On Pauli-based computation

Group: Quantum and Linear Optical Computation (INL)
PhD Project: Optimizing models of hybrid quantum/classical computation

F. C. R. Peres | 7th of July 2021 → (cont.) 2nd of March 2022

Supervisor: Professor Ernesto Galvão
Co-supervisor: Professor João Lopes dos Santos

Presentation overview

1. Introductory concepts

Presentation overview

1. Introductory concepts

2. PBC: universality and resource minimization

Presentation overview

1. Introductory concepts

2. PBC: universality and resource minimization

3. PBC and hybrid computation

Key definition: [Pauli operators on n qubits]

$$P = \alpha \sigma_1^{(i)} \otimes \sigma_2^{(j)} \otimes \ldots \otimes \sigma_n^{(k)}$$

$$\{\pm 1, \ \pm i\}$$

$$\sigma^{(i)} = \{I, X, Y, Z\}$$

Concept: [PAULI GROUP ON n QUBITS]

$4 \cdot 4^n$ elements

$\pm 1, \ \pm i$

I, X, Y, Z

Example: [Pauli Group - $n = 1$]

$$\mathscr{P}_1 = \{\pm I,\ \pm iI,\ \pm X,\ \pm iX,\ \pm Y,\ \pm iY,\ \pm Z,\ \pm iZ\}$$

~~$\mathscr{P}_1 = \langle X,\ Y,\ Z \rangle$~~ or $\mathscr{P}_1 = \langle X, Z \rangle$ & phase i

Example: [Pauli Group - $n = 2$]

$$\mathcal{P}_2 = \langle X \otimes I,\, I \otimes X,\, Z \otimes I,\, I \otimes Z \rangle$$

$$P = iY \otimes Z \;= (Z \otimes I)(X \otimes I)(I \otimes Z)$$

$$P' = Y \otimes Z \;= -i(Z \otimes I)(X \otimes I)(I \otimes Z)$$

$2n$ generators

$$\mathscr{P}_n = \langle X_1, X_2, \ldots, X_n, Z_1, Z_2, \ldots, Z_n \rangle$$

Definition: [Clifford Unitary]

$$C\mathscr{P}_n C^\dagger = \mathscr{P}_n \Leftrightarrow CP_iC^\dagger = P_j\,.$$

Generators:

- Hadamard (H);
- Phase (S);
- Controlled-NOT (CX) gates.

Action of the Hadamard gate:

$$X \longrightarrow HXH^\dagger = Z$$

$$H = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$Z \longrightarrow HZH^\dagger = X$$

Action of the phase gate:

$$S = \mathrm{diag}\,(1, i)$$

$$X \longrightarrow SXS^{\dagger} = Y$$

$$Z \longrightarrow SZS^{\dagger} = Z$$

Action of the controlled-NOT gate:

$$(X \otimes I) \longrightarrow (X \otimes X)$$

$$(I \otimes X) \longrightarrow (I \otimes X)$$

$$CX_{12} = \begin{pmatrix} I & 0 \\ 0 & X \end{pmatrix}$$

$$(Z \otimes I) \longrightarrow (Z \otimes I)$$

$$(I \otimes Z) \longrightarrow (Z \otimes Z)$$

Definition: [STABILIZER STATE OF n QUBITS]

$$P_i \left|\psi\right\rangle = \left|\psi\right\rangle, \ \ \forall P_i \in \mathcal{S} = \left\langle P_1, \ldots, P_n \right\rangle$$

Examples: [2-QUBIT STATES]

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

$$\mathcal{S} = \langle X \otimes X, Z \otimes Z \rangle$$

Examples: [2-QUBIT STATES]

$$|0\rangle \otimes \frac{|0\rangle + e^{i\pi/2}|1\rangle}{\sqrt{2}} \qquad \mathcal{S} = \langle Z \otimes I, I \otimes Y \rangle$$

Examples: [2-QUBIT STATES]

$$|0\rangle \otimes \frac{|0\rangle + e^{i\pi/4}|1\rangle}{\sqrt{2}}$$

Eigenvector of

$$Z \otimes I$$

Examples: [2-QUBIT STATES]

