Prove that a classical probabilistic machine solves $\mathcal{I}$ with probability at most $1 - \delta$ on a uniformly random input.

This step will require new ideas!

$+$

Extend the definition of the problem to account for noise [BGKT19]:
Let $\mathcal{I}$ be the task above. Suppose y is a valid output on input x.
For the "extended" task $\mathcal{I}'$, all $\mathcal{Y}$ such that $Dec(\mathcal{Y}) = y$ are valid outputs on input x.

Outline: Three steps to prove a noisy separation

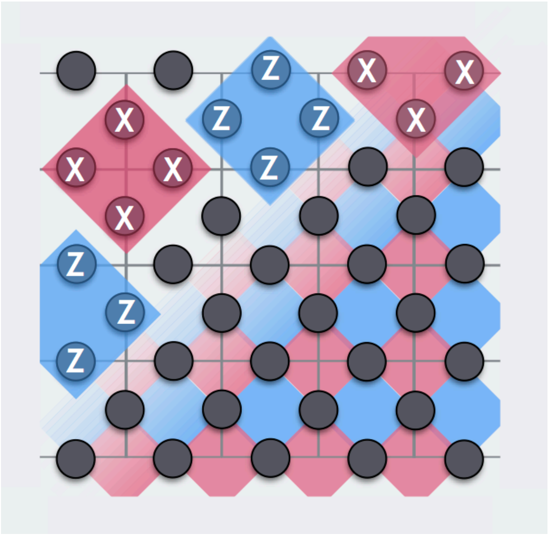
Noiseless average-case separation:
Let $\mathcal{I}$ be a task solved by a **noiseless** QNC^0 circuit on all inputs with certainty.
Prove that a classical probabilistic machine solves $\mathcal{I}$ with probability at most $1 - \delta$ on a uniformly random input.

This step will require new ideas!

+

Extend the definition of the problem to account for noise [BGKT19]:
Let $\mathcal{I}$ be the task above. Suppose y is a valid output on input x.
For the "extended" task $\mathcal{I}'$, all $\mathcal{Y}$ such that $Dec(\mathcal{Y}) = y$ are valid outputs on input x.

$\mathcal{I}'$ output:

$Dec($  $) = y$

$\mathcal{I}$ output:

Outline: Three steps to prove a noisy separation

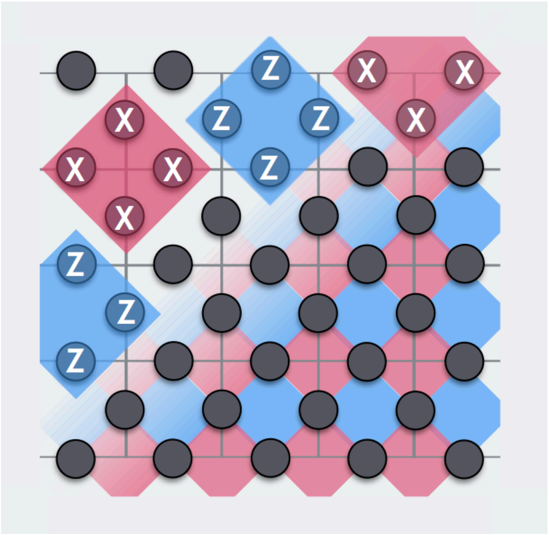
Noiseless average-case separation:
Let $\mathscr{I}$ be a task solved by a **noiseless** QNC^0 circuit on all inputs with certainty.
Prove that a classical probabilistic machine solves $\mathscr{I}$ with probability at most $1 - \delta$ on a uniformly random input.

This step will require new ideas!

$+$

Extend the definition of the problem to account for noise [BGKT19]:
Let $\mathscr{I}$ be the task above. Suppose y is a valid output on input x.
For the "extended" task $\mathscr{I}'$, all $\mathscr{Y}$ such that $Dec(\mathscr{Y}) = y$ are valid outputs on input x.

$\mathscr{I}'$ output:

$Dec($  $) = y$

$\mathscr{I}$ output:

$=$

Noisy separation:
The task $\mathscr{I}'$ is solved by a **noisy** QNC^0 circuit on all inputs w/p $1 - o(1)$.
A classical probabilistic machine solves $\mathscr{I}'$ with probability at most $1 - \delta$ on a uniformly random input.

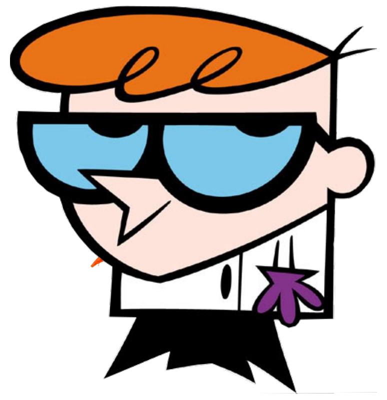
Main result

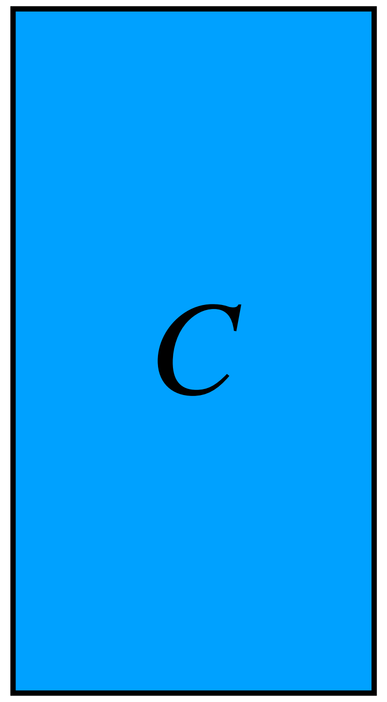
Noiseless average-case separation (This work):
There is an interactive task solved by a **noiseless** QNC^0 circuit on all inputs with certainty.
Let $\mathscr{R}$ be a classical probabilistic machine that solves the same task with probability $420/421$ over uniform input. Then $\oplus\mathsf{L} \subseteq (\mathsf{AC}^0)^{\mathscr{R}}$.

Main result

Noiseless average-case separation (This work):
There is an interactive task solved by a **noiseless** QNC^0 circuit on all inputs with certainty. Let $\mathscr{R}$ be a classical probabilistic machine that solves the same task with probability $420/421$ over uniform input. Then $\oplus\mathsf{L} \subseteq (\mathsf{AC}^0)^{\mathscr{R}}$.

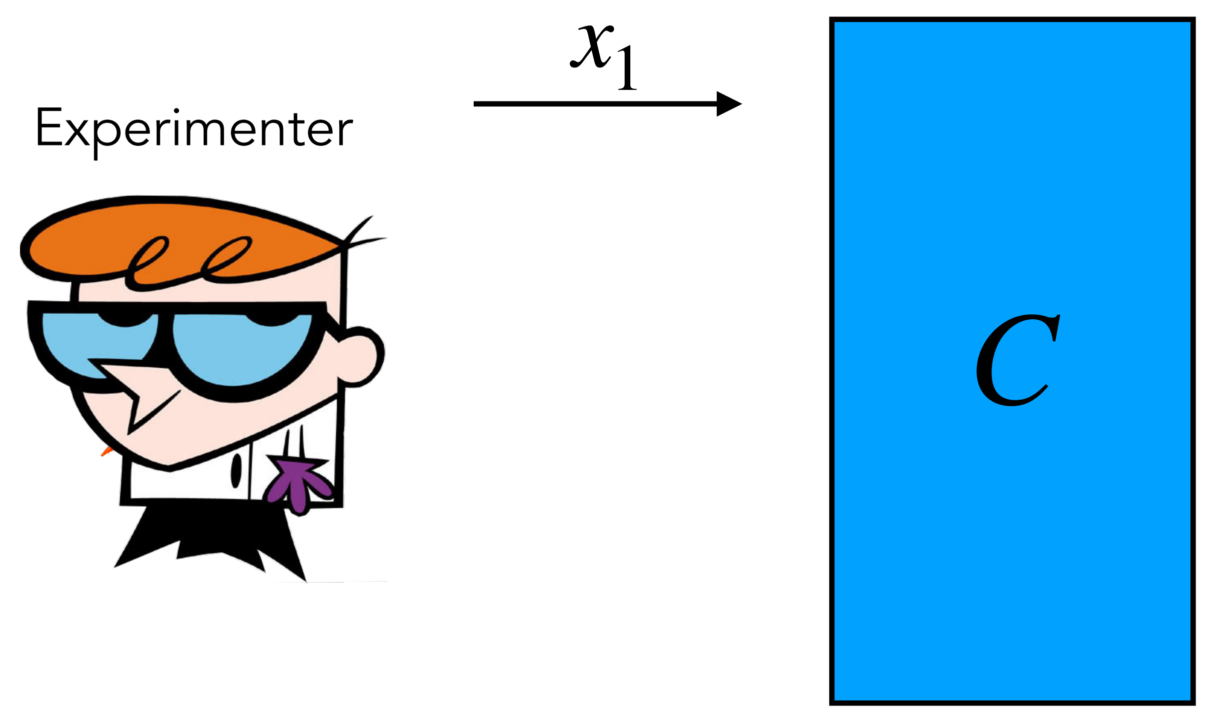
Experimenter





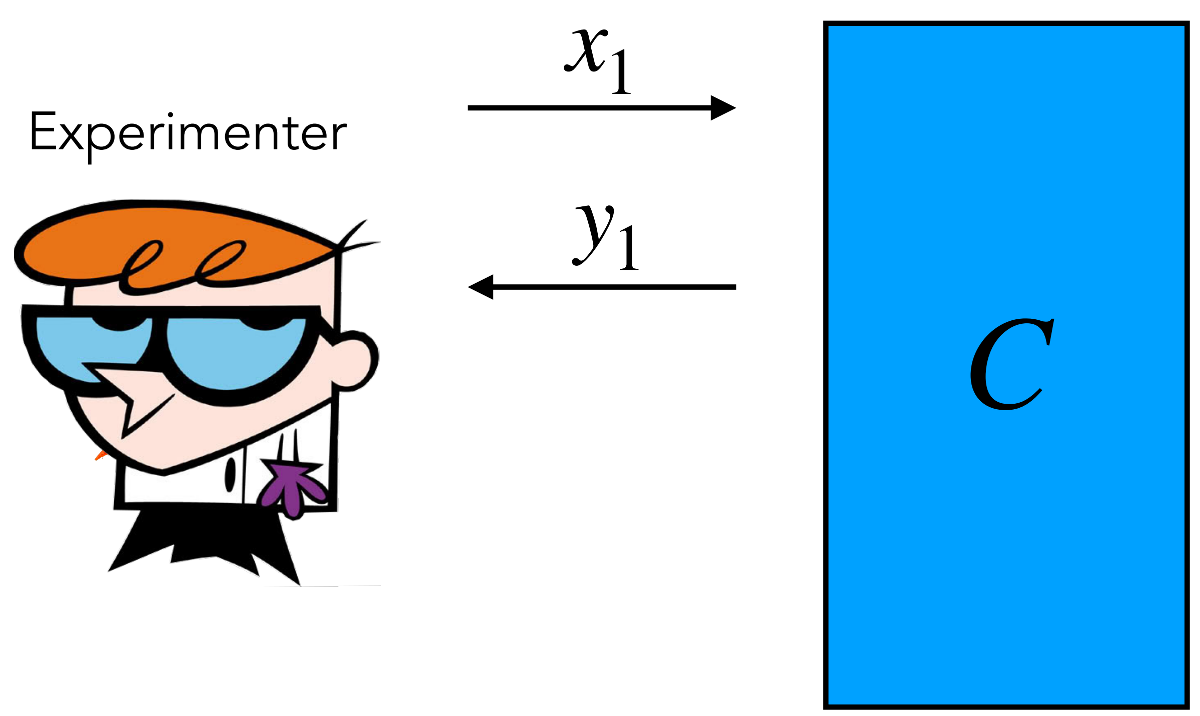
Main result

Noiseless average-case separation (This work):
There is an interactive task solved by a **noiseless** QNC^0 circuit on all inputs with certainty.
Let $\mathscr{R}$ be a classical probabilistic machine that solves the same task with probability $420/421$ over uniform input. Then $\oplus\mathsf{L} \subseteq (\mathsf{AC}^0)^{\mathscr{R}}$.



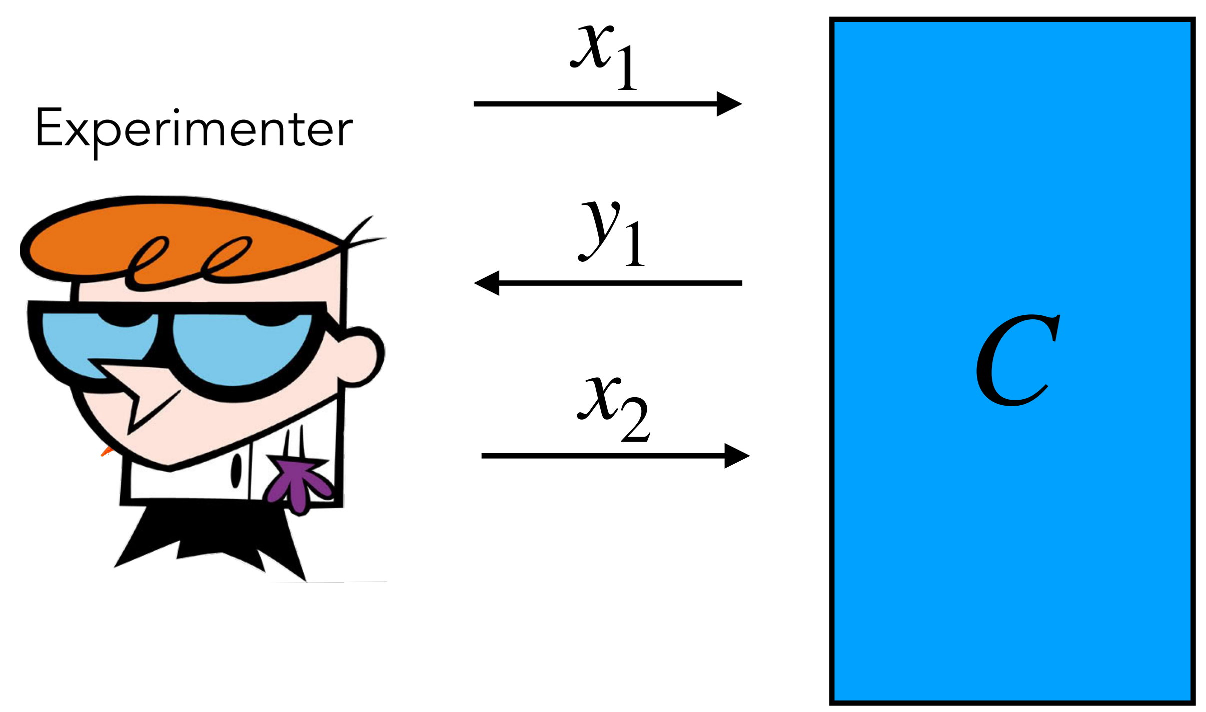
Main result

Noiseless average-case separation (This work):
There is an interactive task solved by a **noiseless** QNC^0 circuit on all inputs with certainty. Let $\mathscr{R}$ be a classical probabilistic machine that solves the same task with probability $420/421$ over uniform input. Then $\oplus\mathsf{L} \subseteq (\mathsf{AC}^0)^{\mathscr{R}}$.



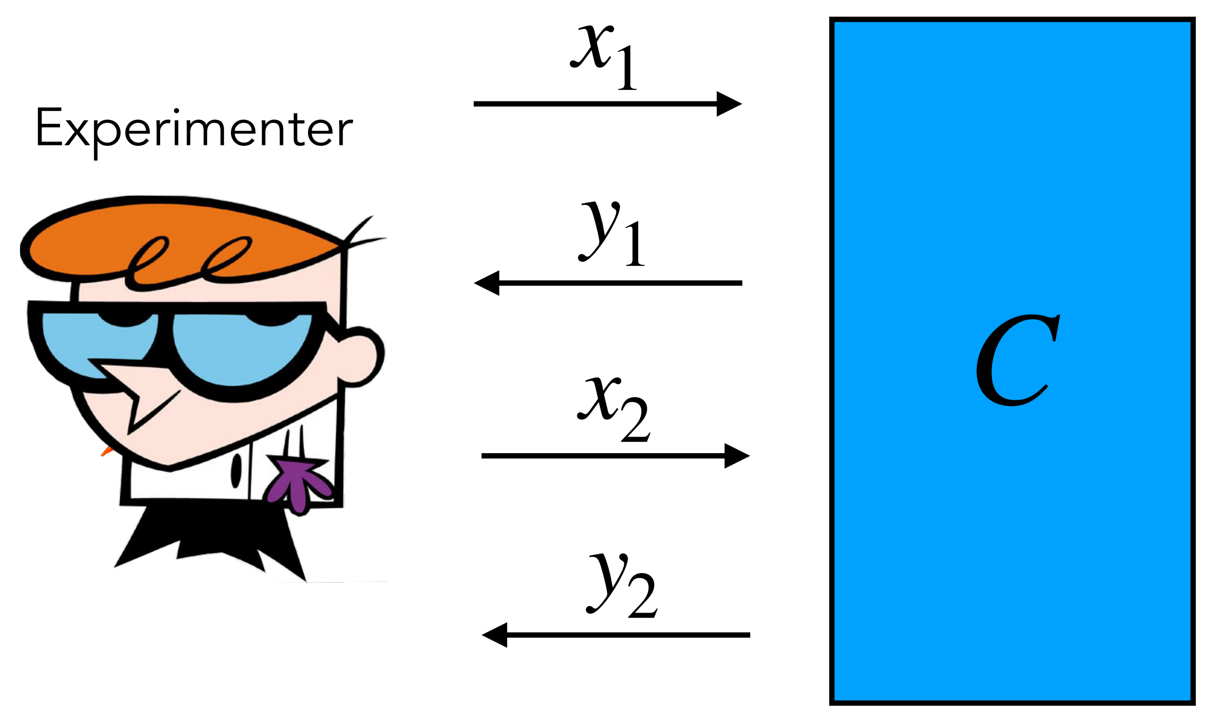
Main result

Noiseless average-case separation (This work):
There is an interactive task solved by a **noiseless** QNC^0 circuit on all inputs with certainty. Let $\mathscr{R}$ be a classical probabilistic machine that solves the same task with probability $420/421$ over uniform input. Then $\oplus\mathsf{L} \subseteq (\mathsf{AC}^0)^{\mathscr{R}}$.



Main result

Noiseless average-case separation (This work):
There is an interactive task solved by a **noiseless** QNC^0 circuit on all inputs with certainty.
Let $\mathscr{R}$ be a classical probabilistic machine that solves the same task with probability $420/421$ over uniform input. Then $\oplus\mathsf{L} \subseteq (\mathsf{AC}^0)^{\mathscr{R}}$.

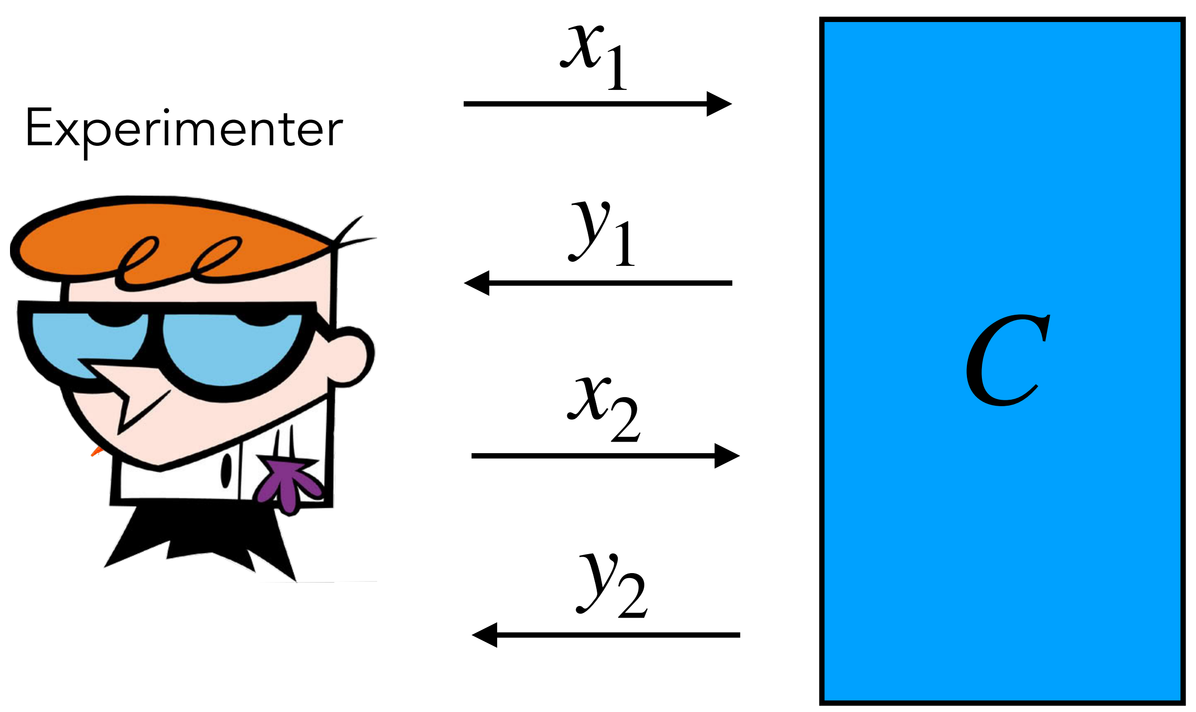


Main result

Noiseless average-case separation (This work):
There is an interactive task solved by a **noiseless** QNC^0 circuit on all inputs with certainty. Let $\mathscr{R}$ be a classical probabilistic machine that solves the same task with probability $420/421$ over uniform input. Then $\oplus L \subseteq (AC^0)^{\mathscr{R}}$.

+

Extend the definition of the interactive problem to account for noise [BGKT19]:
Let $\mathscr{I}$ be the interactive problem above.
If (x_1, y_1, x_2, y_2) is a valid transcript for $\mathscr{I}$, then all $(x_1, \mathscr{Y}_1, x_2, \mathscr{Y}_2)$ such that $Dec(\mathscr{Y}_1) = y_1$ and $Dec(\mathscr{Y}_2) = y_2$ are valid transcripts for the "extended" problem $\mathscr{I}'$.



Main result

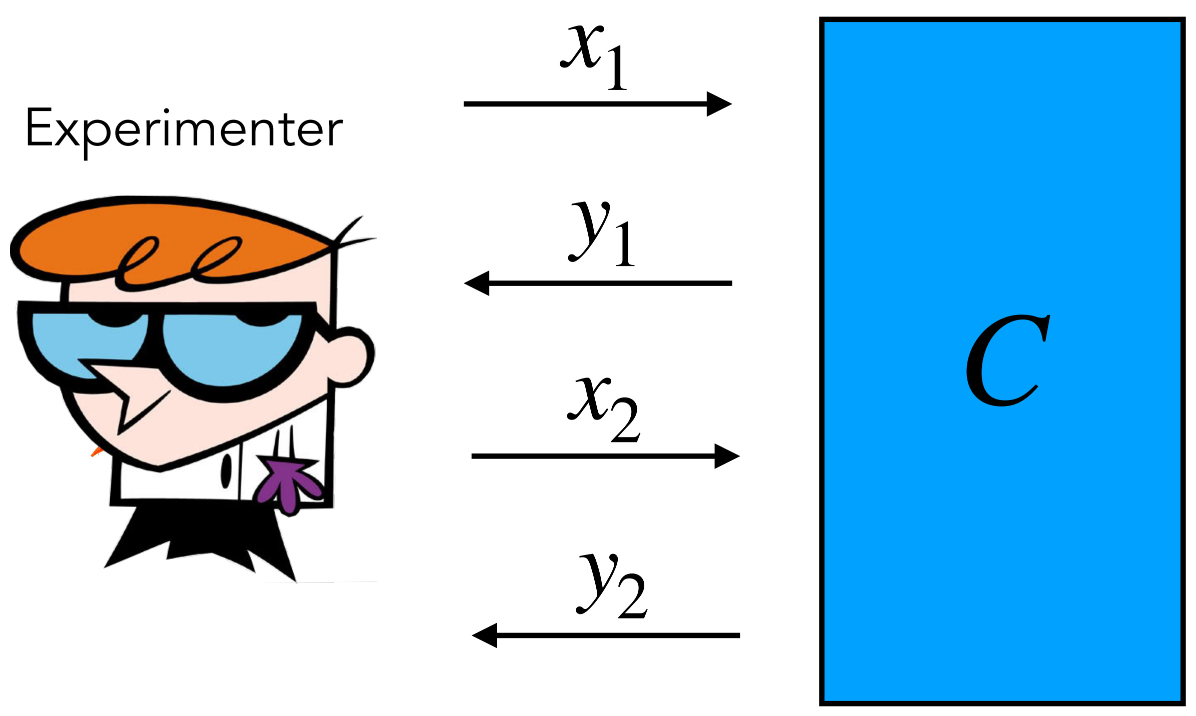
Noiseless average-case separation (This work):
There is an interactive task solved by a **noiseless** QNC^0 circuit on all inputs with certainty. Let $\mathscr{R}$ be a classical probabilistic machine that solves the same task with probability $420/421$ over uniform input. Then $\oplus\mathsf{L} \subseteq (\mathsf{AC}^0)^{\mathscr{R}}$.

+

Extend the definition of the interactive problem to account for noise [BGKT19]:
Let $\mathscr{I}$ be the interactive problem above.
If (x_1, y_1, x_2, y_2) is a valid transcript for $\mathscr{I}$, then all $(x_1, \mathscr{Y}_1, x_2, \mathscr{Y}_2)$ such that $Dec(\mathscr{Y}_1) = y_1$ and $Dec(\mathscr{Y}_2) = y_2$ are valid transcripts for the "extended" problem $\mathscr{I}'$.

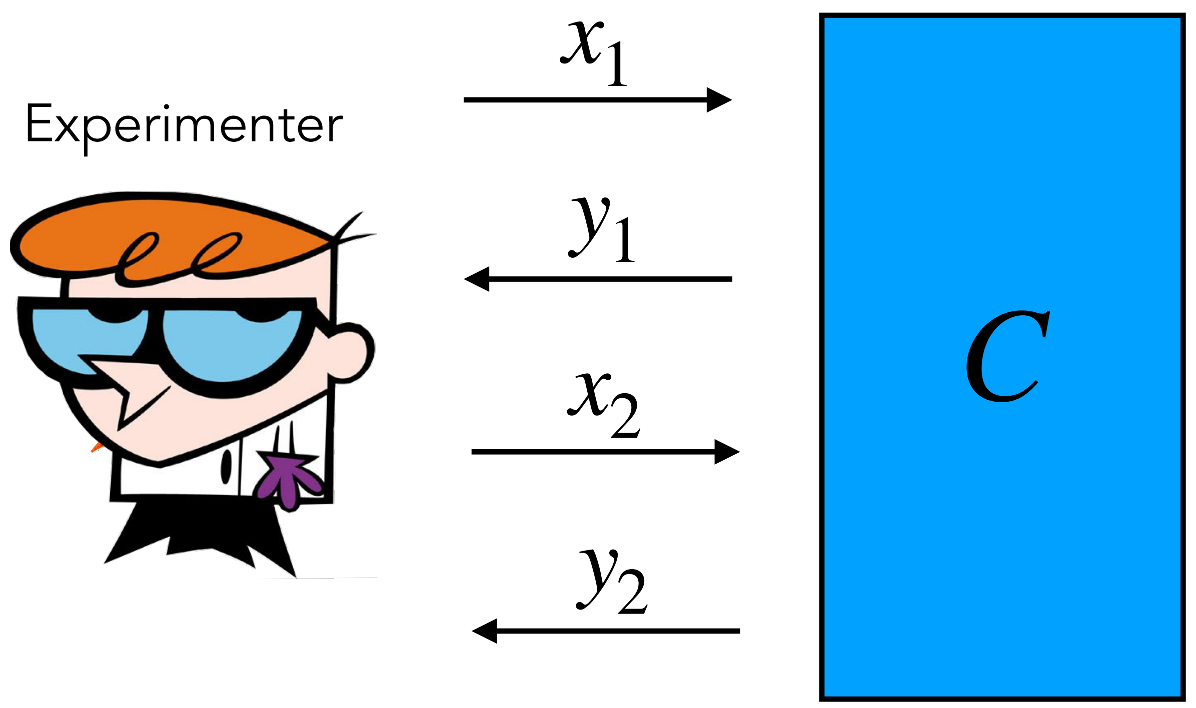
=

Noisy separation:
There is an interactive task solved by a **noisy** QNC^0 circuit on all inputs w/p $1 - o(1)$.
Let $\mathscr{R}$ be a classical probabilistic machine that solves the same task with probability $420/421$ over uniform input. Then $\oplus\mathsf{L} \subseteq (\mathsf{qAC}^0)^{\mathscr{R}}$.



