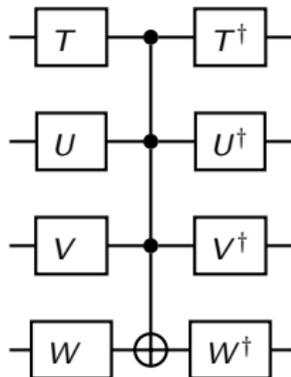


# Bounds on the $\text{QAC}^0$ Complexity of Approximating Parity



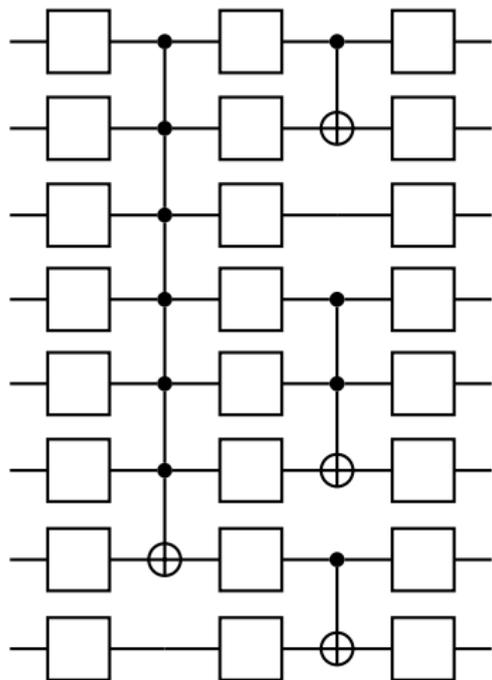
Gregory Rosenthal

University of Toronto

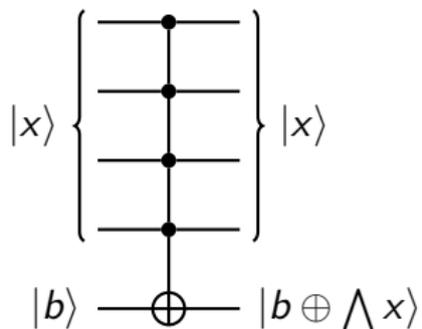
ITCS 2021



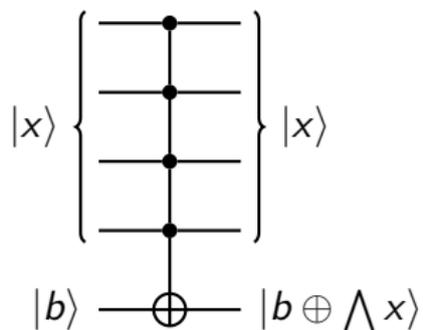
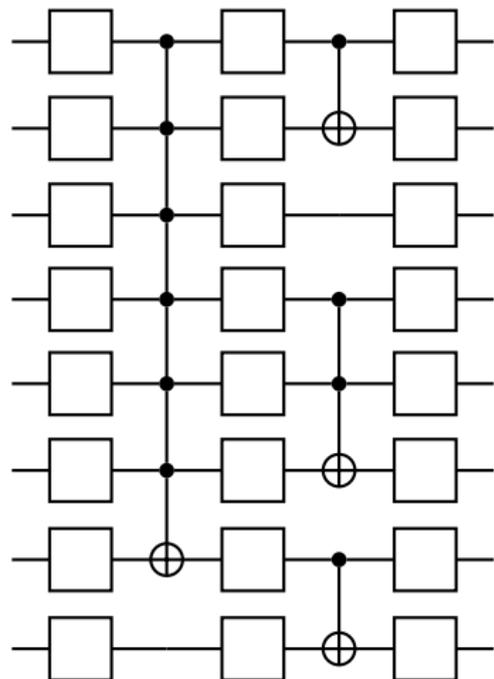
# QAC<sup>0</sup>



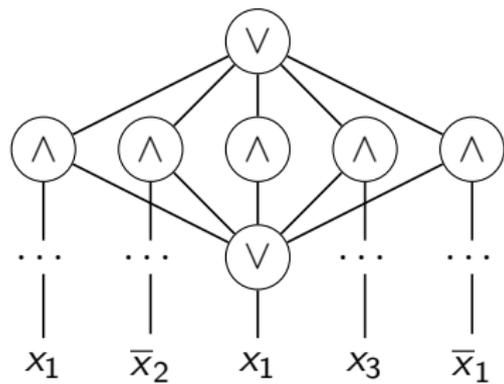
► constant depth



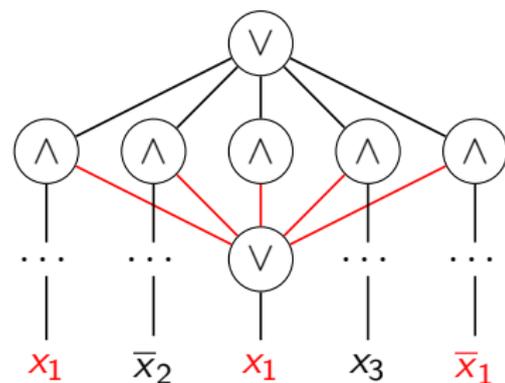
# QAC



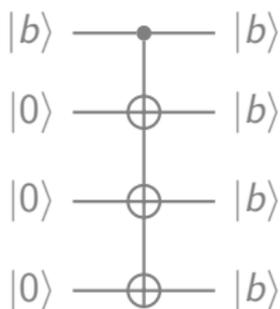
$AC^0$



# Fanout & Motivation

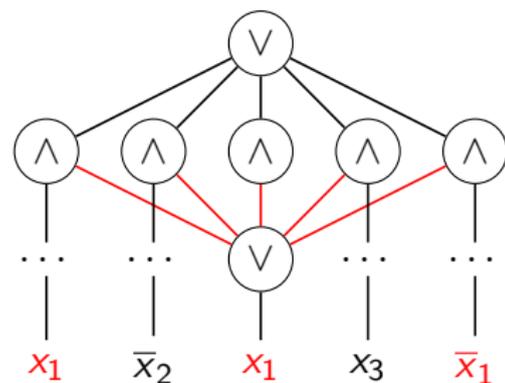


$\forall b \in \{0, 1\}$ :

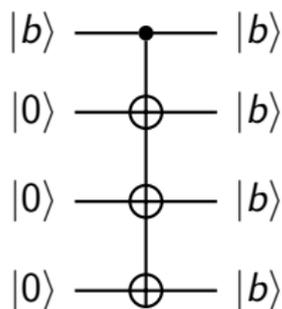


- ▶ Is fanout in  $\text{QAC}^0$ ?
- ▶ Fanout  $\sim$  Parity [GHMP'02]
- ▶ Parity  $\notin \text{AC}^0$  [H'86]
- ▶  $\text{TC}^0 \subseteq \text{QAC}^0[\text{parity/fanout}]$  [HS'05, TT'16]

# Fanout & Motivation

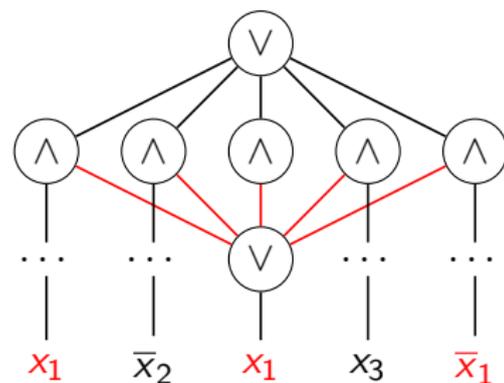


$\forall b \in \{0, 1\}$ :

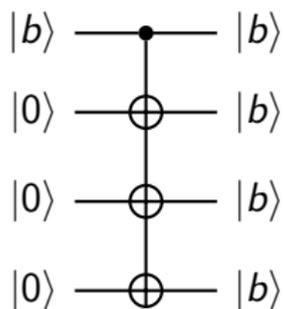


- ▶ Is fanout in  $\text{QAC}^0$ ?
- ▶ Fanout  $\sim$  Parity [GHMP'02]
- ▶ Parity  $\notin \text{AC}^0$  [H'86]
- ▶  $\text{TC}^0 \subseteq \text{QAC}^0[\text{parity/fanout}]$  [HS'05, TT'16]

# Fanout & Motivation

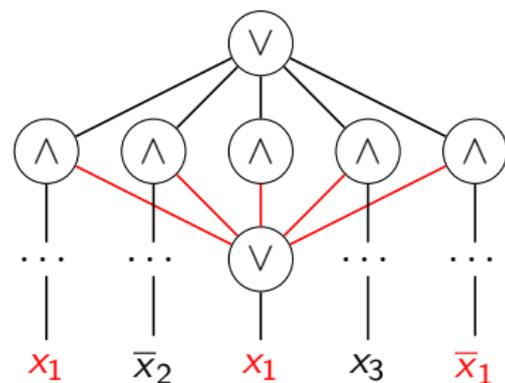


$\forall b \in \{0, 1\}$ :

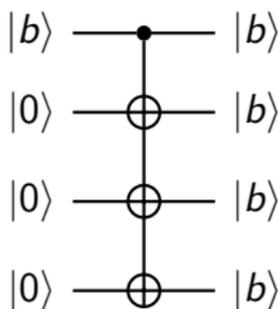


- ▶ Is fanout in  $\text{QAC}^0$ ?
- ▶ Fanout  $\sim$  Parity [GHMP'02]
- ▶ Parity  $\notin \text{AC}^0$  [H'86]
- ▶  $\text{TC}^0 \subseteq \text{QAC}^0[\text{parity/fanout}]$  [HS'05, TT'16]

# Fanout & Motivation

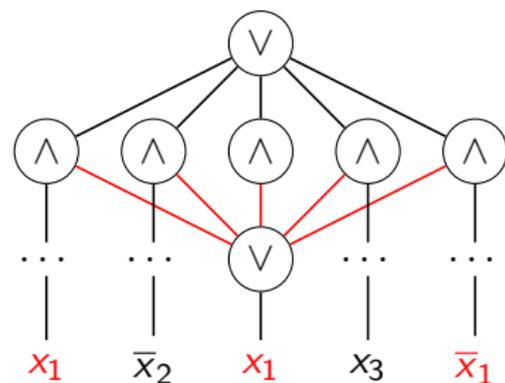


$\forall b \in \{0, 1\}$ :

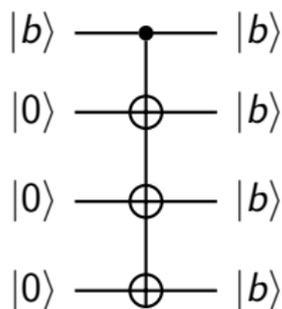


- ▶ Is fanout in  $\text{QAC}^0$ ?
- ▶ Fanout  $\sim$  Parity [GHMP'02]
- ▶ Parity  $\notin \text{AC}^0$  [H'86]
- ▶  $\text{TC}^0 \subseteq \text{QAC}^0[\text{parity/fanout}]$  [HS'05, TT'16]