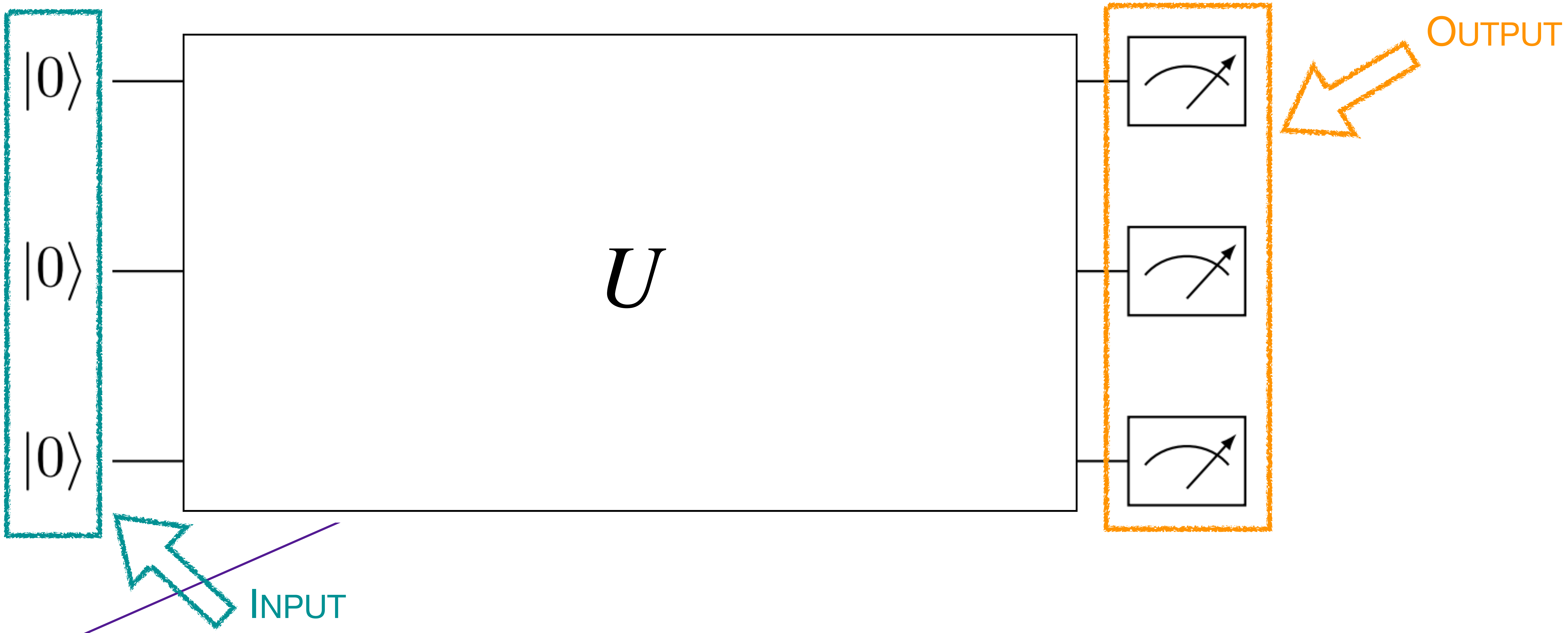
$$|0\rangle \otimes \frac{|0\rangle + e^{i\pi/4}|1\rangle}{\sqrt{2}}$$

Eigenvector of

$$Z \otimes I$$

Examples: [2-QUBIT STATES]

$$|0\rangle \otimes \frac{|0\rangle + e^{i\pi/4}|1\rangle}{\sqrt{2}}$$

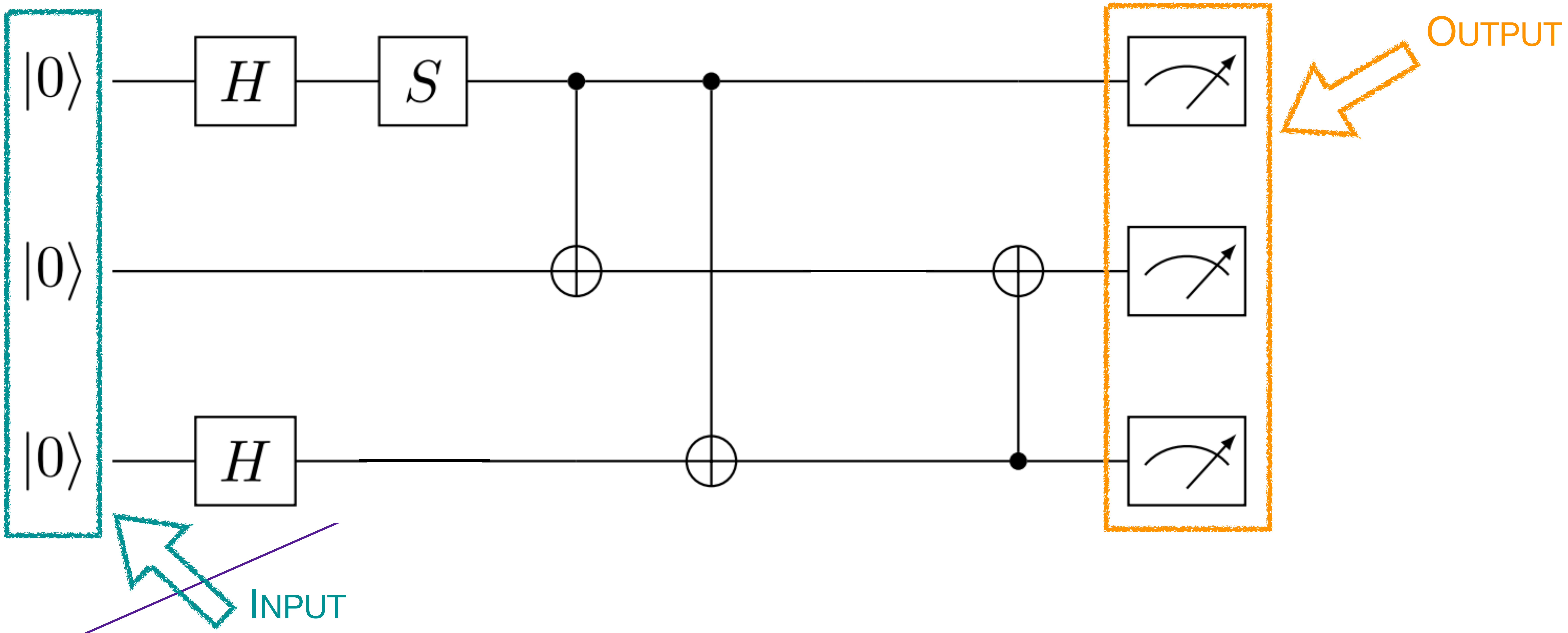

|0⟩
|0⟩
|0⟩
U
Output
Input

Quantum circuits with:

- stabilizer state inputs,
- Clifford gates,
- and Pauli measurements

are efficiently classically simulable.