Main result

Noiseless average-case separation (This work):
There is an interactive task solved by a **noiseless** QNC^0 circuit on all inputs with certainty.
Let $\mathscr{R}$ be a classical probabilistic machine that solves the same task with probability $420/421$ over uniform input. Then $\oplus\mathsf{L} \subseteq (\mathsf{AC}^0)^{\mathscr{R}}$.



+

Extend the definition of the interactive problem to account for noise [BGKT19]:
Let $\mathscr{I}$ be the interactive problem above.
If (x_1, y_1, x_2, y_2) is a valid transcript for $\mathscr{I}$, then all $(x_1, \mathscr{Y}_1, x_2, \mathscr{Y}_2)$ such that $Dec(\mathscr{Y}_1) = y_1$ and $Dec(\mathscr{Y}_2) = y_2$ are valid transcripts for the "extended" problem $\mathscr{I}'$.

=

Noisy separation:
There is an interactive task solved by a **noisy** QNC^0 circuit on all inputs w/p $1 - o(1)$.
Let $\mathscr{R}$ be a classical probabilistic machine that solves the same task with probability $420/421$ over uniform input. Then $\oplus\mathsf{L} \subseteq (\mathsf{qAC}^0)^{\mathscr{R}}$.

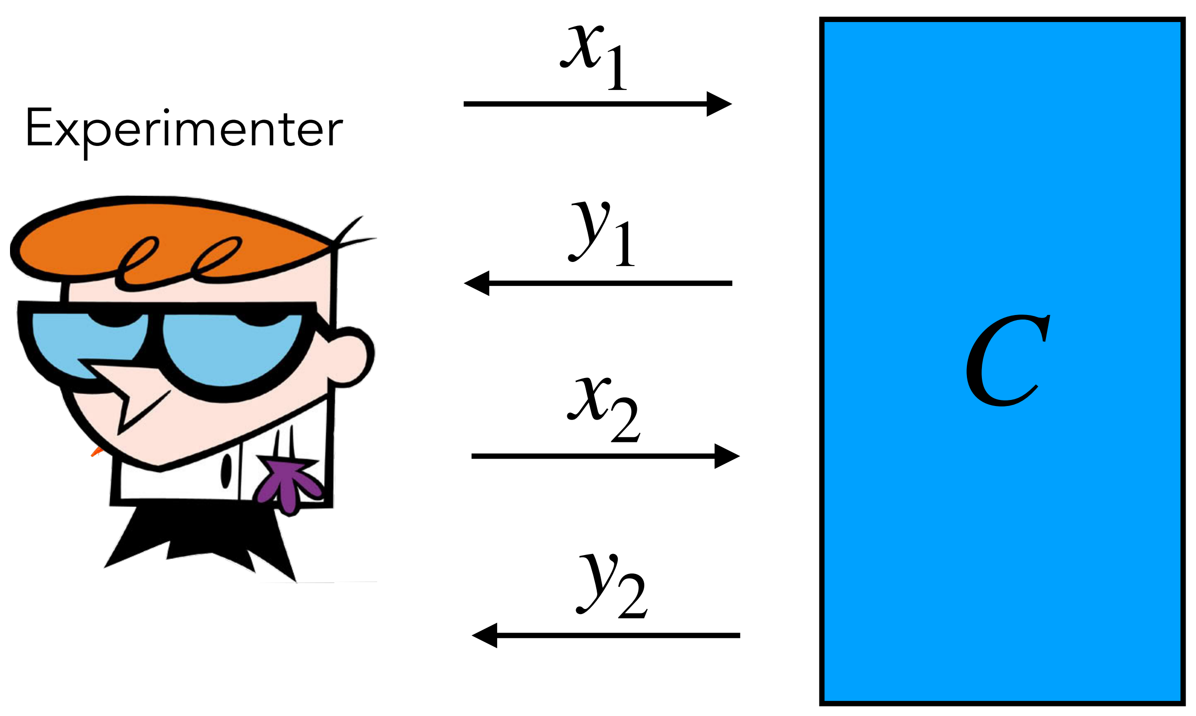
$\Longrightarrow$

Unconditional: Noisy QNC^0 vs. $\mathsf{AC}^0[p]$ separation

Conditional: If $\oplus\mathsf{L} \not\subseteq (\mathsf{qAC}^0)^{\mathsf{L}}$, then noisy QNC^0 vs. L separation

Main result

Noiseless average-case separation (This work):
There is an interactive task solved by a **noiseless** QNC^0 circuit on all inputs with certainty.
Let $\mathscr{R}$ be a classical probabilistic machine that solves the same task with probability $420/421$ over uniform input. Then $\oplus\mathrm{L} \subseteq (\mathrm{AC}^0)^{\mathscr{R}}$.



$+$

Extend the definition of the interactive problem to account for noise [BGKT19]:
Let $\mathscr{I}$ be the interactive problem above.
If (x_1, y_1, x_2, y_2) is a valid transcript for $\mathscr{I}$, then all $(x_1, \mathscr{Y}_1, x_2, \mathscr{Y}_2)$ such that $Dec(\mathscr{Y}_1) = y_1$ and $Dec(\mathscr{Y}_2) = y_2$ are valid transcripts for the "extended" problem $\mathscr{I}'$.

$=$

Noisy separation:
There is an interactive task solved by a **noisy** QNC^0 circuit on all inputs w/p $1 - o(1)$.
Let $\mathscr{R}$ be a classical probabilistic machine that solves the same task with probability $420/421$ over uniform input. Then $\oplus\mathrm{L} \subseteq (\mathrm{qAC}^0)^{\mathscr{R}}$.

$\Longrightarrow$

Unconditional: Noisy QNC^0 vs. $\mathrm{AC}^0[p]$ separation

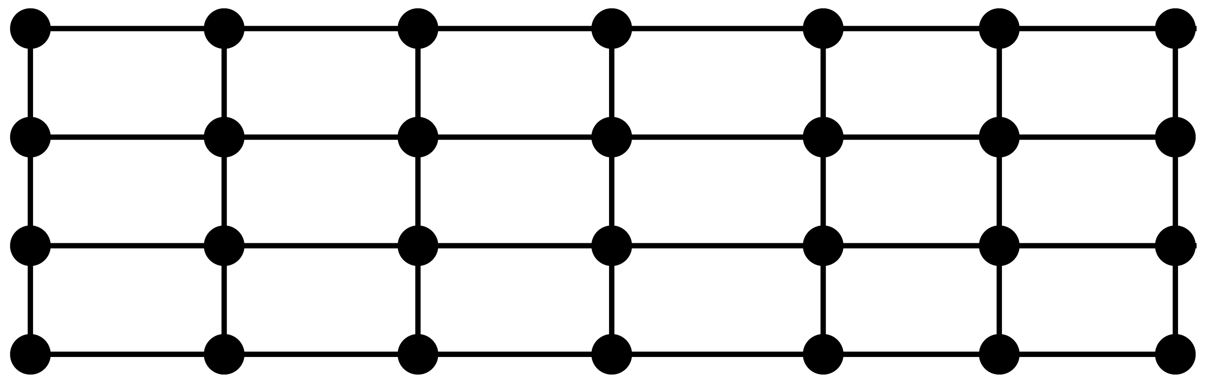
Conditional: If $\oplus\mathrm{L} \not\subseteq (\mathrm{qAC}^0)^{\mathrm{L}}$, then noisy QNC^0 vs. L separation

Noiseless average-case separation

Noiseless average-case separation:
There is an interactive task solved by a **noiseless** QNC^0 circuit on all inputs with certainty. Let $\mathscr{R}$ be a classical probabilistic machine that solves the same task with probability $420/421$ over uniform input. Then $\oplus\mathsf{L} \subseteq (\mathsf{AC}^0)^{\mathscr{R}}$.

Noiseless average-case separation

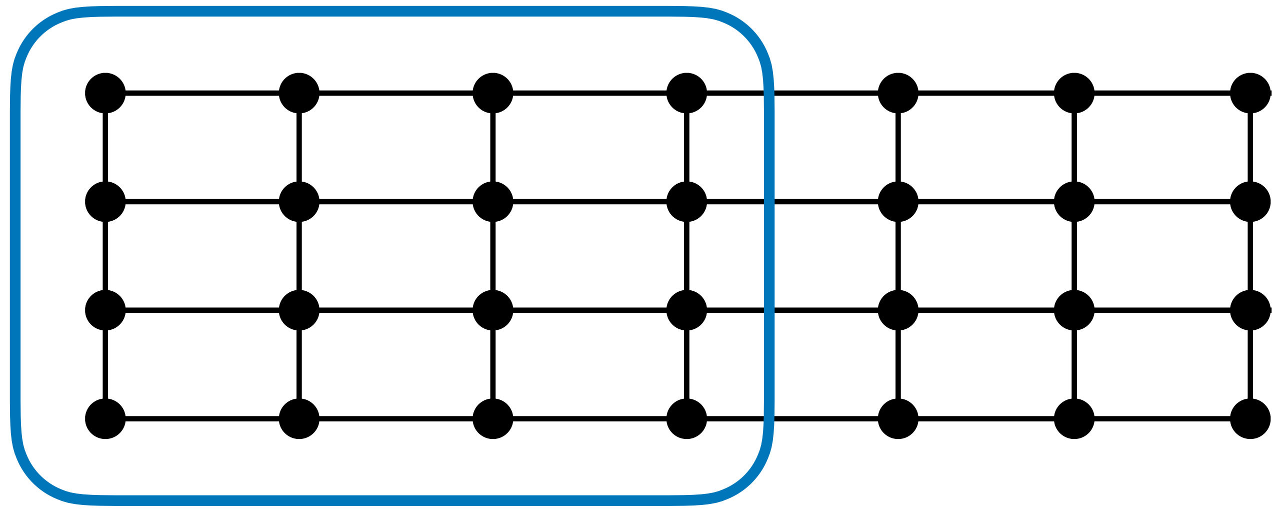
Noiseless average-case separation:
There is an interactive task solved by a **noiseless** QNC^0 circuit on all inputs with certainty. Let $\mathscr{R}$ be a classical probabilistic machine that solves the same task with probability $420/421$ over uniform input. Then $\oplus\mathsf{L} \subseteq (\mathsf{AC}^0)^{\mathscr{R}}$.



Noiseless average-case separation

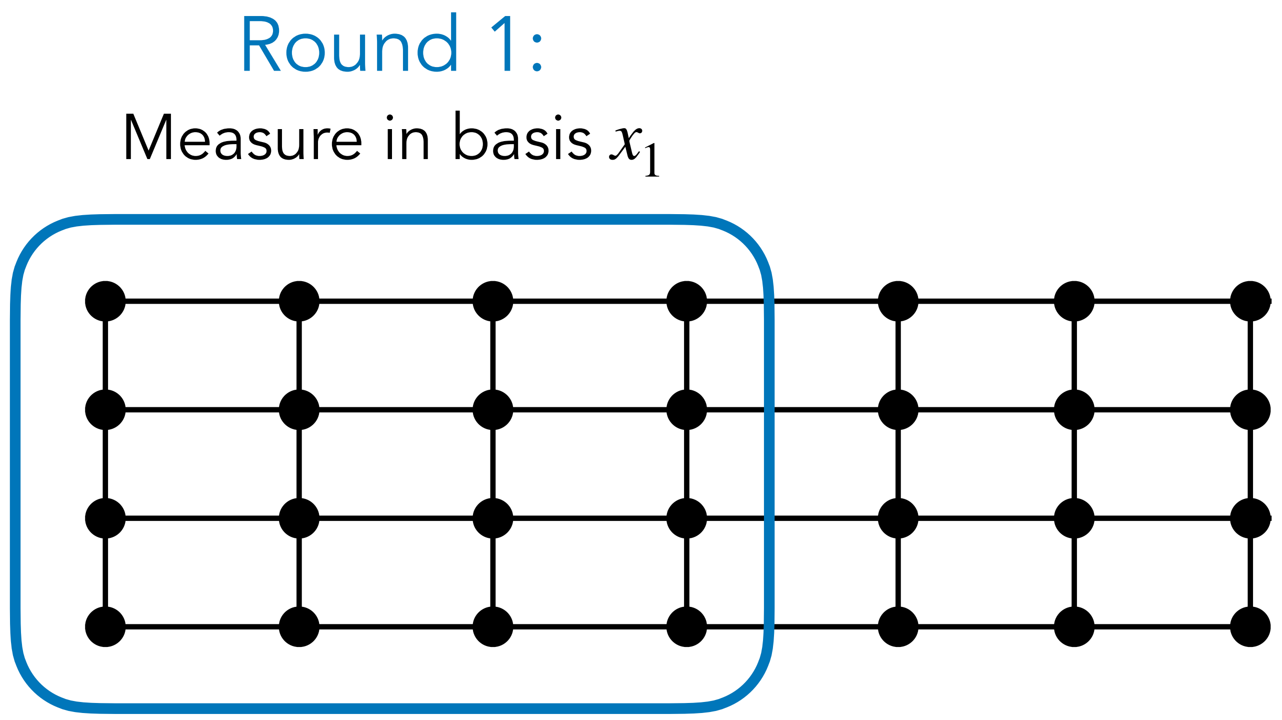
Noiseless average-case separation:
There is an interactive task solved by a **noiseless** QNC^0 circuit on all inputs with certainty. Let $\mathscr{R}$ be a classical probabilistic machine that solves the same task with probability $420/421$ over uniform input. Then $\oplus\mathsf{L} \subseteq (\mathsf{AC}^0)^{\mathscr{R}}$.

Round 1:



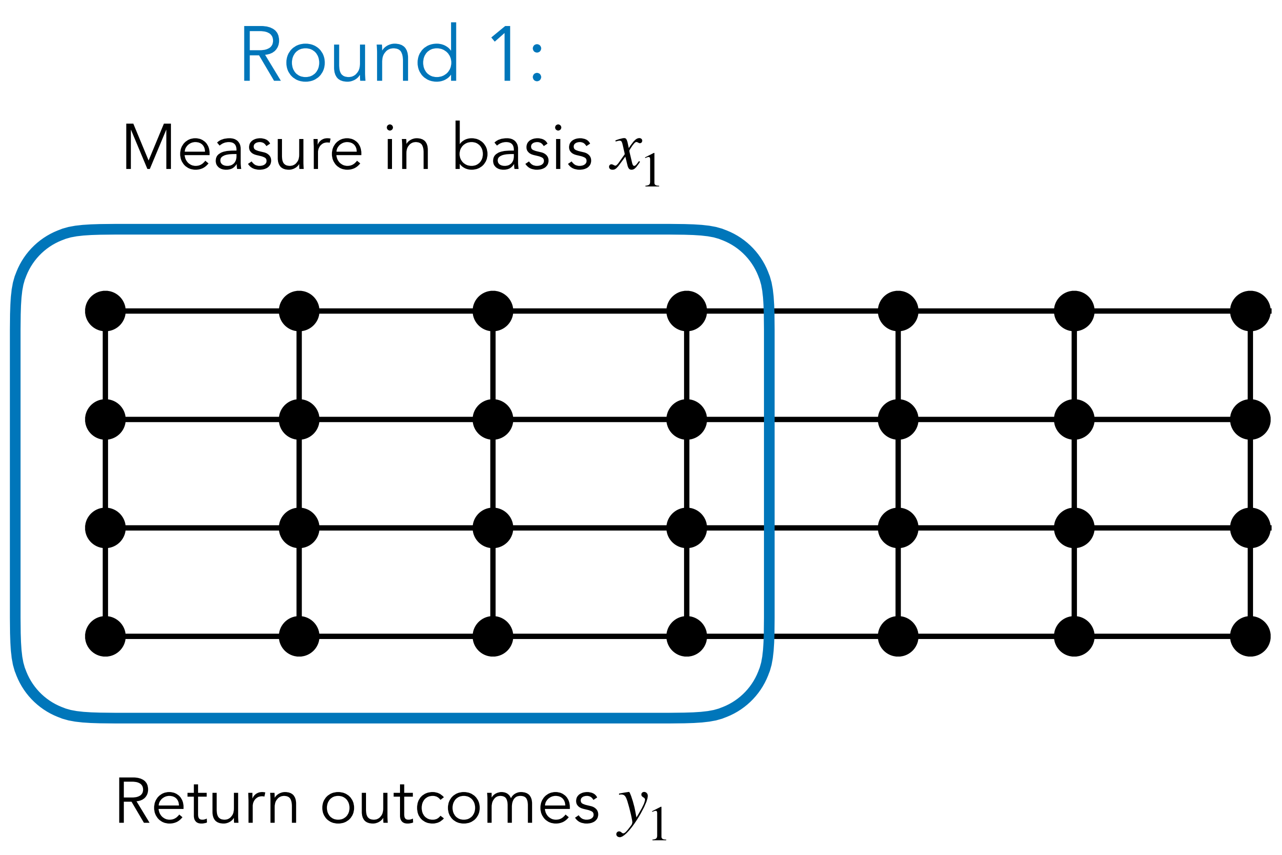
Noiseless average-case separation

Noiseless average-case separation:
There is an interactive task solved by a **noiseless** QNC^0 circuit on all inputs with certainty. Let $\mathscr{R}$ be a classical probabilistic machine that solves the same task with probability $420/421$ over uniform input. Then $\oplus\mathsf{L} \subseteq (\mathsf{AC}^0)^{\mathscr{R}}$.



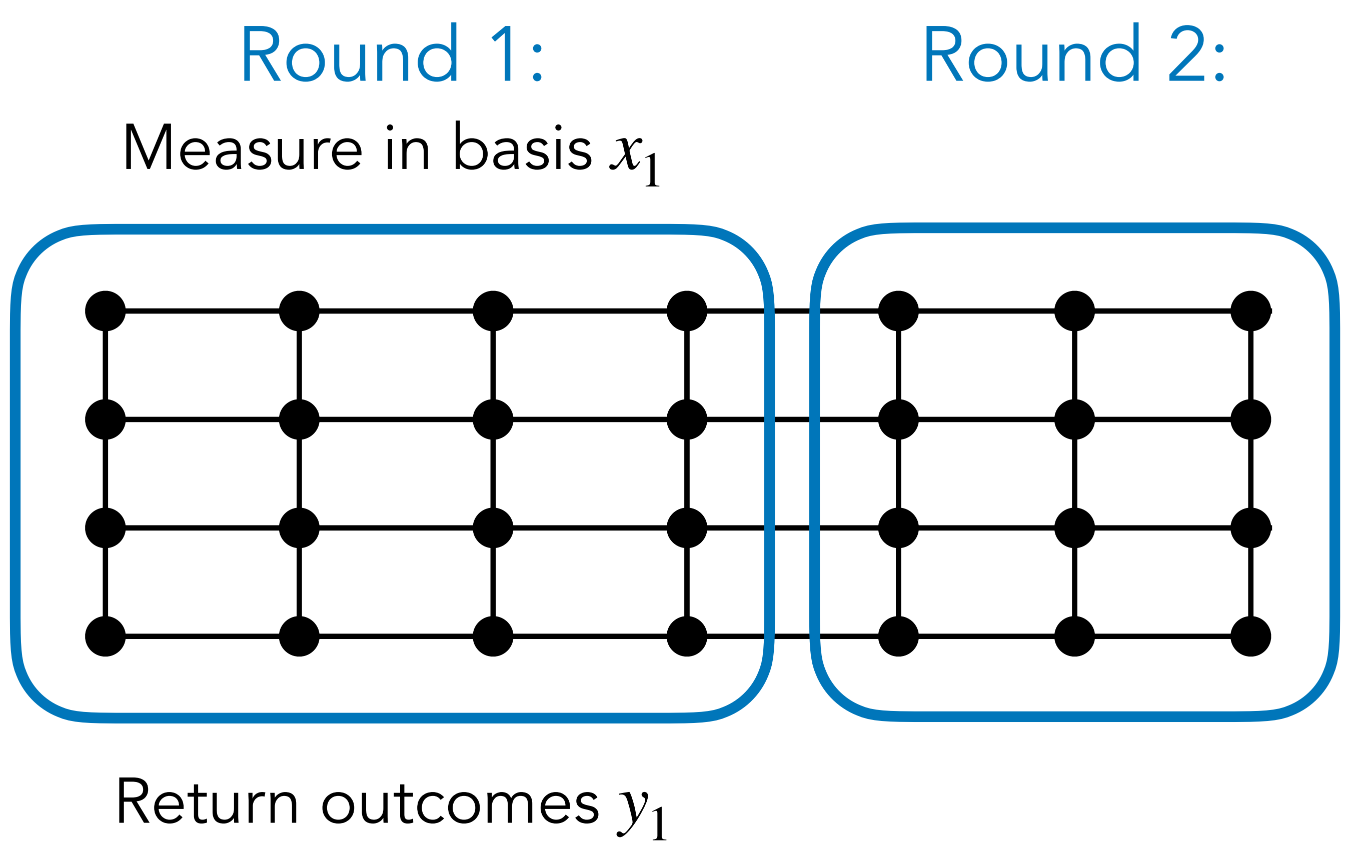
Noiseless average-case separation

Noiseless average-case separation:
There is an interactive task solved by a **noiseless** QNC^0 circuit on all inputs with certainty. Let $\mathscr{R}$ be a classical probabilistic machine that solves the same task with probability $420/421$ over uniform input. Then $\oplus\mathsf{L} \subseteq (\mathsf{AC}^0)^{\mathscr{R}}$.



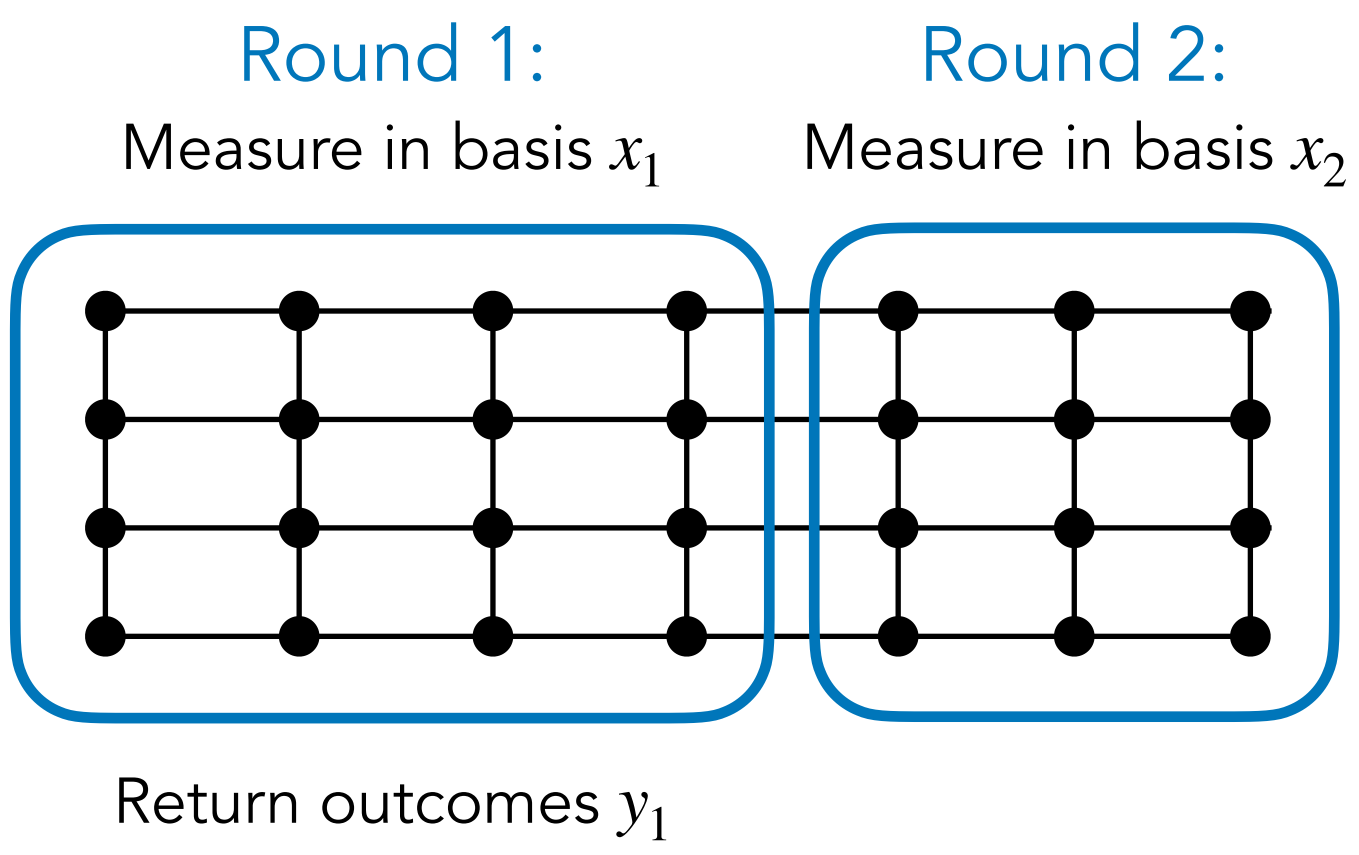
Noiseless average-case separation

Noiseless average-case separation:
There is an interactive task solved by a **noiseless** QNC^0 circuit on all inputs with certainty. Let $\mathscr{R}$ be a classical probabilistic machine that solves the same task with probability $420/421$ over uniform input. Then $\oplus\mathsf{L} \subseteq (\mathsf{AC}^0)^{\mathscr{R}}$.