# Fanout & Motivation

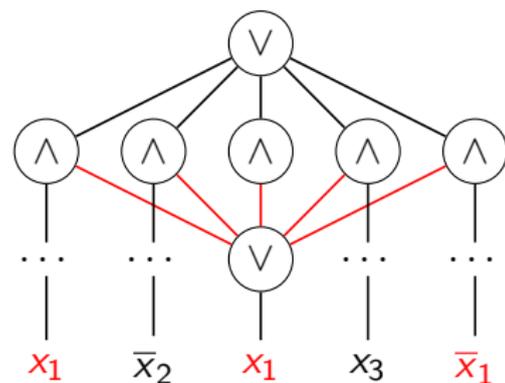


$\forall b \in \{0, 1\}$ :

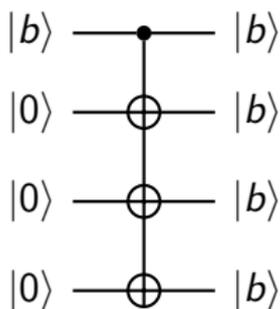


- ▶ Is fanout in  $\text{QAC}^0$ ?
- ▶ Fanout  $\sim$  Parity [GHMP'02]
- ▶ Parity  $\notin \text{AC}^0$  [H'86]
- ▶  $\text{TC}^0 \subseteq \text{QAC}^0[\text{parity/fanout}]$  [HS'05, TT'16]

# Fanout & Motivation



$\forall b \in \{0, 1\}$ :



- ▶ Is fanout in  $\text{QAC}^0$ ?
- ▶ Fanout  $\sim$  Parity [GHMP'02]
- ▶ Parity  $\notin \text{AC}^0$  [H'86]
- ▶  $\text{TC}^0 \subseteq \text{QAC}^0[\text{parity/fanout}]$  [HS'05, TT'16]

# Bounds for Parity/Fanout

## Prior Results

	Depth*	Size*	Ancillae	
U.B.	$\sim \log n$	$O(n)$	$O(n)$	[GHMP'02]
L.B.	$\sim \log(n/(a+1))$	$\infty$	$a$	[FFGHZ'06]
L.B.	2	$\infty$	$\infty$	[PFGT'20]

## Our Results

	Depth*	Size*	Ancillae	Approx.
U.B.	$d \geq 7$	$e^{n^{O(1/d)} \log(n/\varepsilon)}$	$e^{n^{O(1/d)} \log(n/\varepsilon)}$	$1 - \varepsilon$
L.B.	$\sim$ tight for a certain generalization of the U.B. circuit			
L.B.	$d$	$0.2n/(d+1)$	$\infty$	$1/2 + e^{-\Omega(n/d)}$
L.B.	2	$\infty$	$\infty$	$1/2 + e^{-\Omega(n)}$

\*counting *multi-qubit* gates only

# Bounds for Parity/Fanout

## Prior Results

	Depth*	Size*	Ancillae	
U.B.	$\sim \log n$	$O(n)$	$O(n)$	[GHMP'02]
L.B.	$\sim \log(n/(a+1))$	$\infty$	$a$	[FFGHZ'06]
L.B.	2	$\infty$	$\infty$	[PFGT'20]

## Our Results

	Depth*	Size*	Ancillae	Approx.
U.B.	$d \geq 7$	$e^{n^{O(1/d)} \log(n/\varepsilon)}$	$e^{n^{O(1/d)} \log(n/\varepsilon)}$	$1 - \varepsilon$
L.B.	$\sim$ tight for a certain generalization of the U.B. circuit			
L.B.	$d$	$0.2n/(d+1)$	$\infty$	$1/2 + e^{-\Omega(n/d)}$
L.B.	2	$\infty$	$\infty$	$1/2 + e^{-\Omega(n)}$

\* counting *multi-qubit* gates only

# Bounds for Parity/Fanout

## Prior Results

	Depth*	Size*	Ancillae	
U.B.	$\sim \log n$	$O(n)$	$O(n)$	[GHMP'02]
L.B.	$\sim \log(n/(a+1))$	$\infty$	$a$	[FFGHZ'06]
L.B.	2	$\infty$	$\infty$	[PFGT'20]

## Our Results

	Depth*	Size*	Ancillae	Approx.
U.B.	$d \geq 7$	$e^{n^{O(1/d)} \log(n/\varepsilon)}$	$e^{n^{O(1/d)} \log(n/\varepsilon)}$	$1 - \varepsilon$
L.B.	$\sim$ tight for a certain generalization of the U.B. circuit			
L.B.	$d$	$0.2n/(d+1)$	$\infty$	$1/2 + e^{-\Omega(n/d)}$
L.B.	2	$\infty$	$\infty$	$1/2 + e^{-\Omega(n)}$

\*counting *multi-qubit* gates only

# Bounds for Parity/Fanout

## Prior Results

	Depth*	Size*	Ancillae	
U.B.	$\sim \log n$	$O(n)$	$O(n)$	[GHMP'02]
L.B.	$\sim \log(n/(a+1))$	$\infty$	$a$	[FFGHZ'06]
L.B.	2	$\infty$	$\infty$	[PFGT'20]

## Our Results

	Depth*	Size*	Ancillae	Approx.
U.B.	$d \geq 7$	$e^{n^{O(1/d)} \log(n/\varepsilon)}$	$e^{n^{O(1/d)} \log(n/\varepsilon)}$	$1 - \varepsilon$
L.B.	$\sim$ tight for a certain generalization of the U.B. circuit			
L.B.	$d$	$0.2n/(d+1)$	$\infty$	$1/2 + e^{-\Omega(n/d)}$
L.B.	2	$\infty$	$\infty$	$1/2 + e^{-\Omega(n)}$

\*counting *multi-qubit* gates only

# Bounds for Parity/Fanout

## Prior Results

	Depth*	Size*	Ancillae	
U.B.	$\sim \log n$	$O(n)$	$O(n)$	[GHMP'02]
L.B.	$\sim \log(n/(a+1))$	$\infty$	$a$	[FFGHZ'06]
L.B.	2	$\infty$	$\infty$	[PFGT'20]

## Our Results

	Depth*	Size*	Ancillae	Approx.
U.B.	$d \geq 7$	$e^{n^{O(1/d)} \log(n/\varepsilon)}$	$e^{n^{O(1/d)} \log(n/\varepsilon)}$	$1 - \varepsilon$
L.B.	$\sim$ tight for a certain generalization of the U.B. circuit			
L.B.	$d$	$0.2n/(d+1)$	$\infty$	$1/2 + e^{-\Omega(n/d)}$
L.B.	2	$\infty$	$\infty$	$1/2 + e^{-\Omega(n)}$

\*counting *multi-qubit* gates only

# Bounds for Parity/Fanout

## Prior Results

	Depth*	Size*	Ancillae	
U.B.	$\sim \log n$	$O(n)$	$O(n)$	[GHMP'02]
L.B.	$\sim \log(n/(a+1))$	$\infty$	$a$	[FFGHZ'06]
L.B.	2	$\infty$	$\infty$	[PFGT'20]

## Our Results

	Depth*	Size*	Ancillae	Approx.
<b>U.B.</b>	$d \geq 7$	$e^{n^{O(1/d)} \log(n/\varepsilon)}$	$e^{n^{O(1/d)} \log(n/\varepsilon)}$	$1 - \varepsilon$
L.B.	$\sim$ tight for a certain generalization of the U.B. circuit			
L.B.	$d$	$0.2n/(d+1)$	$\infty$	$1/2 + e^{-\Omega(n/d)}$
L.B.	2	$\infty$	$\infty$	$1/2 + e^{-\Omega(n)}$

\*counting *multi-qubit* gates only

# Bounds for Parity/Fanout

## Prior Results

	Depth*	Size*	Ancillae	
U.B.	$\sim \log n$	$O(n)$	$O(n)$	[GHMP'02]
L.B.	$\sim \log(n/(a+1))$	$\infty$	$a$	[FFGHZ'06]
L.B.	2	$\infty$	$\infty$	[PFGT'20]

## Our Results

	Depth*	Size*	Ancillae	Approx.
U.B.	$d \geq 7$	$e^{n^{O(1/d)} \log(n/\varepsilon)}$	$e^{n^{O(1/d)} \log(n/\varepsilon)}$	$1 - \varepsilon$
L.B.	$\sim$ tight for a certain generalization of the U.B. circuit			
L.B.	$d$	$0.2n/(d+1)$	$\infty$	$1/2 + e^{-\Omega(n/d)}$
L.B.	2	$\infty$	$\infty$	$1/2 + e^{-\Omega(n)}$

\*counting *multi-qubit* gates only

# Bounds for Parity/Fanout

## Prior Results

	Depth*	Size*	Ancillae	
U.B.	$\sim \log n$	$O(n)$	$O(n)$	[GHMP'02]
L.B.	$\sim \log(n/(a+1))$	$\infty$	$a$	[FFGHZ'06]
L.B.	2	$\infty$	$\infty$	[PFGT'20]

## Our Results

	Depth*	Size*	Ancillae	Approx.
U.B.	$d \geq 7$	$e^{n^{O(1/d)} \log(n/\varepsilon)}$	$e^{n^{O(1/d)} \log(n/\varepsilon)}$	$1 - \varepsilon$
L.B.	$\sim$ tight for a certain generalization of the U.B. circuit			
L.B.	$d$	$0.2n/(d+1)$	$\infty$	$1/2 + e^{-\Omega(n/d)}$
L.B.	2	$\infty$	$\infty$	$1/2 + e^{-\Omega(n)}$

\*counting *multi-qubit* gates only

# Bounds for Parity/Fanout

## Prior Results

	Depth*	Size*	Ancillae	
U.B.	$\sim \log n$	$O(n)$	$O(n)$	[GHMP'02]
L.B.	$\sim \log(n/(a+1))$	$\infty$	$a$	[FFGHZ'06]
L.B.	2	$\infty$	$\infty$	[PFGT'20]

## Our Results

	Depth*	Size*	Ancillae	Approx.
U.B.	$d \geq 7$	$e^{n^{O(1/d)} \log(n/\varepsilon)}$	$e^{n^{O(1/d)} \log(n/\varepsilon)}$	$1 - \varepsilon$
L.B.	$\sim$ tight for a certain generalization of the U.B. circuit			
L.B.	$d$	$0.2n/(d+1)$	$\infty$	$1/2 + e^{-\Omega(n/d)}$
L.B.	2	$\infty$	$\infty$	$1/2 + e^{-\Omega(n)}$

\*counting *multi-qubit* gates only

# Bounds for Parity/Fanout

## Prior Results

	Depth*	Size*	Ancillae	
U.B.	$\sim \log n$	$O(n)$	$O(n)$	[GHMP'02]
L.B.	$\sim \log(n/(a+1))$	$\infty$	$a$	[FFGHZ'06]
L.B.	2	$\infty$	$\infty$	[PFGT'20]

## Our Results

	Depth*	Size*	Ancillae	Approx.
U.B.	$d \geq 7$	$e^{n^{O(1/d)} \log(n/\varepsilon)}$	$e^{n^{O(1/d)} \log(n/\varepsilon)}$	$1 - \varepsilon$
L.B.	$\sim$ tight for a certain generalization of the U.B. circuit			
L.B.	$d$	$0.2n/(d+1)$	$\infty$	$1/2 + e^{-\Omega(n/d)}$
L.B.	2	$\infty$	$\infty$	$1/2 + e^{-\Omega(n)}$

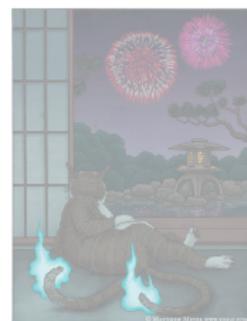
\*counting *multi-qubit* gates only

# Parity/Fanout $\sim$ Nekomata

Cat State	Nekomata
$\frac{1}{\sqrt{2}} \sum_{b=0}^1  b\rangle^n$	$\frac{1}{\sqrt{2}} \sum_{b=0}^1  b\rangle^n  \psi_b\rangle$
	

- ▶ I.e. some  $n$  qubits of a nekomata measure to  $0^n$  and  $1^n$  each with probability  $1/2$ .
- ▶  $\Rightarrow$  [GHMP'02]:  
Fanout  $\left( \frac{|0\rangle + |1\rangle}{\sqrt{2}} |0\rangle^{n-1} \right) = \frac{1}{\sqrt{2}} \sum_{b=0}^1 \text{Fanout} \left( |b\rangle |0\rangle^{n-1} \right) = |\text{Nekomata}\rangle$ .
- ▶  $\Leftarrow$ : Next slide.