GOTTESMAN-KNILL THEOREM

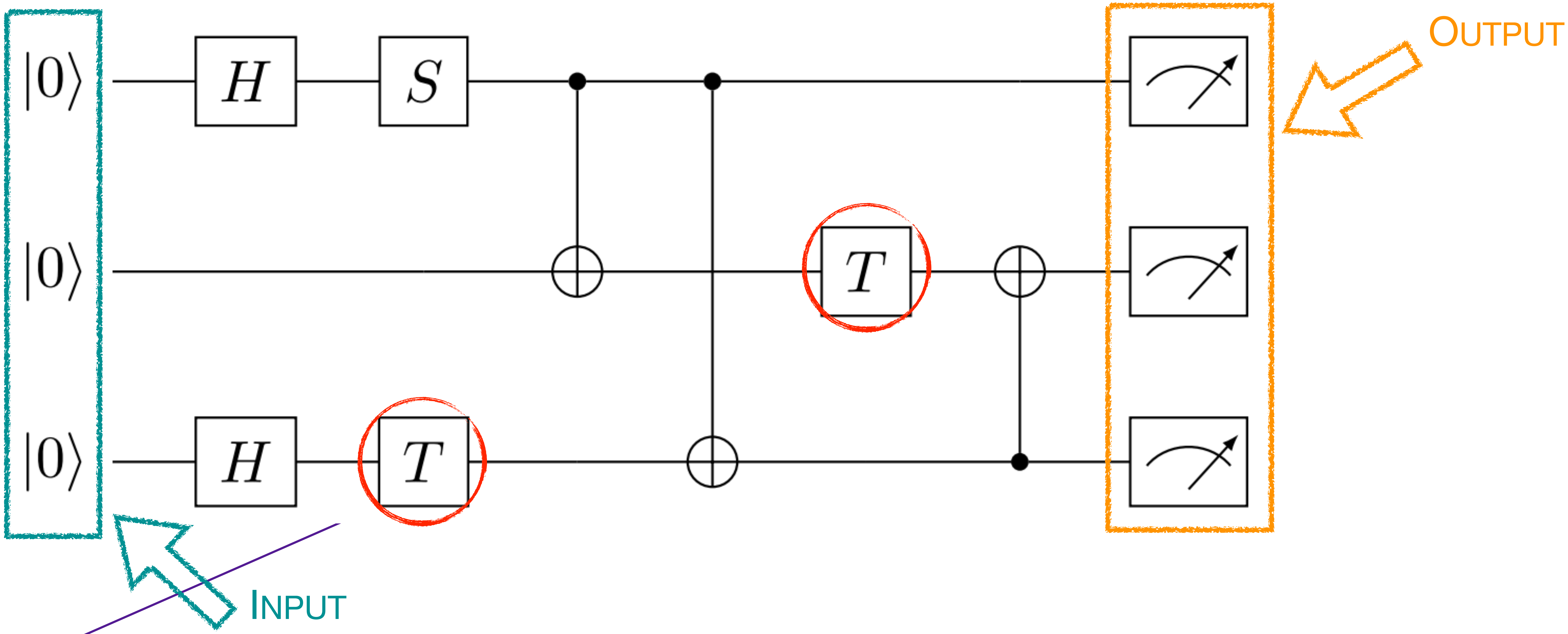


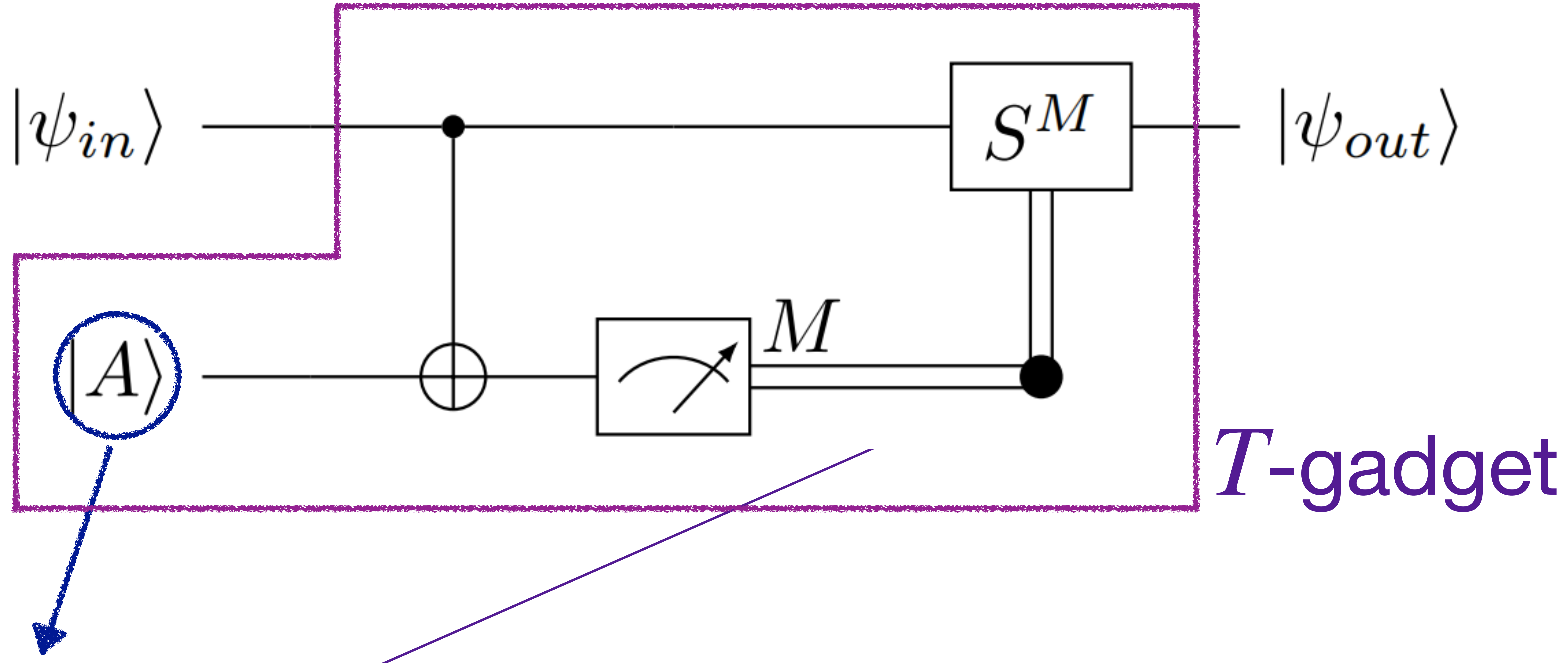
|0⟩
|0⟩
|0⟩
H
S
H
OUTPUT
INPUT

But…

Clifford+T circuits are universal for quantum computation!