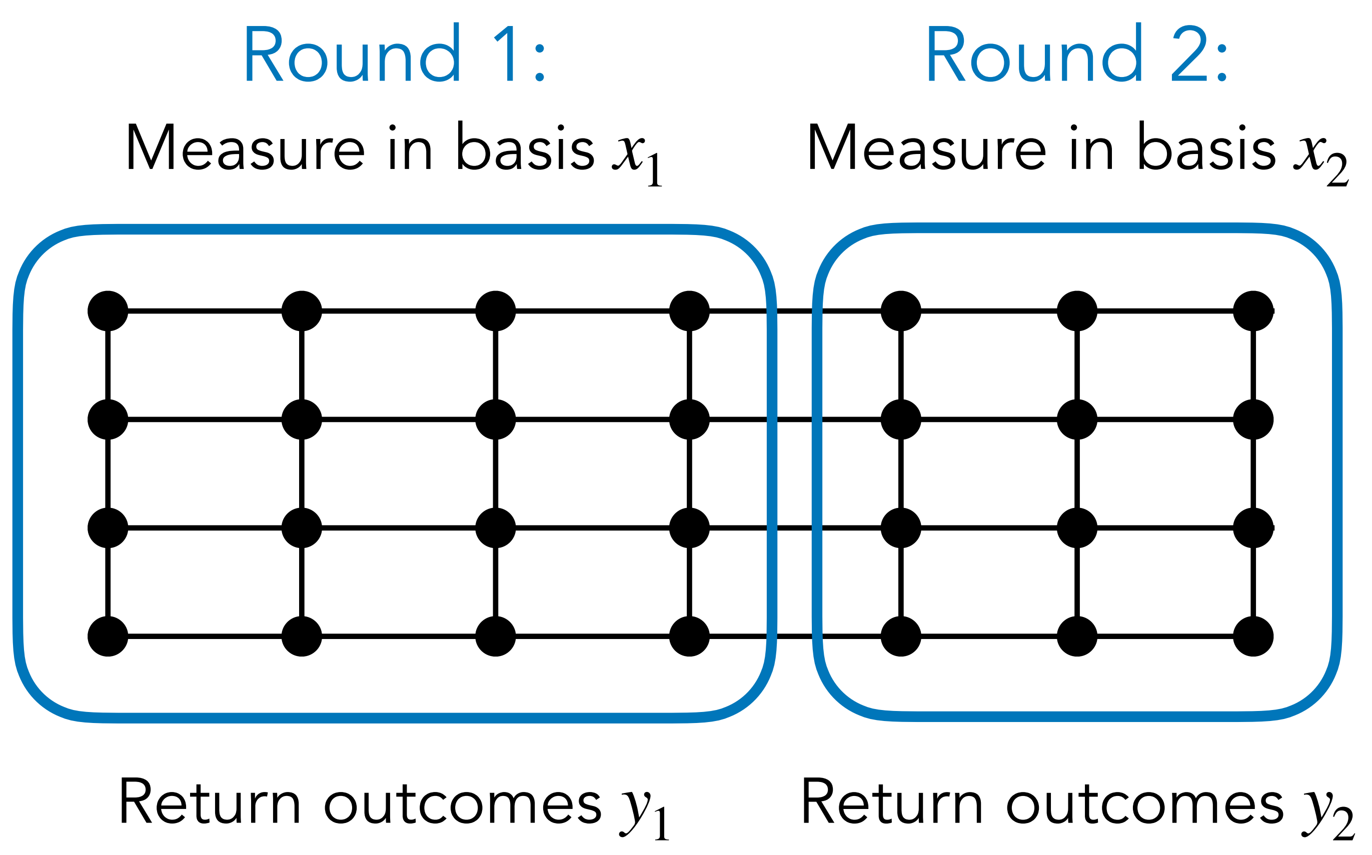
Noiseless average-case separation

Noiseless average-case separation:
There is an interactive task solved by a **noiseless** QNC^0 circuit on all inputs with certainty. Let $\mathscr{R}$ be a classical probabilistic machine that solves the same task with probability $420/421$ over uniform input. Then $\oplus\mathsf{L} \subseteq (\mathsf{AC}^0)^{\mathscr{R}}$.



Noiseless average-case separation

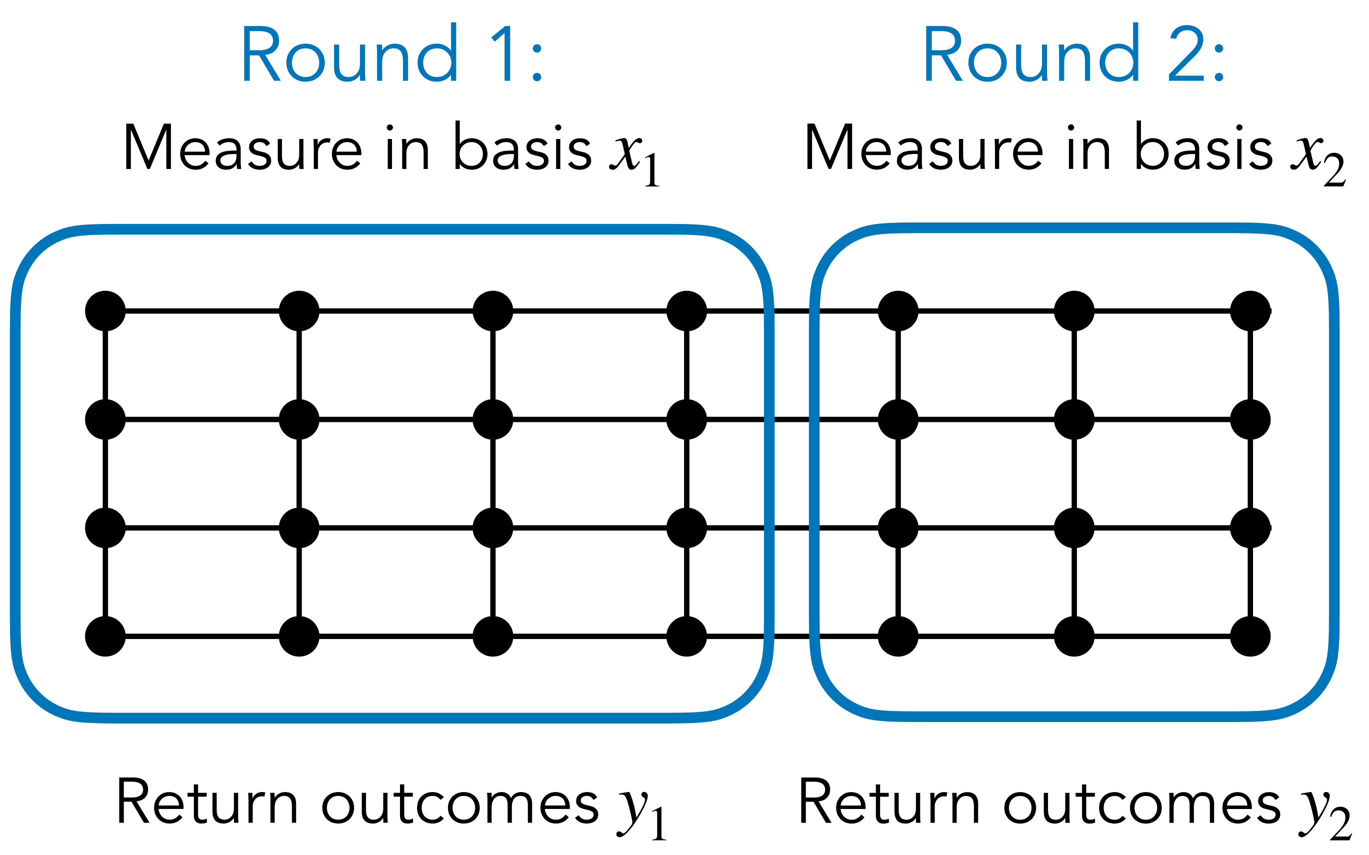
Noiseless average-case separation:
There is an interactive task solved by a **noiseless** QNC^0 circuit on all inputs with certainty. Let $\mathscr{R}$ be a classical probabilistic machine that solves the same task with probability $420/421$ over uniform input. Then $\oplus\mathrm{L} \subseteq (\mathrm{AC}^0)^{\mathscr{R}}$.



Noiseless average-case separation

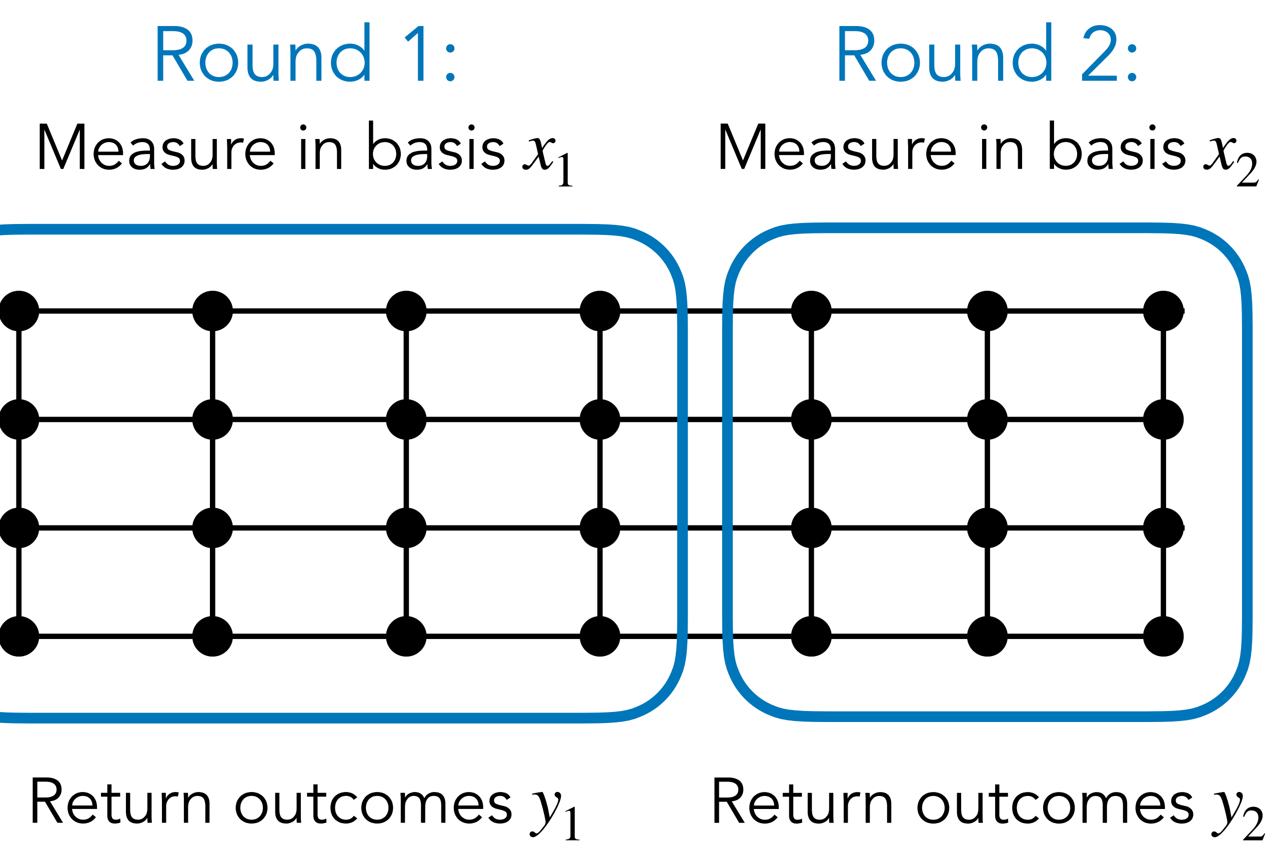
Noiseless average-case separation:
There is an interactive task solved by a **noiseless** QNC^0 circuit on all inputs with certainty. Let $\mathscr{R}$ be a classical probabilistic machine that solves the same task with probability $420/421$ over uniform input. Then $\oplus\mathsf{L} \subseteq (\mathsf{AC}^0)^{\mathscr{R}}$.

promise



Noiseless average-case separation

Noiseless average-case separation:
There is an interactive task solved by a **noiseless** QNC^0 circuit on all inputs with certainty. Let $\mathscr{R}$ be a classical probabilistic machine that solves the same task with probability $420/421$ over uniform input. Then $\oplus\mathsf{L} \subseteq (\mathsf{AC}^0)^{\mathscr{R}}$.

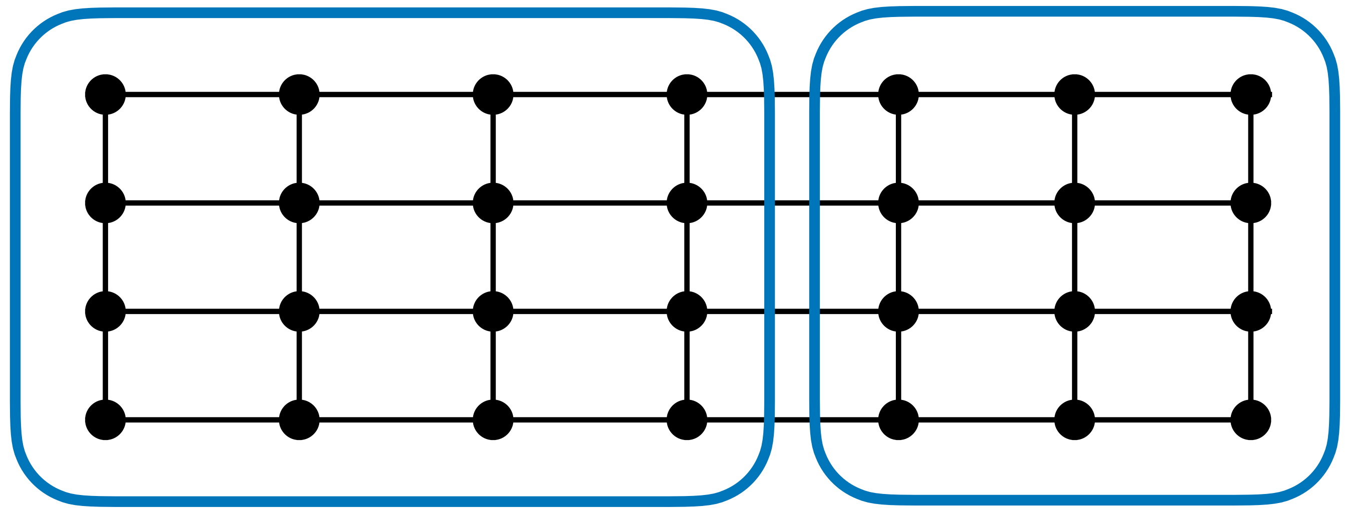


Noiseless average-case separation

Noiseless average-case separation:
There is an interactive task solved by a **noiseless** QNC^0 circuit on all inputs with certainty. Let $\mathscr{R}$ be a classical probabilistic machine that solves the same task with probability $420/421$ over uniform input. Then $\oplus\mathrm{L} \subseteq (\mathrm{AC}^0)^{\mathscr{R}}$.

Round 1:
Measure in basis x_1

Round 2:
Measure in basis x_2



Return outcomes y_1

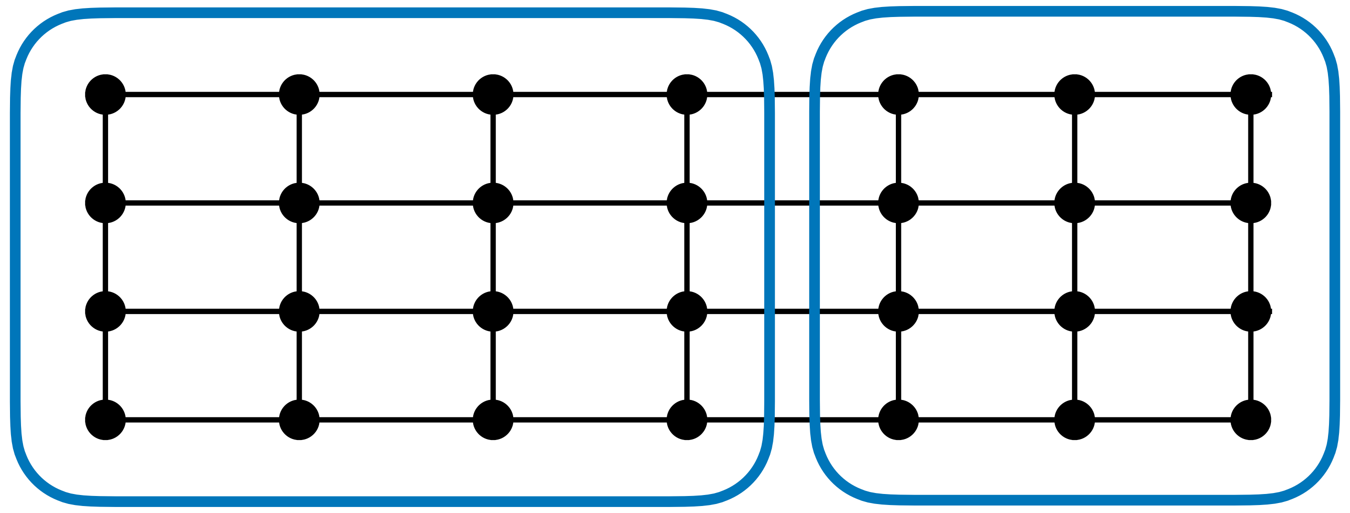
Return outcomes y_2

It is **average-case** $\oplus$L-hard to return valid Pauli measurement outcomes of a grid state*.

* = For an interactive promise problem

Noiseless average-case separation

Noiseless average-case separation:
There is an interactive task solved by a **noiseless** QNC^0 circuit on all inputs with certainty. Let $\mathscr{R}$ be a classical probabilistic machine that solves the same task with probability $420/421$ over uniform input. Then $\oplus\mathsf{L} \subseteq (\mathsf{AC}^0)^{\mathscr{R}}$.



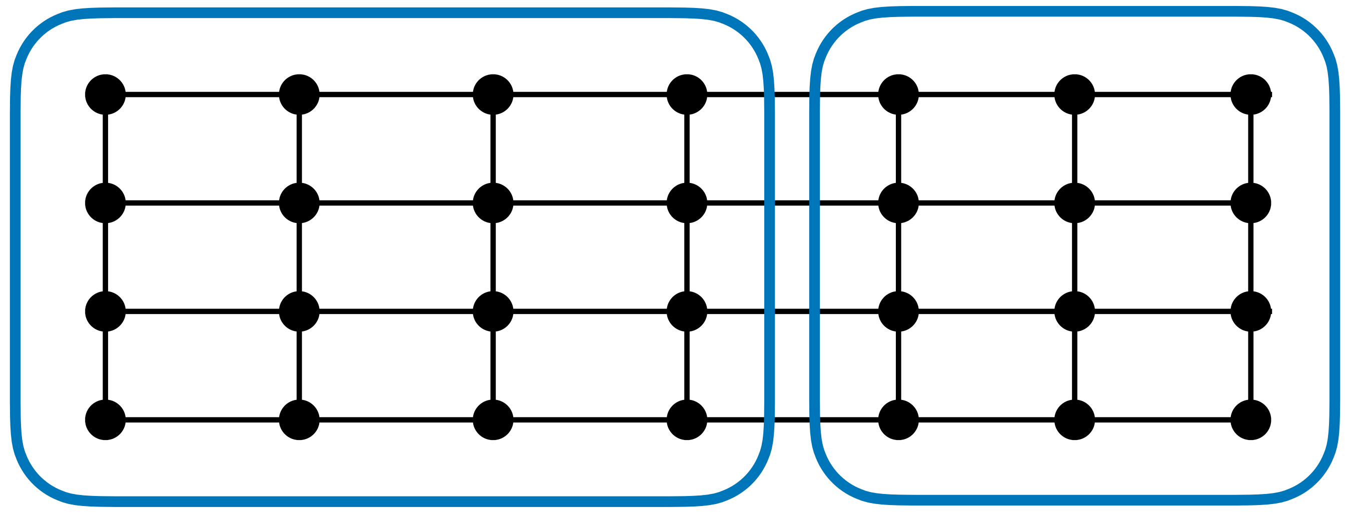
It is **average-case** $\oplus$L-hard to return valid Pauli measurement outcomes of a grid state*.

* = For an interactive promise problem

How to prove average-case $\oplus$L-hardness
for the interactive problem?

Noiseless average-case separation

Noiseless average-case separation:
There is an interactive task solved by a **noiseless** QNC^0 circuit on all inputs with certainty. Let $\mathscr{R}$ be a classical probabilistic machine that solves the same task with probability $420/421$ over uniform input. Then $\oplus\mathsf{L} \subseteq (\mathsf{AC}^0)^{\mathscr{R}}$.

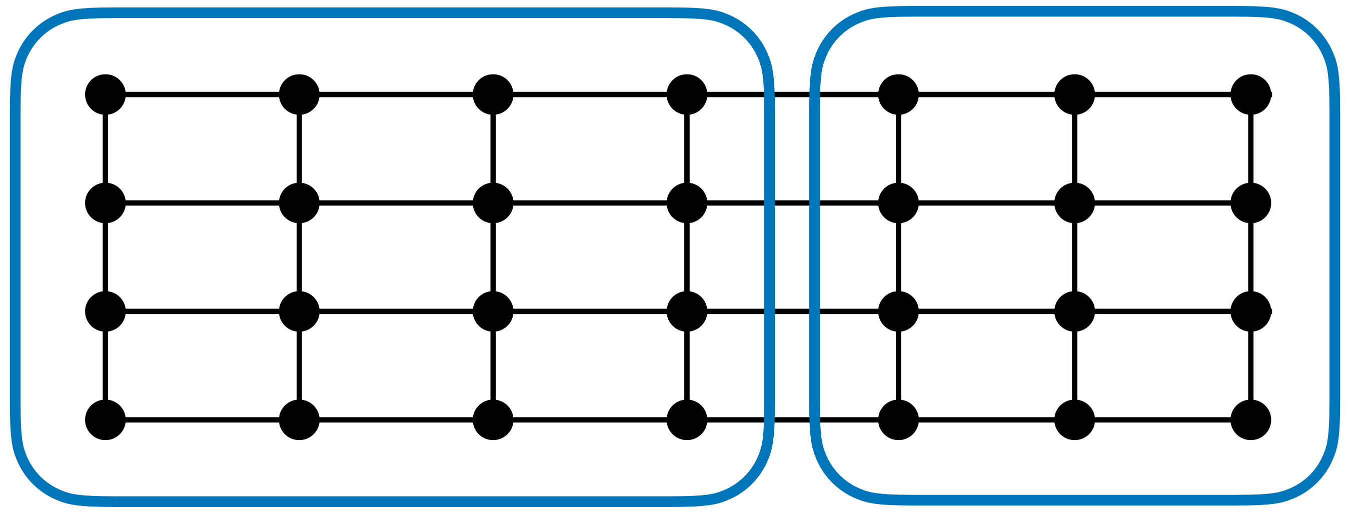


It is **average-case** $\oplus$L-hard to return valid Pauli measurement outcomes of a grid state*.

* = For an interactive promise problem

How to prove average-case $\oplus$L-hardness for the interactive problem?
Construct a worst-to-average-case reduction from a $\oplus$L-hard problem.

Noiseless average-case separation



Noiseless average-case separation:
There is an interactive task solved by a **noiseless** QNC^0 circuit on all inputs with certainty. Let $\mathscr{R}$ be a classical probabilistic machine that solves the same task with probability $420/421$ over uniform input. Then $\oplus\mathsf{L} \subseteq (\mathsf{AC}^0)^{\mathscr{R}}$.

It is **average-case** ⊕L-hard to return valid Pauli measurement outcomes of a grid state*.

* = For an interactive promise problem

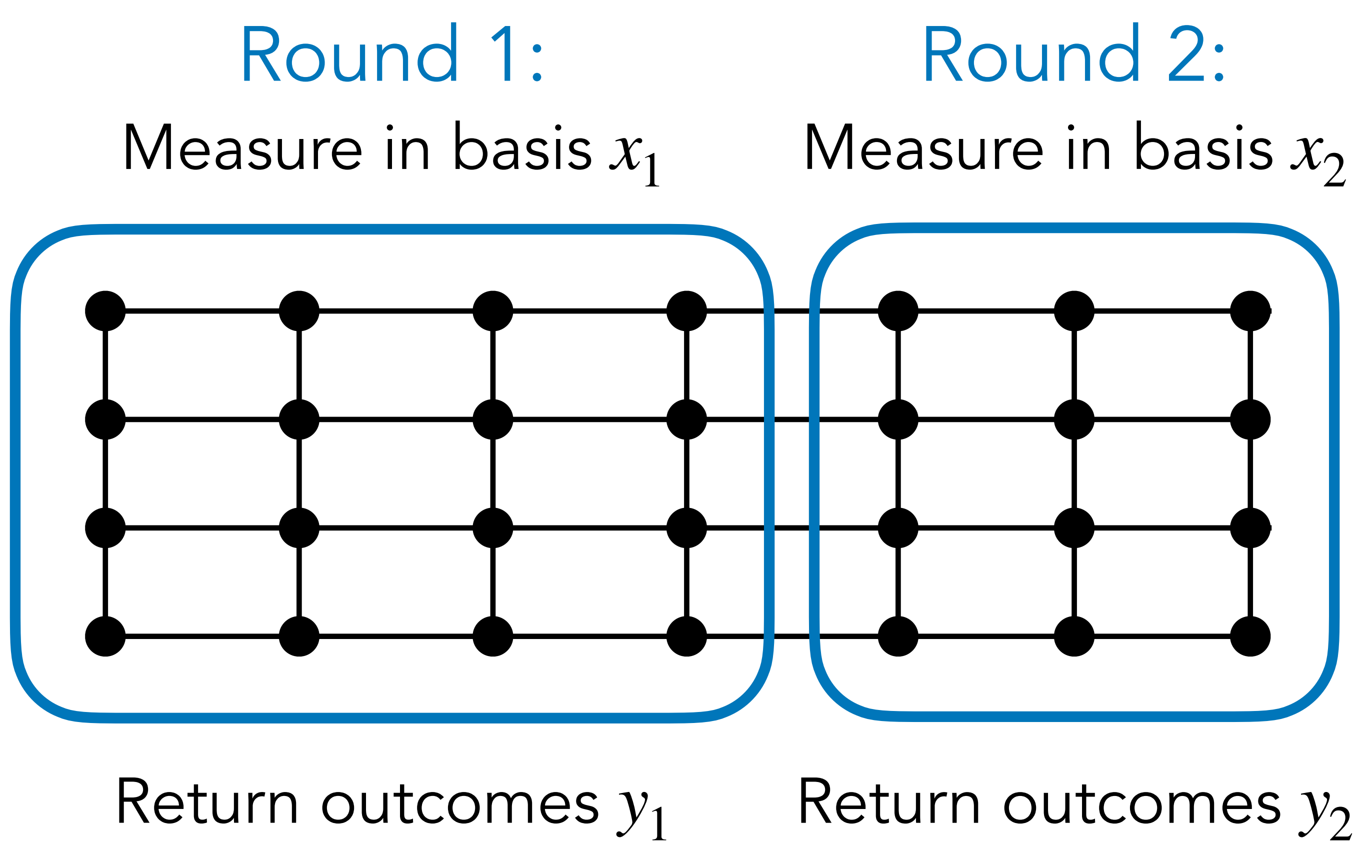
How to prove average-case ⊕L-hardness for the interactive problem?

Construct a worst-to-average-case reduction from a ⊕L-hard problem.

→ Use the ability to classically solve the interactive problem on **random** (average-case) instances to solve a **worst-case** ⊕L-hard problem instance

Noiseless average-case separation

Noiseless average-case separation:
There is an interactive task solved by a **noiseless** QNC^0 circuit on all inputs with certainty. Let $\mathscr{R}$ be a classical probabilistic machine that solves the same task with probability $420/421$ over uniform input. Then $\oplus\mathrm{L} \subseteq (\mathrm{AC}^0)^{\mathscr{R}}$.



It is **average-case** $\oplus$L-hard to return valid Pauli measurement outcomes of a grid state*.

* = For an interactive promise problem

How to prove average-case $\oplus$L-hardness for the interactive problem?

Construct a worst-to-average-case reduction from a $\oplus$L-hard problem.