# Parity/Fanout $\sim$ Nekomata

Cat State	Nekomata
$\frac{1}{\sqrt{2}} \sum_{b=0}^1  b\rangle^n$	$\frac{1}{\sqrt{2}} \sum_{b=0}^1  b\rangle^n  \psi_b\rangle$
	

- ▶ I.e. some  $n$  qubits of a nekomata measure to  $0^n$  and  $1^n$  each with probability  $1/2$ .
- ▶  $\Rightarrow$  [GHMP'02]:  
Fanout  $\left( \frac{|0\rangle + |1\rangle}{\sqrt{2}} |0\rangle^{n-1} \right) = \frac{1}{\sqrt{2}} \sum_{b=0}^1 \text{Fanout} \left( |b\rangle |0\rangle^{n-1} \right) = |\text{猫}\rangle$ .
- ▶  $\Leftarrow$ : Next slide.

# Parity/Fanout $\sim$ Nekomata

Cat State	Nekomata
$\frac{1}{\sqrt{2}} \sum_{b=0}^1  b\rangle^n$	$\frac{1}{\sqrt{2}} \sum_{b=0}^1  b\rangle^n  \psi_b\rangle$
	

- ▶ I.e. some  $n$  qubits of a nekomata measure to  $0^n$  and  $1^n$  each with probability  $1/2$ .
- ▶  $\Rightarrow$  [GHMP'02]:  
Fanout  $\left( \frac{|0\rangle + |1\rangle}{\sqrt{2}} |0\rangle^{n-1} \right) = \frac{1}{\sqrt{2}} \sum_{b=0}^1 \text{Fanout} \left( |b\rangle |0\rangle^{n-1} \right) = |\text{Nekomata}\rangle$ .
- ▶  $\Leftarrow$ : Next slide.

# Parity/Fanout $\sim$ Nekomata

Cat State	Nekomata
$\frac{1}{\sqrt{2}} \sum_{b=0}^1  b\rangle^n$	$\frac{1}{\sqrt{2}} \sum_{b=0}^1  b\rangle^n  \psi_b\rangle$
	

- ▶ I.e. some  $n$  qubits of a nekomata measure to  $0^n$  and  $1^n$  each with probability  $1/2$ .
- ▶  $\Rightarrow$  [GHMP'02]:  
Fanout  $\left( \frac{|0\rangle + |1\rangle}{\sqrt{2}} |0\rangle^{n-1} \right) = \frac{1}{\sqrt{2}} \sum_{b=0}^1 \text{Fanout} \left( |b\rangle |0\rangle^{n-1} \right) = |\text{Nekomata}\rangle$ .
- ▶  $\Leftarrow$ : Next slide.

# Parity/Fanout $\sim$ Nekomata

Cat State	Nekomata
$\frac{1}{\sqrt{2}} \sum_{b=0}^1  b\rangle^n$	$\frac{1}{\sqrt{2}} \sum_{b=0}^1  b\rangle^n  \psi_b\rangle$
	

- ▶ I.e. some  $n$  qubits of a nekomata measure to  $0^n$  and  $1^n$  each with probability  $1/2$ .
- ▶  $\Rightarrow$  [GHMP'02]:  
Fanout  $\left( \frac{|0\rangle + |1\rangle}{\sqrt{2}} |0\rangle^{n-1} \right) = \frac{1}{\sqrt{2}} \sum_{b=0}^1 \text{Fanout}(|b\rangle |0\rangle^{n-1}) = |\text{Nekomata}\rangle$ .
- ▶  $\Leftarrow$ : Next slide.

# Parity/Fanout $\sim$ Nekomata

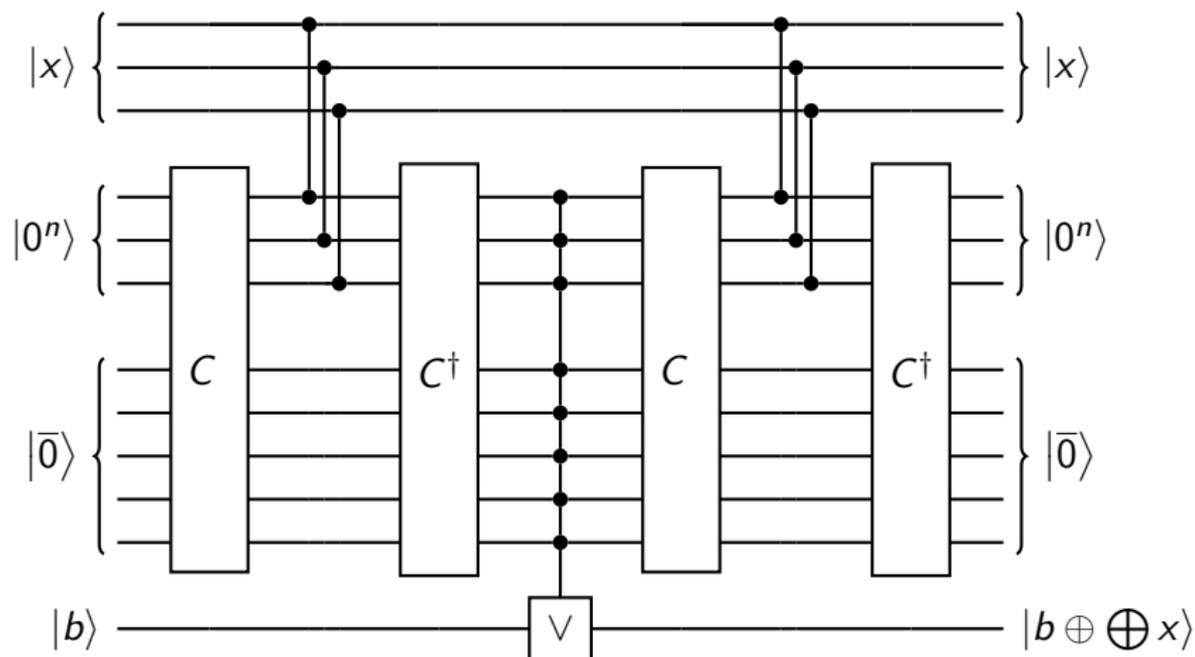
Cat State	Nekomata
$\frac{1}{\sqrt{2}} \sum_{b=0}^1  b\rangle^n$	$\frac{1}{\sqrt{2}} \sum_{b=0}^1  b\rangle^n  \psi_b\rangle$
	

- ▶ I.e. some  $n$  qubits of a nekomata measure to  $0^n$  and  $1^n$  each with probability  $1/2$ .
- ▶  $\Rightarrow$  [GHMP'02]:  

$$\text{Fanout}\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}|0\rangle^{n-1}\right) = \frac{1}{\sqrt{2}} \sum_{b=0}^1 \text{Fanout}\left(|b\rangle|0\rangle^{n-1}\right) = |\text{cat}\rangle.$$
- ▶  $\Leftarrow$ : Next slide.

# Nekomata $\Rightarrow$ Parity

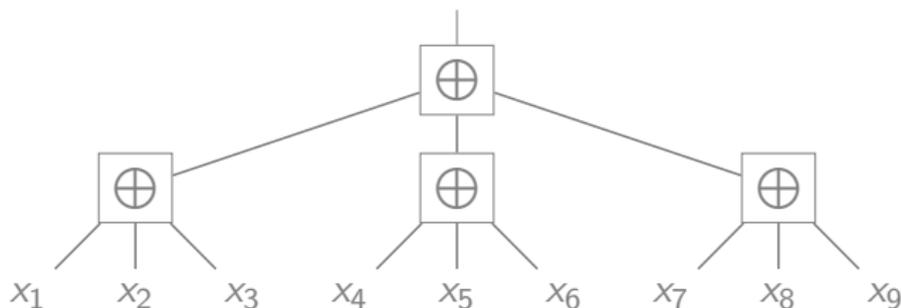
- ▶ If  $C|\bar{0}\rangle$  is a nekomata ( $\frac{1}{\sqrt{2}} \sum_{b=0}^1 |b\rangle^n |\psi_b\rangle$ ) then:



# Upper Bounds for Approximate Parity/Fanout

	Depth	Size	Ancillae	Approx.
U.B.	$d \geq 7$	$e^{n^{O(1/d)} \log(n/\varepsilon)}$	$e^{n^{O(1/d)} \log(n/\varepsilon)}$	$1 - \varepsilon$

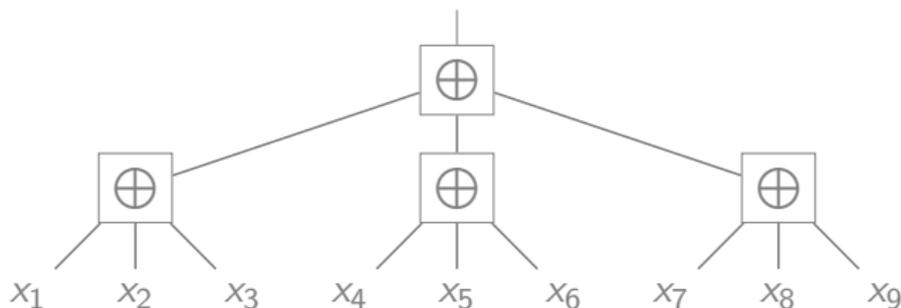
- ▶ Depth-2 exponential-size U.B. for approximate nekomata  $\Rightarrow$  depth-11 U.B.
- ▶ Further optimization  $\Rightarrow$  depth-7 U.B.
- ▶ Downward self-reducibility of parity  $\Rightarrow$  depth- $d$  U.B.