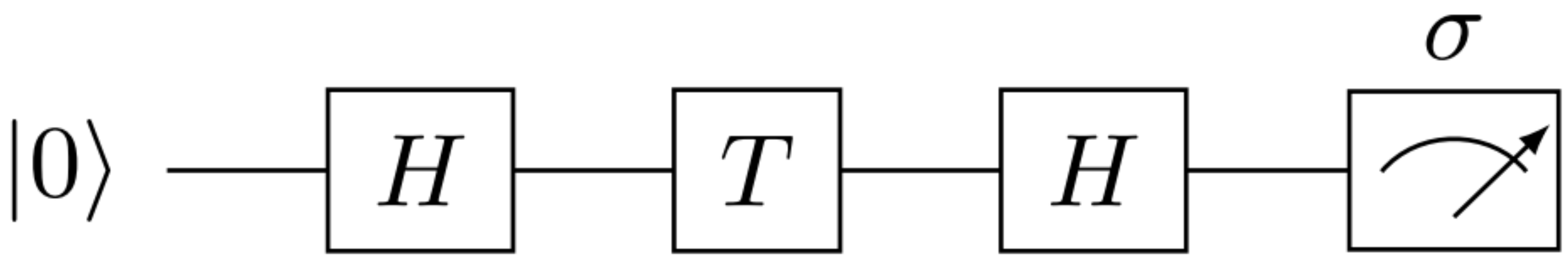
$$T = \mathrm{diag}(1, e^{i\pi/4})\,.$$

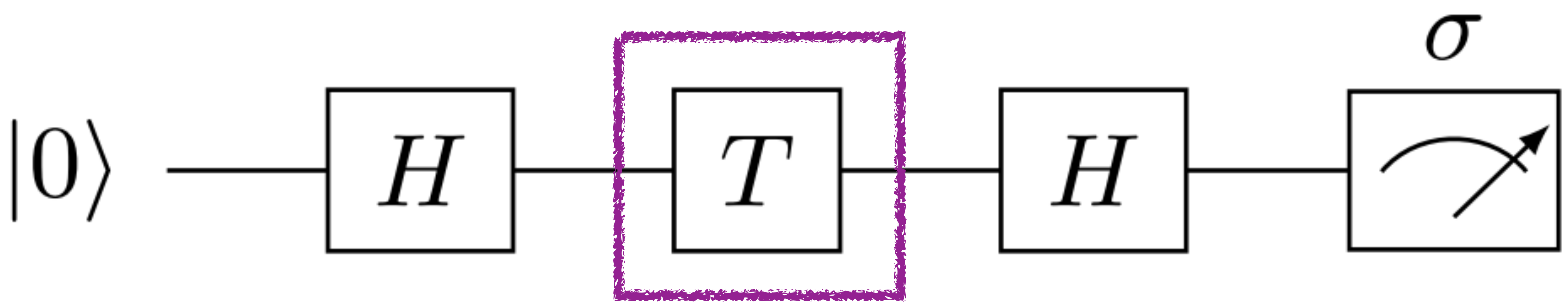

|0⟩
|0⟩
|0⟩
H
S
H
T
T
OUTPUT
INPUT

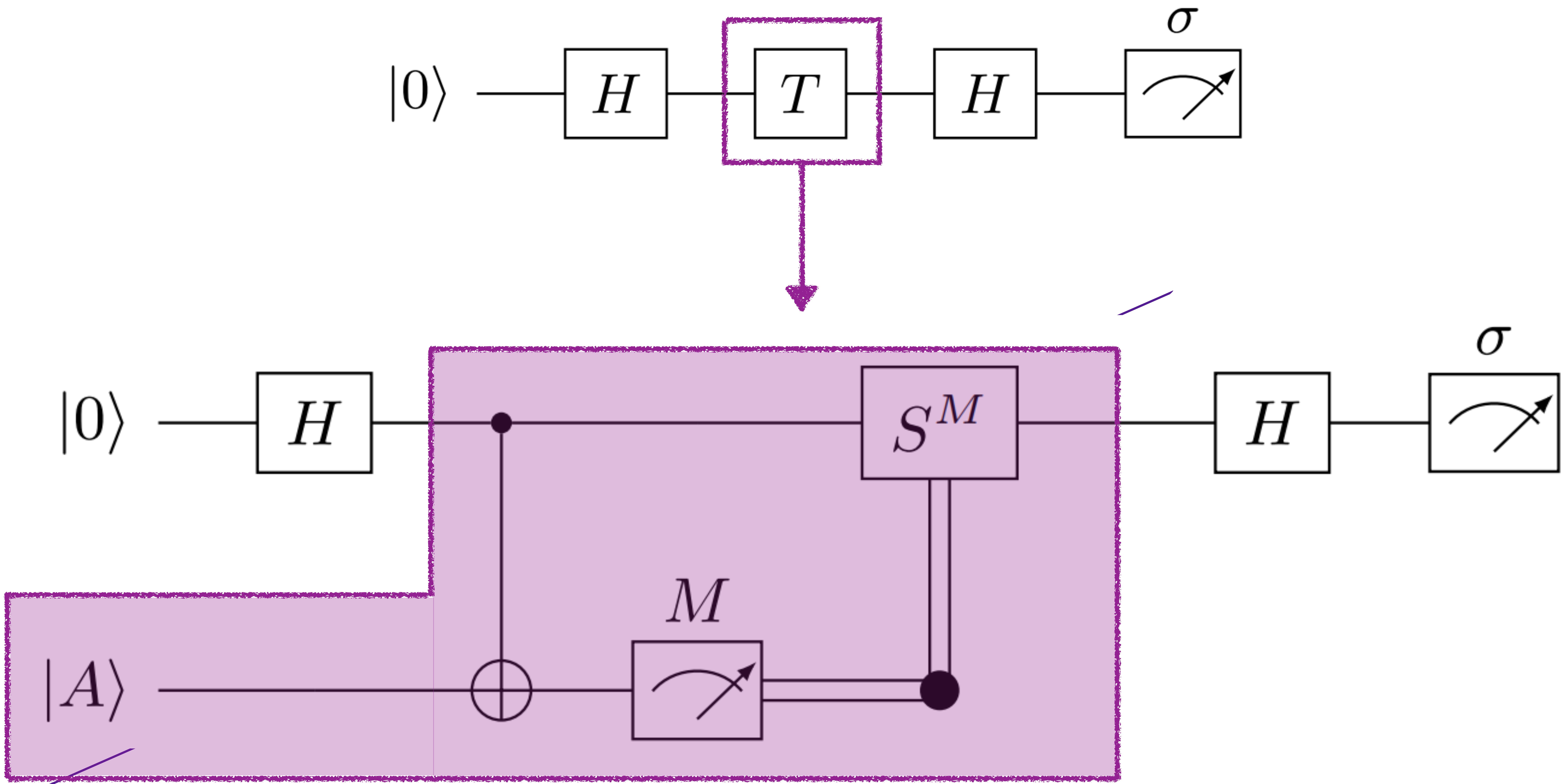


$$|A\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\pi/4}|1\rangle\right)$$

$$|\psi_{out}\rangle = T|\psi_{in}\rangle$$


|0⟩
H
T
H
σ


|0⟩
H
T
H
σ


|0⟩
H
T
H
σ
|0⟩
H
S^M
H
σ
M
|A⟩