(different from [BGKT], who prove average-case hardness using nonlocal games instead)

→ Use the ability to classically solve the interactive problem on **random** (average-case) instances to solve a **worst-case** $\oplus$L-hard problem instance

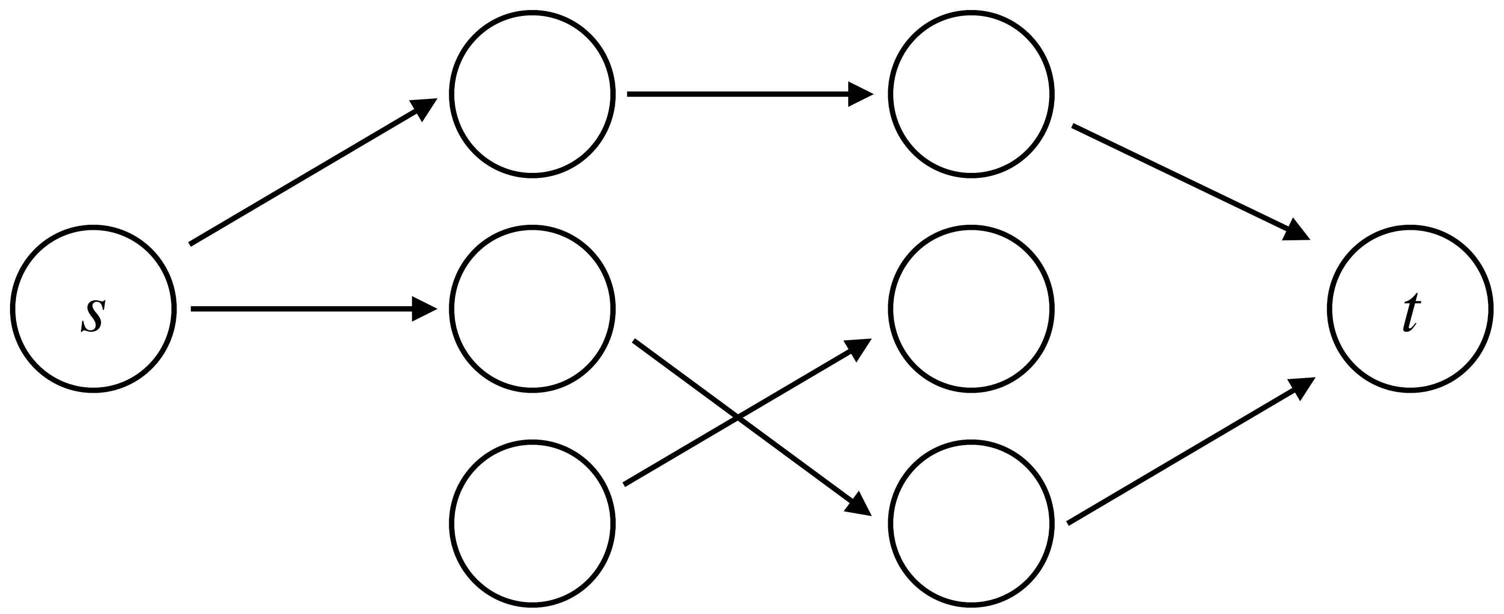
Worst-case $\oplus$L-hard problems

It is $\oplus$L-hard to determine the parity of the number of $s \to t$ paths in a (layered) DAG.

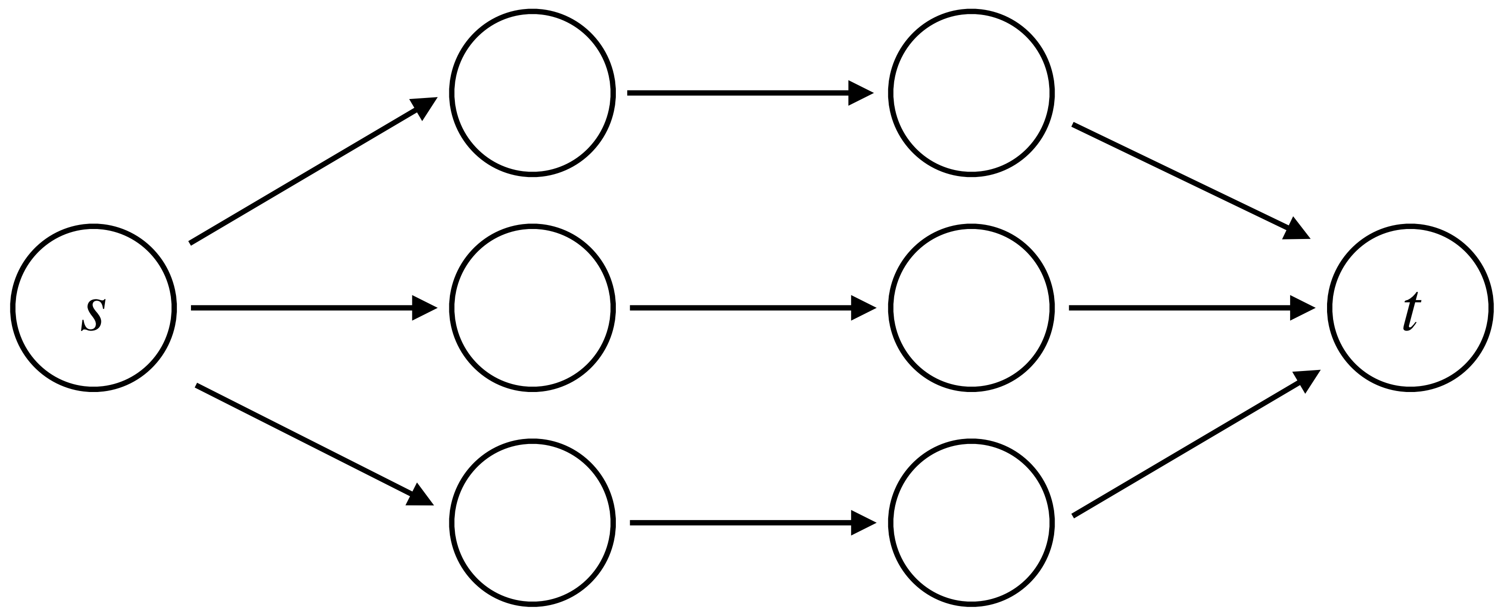
Worst-case ⊕L-hard problems

It is ⊕L-hard to determine the parity of the number of $s \to t$ paths in a (layered) DAG.

Even parity



Odd parity

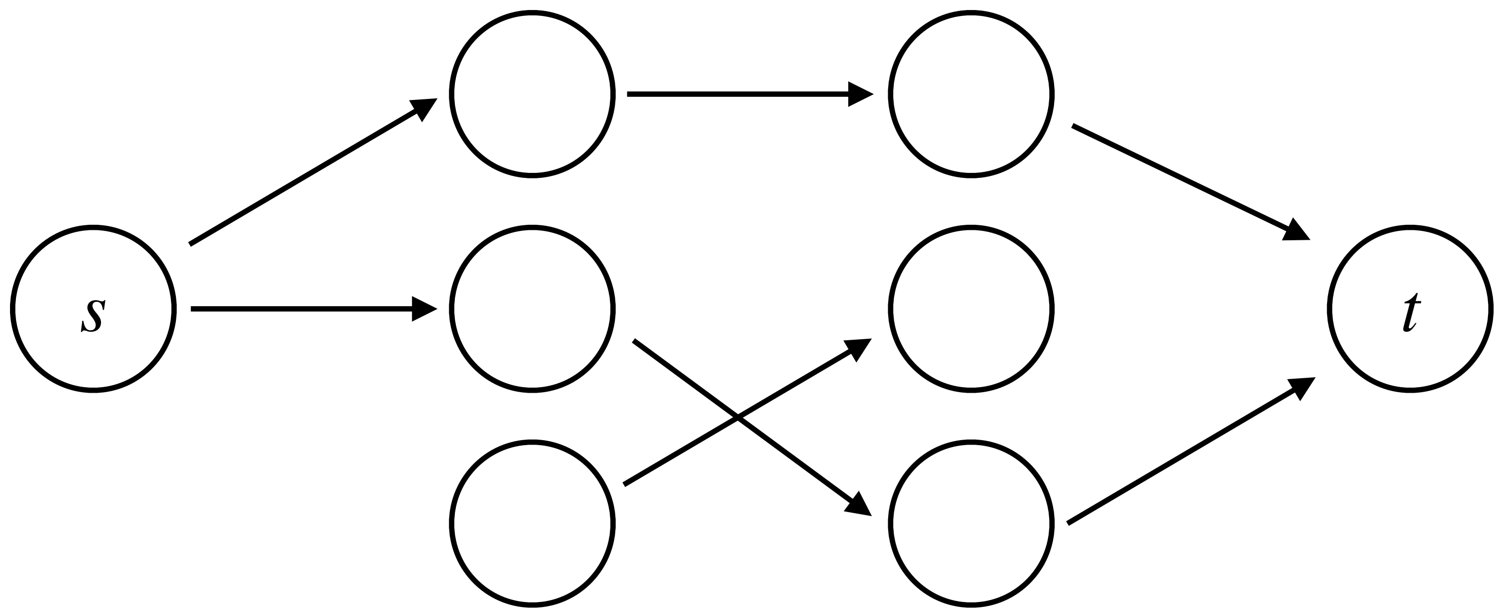


Worst-case $\oplus$L-hard problems

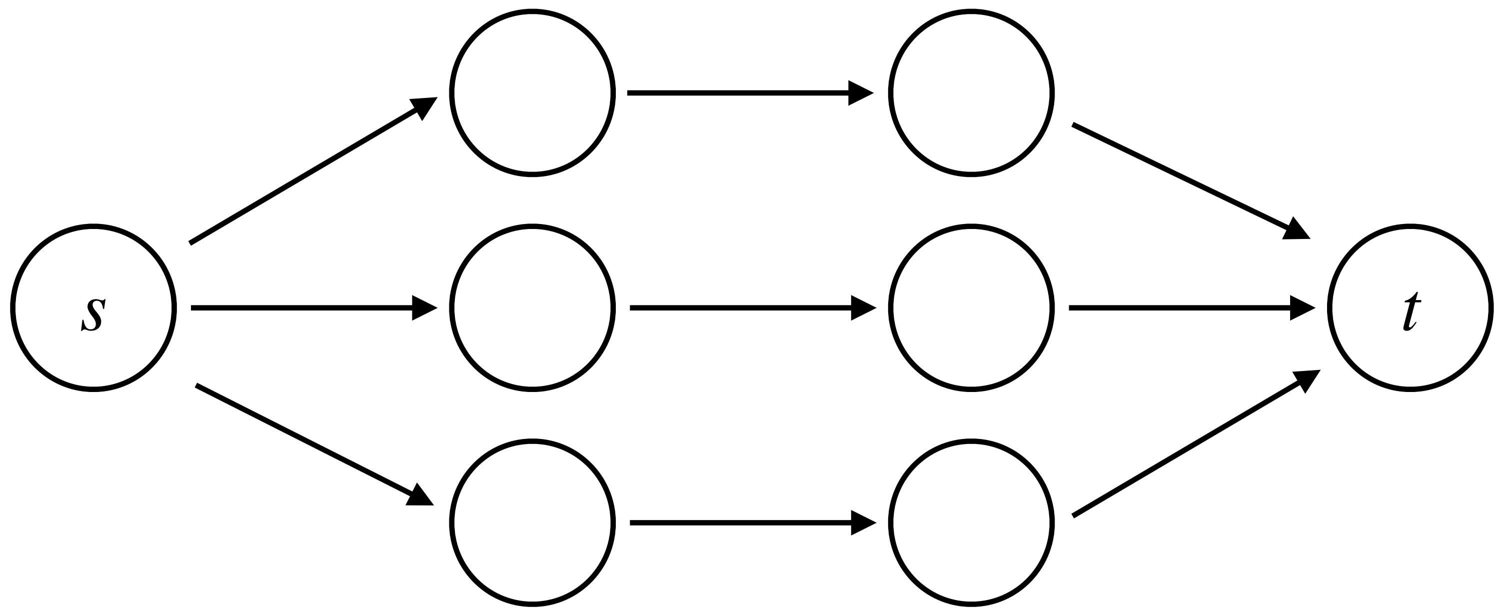
It is $\oplus$L-hard to determine the parity of the number of $s \to t$ paths in a (layered) DAG.

[GS20]: It is also $\oplus$L-hard to determine whether CNOT gates $g_1, \ldots, g_n$ multiply to 3-cycle or identity.

Even parity



Odd parity

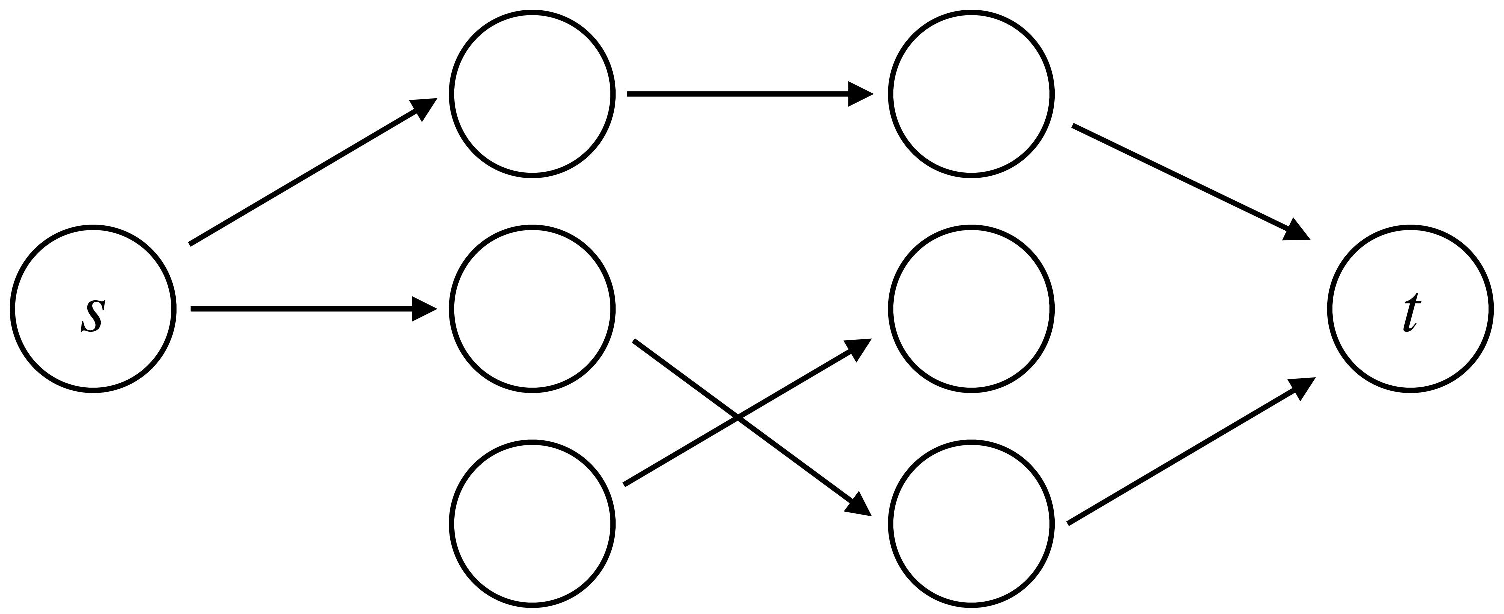


Worst-case $\oplus$L-hard problems

It is $\oplus$L-hard to determine the parity of the number of $s \to t$ paths in a (layered) DAG.

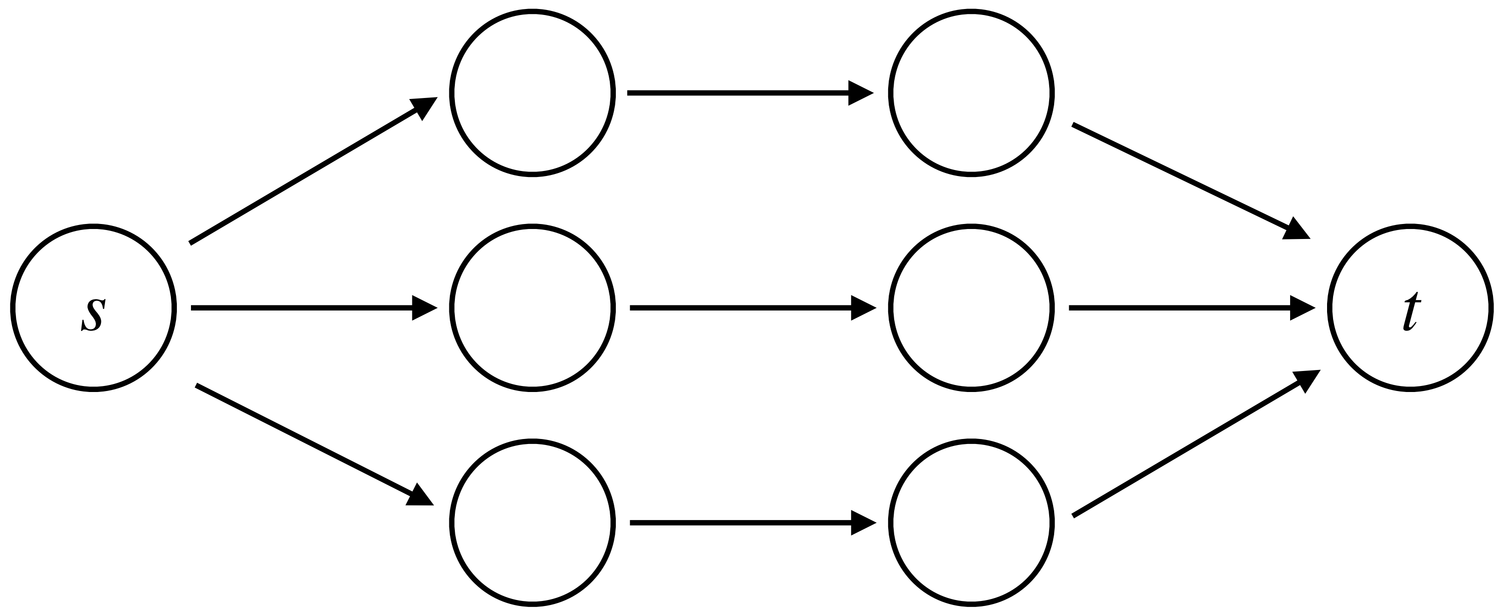
[GS20]: It is also $\oplus$L-hard to determine whether CNOT gates $g_1, \ldots, g_n$ multiply to 3-cycle or identity.

Even parity



$$\Longrightarrow \quad g_1 g_2 \ldots g_n = I$$

Odd parity

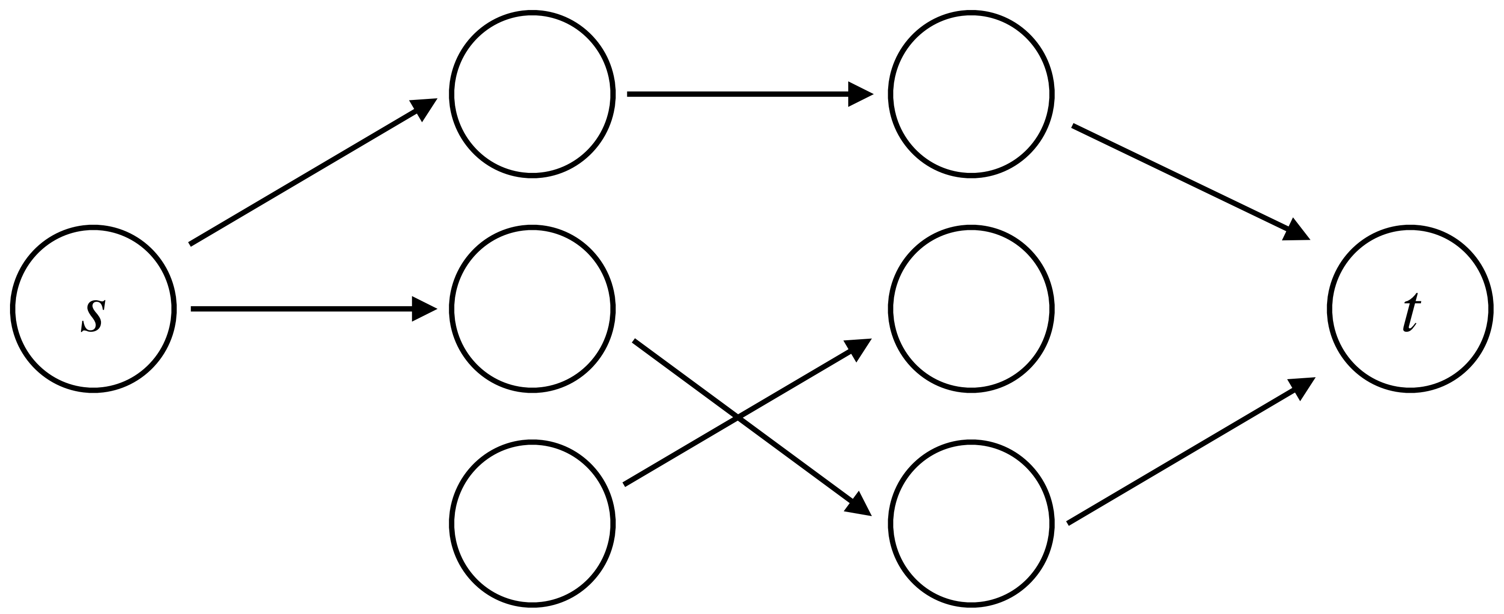


Worst-case ⊕L-hard problems

It is ⊕L-hard to determine the parity of the number of $s \to t$ paths in a (layered) DAG.

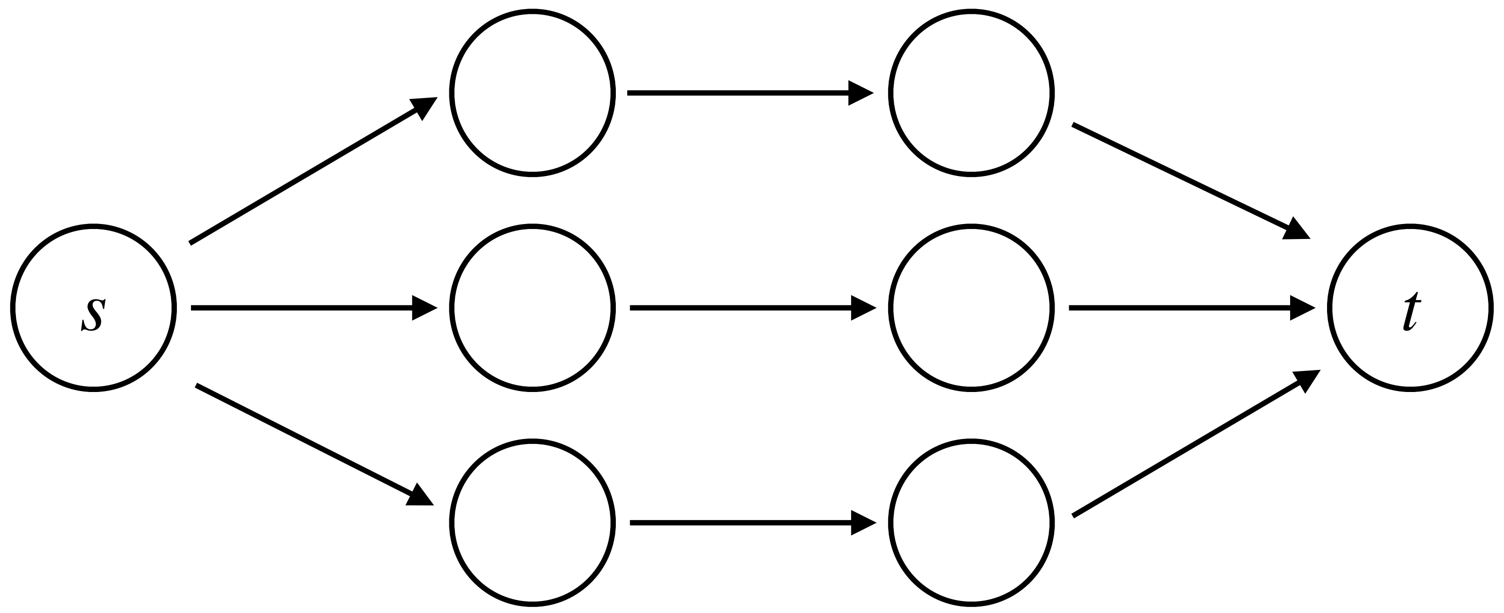
[GS20]: It is also ⊕L-hard to determine whether CNOT gates $g_1, \ldots, g_n$ multiply to 3-cycle or identity.

Even parity



$$\implies \quad g_1 g_2 \cdots g_n = I$$

Odd parity



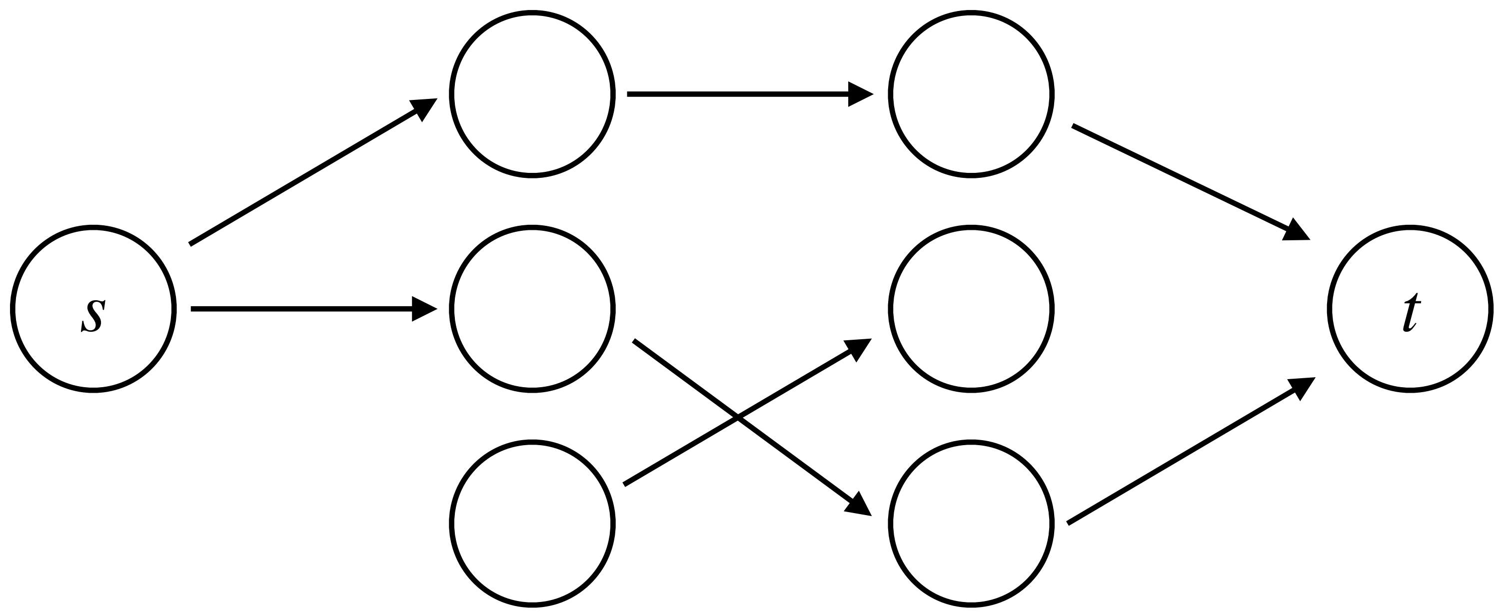
$$\implies \quad g_1 g_2 \cdots g_n = C_3$$

Worst-case $\oplus$L-hard problems

It is $\oplus$L-hard to determine the parity of the number of $s \to t$ paths in a (layered) DAG.