# Upper Bounds for Approximate Parity/Fanout

	Depth	Size	Ancillae	Approx.
U.B.	$d \geq 7$	$e^{n^{O(1/d)} \log(n/\varepsilon)}$	$e^{n^{O(1/d)} \log(n/\varepsilon)}$	$1 - \varepsilon$

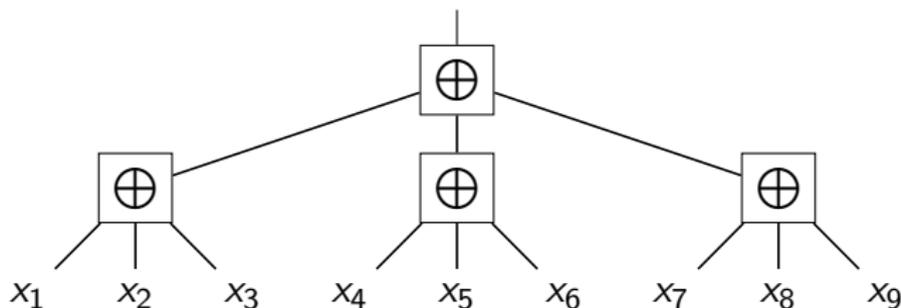
- ▶ Depth-2 exponential-size U.B. for approximate nekomata  $\Rightarrow$  depth-11 U.B.
- ▶ Further optimization  $\Rightarrow$  depth-7 U.B.
- ▶ Downward self-reducibility of parity  $\Rightarrow$  depth- $d$  U.B.



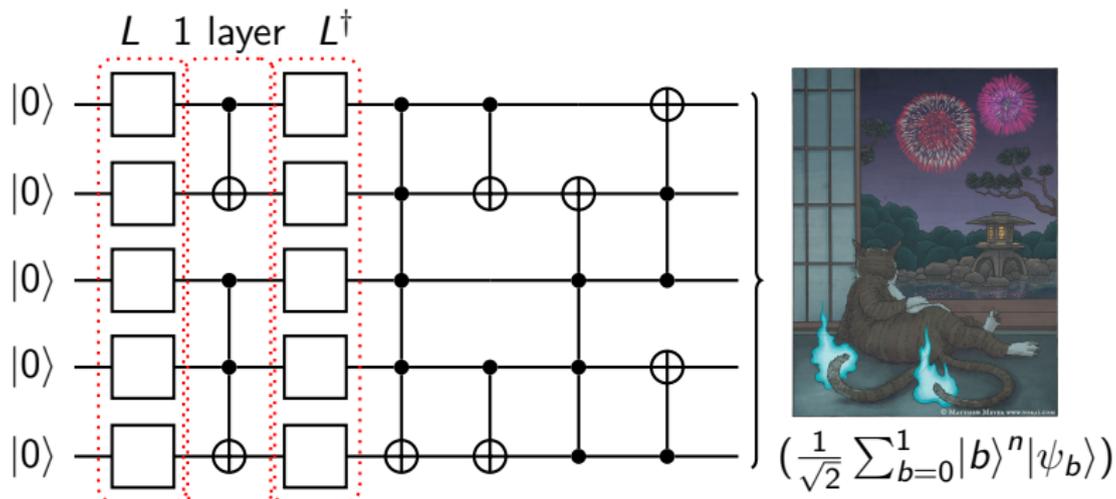
# Upper Bounds for Approximate Parity/Fanout

	Depth	Size	Ancillae	Approx.
U.B.	$d \geq 7$	$e^{n^{O(1/d)} \log(n/\varepsilon)}$	$e^{n^{O(1/d)} \log(n/\varepsilon)}$	$1 - \varepsilon$

- ▶ Depth-2 exponential-size U.B. for approximate nekomata  $\Rightarrow$  depth-11 U.B.
- ▶ Further optimization  $\Rightarrow$  depth-7 U.B.
- ▶ Downward self-reducibility of parity  $\Rightarrow$  depth- $d$  U.B.



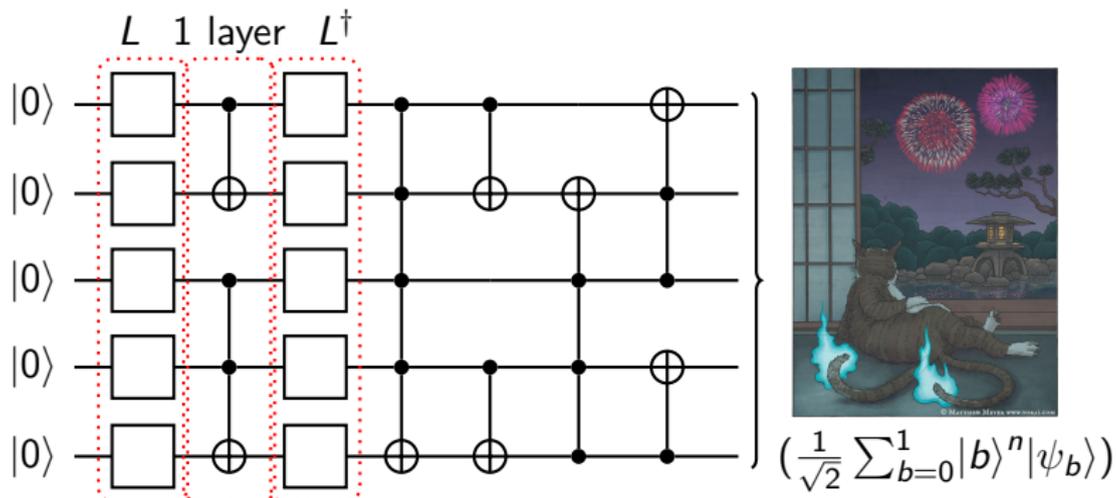
# Bounds for Nekomata in “Mostly Classical” Circuits



	Depth	Size	# Qubits	Approx.
<b>U.B.</b>	2	$e^{O(n \log(n/\varepsilon))}$	$e^{O(n \log(n/\varepsilon))}$	$\geq 1 - \varepsilon$
<b>L.B.</b>	$o(\log n)$	$e^{n^{1-\Omega(1)}}$	$\infty$	$\leq 1/2 + e^{-n^{\Omega(1)}}$

► Approx. =  $\max |\langle \nu | C | \bar{0} \rangle|^2$  over all nekomata  $|\nu\rangle$ .

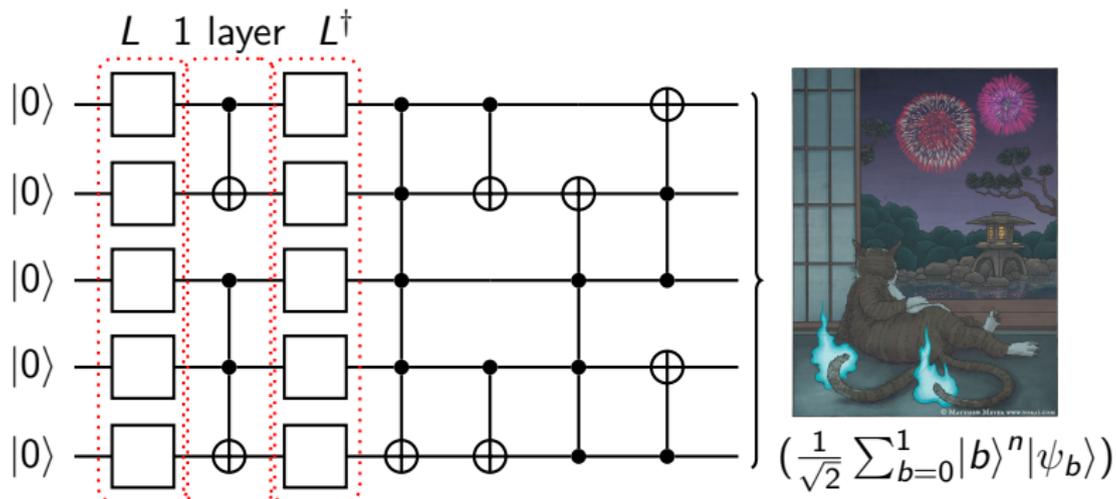
# Bounds for Nekomata in “Mostly Classical” Circuits



	Depth	Size	# Qubits	Approx.
<b>U.B.</b>	2	$e^{O(n \log(n/\varepsilon))}$	$e^{O(n \log(n/\varepsilon))}$	$\geq 1 - \varepsilon$
<b>L.B.</b>	$o(\log n)$	$e^{n^{1-\Omega(1)}}$	$\infty$	$\leq 1/2 + e^{-n^{\Omega(1)}}$

► Approx. =  $\max |\langle \nu | C | \bar{0} \rangle|^2$  over all nekomata  $|\nu\rangle$ .

# Bounds for Nekomata in “Mostly Classical” Circuits



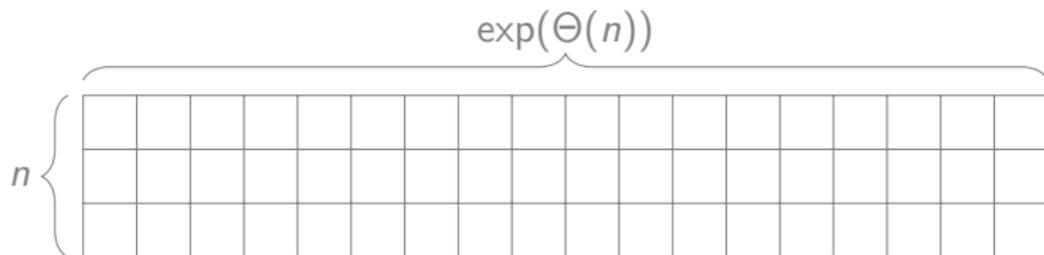
	Depth	Size	# Qubits	Approx.
<b>U.B.</b>	2	$e^{O(n \log(n/\varepsilon))}$	$e^{O(n \log(n/\varepsilon))}$	$\geq 1 - \varepsilon$
<b>L.B.</b>	$o(\log n)$	$e^{n^{1-\Omega(1)}}$	$\infty$	$\leq 1/2 + e^{-n^{\Omega(1)}}$

► Approx. =  $\max |\langle \nu | C | \bar{0} \rangle|^2$  over all nekomata  $|\nu\rangle$ .

# Bounds for Nekomata in M.C. Circuits – Proofs

*Upper Bound:*

- ▶ Goal: sample  $0^n$  and  $1^n$  each with probability  $\approx 1/2$ .



1. In each column, independently sample  $1^n$  with probability  $\exp(-\Theta(n))$  and  $0^n$  otherwise.
  - ▶  $(I - 2|\tilde{1}^n\rangle\langle\tilde{1}^n|)|0^n\rangle$  where  $|\tilde{1}\rangle \approx |1\rangle$
2. Compute the OR of each row.

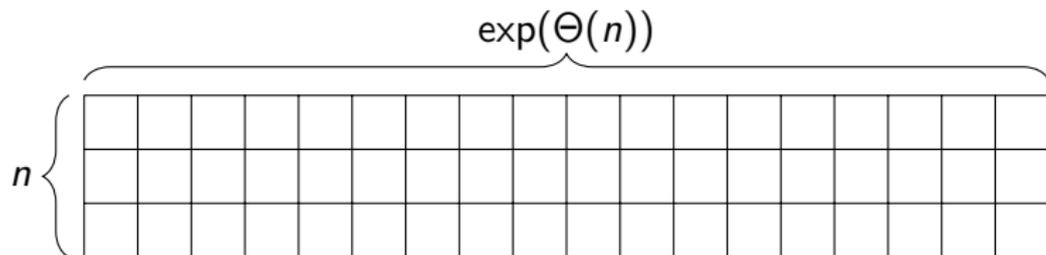
*Lower Bound:*

- ▶ Concentration inequality for Hamming weight, via [GLSS'15].

# Bounds for Nekomata in M.C. Circuits – Proofs

*Upper Bound:*

- ▶ Goal: sample  $0^n$  and  $1^n$  each with probability  $\approx 1/2$ .