Pauli-based computation:

S. Bravyi, G. Smith, and J. A. Smolin, Phys. Rev. X **6**, 021043 (2016), arXiv:1506.01396.

Definition: [PAULI-BASED MODEL OF COMPUTATION]

Definition: [PAULI-BASED MODEL OF COMPUTATION]

- Input: product state $|A\rangle^{\otimes t}$

Definition: [PAULI-BASED MODEL OF COMPUTATION]

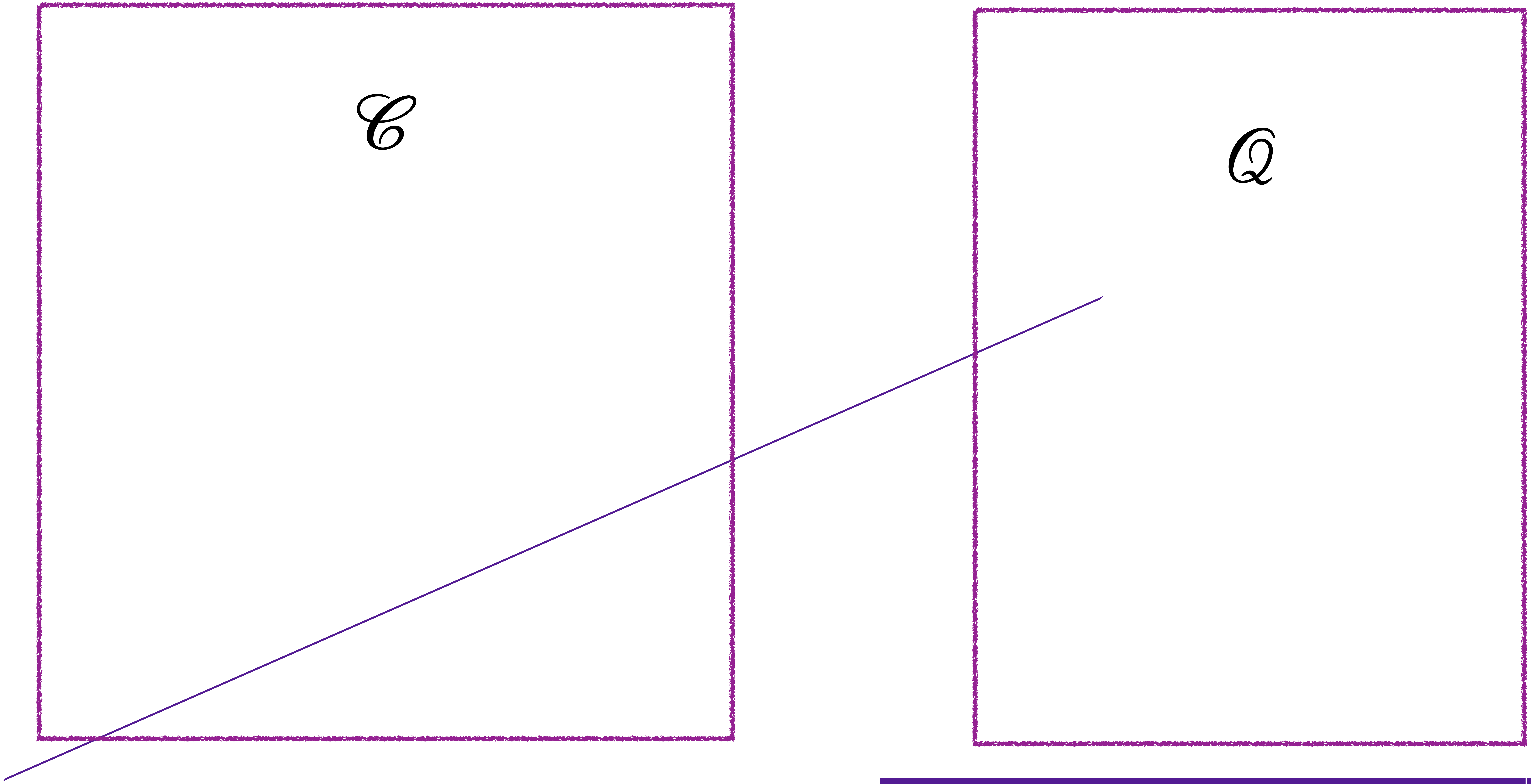
- Input: product state $|A\rangle^{\otimes t}$