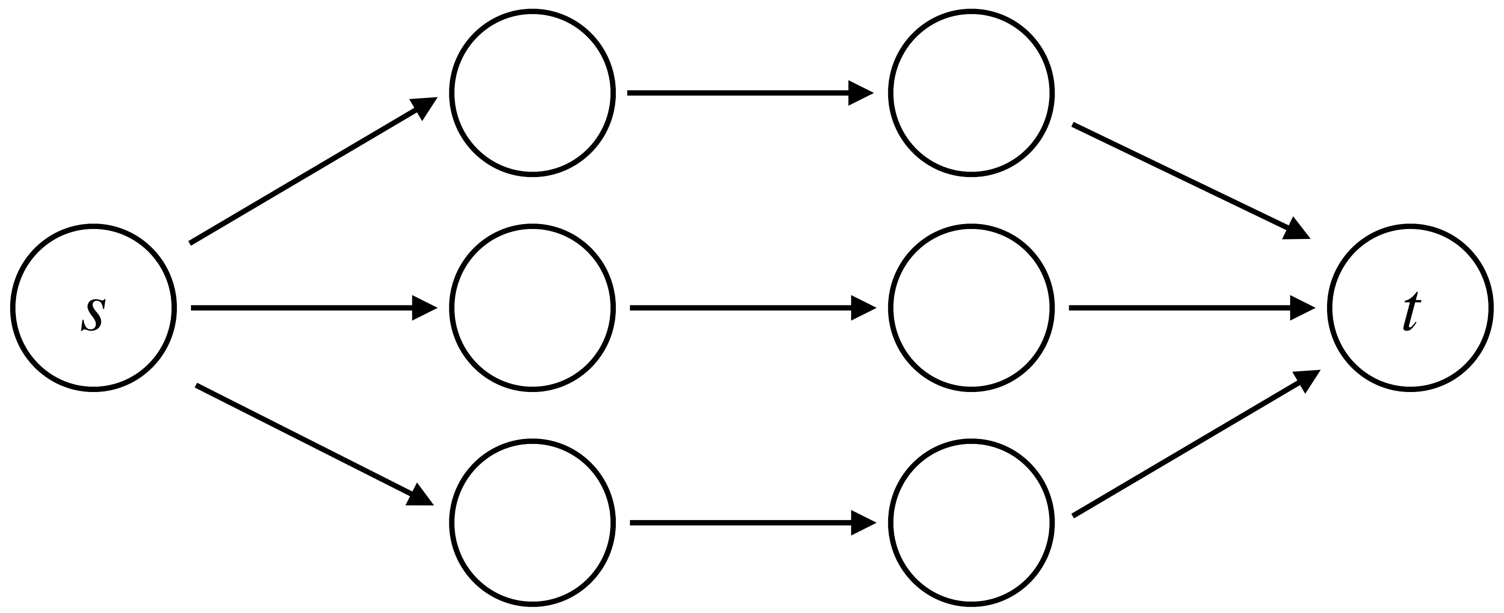
[GS20]: It is also $\oplus$L-hard to determine whether CNOT gates $g_1, \ldots, g_n$ multiply to 3-cycle or identity.

Even parity



$\implies$ $g_1 g_2 \ldots g_n = I$

Odd parity



$\implies$ $g_1 g_2 \ldots g_n = C_3$

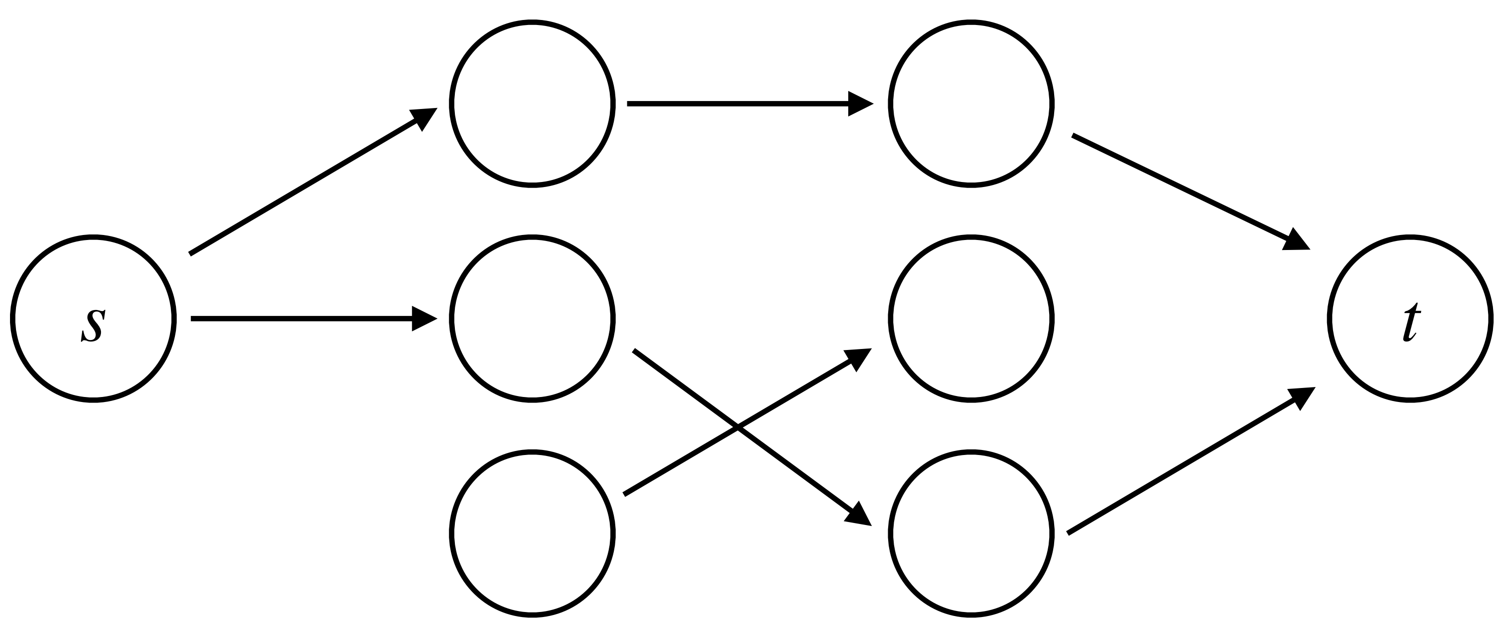
[GS20]: Measurement results from grid state determine whether $g_1 \ldots g_n = I$ or C_3.

Worst-case $\oplus$L-hard problems

It is $\oplus$L-hard to determine the parity of the number of $s \to t$ paths in a (layered) DAG.

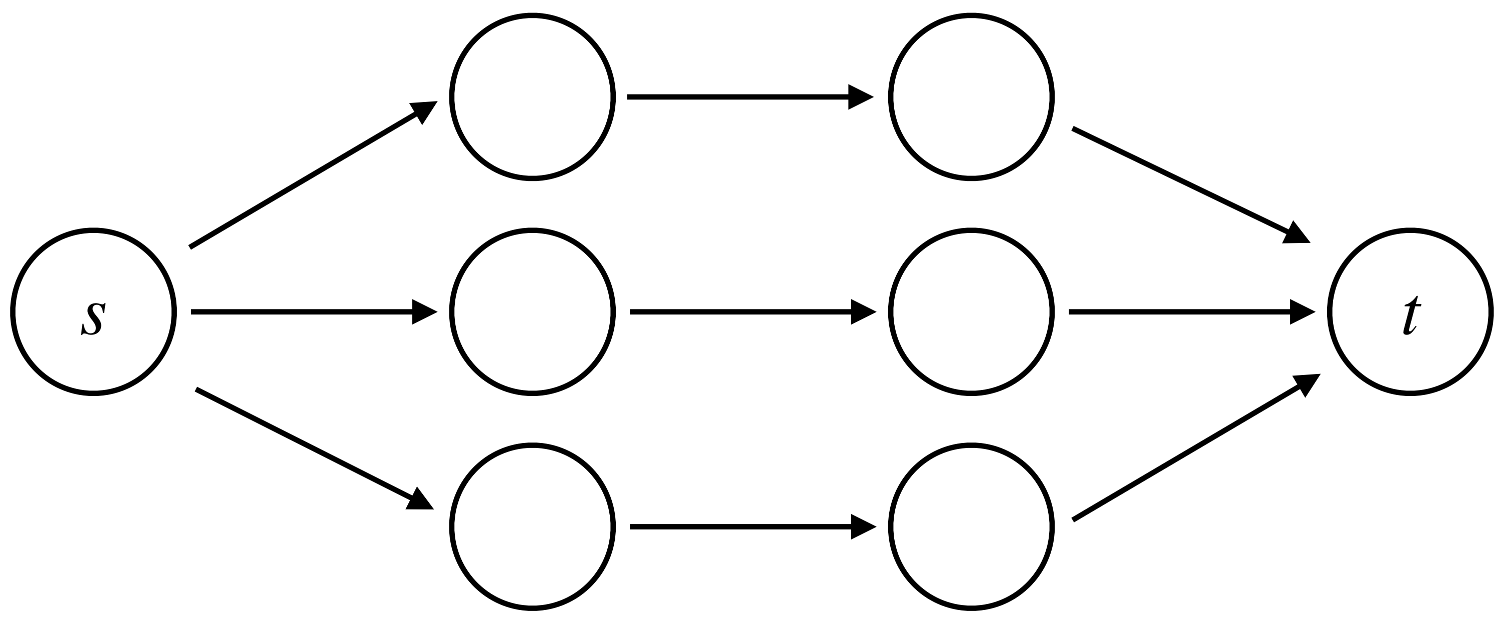
[GS20]: It is also $\oplus$L-hard to determine whether CNOT gates $g_1, \ldots, g_n$ multiply to 3-cycle or identity.

Even parity



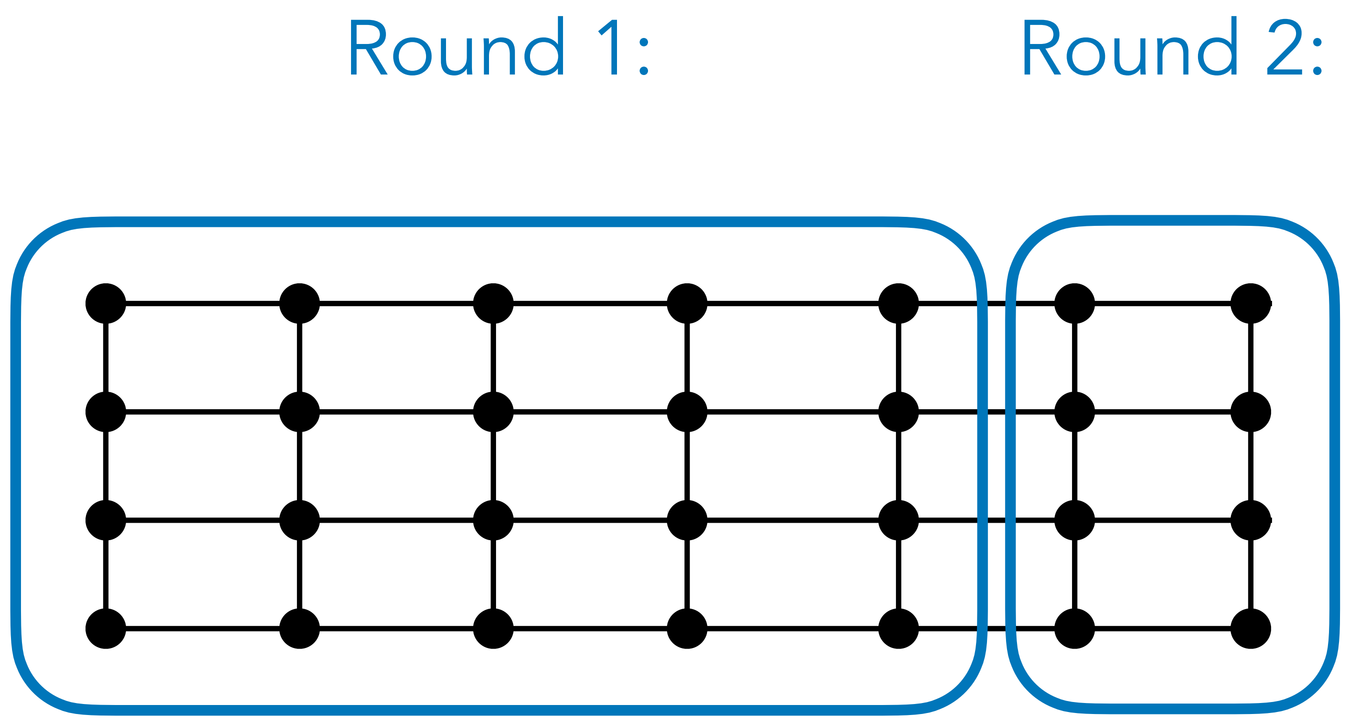
$\Longrightarrow \quad g_1 g_2 \cdots g_n = I$

Odd parity



$\Longrightarrow \quad g_1 g_2 \cdots g_n = C_3$

[GS20]: Measurement results from grid state determine whether $g_1 \ldots g_n = I$ or C_3.

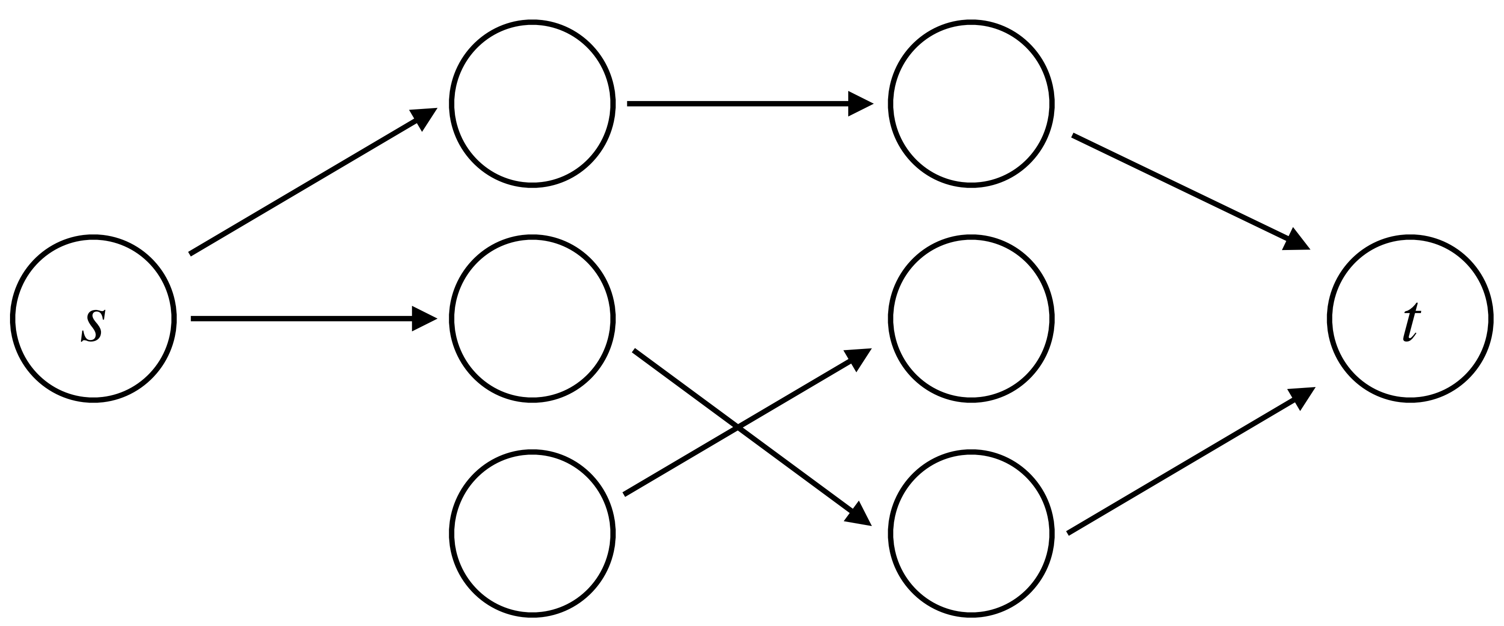


Worst-case ⊕L-hard problems

It is ⊕L-hard to determine the parity of the number of $s \to t$ paths in a (layered) DAG.

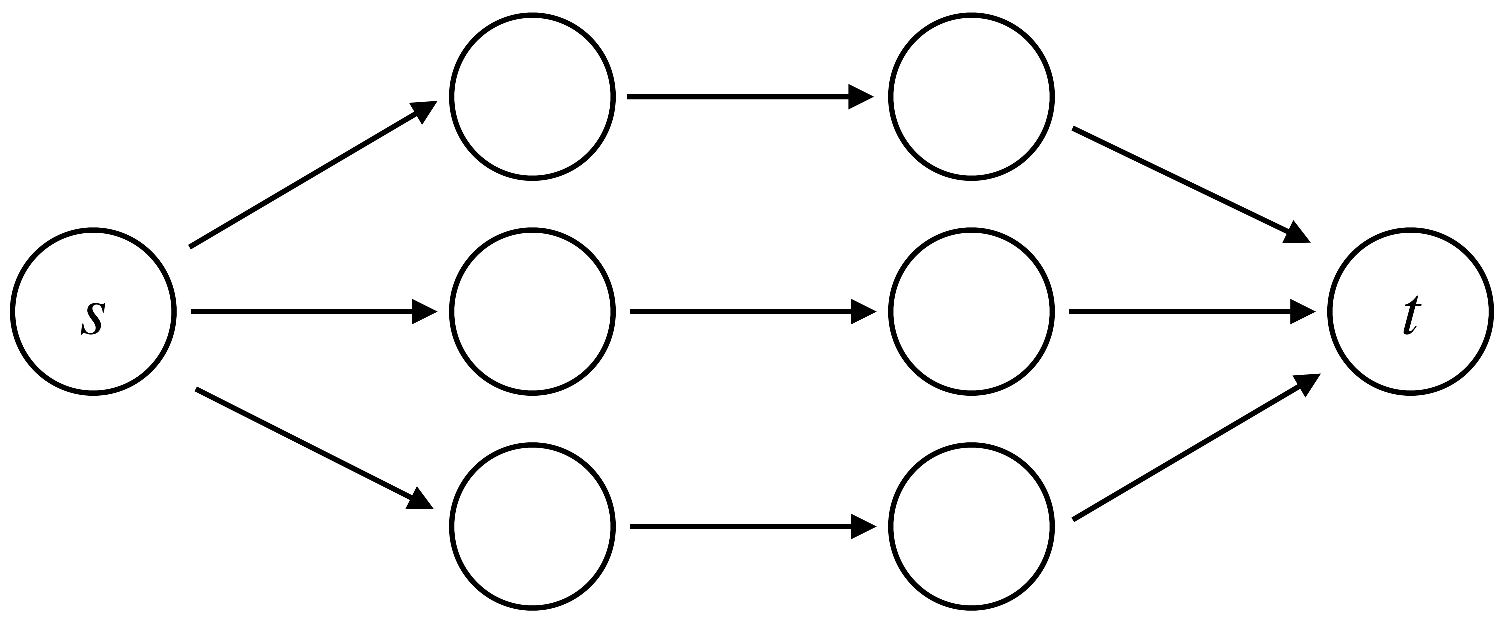
[GS20]: It is also ⊕L-hard to determine whether CNOT gates $g_1, \ldots, g_n$ multiply to 3-cycle or identity.

Even parity



$\Longrightarrow \quad g_1 g_2 \cdots g_n = I$

Odd parity

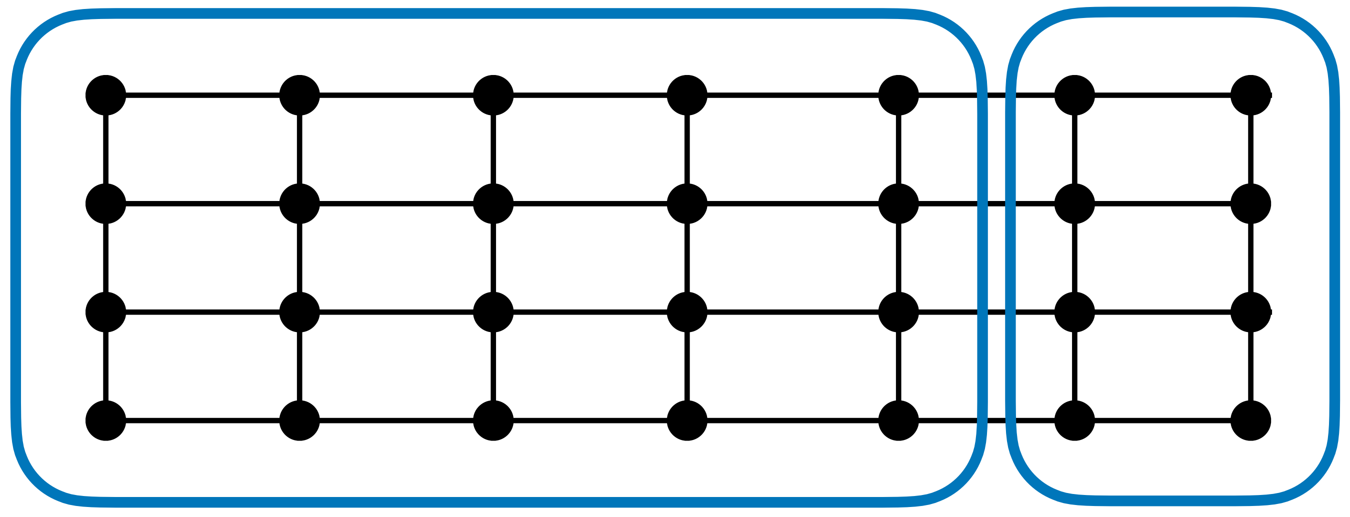


$\Longrightarrow \quad g_1 g_2 \cdots g_n = C_3$

[GS20]: Measurement results from grid state determine whether $g_1 \ldots g_n = I$ or C_3.

Sample $(P_1, \ldots, P_m) \leftarrow \gamma(g_1, \ldots, g_n)$

Round 1: Round 2:

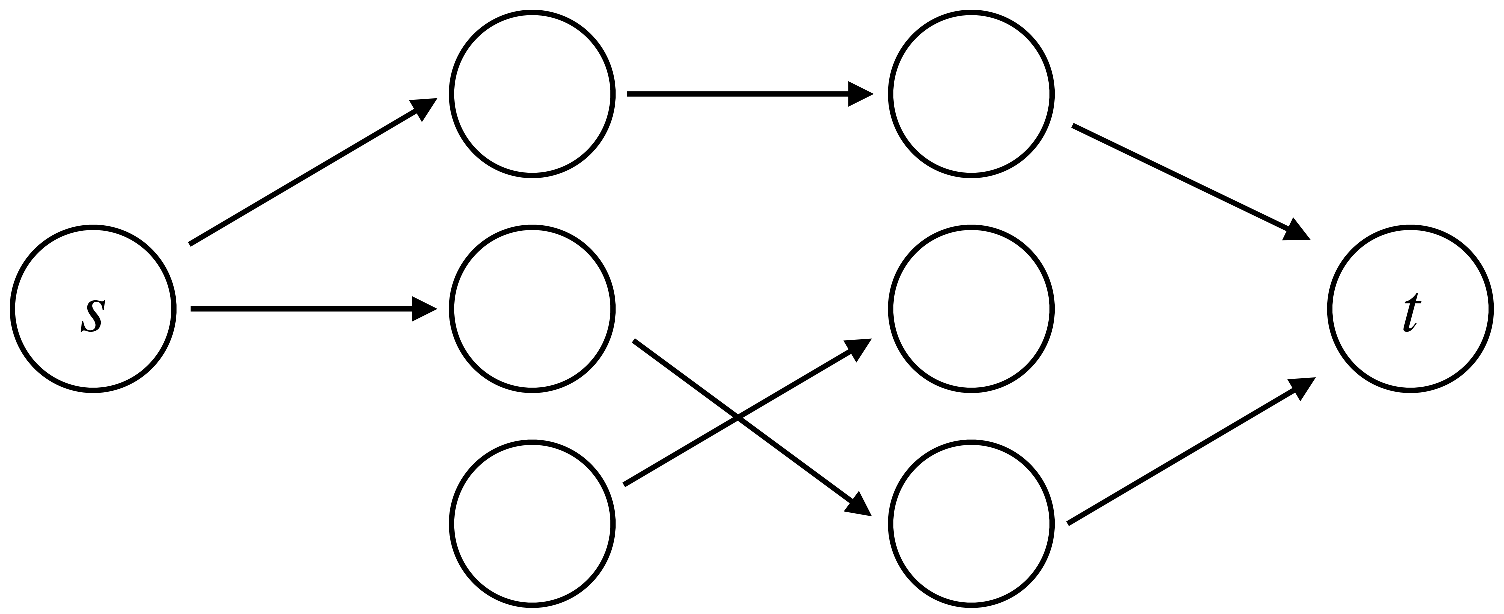


Worst-case ⊕L-hard problems

It is ⊕L-hard to determine the parity of the number of $s \to t$ paths in a (layered) DAG.

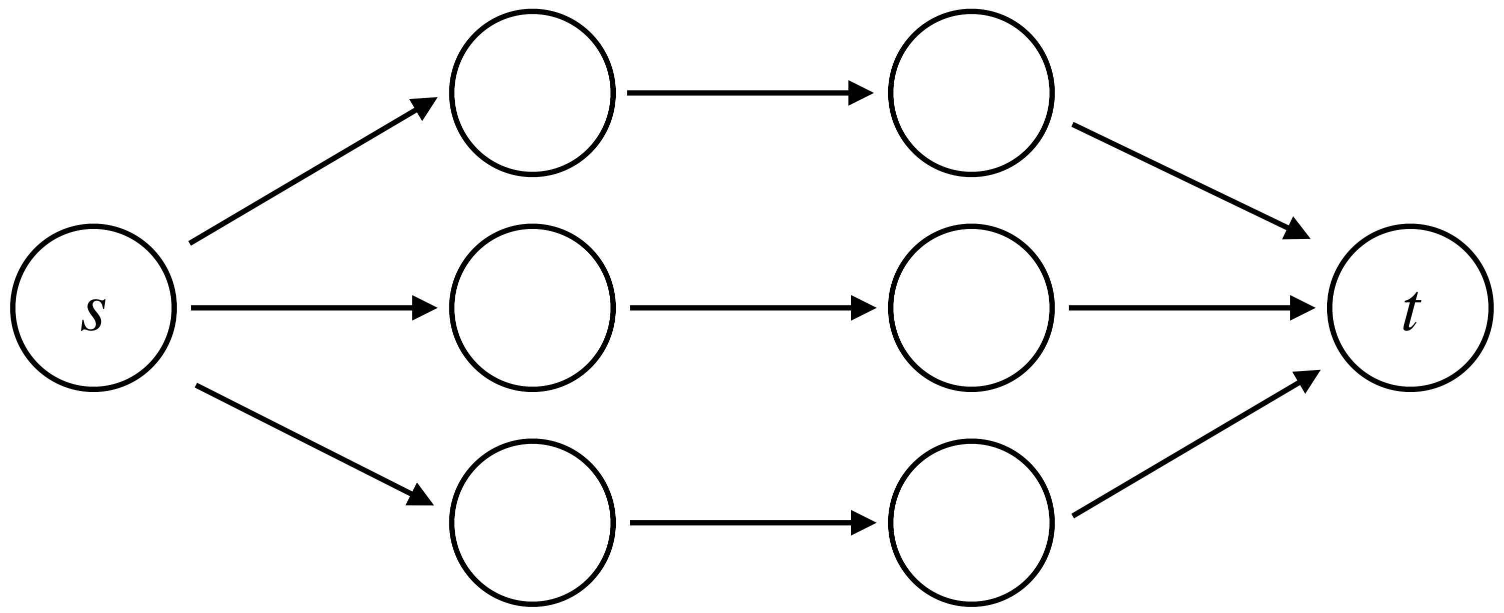
[GS20]: It is also ⊕L-hard to determine whether CNOT gates $g_1, \ldots, g_n$ multiply to 3-cycle or identity.