1. In each column, independently sample  $1^n$  with probability  $\exp(-\Theta(n))$  and  $0^n$  otherwise.
  - ▶  $(I - 2|\tilde{1}^n\rangle\langle\tilde{1}^n|)|0^n\rangle$  where  $|\tilde{1}\rangle \approx |1\rangle$
2. Compute the OR of each row.

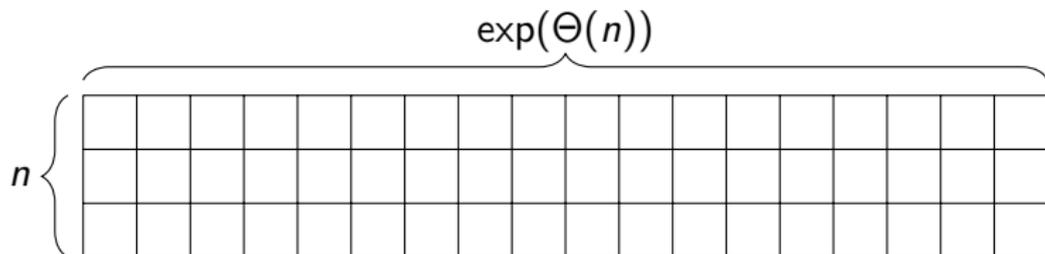
*Lower Bound:*

- ▶ Concentration inequality for Hamming weight, via [GLSS'15].

# Bounds for Nekomata in M.C. Circuits – Proofs

*Upper Bound:*

- ▶ Goal: sample  $0^n$  and  $1^n$  each with probability  $\approx 1/2$ .



1. In each column, independently sample  $1^n$  with probability  $\exp(-\Theta(n))$  and  $0^n$  otherwise.
  - ▶  $(I - 2|\tilde{1}^n\rangle\langle\tilde{1}^n|)|0^n\rangle$  where  $|\tilde{1}\rangle \approx |1\rangle$
2. Compute the OR of each row.

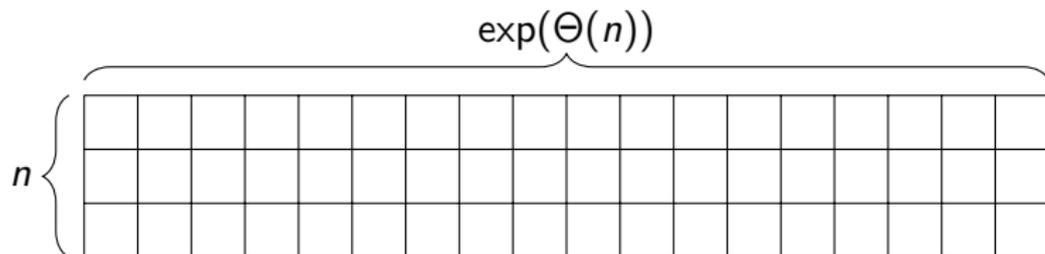
*Lower Bound:*

- ▶ Concentration inequality for Hamming weight, via [GLSS'15].

# Bounds for Nekomata in M.C. Circuits – Proofs

*Upper Bound:*

- ▶ Goal: sample  $0^n$  and  $1^n$  each with probability  $\approx 1/2$ .



1. In each column, independently sample  $1^n$  with probability  $\exp(-\Theta(n))$  and  $0^n$  otherwise.
  - ▶  $(I - 2|\tilde{1}^n\rangle\langle\tilde{1}^n|)|0^n\rangle$  where  $|\tilde{1}\rangle \approx |1\rangle$
2. Compute the OR of each row.

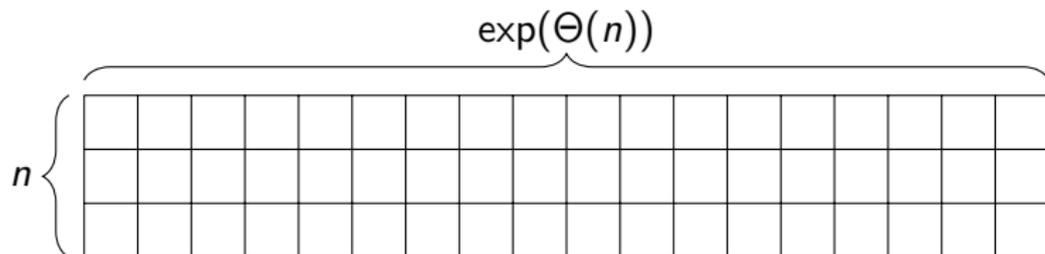
*Lower Bound:*

- ▶ Concentration inequality for Hamming weight, via [GLSS'15].

# Bounds for Nekomata in M.C. Circuits – Proofs

*Upper Bound:*

- ▶ Goal: sample  $0^n$  and  $1^n$  each with probability  $\approx 1/2$ .



1. In each column, independently sample  $1^n$  with probability  $\exp(-\Theta(n))$  and  $0^n$  otherwise.
  - ▶  $(I - 2|\tilde{1}^n\rangle\langle\tilde{1}^n|)|0^n\rangle$  where  $|\tilde{1}\rangle \approx |1\rangle$
2. Compute the OR of each row.

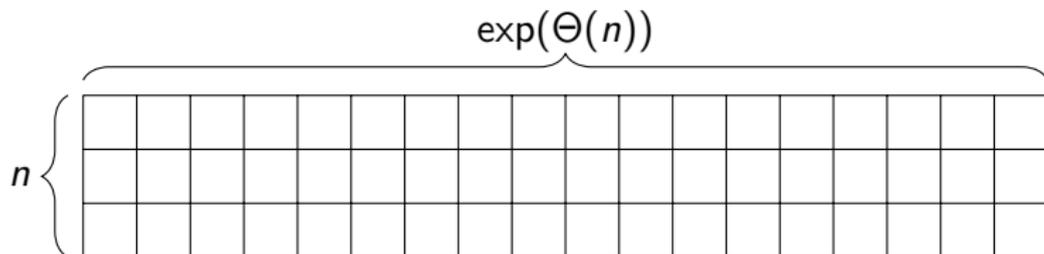
*Lower Bound:*

- ▶ Concentration inequality for Hamming weight, via [GLSS'15].

# Bounds for Nekomata in M.C. Circuits – Proofs

*Upper Bound:*

- ▶ Goal: sample  $0^n$  and  $1^n$  each with probability  $\approx 1/2$ .



1. In each column, independently sample  $1^n$  with probability  $\exp(-\Theta(n))$  and  $0^n$  otherwise.
  - ▶  $(I - 2|\tilde{1}^n\rangle\langle\tilde{1}^n|)|0^n\rangle$  where  $|\tilde{1}\rangle \approx |1\rangle$
2. Compute the OR of each row.

*Lower Bound:*

- ▶ Concentration inequality for Hamming weight, via [GLSS'15].

# Remaining Proof Summaries & Result Clarifications

## Depth- $d$ , Size- $0.2n/(d + 1)$ Circuits $C$ :

- ▶ Normal form (see next slide) & triangle inequality  $\Rightarrow$  L.B. for nekomata:
- ▶  $|\langle \nu | C | \bar{0} \rangle|^2 \leq 1/2 + e^{-\Omega(n/d)}$  for all nekomata  $|\nu\rangle$ .
- ▶ Implies L.B. for parity/fanout.

## Depth-2 Circuits $C$ :

- ▶ Measure ancillae to kill off gates, apply (a generalization of) the above theorem  $\Rightarrow$  L.B. for  $|\boxtimes\rangle$ :
- ▶  $|\langle \boxtimes, \psi | C | \bar{0} \rangle|^2 \leq 1/2 + e^{-\Omega(n)}$  for all states  $|\psi\rangle$ .
- ▶ Implies L.B. for parity/fanout.

# Remaining Proof Summaries & Result Clarifications

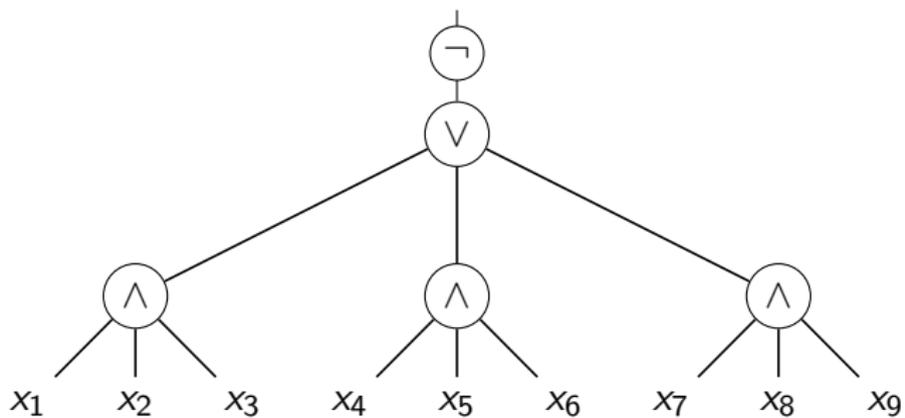
## Depth- $d$ , Size- $0.2n/(d + 1)$ Circuits $C$ :

- ▶ Normal form (see next slide) & triangle inequality  $\Rightarrow$  L.B. for nekomata:
- ▶  $|\langle \nu | C | \bar{0} \rangle|^2 \leq 1/2 + e^{-\Omega(n/d)}$  for all nekomata  $|\nu\rangle$ .
- ▶ Implies L.B. for parity/fanout.

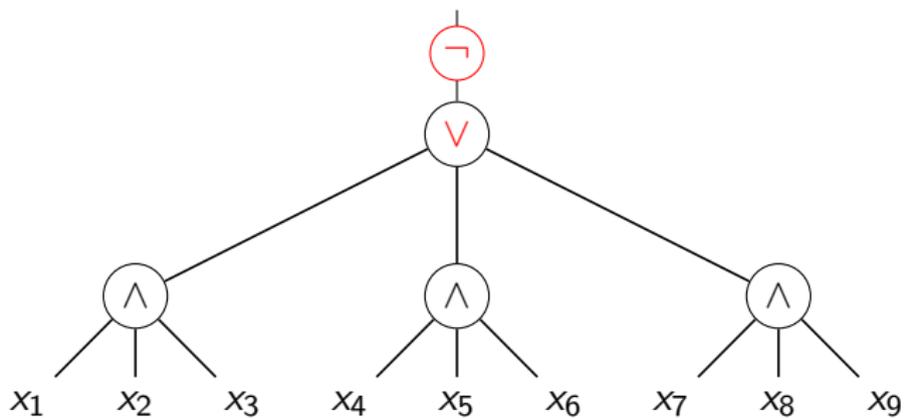
## Depth-2 Circuits $C$ :

- ▶ Measure ancillae to kill off gates, apply (a generalization of) the above theorem  $\Rightarrow$  L.B. for  $|\boxtimes\rangle$ :
- ▶  $|\langle \boxtimes, \psi | C | \bar{0} \rangle|^2 \leq 1/2 + e^{-\Omega(n)}$  for all states  $|\psi\rangle$ .
- ▶ Implies L.B. for parity/fanout.