Definition: [PAULI-BASED MODEL OF COMPUTATION]

- Input: product state $|A\rangle^{\otimes t}$

- Steps: measurements of **independent and pairwise commuting** Pauli operators $P_i \in \mathscr{P}_t$

Theorem: Any Clifford+T quantum circuit $\mathscr{C}$ with t T gates can be simulated by a standard PBC $\mathcal{Q}$ on t qubits.


$\mathscr{C}$
$\mathscr{Q}$

$\mathscr{C}$

- $|0\rangle^{\otimes n}$

$\mathscr{Q}$

$\mathscr{C}$

- $|0\rangle^{\otimes n}$
- $t\ T$ gates

$\mathscr{Q}$

$\mathscr{C}$

- $|0\rangle^{\otimes n}$
- t T gates
- w Z-measurements

$\mathscr{Q}$

$\mathscr{C}$

- $|0\rangle^{\otimes n}$
- t T gates
- w Z-measurements

$\mathscr{Q}$

$\mathscr{C}$

- $|0\rangle^{\otimes n}$
- $t\ T$ gates
- $w\ Z$-measurements

$\mathscr{Q}$

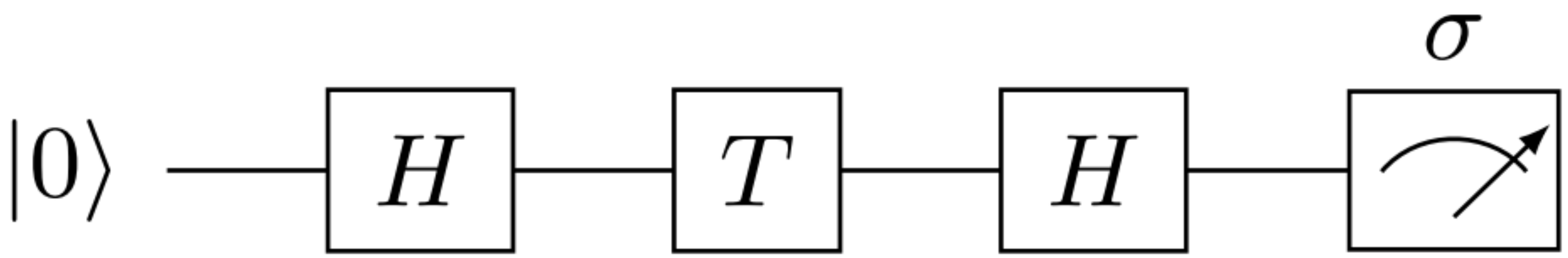
- $|A\rangle^{\otimes t}$

$\mathscr{C}$

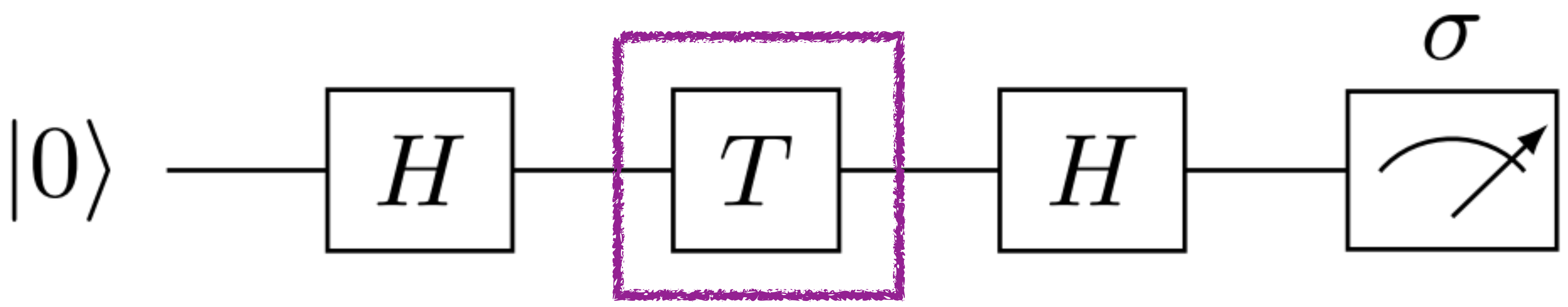
- $|0\rangle^{\otimes n}$
- $t\ T$ gates
- $w\ Z$-measurements