Even parity



$\Longrightarrow \quad g_1 g_2 \ldots g_n = I$

Odd parity



$\Longrightarrow \quad g_1 g_2 \ldots g_n = C_3$

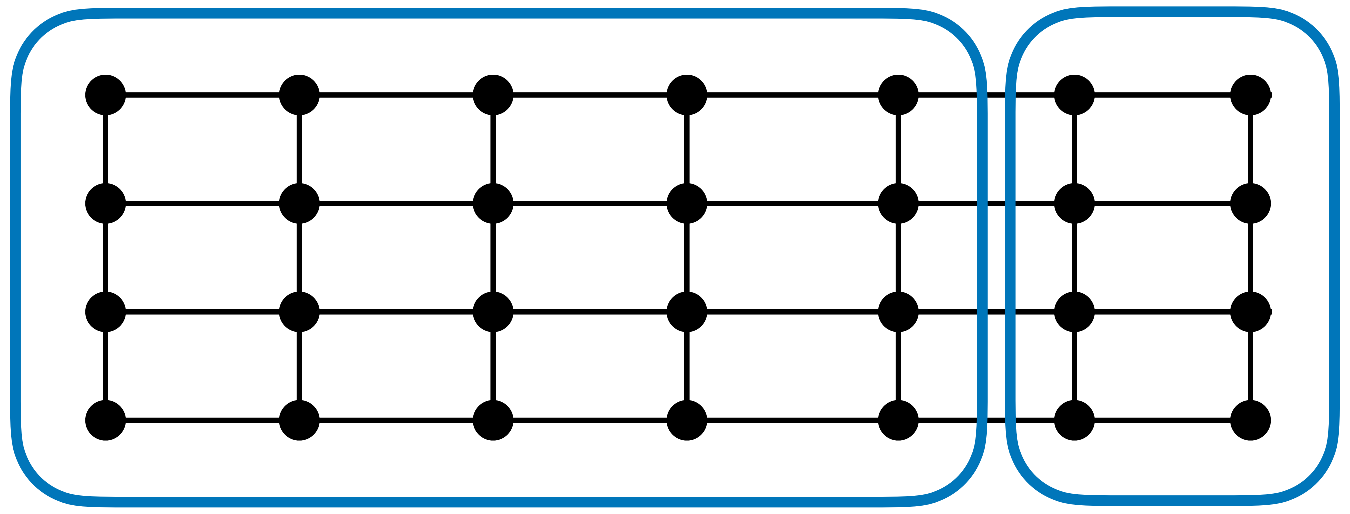
[GS20]: Measurement results from grid state determine whether $g_1 \ldots g_n = I$ or C_3.

Sample $(P_1, \ldots, P_m) \leftarrow \gamma(g_1, \ldots, g_n)$

Round 1:

$x_1 = P_1, \ldots, P_m$

Round 2:

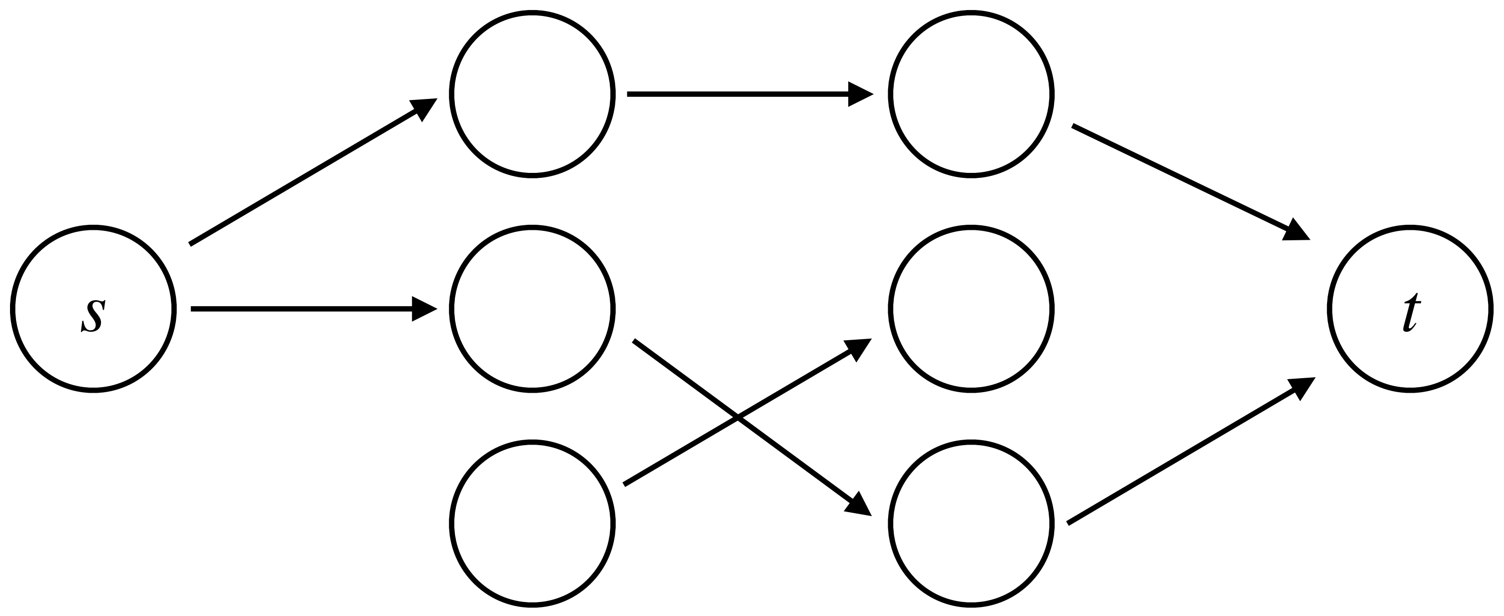


Worst-case ⊕L-hard problems

It is ⊕L-hard to determine the parity of the number of $s \to t$ paths in a (layered) DAG.

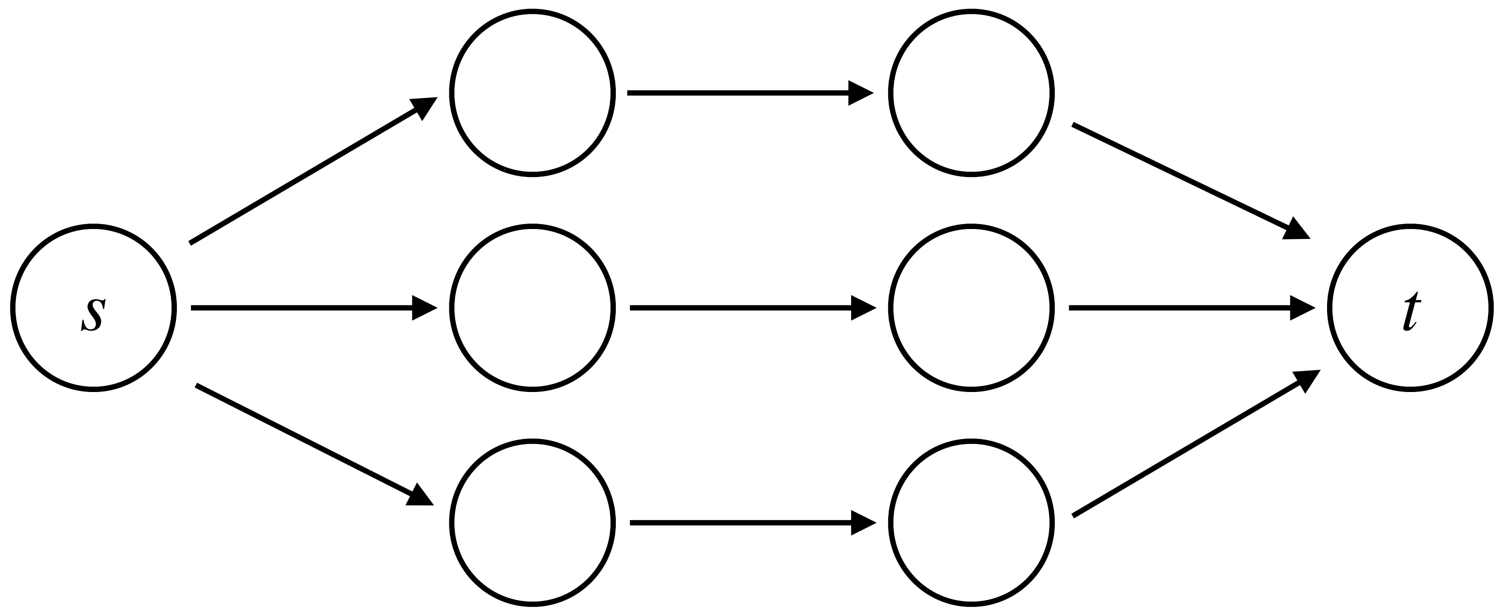
[GS20]: It is also ⊕L-hard to determine whether CNOT gates $g_1, \ldots, g_n$ multiply to 3-cycle or identity.

Even parity



$\Longrightarrow \quad g_1 g_2 \cdots g_n = I$

Odd parity



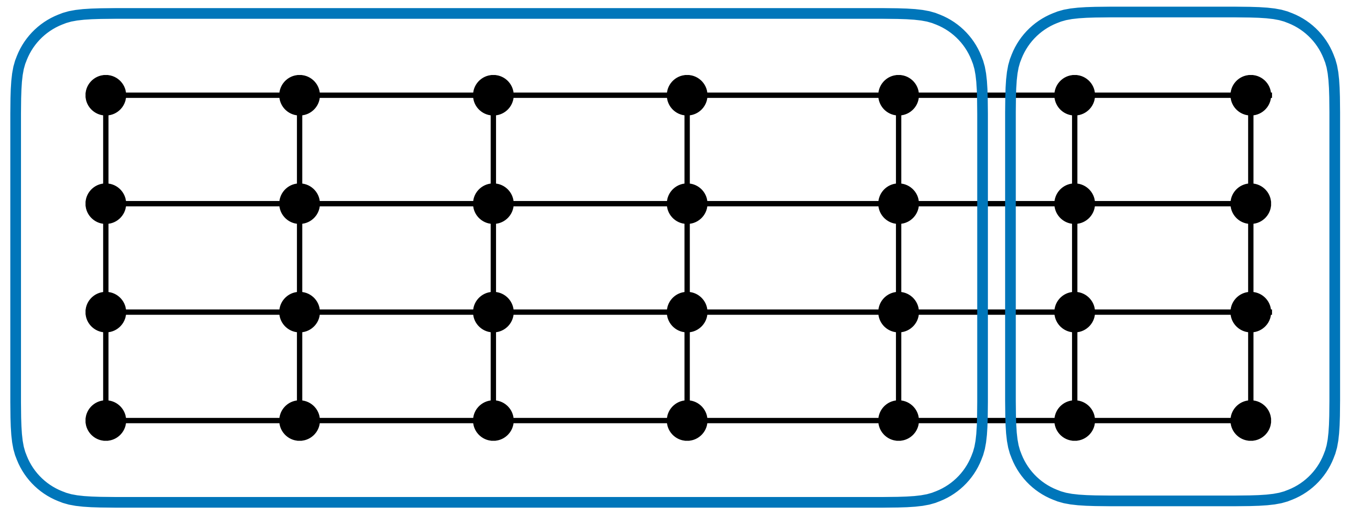
$\Longrightarrow \quad g_1 g_2 \cdots g_n = C_3$

[GS20]: Measurement results from grid state determine whether $g_1 \ldots g_n = I$ or C_3.

Sample $(P_1, \ldots, P_m) \leftarrow \gamma(g_1, \ldots, g_n)$

Round 1: $x_1 = P_1, \ldots, P_m$

Round 2: x_2

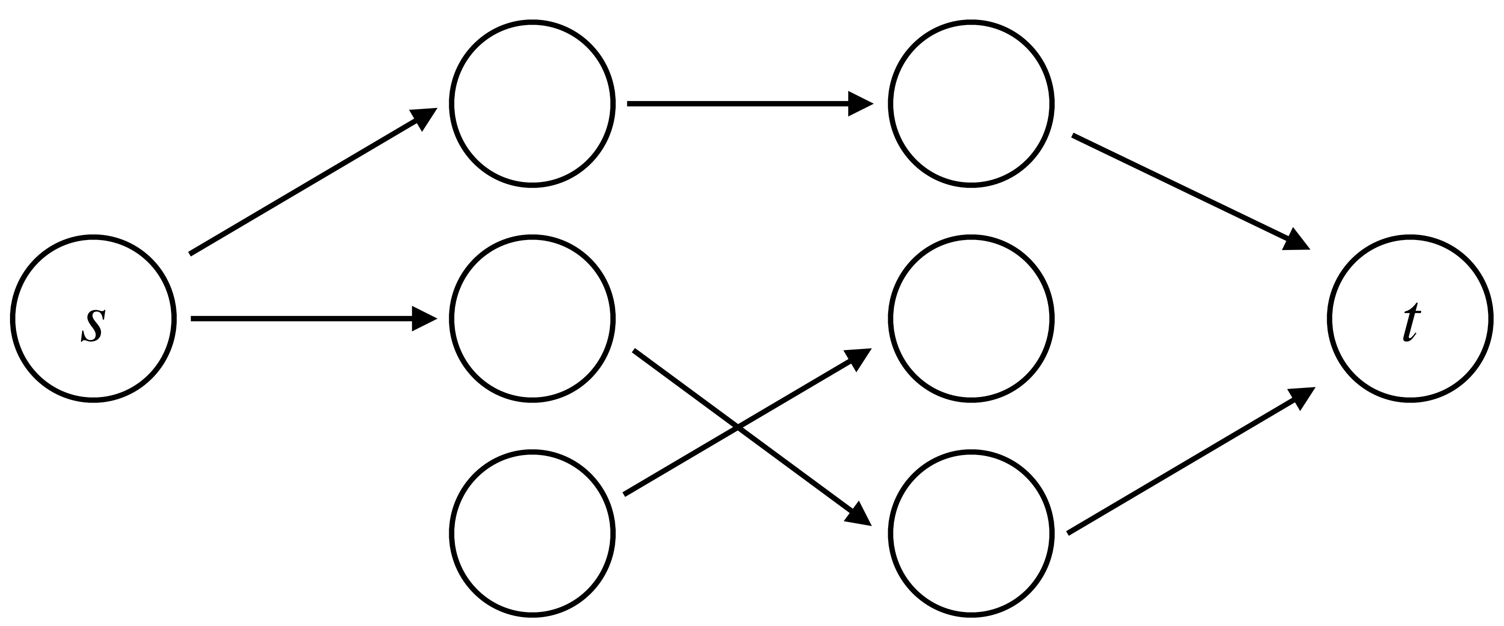


Worst-case $\oplus$L-hard problems

It is $\oplus$L-hard to determine the parity of the number of $s \rightarrow t$ paths in a (layered) DAG.

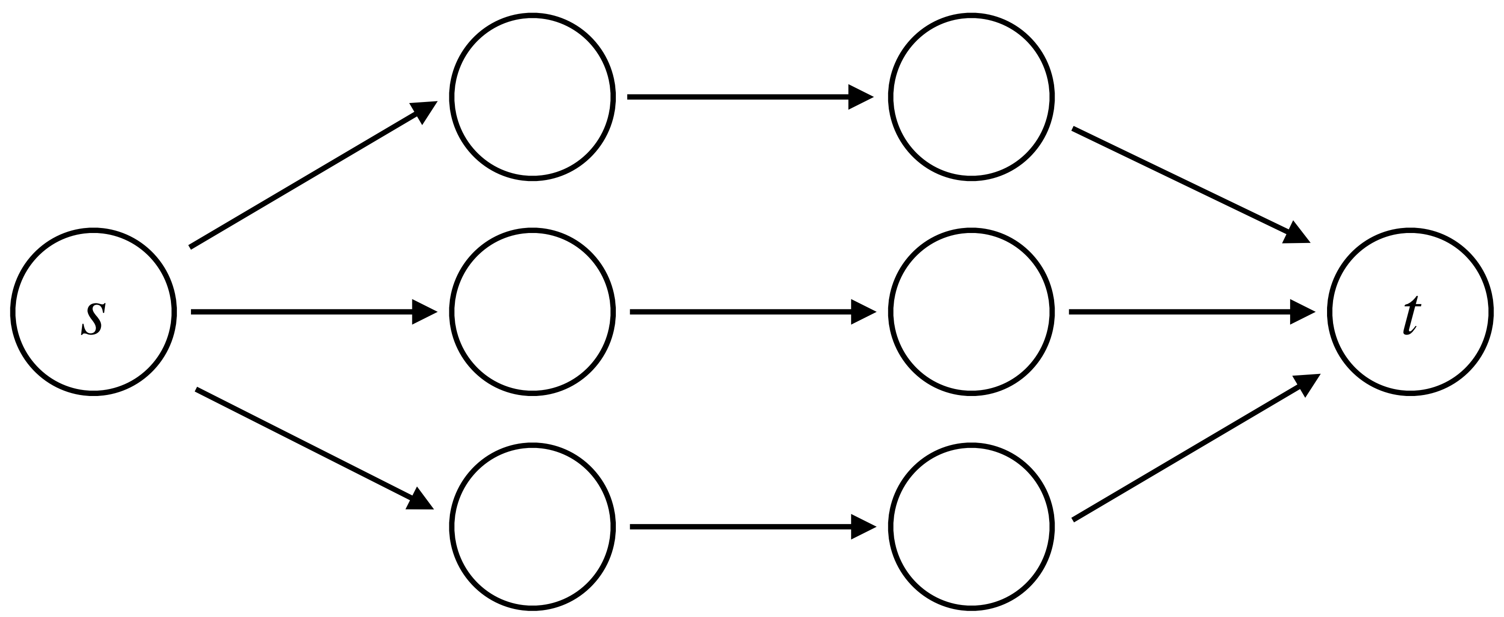
[GS20]: It is also $\oplus$L-hard to determine whether CNOT gates $g_1, \ldots, g_n$ multiply to 3-cycle or identity.

Even parity



$\Longrightarrow \quad g_1 g_2 \ldots g_n = I$

Odd parity



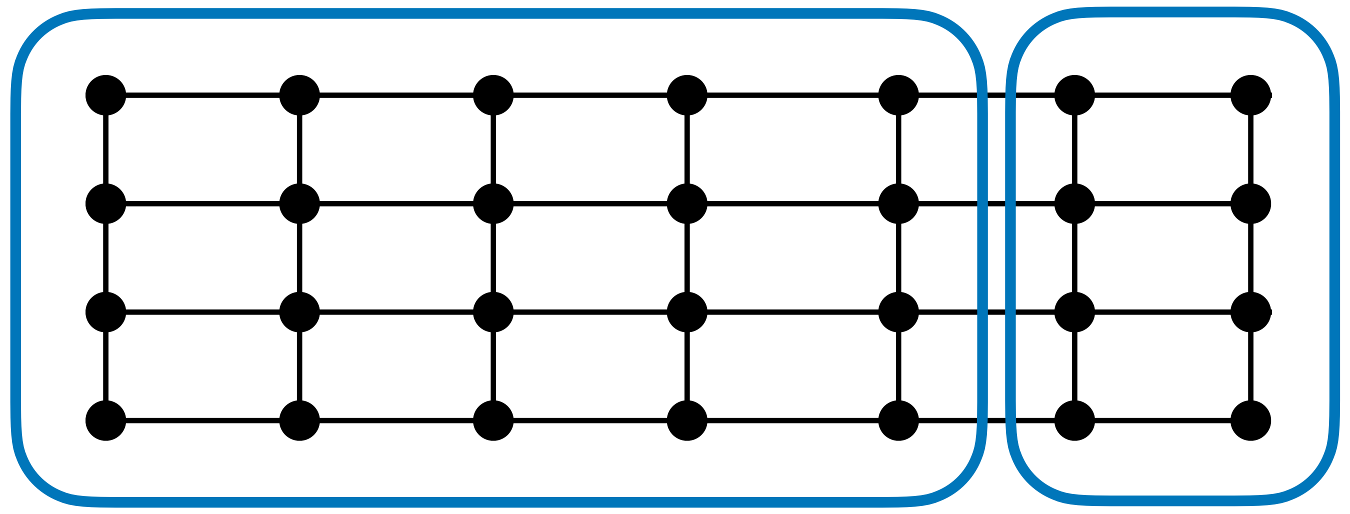
$\Longrightarrow \quad g_1 g_2 \ldots g_n = C_3$

[GS20]: Measurement results from grid state determine whether $g_1 \ldots g_n = I$ or C_3.

Sample $(P_1, \ldots, P_m) \leftarrow \gamma(g_1, \ldots, g_n)$

Round 1: $x_1 = P_1, \ldots, P_m$

Round 2: x_2

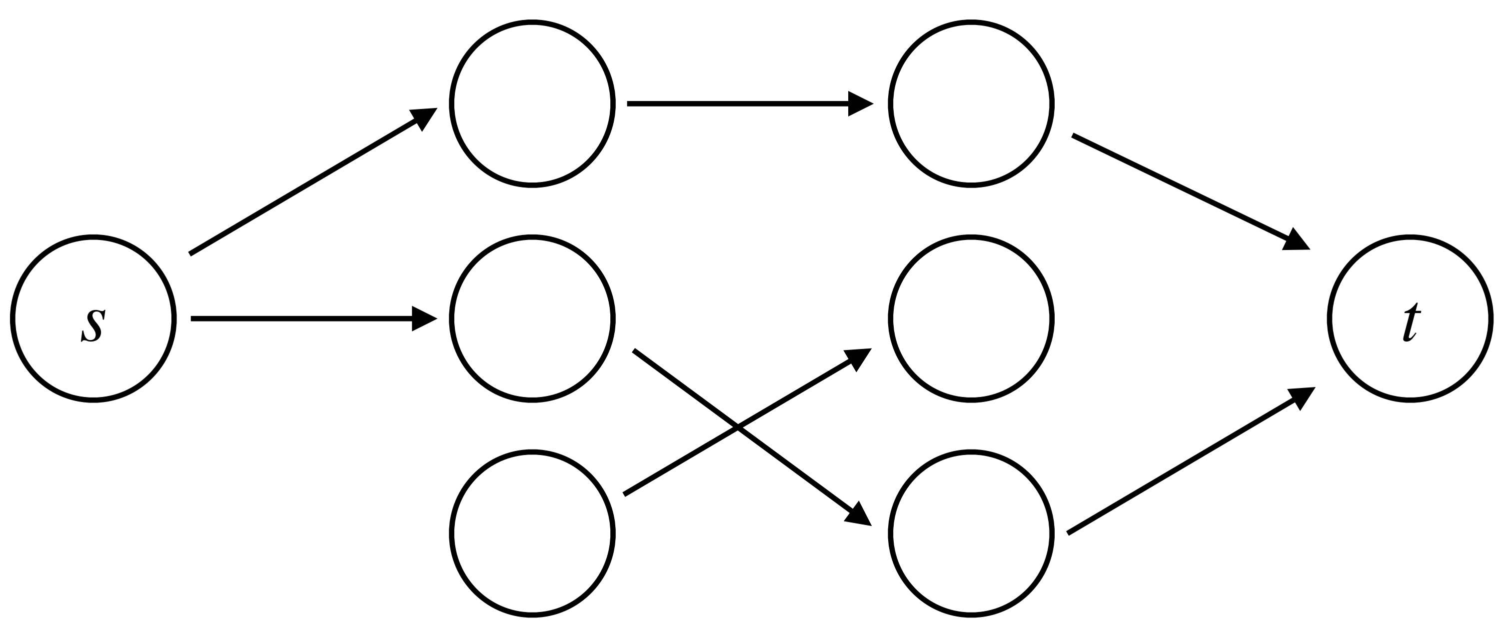


Worst-case ⊕L-hard problems

It is ⊕L-hard to determine the parity of the number of $s \to t$ paths in a (layered) DAG.

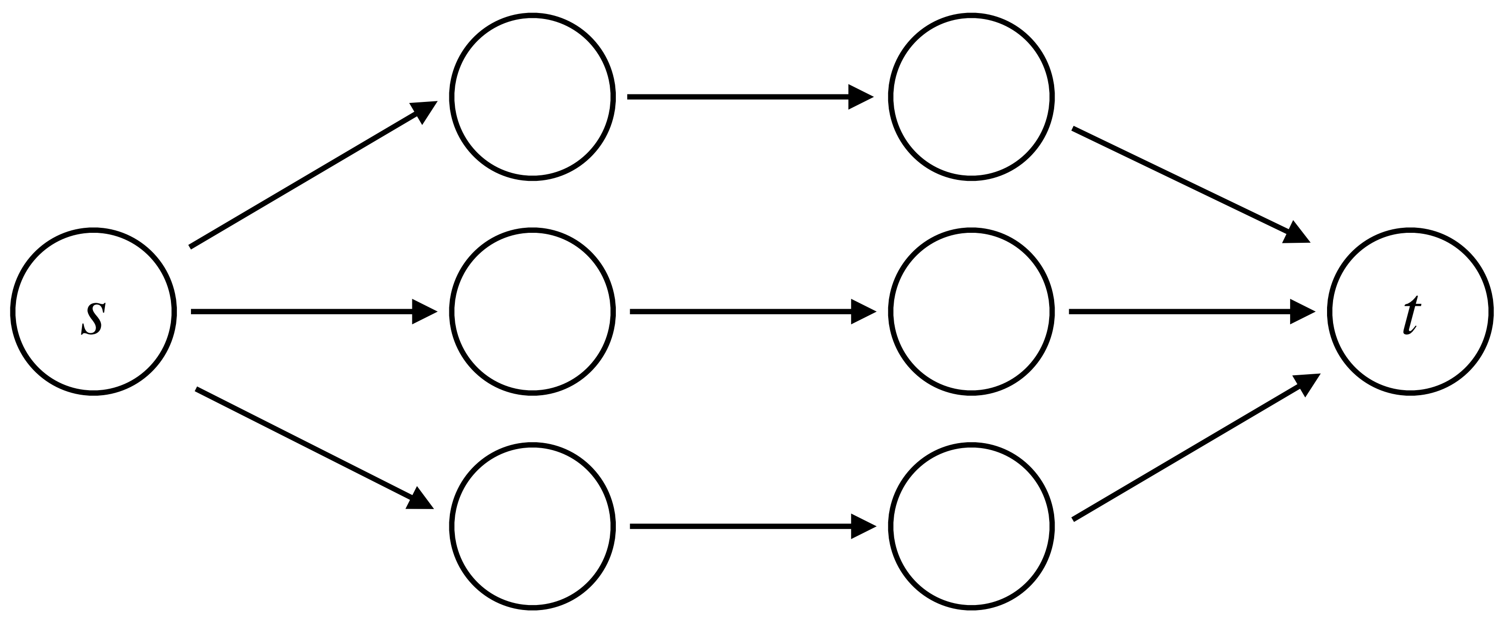
[GS20]: It is also ⊕L-hard to determine whether CNOT gates $g_1, \dots, g_n$ multiply to 3-cycle or identity.