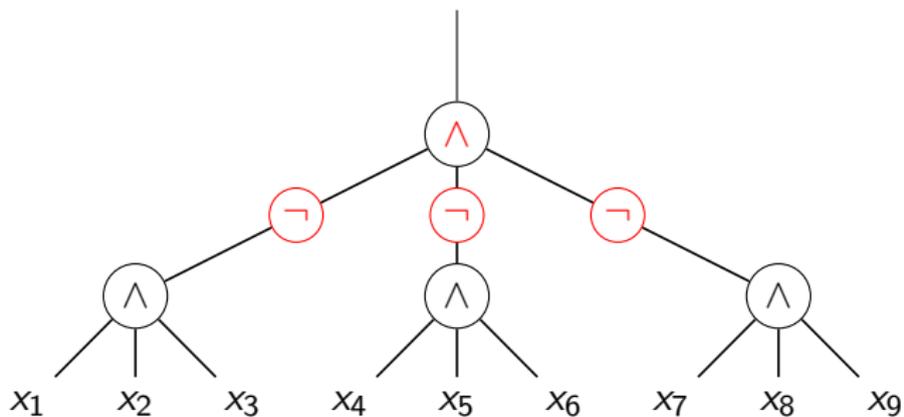
# A Normal Form for QAC Circuits



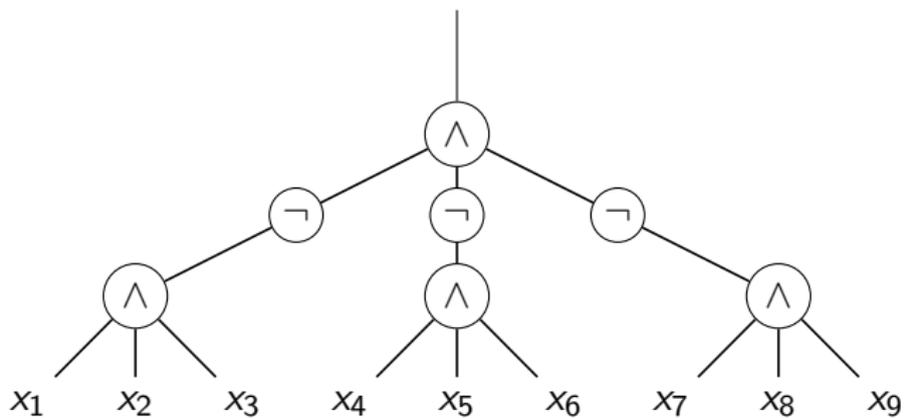
# A Normal Form for QAC Circuits



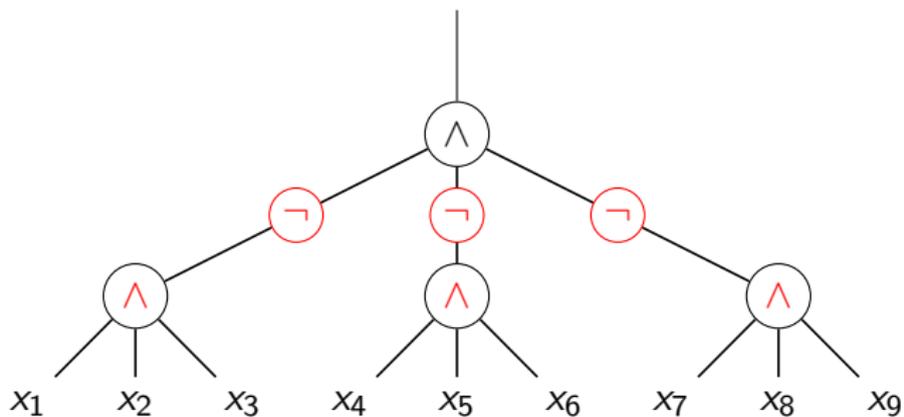
## A Normal Form for QAC Circuits



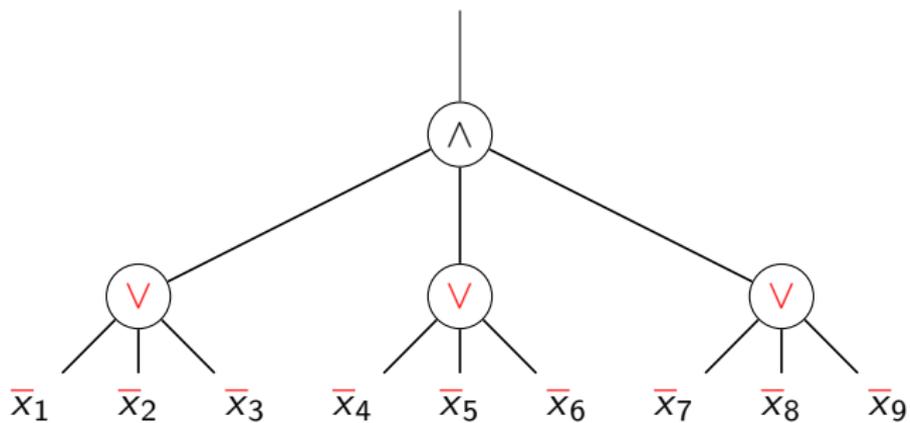
# A Normal Form for QAC Circuits



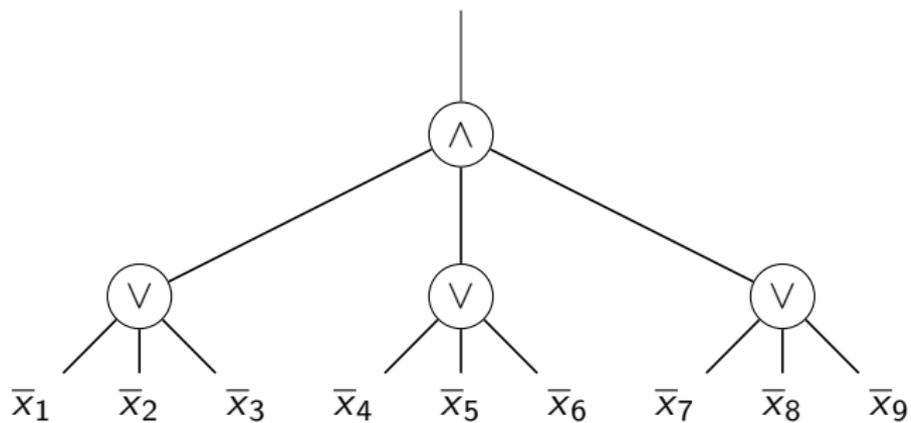
# A Normal Form for QAC Circuits



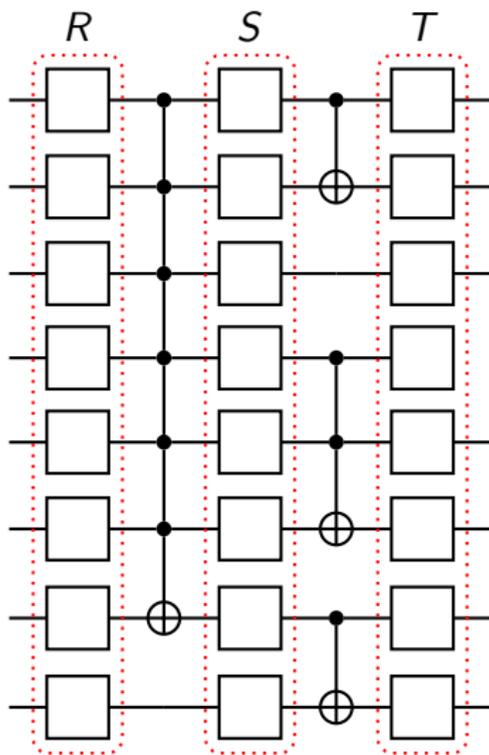
# A Normal Form for QAC Circuits



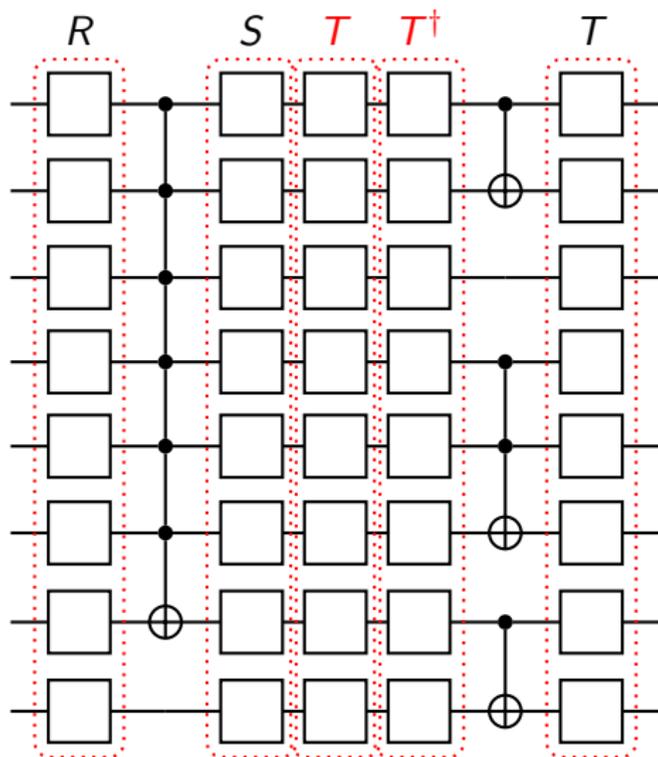
## A Normal Form for QAC Circuits



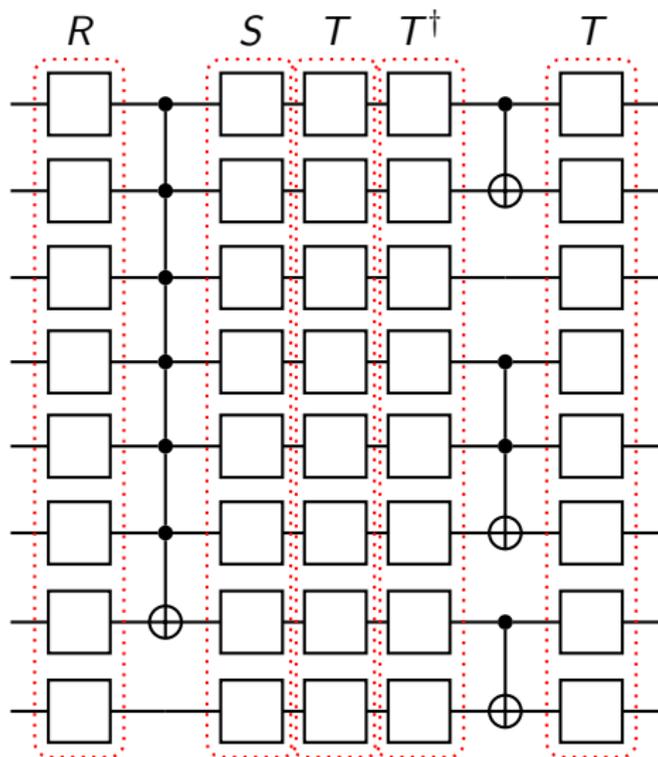
# A Normal Form for QAC Circuits



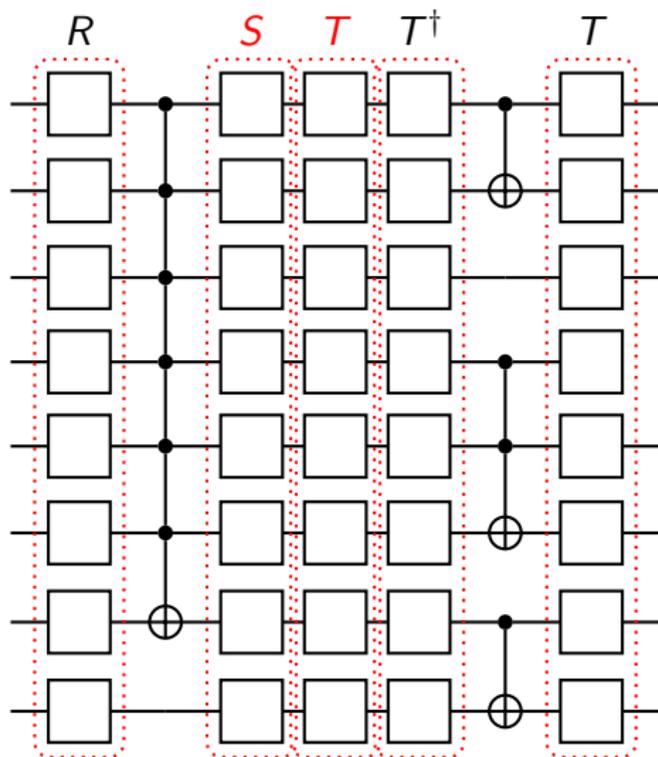