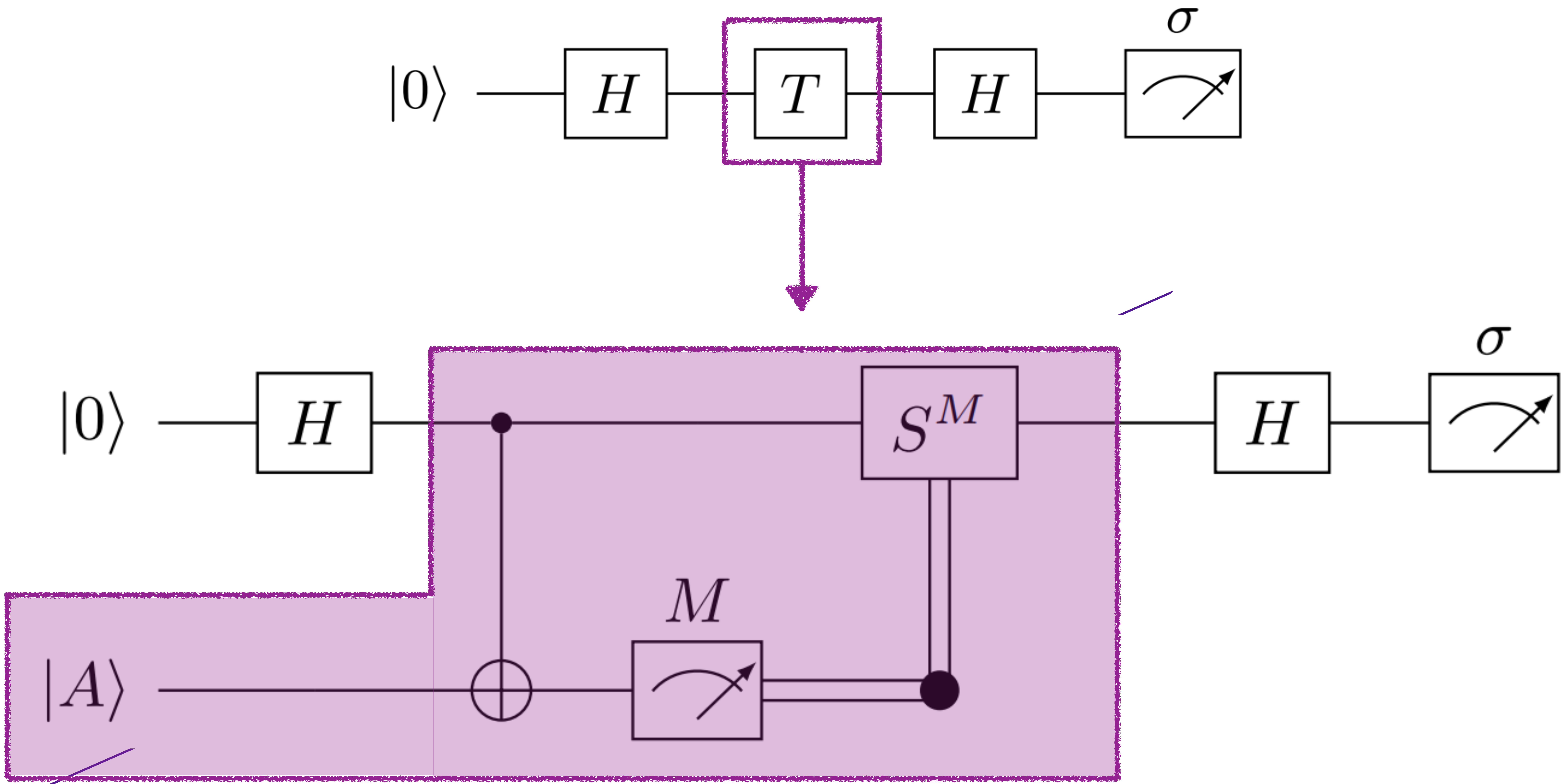
$\mathscr{Q}$

- $|A\rangle^{\otimes t}$
- at most t Pauli measurements

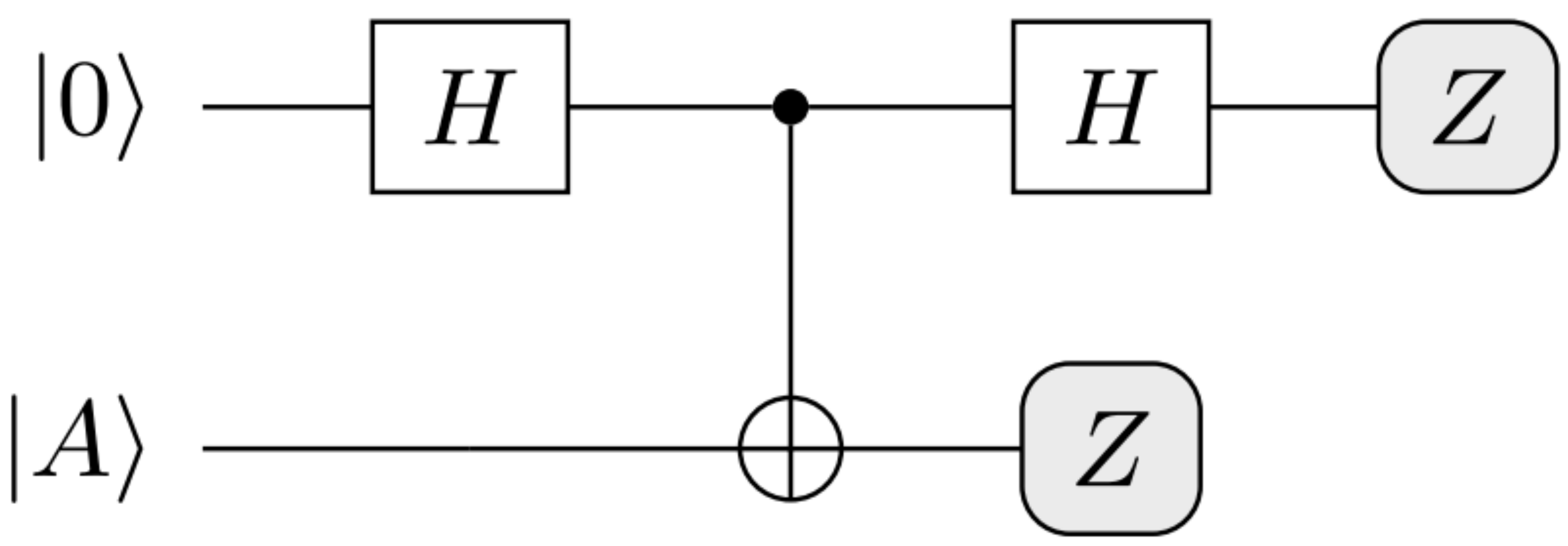