Even parity



$\Longrightarrow \quad g_1 g_2 \dots g_n = I$

Odd parity



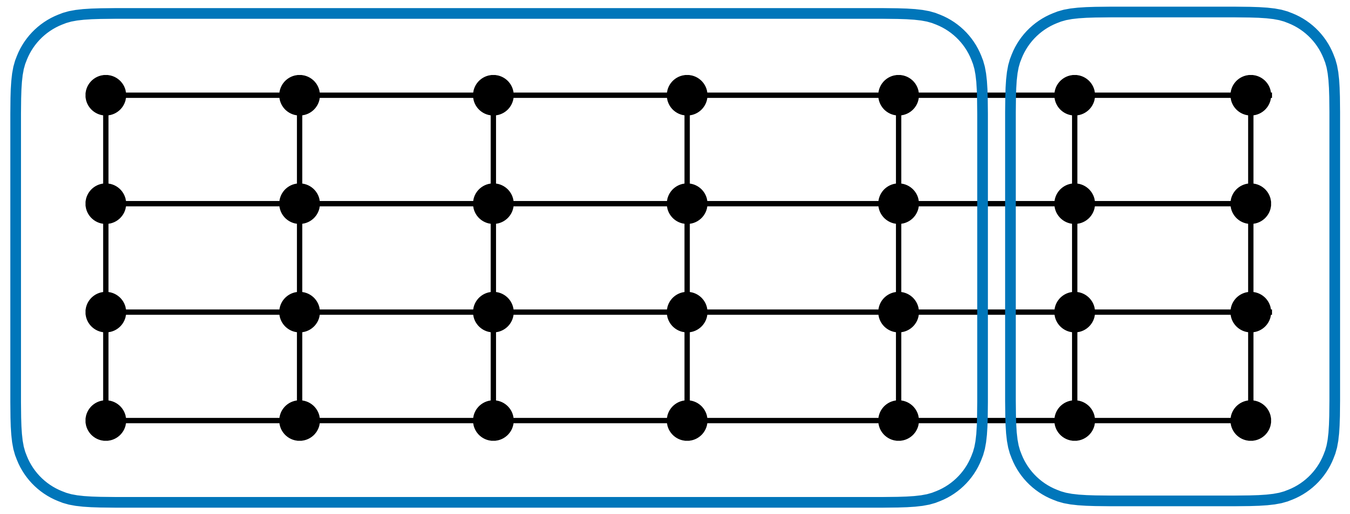
$\Longrightarrow \quad g_1 g_2 \dots g_n = C_3$

[GS20]: Measurement results from grid state determine whether $g_1 \dots g_n = I$ or C_3.

Sample $(P_1, \dots, P_m) \leftarrow \gamma(g_1, \dots, g_n)$

Round 1: $x_1 = P_1, \dots, P_m$

Round 2: x_2



Problem: This only gives us worst-case ⊕L-hardness: $\gamma(g_1, \dots, g_n)$ does not produce "random" instances to first round input

The worst-to-average-case reduction

Problem: $\gamma(g_1, \ldots, g_n)$ does not produce "random" instances to first round input

The worst-to-average-case reduction

Problem: $\gamma(g_1, \ldots, g_n)$ does not produce "random" instances to first round input

It is $\oplus$L-hard to determine the parity of the number of $s \rightarrow t$ paths in layered DAGs.

The worst-to-average-case reduction

Problem: $\gamma(g_1, \ldots, g_n)$ does not produce "random" instances to first round input

Layered DAGs

It is ⊕L-hard to determine the parity of the number of $s \to t$ paths in layered DAGs.

The worst-to-average-case reduction

Problem: $\gamma(g_1, \ldots, g_n)$ does not produce "random" instances to first round input

Layered DAGs

It is ⊕L-hard to determine the parity of the number of $s \rightarrow t$ paths in layered DAGs.

The worst-to-average-case reduction

Problem: $\gamma(g_1, \ldots, g_n)$ does not produce "random" instances to first round input

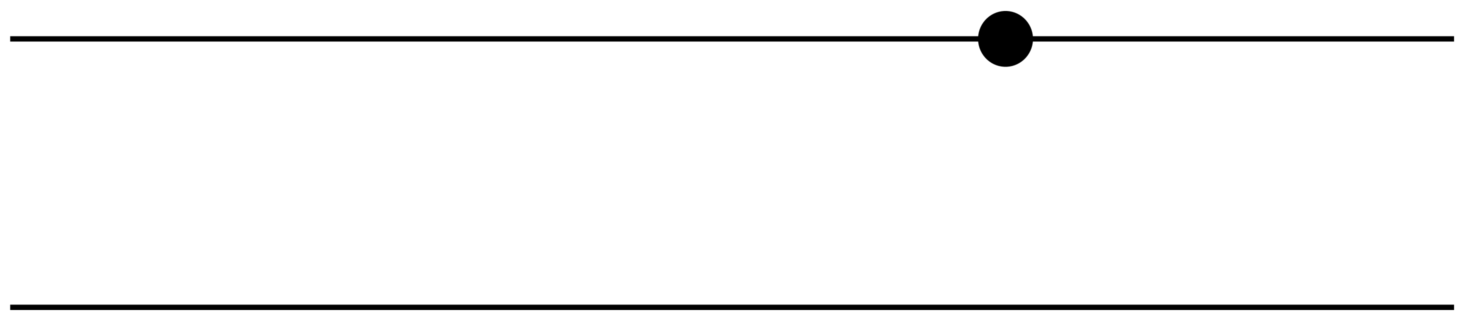
Layered DAGs

It is ⊕L-hard to determine the parity of the number of $s \to t$ paths in layered DAGs.

It is ⊕L-hard to determine whether $g_1, \ldots, g_n$ multiplies to 3-cycle or identity.

The worst-to-average-case reduction

Problem: $\gamma(g_1, \ldots, g_n)$ does not produce "random" instances to first round input



Layered DAGs

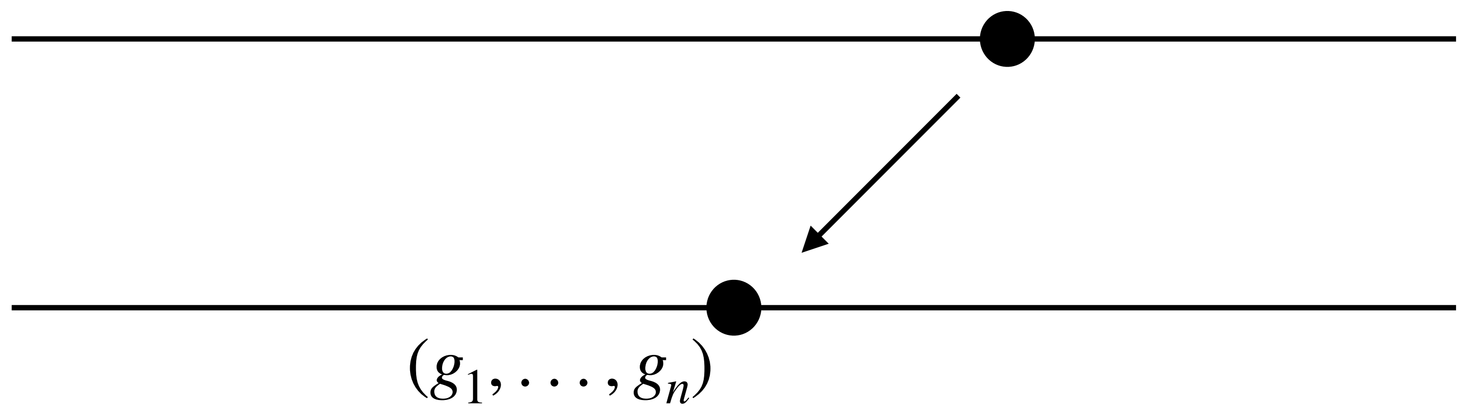
Sequences of CNOT gates

It is $\oplus$L-hard to determine the parity of the number of $s \to t$ paths in layered DAGs.

It is $\oplus$L-hard to determine whether $g_1, \ldots, g_n$ multiplies to 3-cycle or identity.

The worst-to-average-case reduction

Problem: $\gamma(g_1, ..., g_n)$ does not produce "random" instances to first round input



Layered DAGs

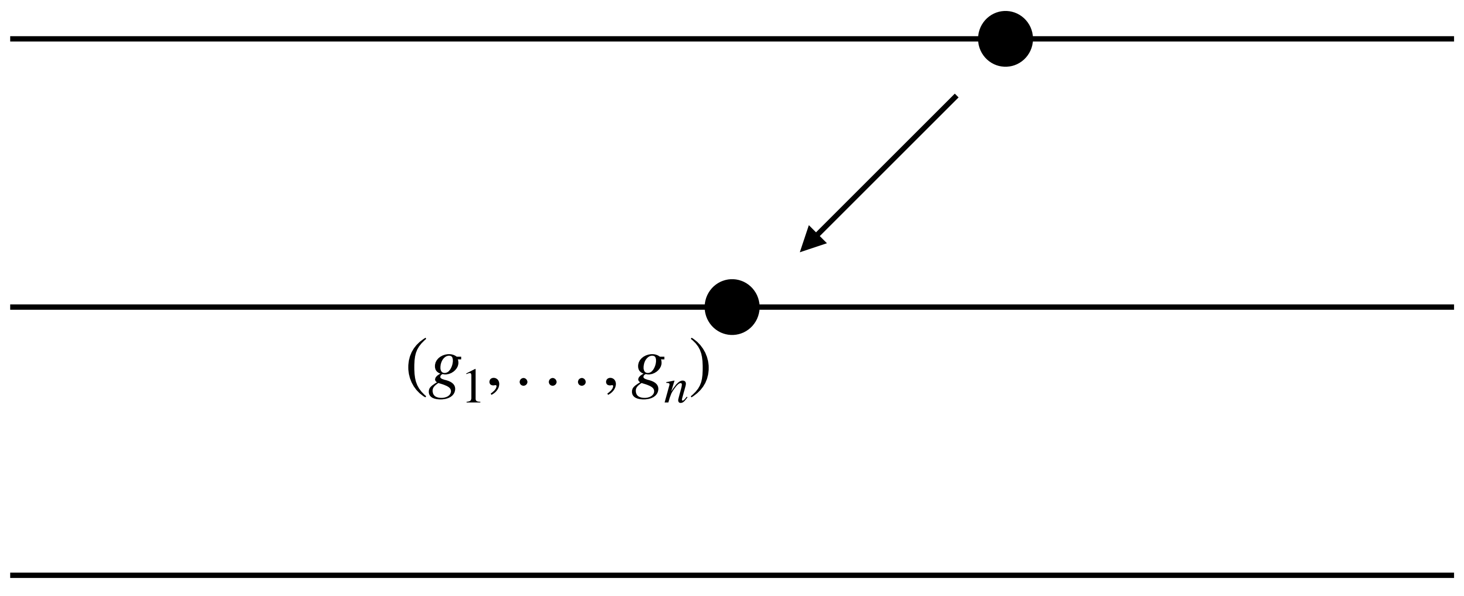
Sequences of CNOT gates

It is ⊕L-hard to determine the parity of the number of $s \to t$ paths in layered DAGs.

It is ⊕L-hard to determine whether $g_1, ..., g_n$ multiplies to 3-cycle or identity.

The worst-to-average-case reduction

Problem: $\gamma(g_1, \ldots, g_n)$ does not produce "random" instances to first round input



Layered DAGs

Sequences of CNOT gates

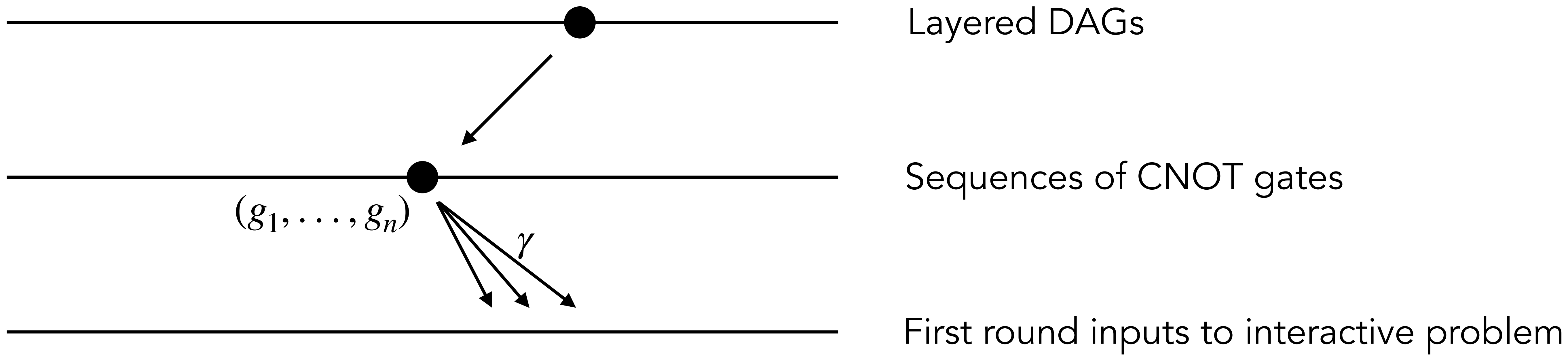
First round inputs to interactive problem

It is ⊕L-hard to determine the parity of the number of $s \to t$ paths in layered DAGs.

It is ⊕L-hard to determine whether $g_1, \ldots, g_n$ multiplies to 3-cycle or identity.

The worst-to-average-case reduction

Problem: $\gamma(g_1, \ldots, g_n)$ does not produce "random" instances to first round input

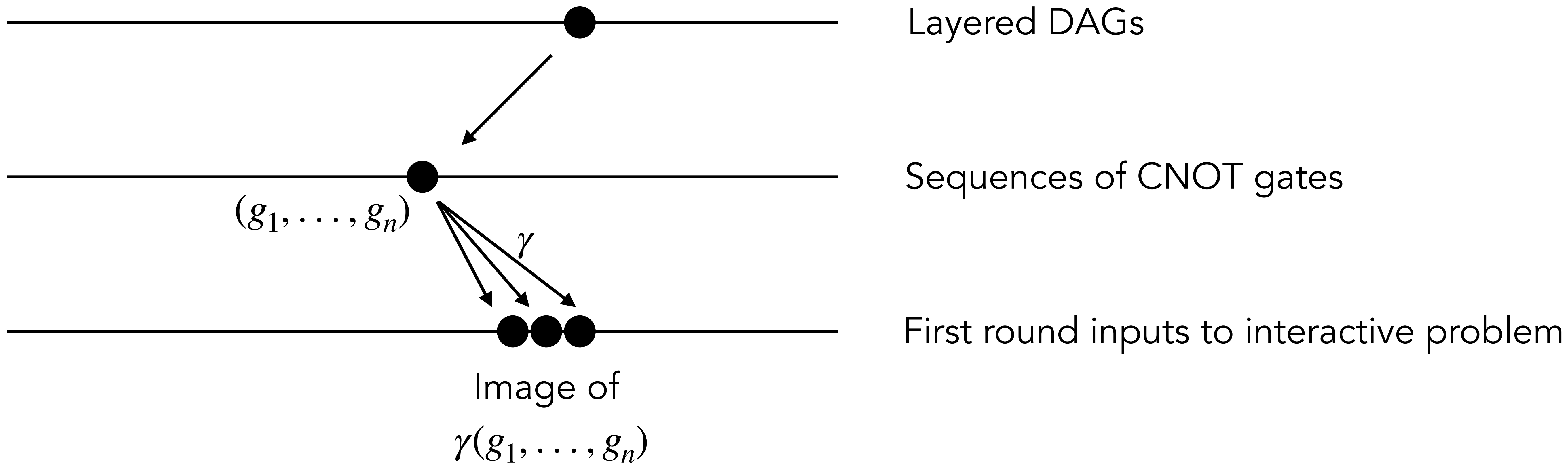


It is ⊕L-hard to determine the parity of the number of $s \to t$ paths in layered DAGs.

It is ⊕L-hard to determine whether $g_1, \ldots, g_n$ multiplies to 3-cycle or identity.

The worst-to-average-case reduction

Problem: $\gamma(g_1, \ldots, g_n)$ does not produce "random" instances to first round input

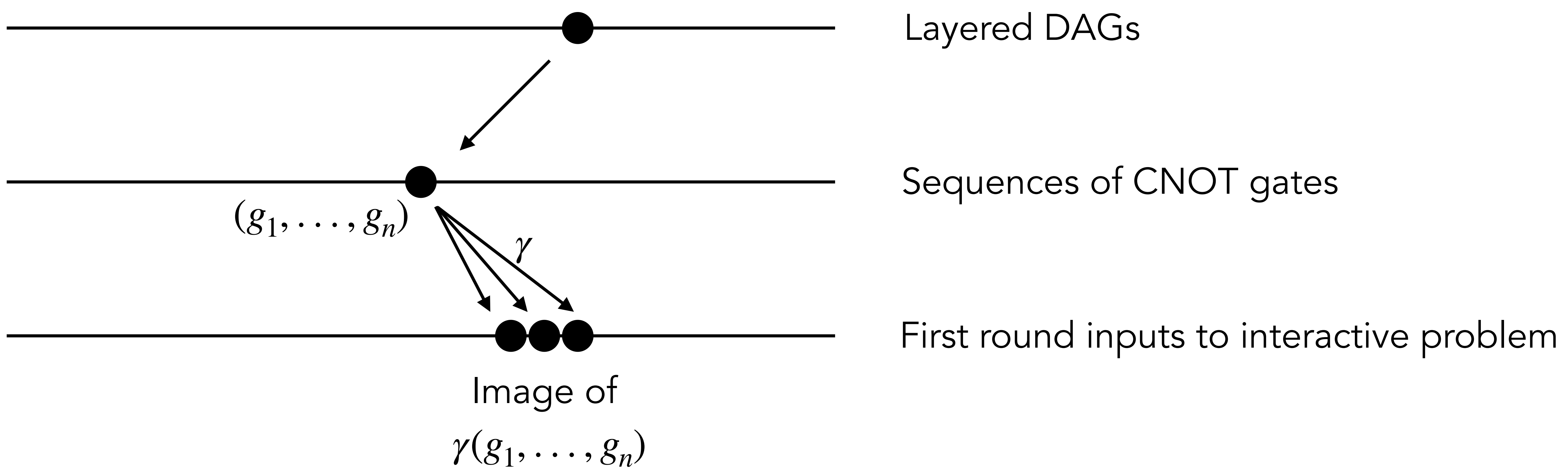


It is ⊕L-hard to determine the parity of the number of $s \to t$ paths in layered DAGs.

It is ⊕L-hard to determine whether $g_1, \ldots, g_n$ multiplies to 3-cycle or identity.

The worst-to-average-case reduction

Problem: $\gamma(g_1, \ldots, g_n)$ does not produce "random" instances to first round input



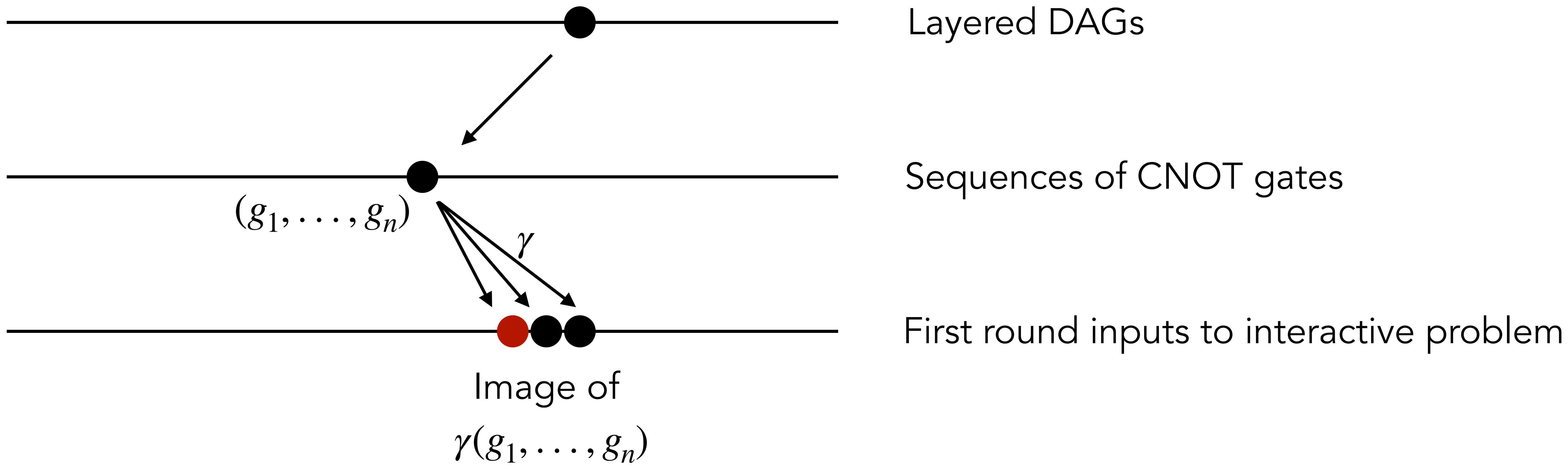
It is ⊕L-hard to determine the parity of the number of $s \to t$ paths in layered DAGs.

It is ⊕L-hard to determine whether $g_1, \ldots, g_n$ multiplies to 3-cycle or identity.

We prove a robustness to small error within the image of $\gamma(g_1, \ldots, g_n)$.

The worst-to-average-case reduction

Problem: $\gamma(g_1, \ldots, g_n)$ does not produce "random" instances to first round input



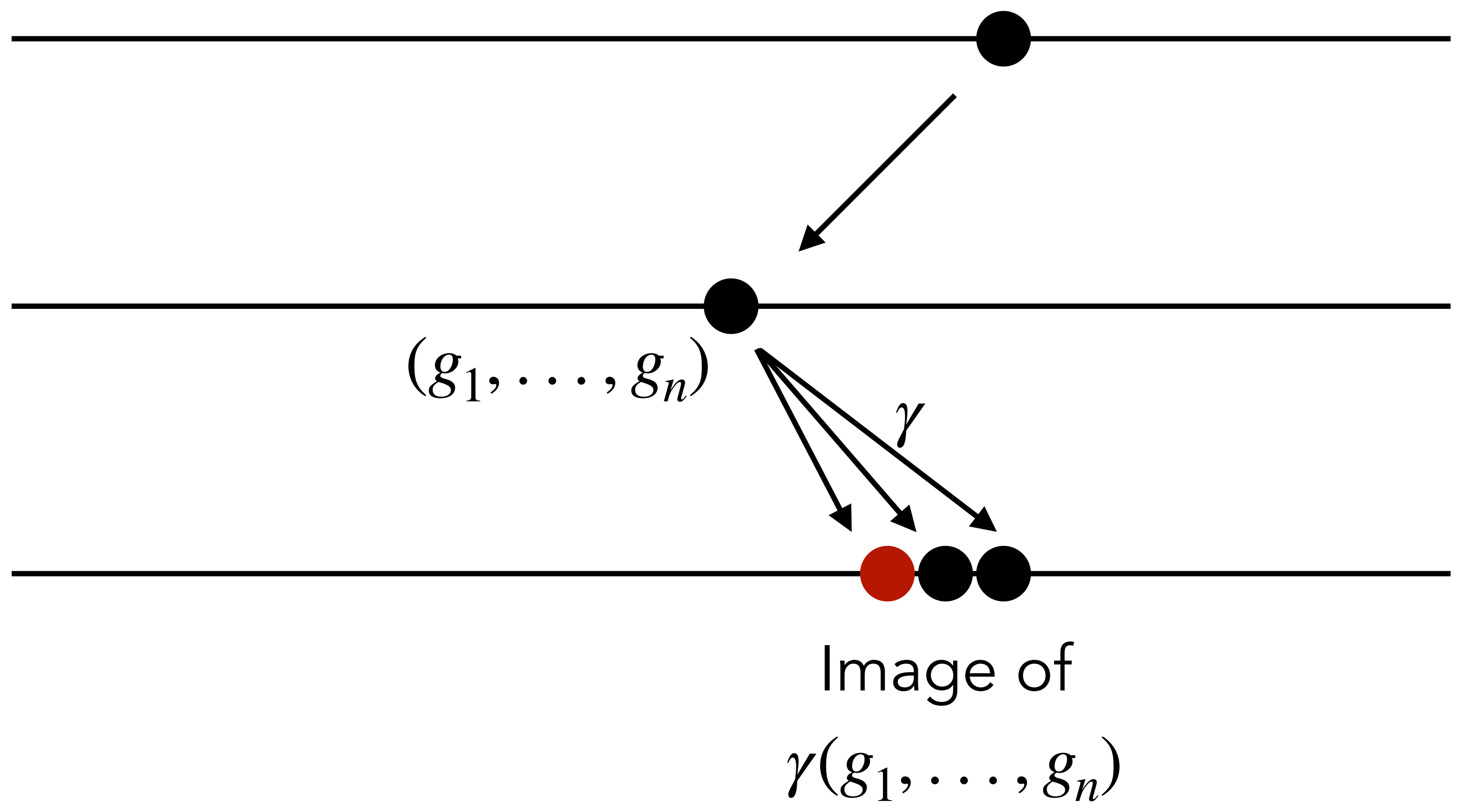
It is ⊕L-hard to determine the parity of the number of $s \to t$ paths in layered DAGs.

It is ⊕L-hard to determine whether $g_1, \ldots, g_n$ multiplies to 3-cycle or identity.

We prove a robustness to small error within the image of $\gamma(g_1, \ldots, g_n)$.

The worst-to-average-case reduction

Problem: $\gamma(g_1, ..., g_n)$ does not produce "random" instances to first round input



Layered DAGs

Sequences of CNOT gates

First round inputs to interactive problem

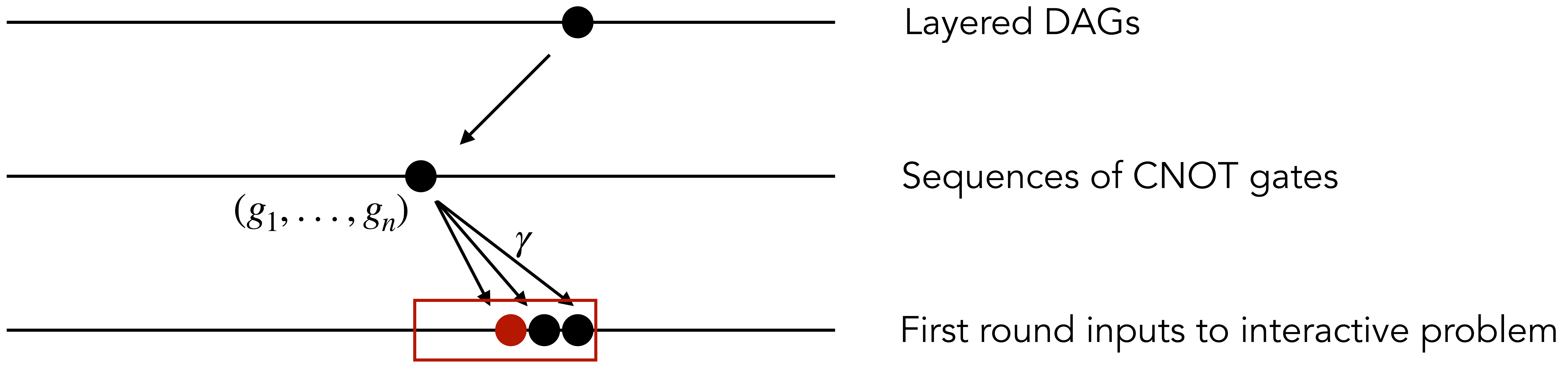
It is ⊕L-hard to determine the parity of the number of $s \to t$ paths in layered DAGs.

It is ⊕L-hard to determine whether $g_1, ..., g_n$ multiplies to 3-cycle or identity.