# A Normal Form for QAC Circuits



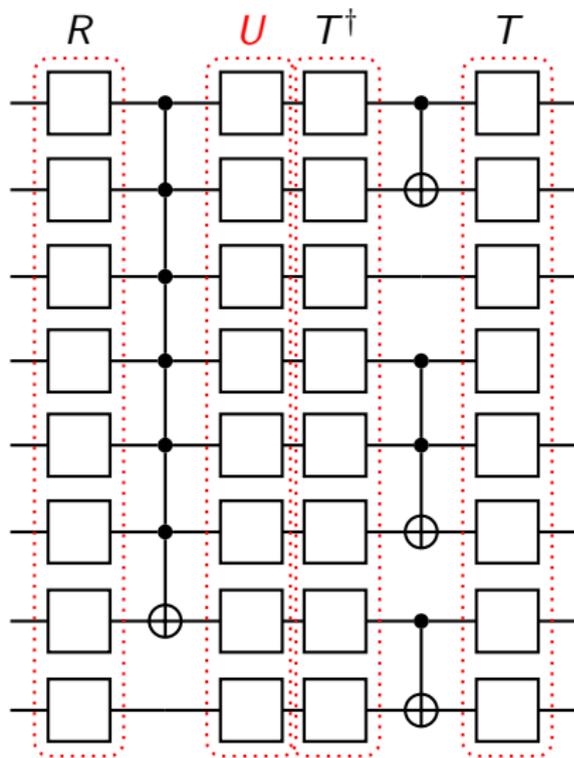
# A Normal Form for QAC Circuits



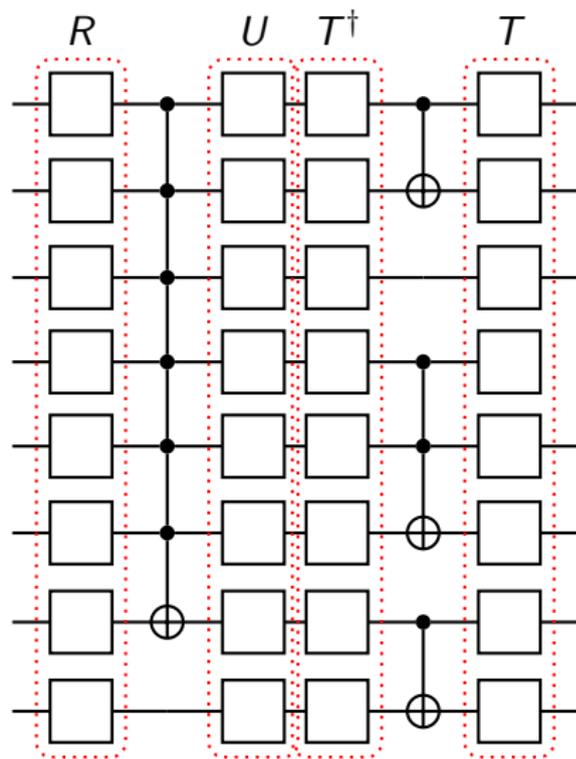
# A Normal Form for QAC Circuits



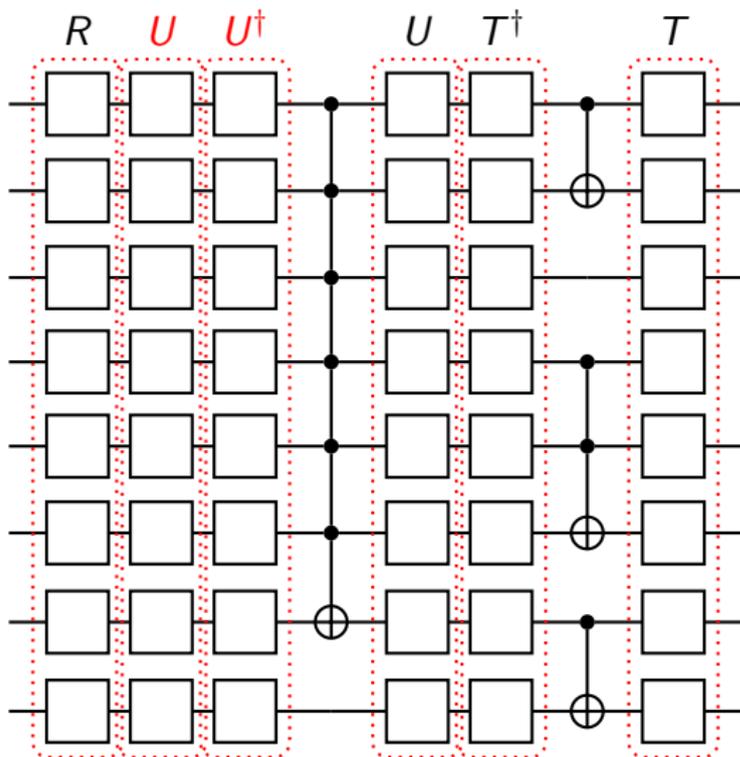
# A Normal Form for QAC Circuits



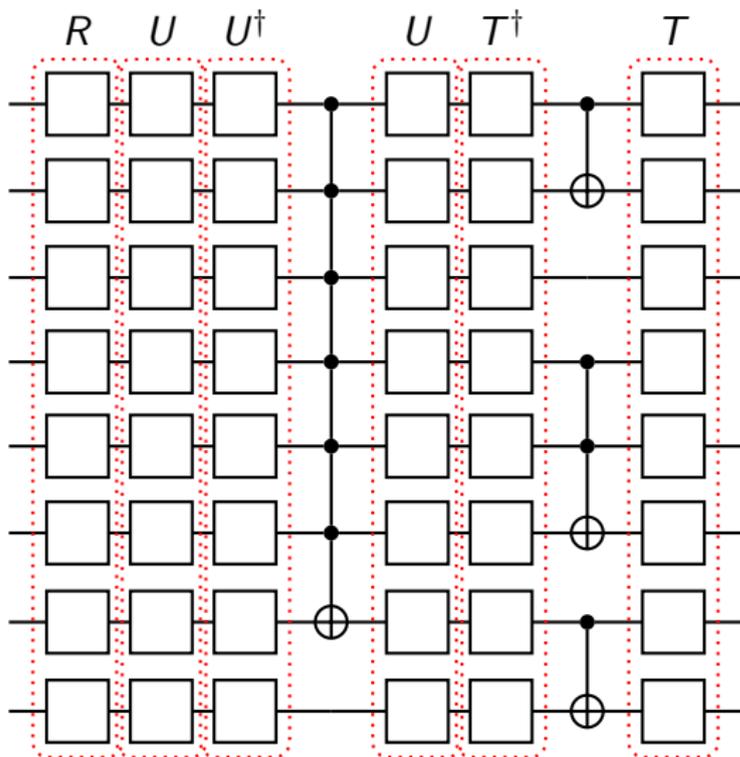
# A Normal Form for QAC Circuits



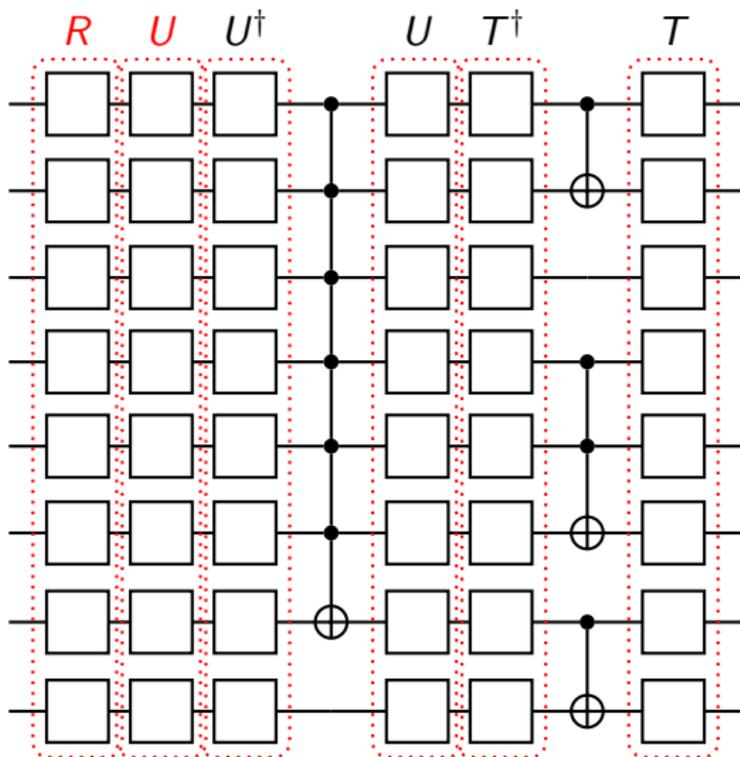
# A Normal Form for QAC Circuits



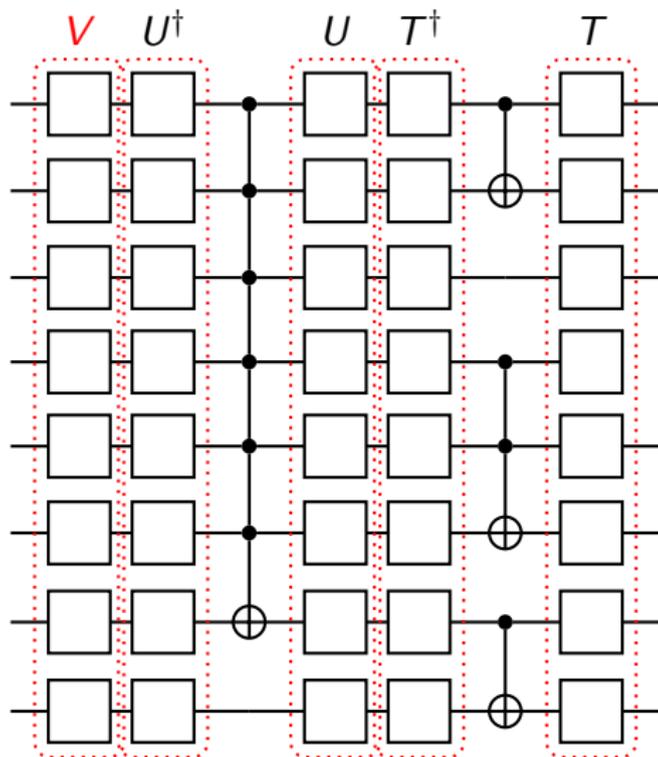
# A Normal Form for QAC Circuits



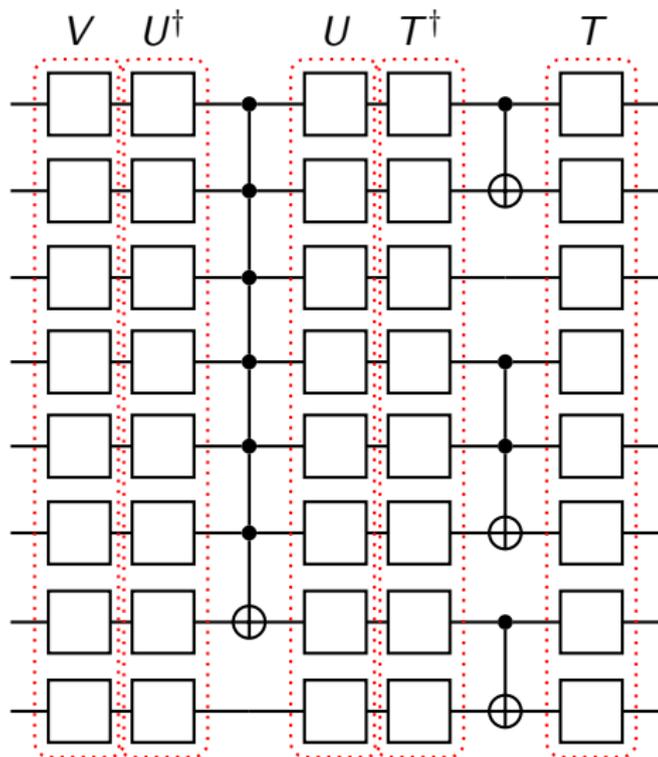
# A Normal Form for QAC Circuits



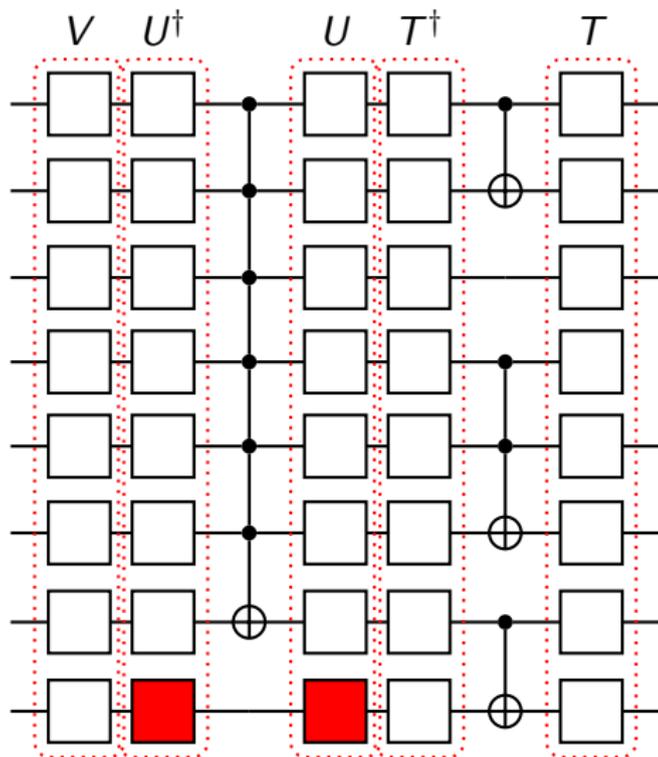
# A Normal Form for QAC Circuits



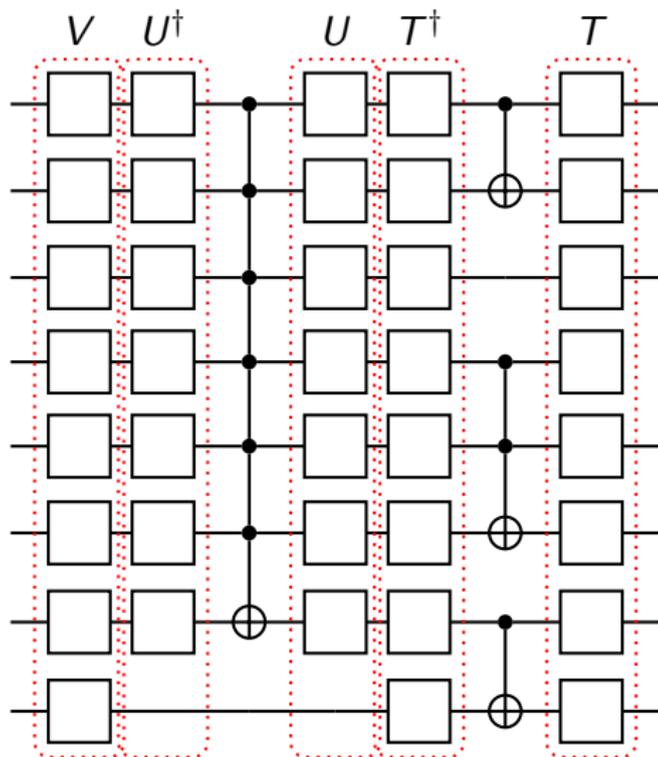
# A Normal Form for QAC Circuits



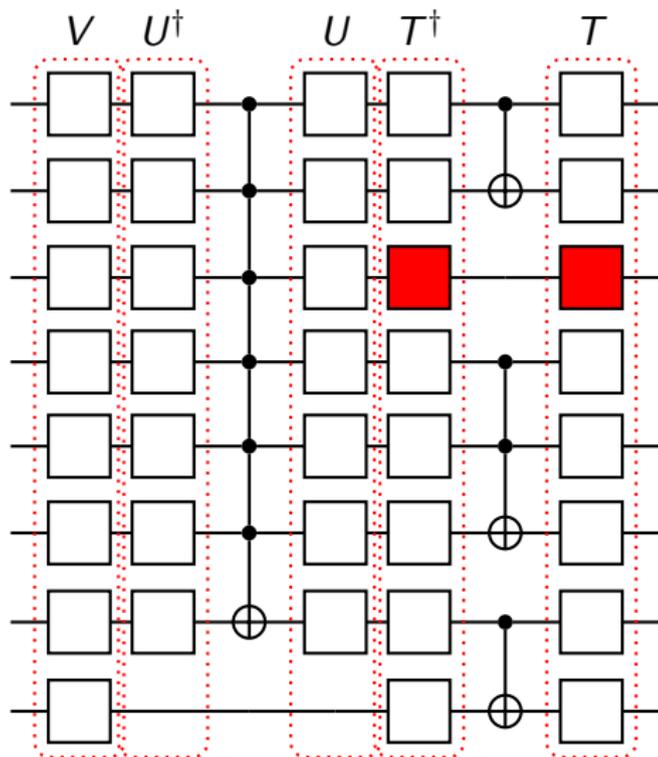
# A Normal Form for QAC Circuits



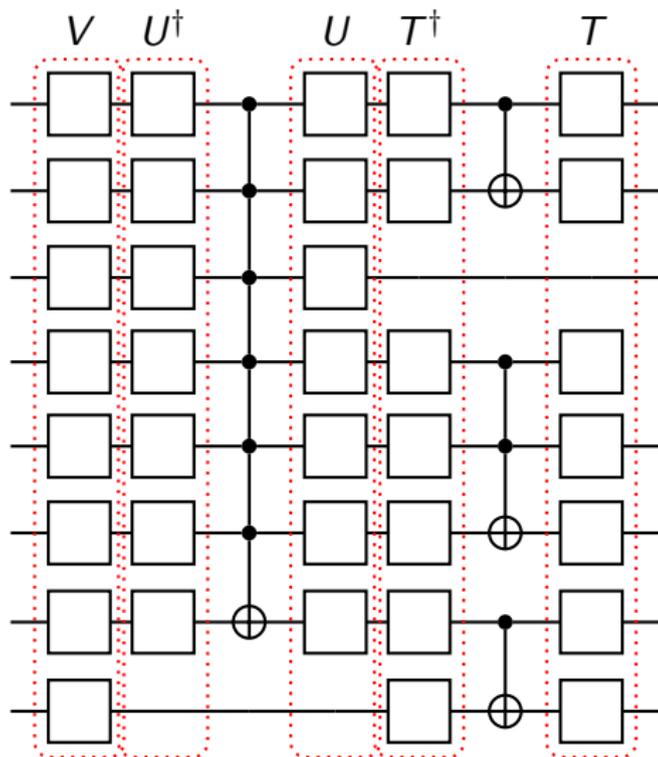
# A Normal Form for QAC Circuits



# A Normal Form for QAC Circuits

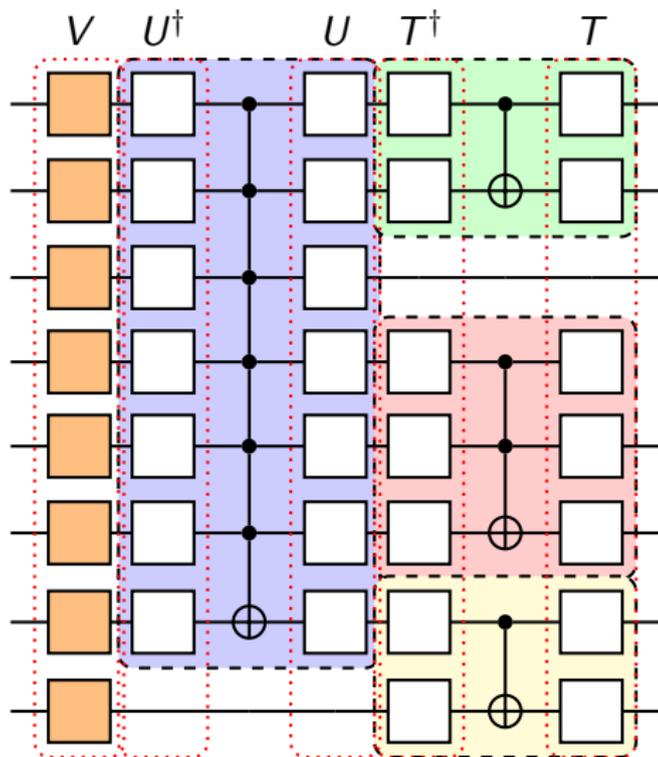


# A Normal Form for QAC Circuits



# A Normal Form for QAC Circuits

- ▶ eigenvalues  $1, \dots, 1, -1$
- ▶  $-1$  eigenvector is product of one-qubit states



# A Normal Form for QAC Circuits

- ▶ eigenvalues  $1, \dots, 1, -1$
- ▶  $-1$  eigenvector is product of one-qubit states