We prove a robustness to small error within the image of $\gamma(g_1, ..., g_n)$. But this is not enough to prove average-case hardness.

The worst-to-average-case reduction

Problem: $\gamma(g_1, \ldots, g_n)$ does not produce "random" instances to first round input



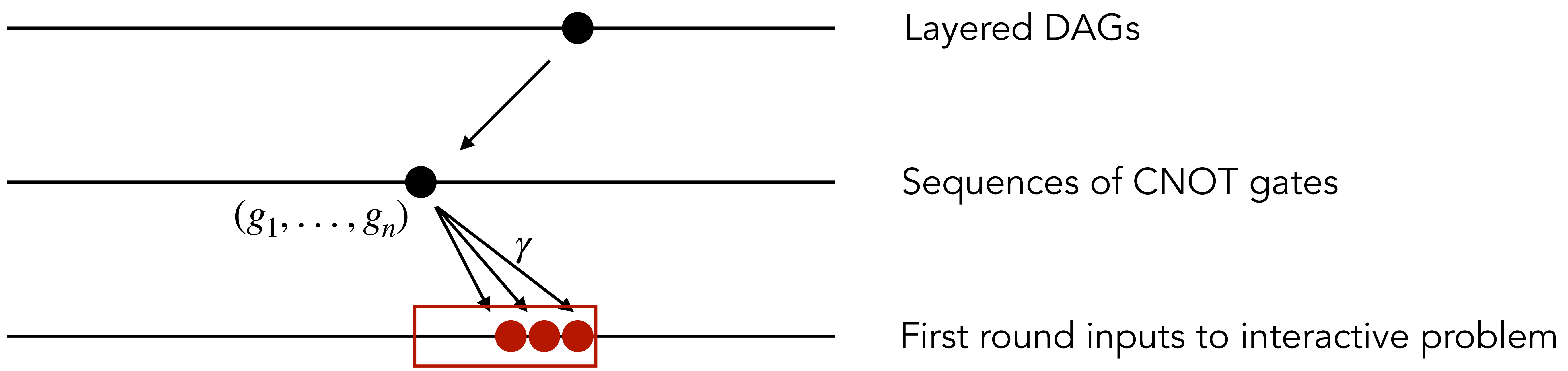
It is ⊕L-hard to determine the parity of the number of $s \to t$ paths in layered DAGs.

It is ⊕L-hard to determine whether $g_1, \ldots, g_n$ multiplies to 3-cycle or identity.

We prove a robustness to small error within the image of $\gamma(g_1, \ldots, g_n)$. But this is not enough to prove average-case hardness.

The worst-to-average-case reduction

Problem: $\gamma(g_1, \ldots, g_n)$ does not produce "random" instances to first round input



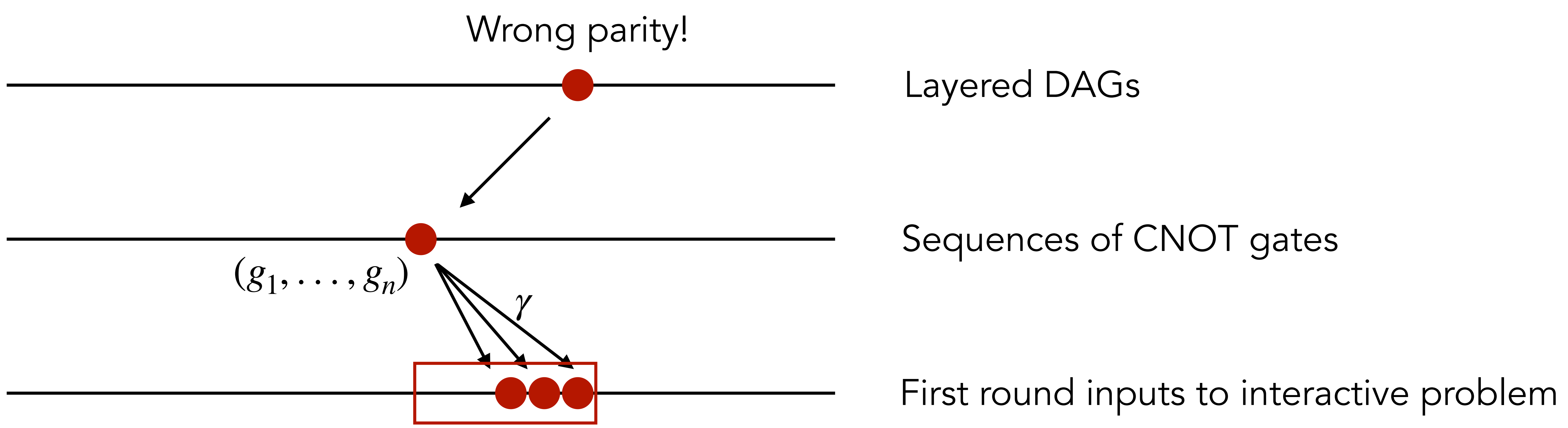
It is ⊕L-hard to determine the parity of the number of $s \to t$ paths in layered DAGs.

It is ⊕L-hard to determine whether $g_1, \ldots, g_n$ multiplies to 3-cycle or identity.

We prove a robustness to small error within the image of $\gamma(g_1, \ldots, g_n)$. But this is not enough to prove average-case hardness.

The worst-to-average-case reduction

Problem: $\gamma(g_1, \ldots, g_n)$ does not produce "random" instances to first round input



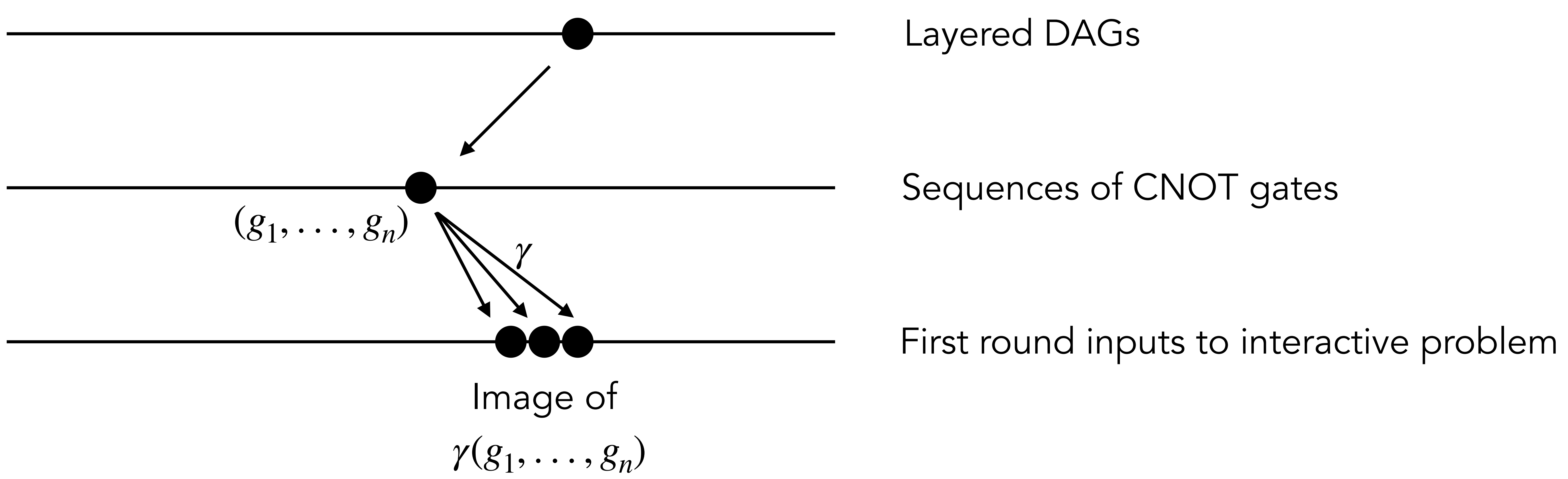
It is ⊕L-hard to determine the parity of the number of $s \to t$ paths in layered DAGs.

It is ⊕L-hard to determine whether $g_1, \ldots, g_n$ multiplies to 3-cycle or identity.

We prove a robustness to small error within the image of $\gamma(g_1, \ldots, g_n)$. But this is not enough to prove average-case hardness.

The worst-to-average-case reduction

Problem: $\gamma(g_1, \ldots, g_n)$ does not produce "random" instances to first round input



It is $\oplus$L-hard to determine the parity of the number of $s \to t$ paths in layered DAGs.

It is $\oplus$L-hard to determine whether $g_1, \ldots, g_n$ multiplies to 3-cycle or identity.

We prove a robustness to small error within the image of $\gamma(g_1, \ldots, g_n)$. But this is not enough to prove average-case hardness.

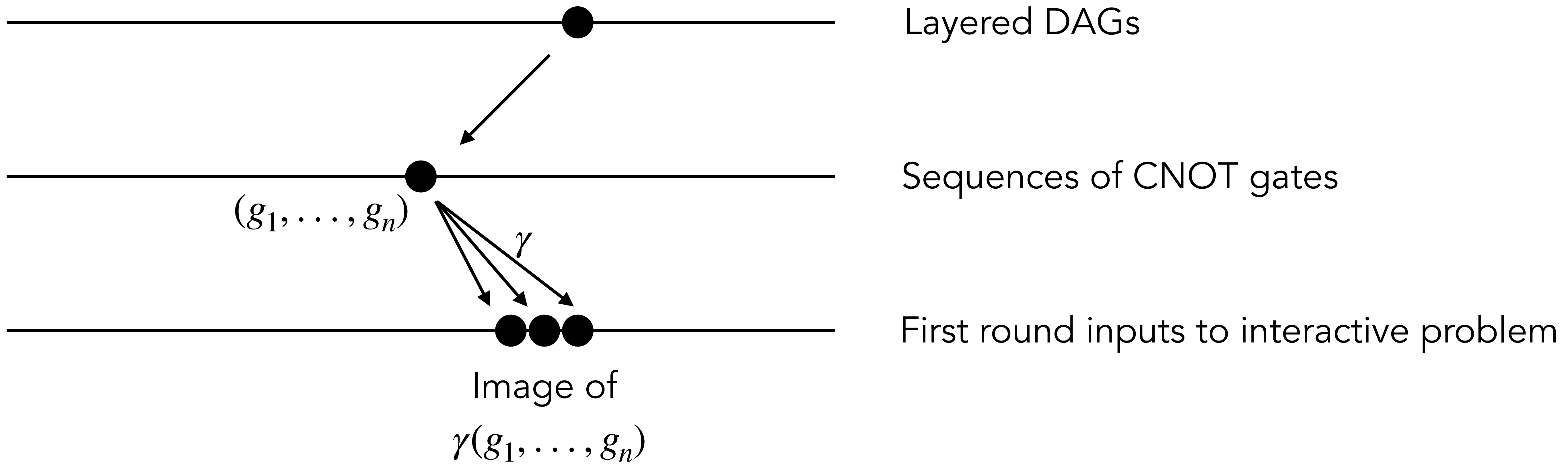
The worst-to-average-case reduction

Problem: $\gamma(g_1, \ldots, g_n)$ does not produce "random" instances to first round input

It is $\oplus$L-hard to determine the parity of the number of $s \to t$ paths in general DAGs.

It is $\oplus$L-hard to determine the parity of the number of $s \to t$ paths in layered DAGs.

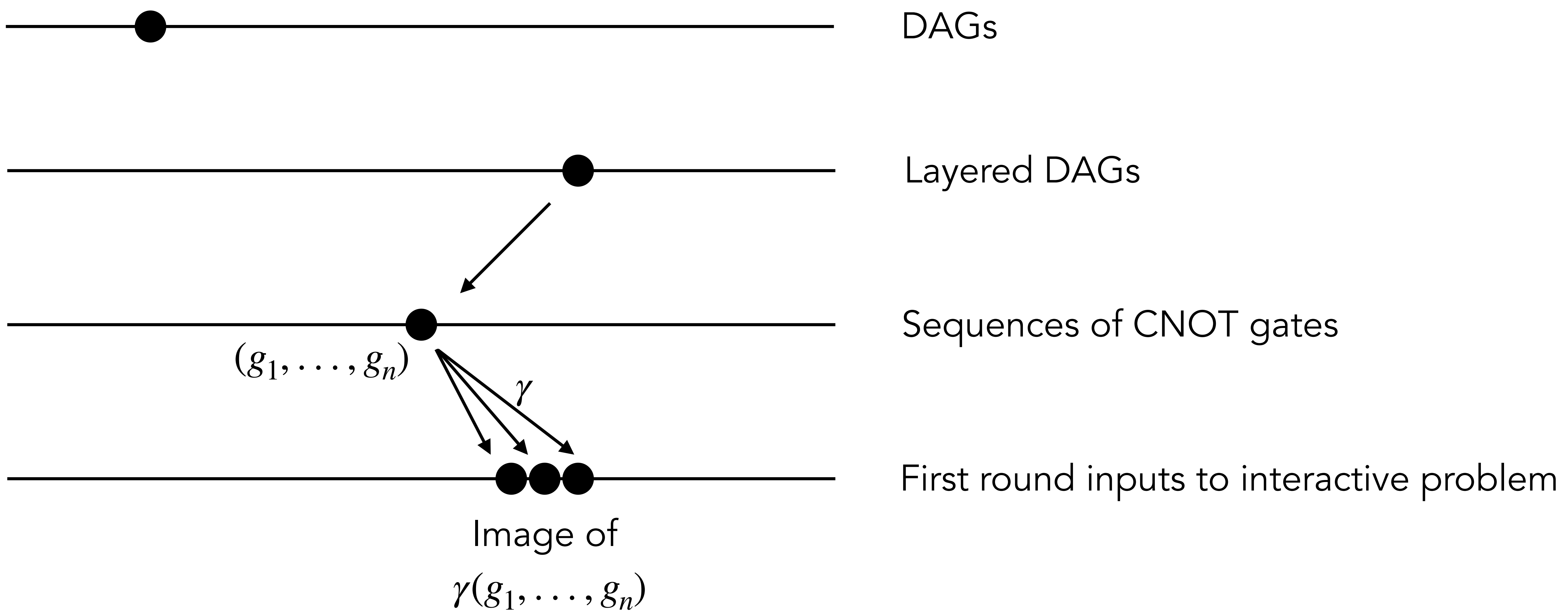
It is $\oplus$L-hard to determine whether $g_1, \ldots, g_n$ multiplies to 3-cycle or identity.



We prove a robustness to small error within the image of $\gamma(g_1, \ldots, g_n)$. But this is not enough to prove average-case hardness.

The worst-to-average-case reduction

Problem: $\gamma(g_1, \ldots, g_n)$ does not produce "random" instances to first round input



It is $\oplus$L-hard to determine the parity of the number of $s \to t$ paths in general DAGs.

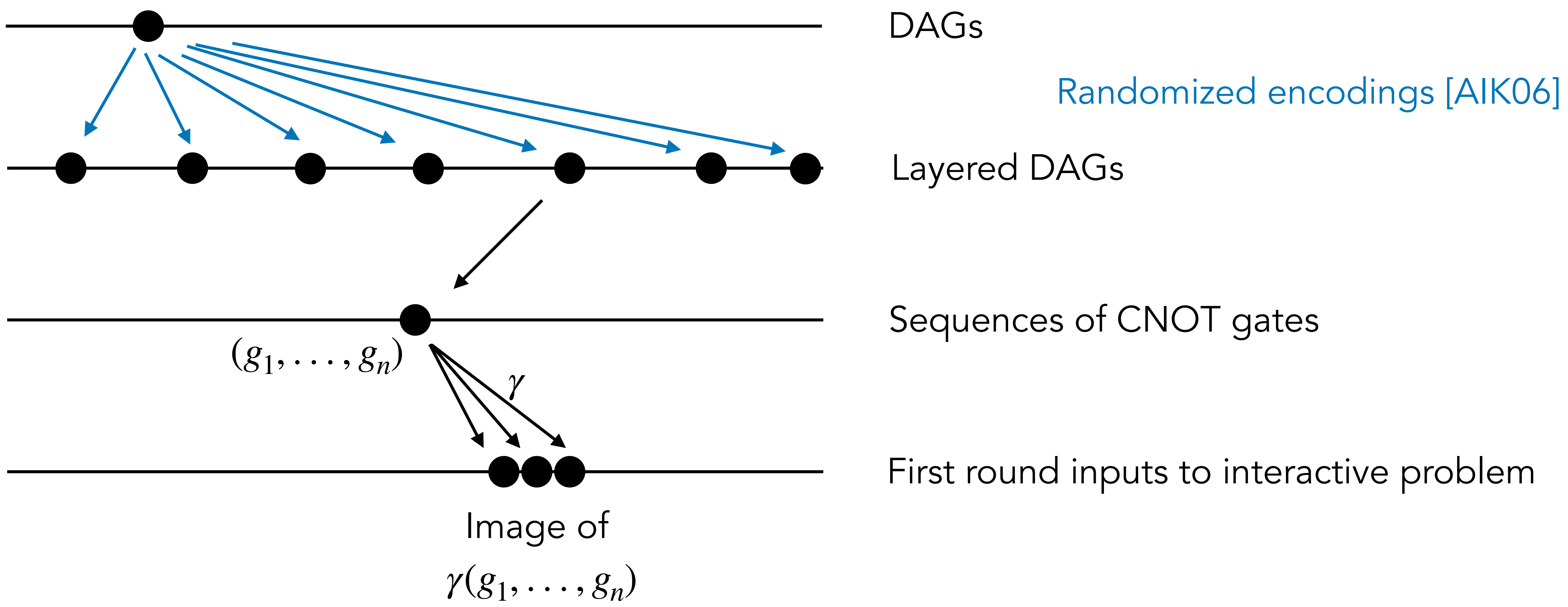
It is $\oplus$L-hard to determine the parity of the number of $s \to t$ paths in layered DAGs.

It is $\oplus$L-hard to determine whether $g_1, \ldots, g_n$ multiplies to 3-cycle or identity.

We prove a robustness to small error within the image of $\gamma(g_1, \ldots, g_n)$. But this is not enough to prove average-case hardness.

The worst-to-average-case reduction

Problem: $\gamma(g_1, ..., g_n)$ does not produce "random" instances to first round input



It is $\oplus$L-hard to determine the parity of the number of $s \to t$ paths in general DAGs.

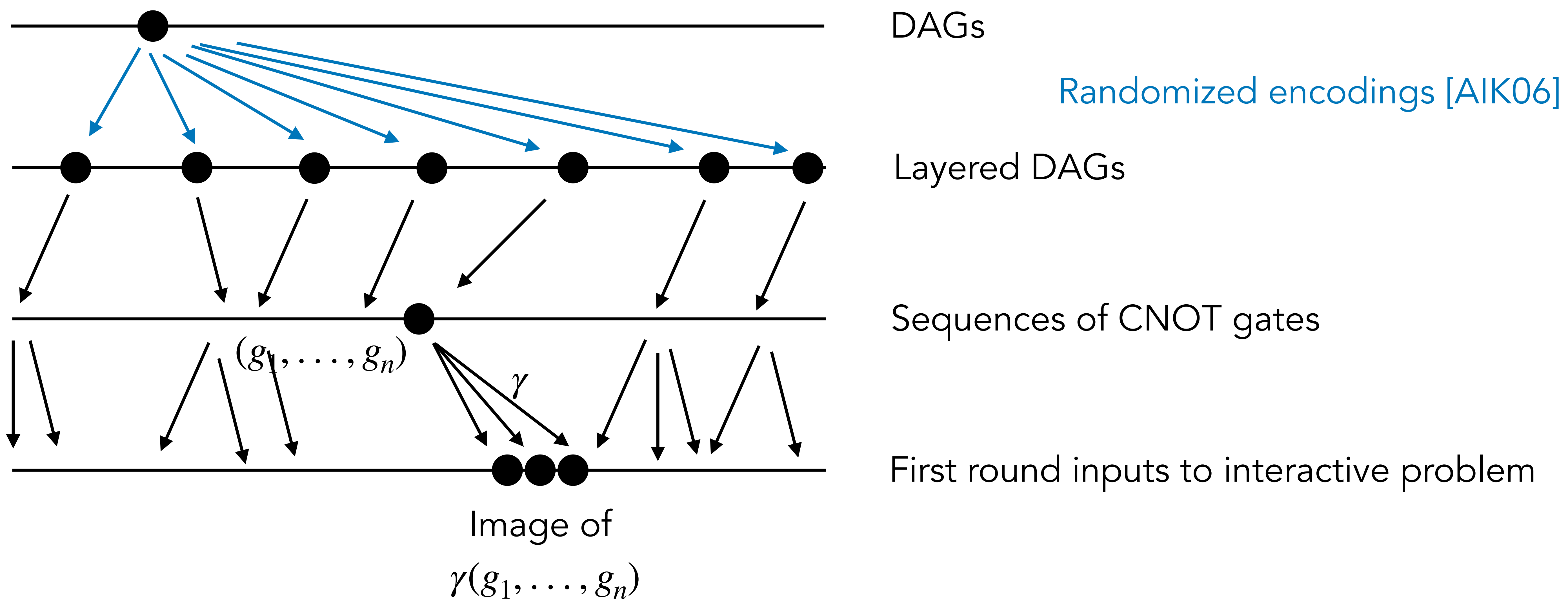
It is $\oplus$L-hard to determine the parity of the number of $s \to t$ paths in layered DAGs.

It is $\oplus$L-hard to determine whether $g_1, ..., g_n$ multiplies to 3-cycle or identity.

We prove a robustness to small error within the image of $\gamma(g_1, ..., g_n)$. But this is not enough to prove average-case hardness.

The worst-to-average-case reduction

Problem: $\gamma(g_1, \ldots, g_n)$ does not produce "random" instances to first round input



It is $\oplus$L-hard to determine the parity of the number of $s \to t$ paths in general DAGs.

It is $\oplus$L-hard to determine the parity of the number of $s \to t$ paths in layered DAGs.

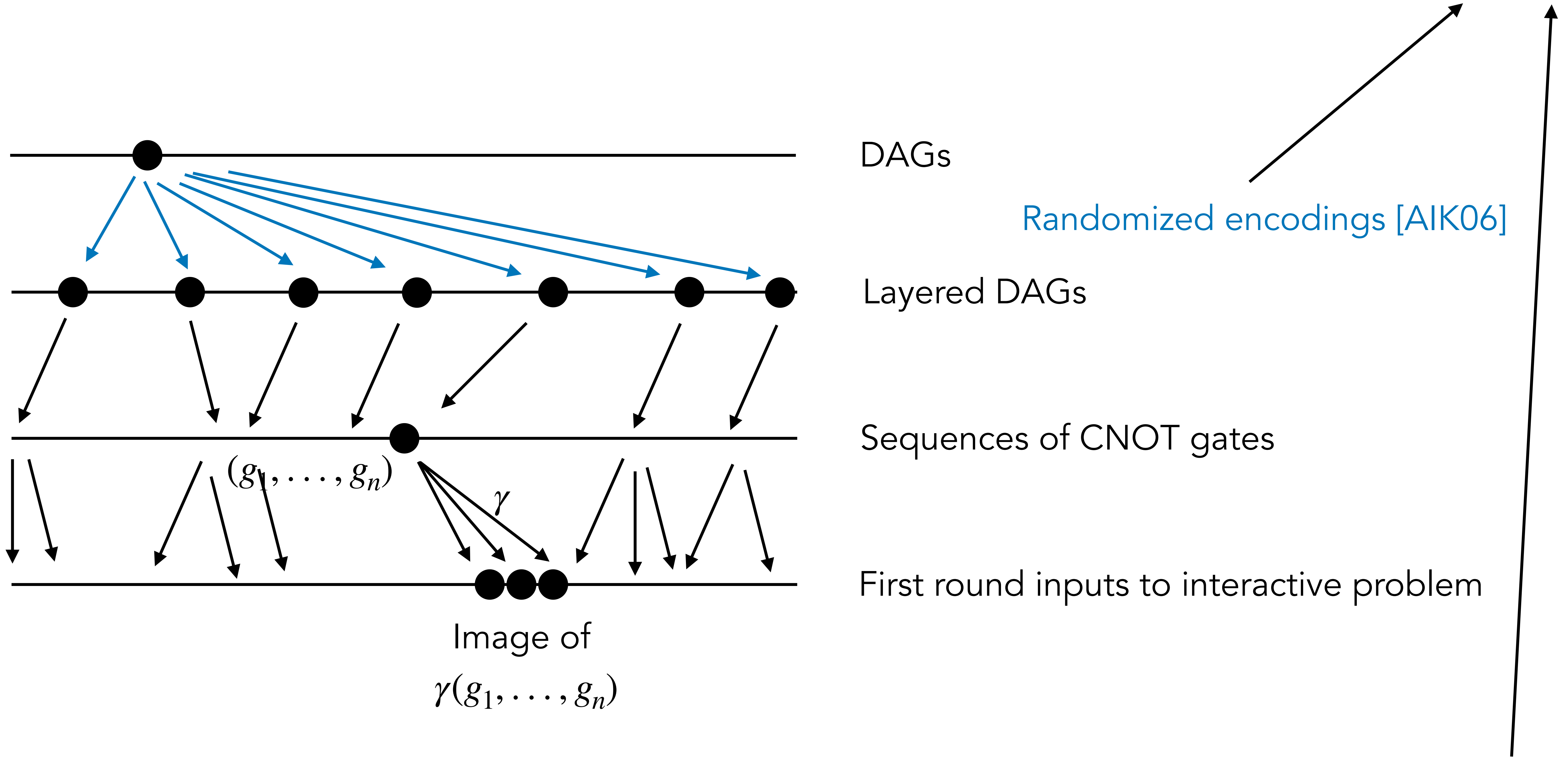
It is $\oplus$L-hard to determine whether $g_1, \ldots, g_n$ multiplies to 3-cycle or identity.

We prove a robustness to small error within the image of $\gamma(g_1, \ldots, g_n)$. But this is not enough to prove average-case hardness.

The worst-to-average-case reduction

Problem: $\gamma(g_1, ..., g_n)$ does not produce "random" instances to first round input

Average-case ⊕L-hard:
Let $\mathscr{R}$ be a classical probabilistic machine that solves the interactive task w/p $420/421$ over uniform input. Then ⊕L $\subseteq (\mathsf{AC}^0)^{\mathscr{R}}$.



It is ⊕L-hard to determine the parity of the number of $s \to t$ paths in general DAGs.

It is ⊕L-hard to determine the parity of the number of $s \to t$ paths in layered DAGs.

It is ⊕L-hard to determine whether $g_1, ..., g_n$ multiplies to 3-cycle or identity.

We prove a robustness to small error within the image of $\gamma(g_1, ..., g_n)$. But this is not enough to prove average-case hardness.

Conclusion

- Simulating grid state measurements is **average-case** $\oplus$L-hard (in some sense)
- Reuse noise-tolerance ideas from [BGKT] to show that a noisy quantum circuit can solve a related grid state measurement task while remaining hard for classical machines

Conclusion

- Simulating grid state measurements is **average-case** $\oplus$L-hard (in some sense)
- Reuse noise-tolerance ideas from [BGKT] to show that a noisy quantum circuit can solve a related grid state measurement task while remaining hard for classical machines

Unconditional separation between noisy QNC^0 circuits and $\mathrm{AC}^0[p]$ circuits

Conditional separation between noisy QNC^0 circuits and log-space machines

Open problems. Questions?

- We show a $\oplus$L-hardness threshold of $420/421$. Can we go lower than this?
  - Worst-to-average-case reductions with stronger randomization?
  - Direct product theorems?
- We have unconditional, noisy separations for relation and interactive problems against constant-depth classical circuits. What about other types of problems, e.g., sampling?
- Can we base our conditional result on simply $\oplus$L $\neq$ L?