$|0\rangle$
H
T
H
σ

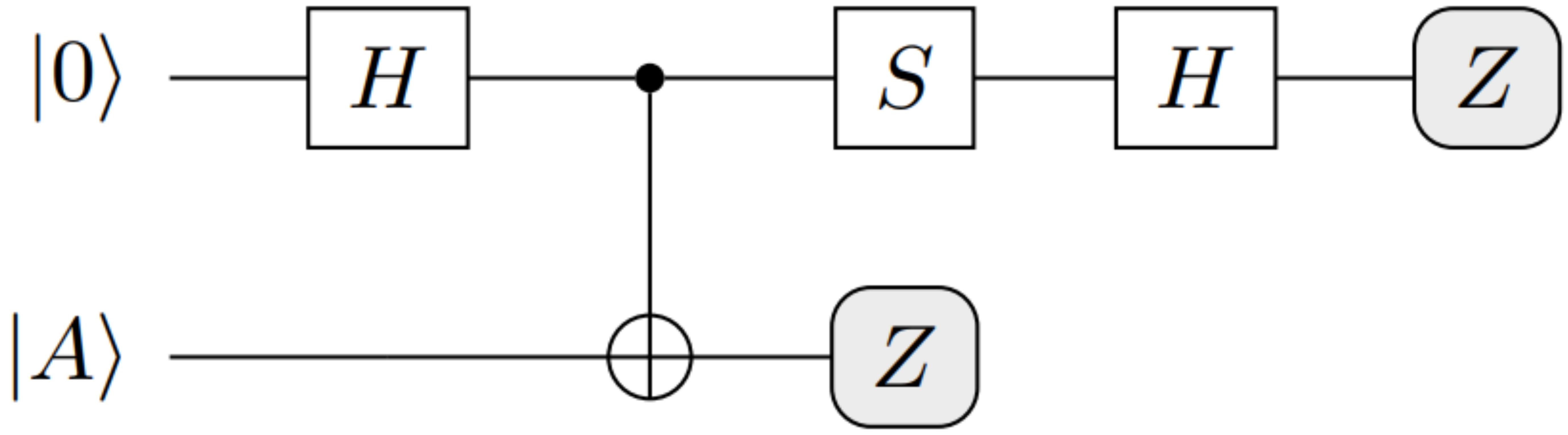

$|0\rangle$
H
T
H
σ



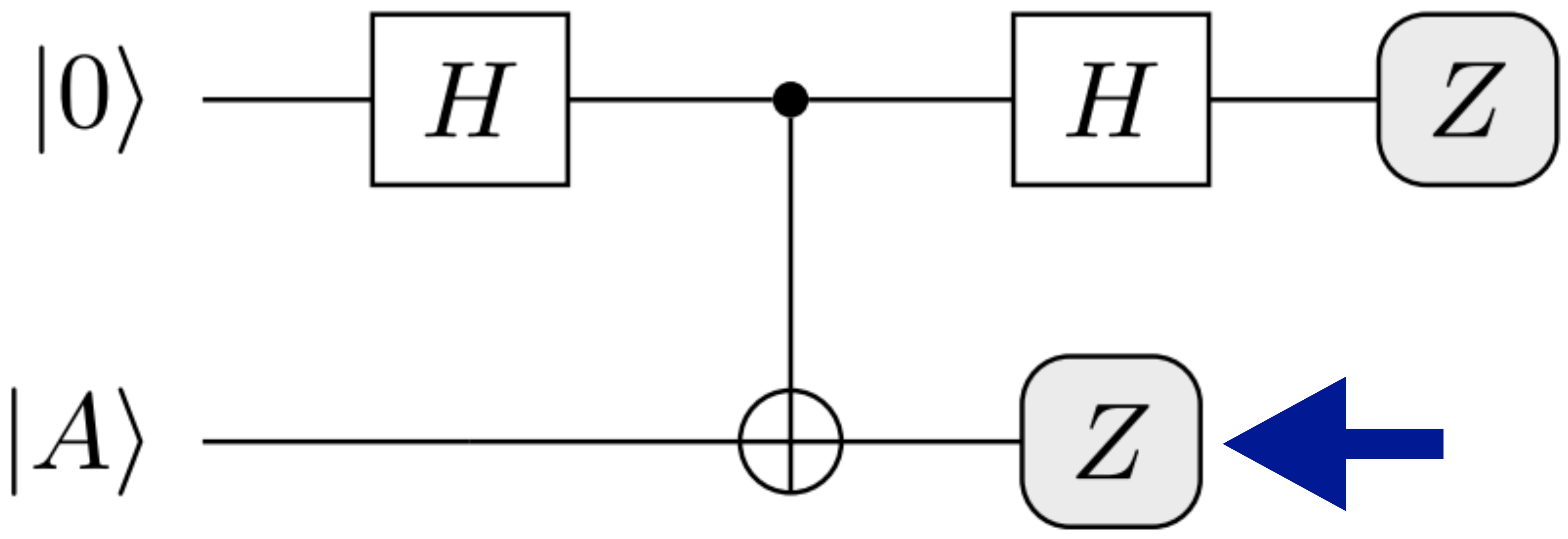
|0⟩
H
T
H
σ
|0⟩
H
S^M
M
|A⟩
H
σ

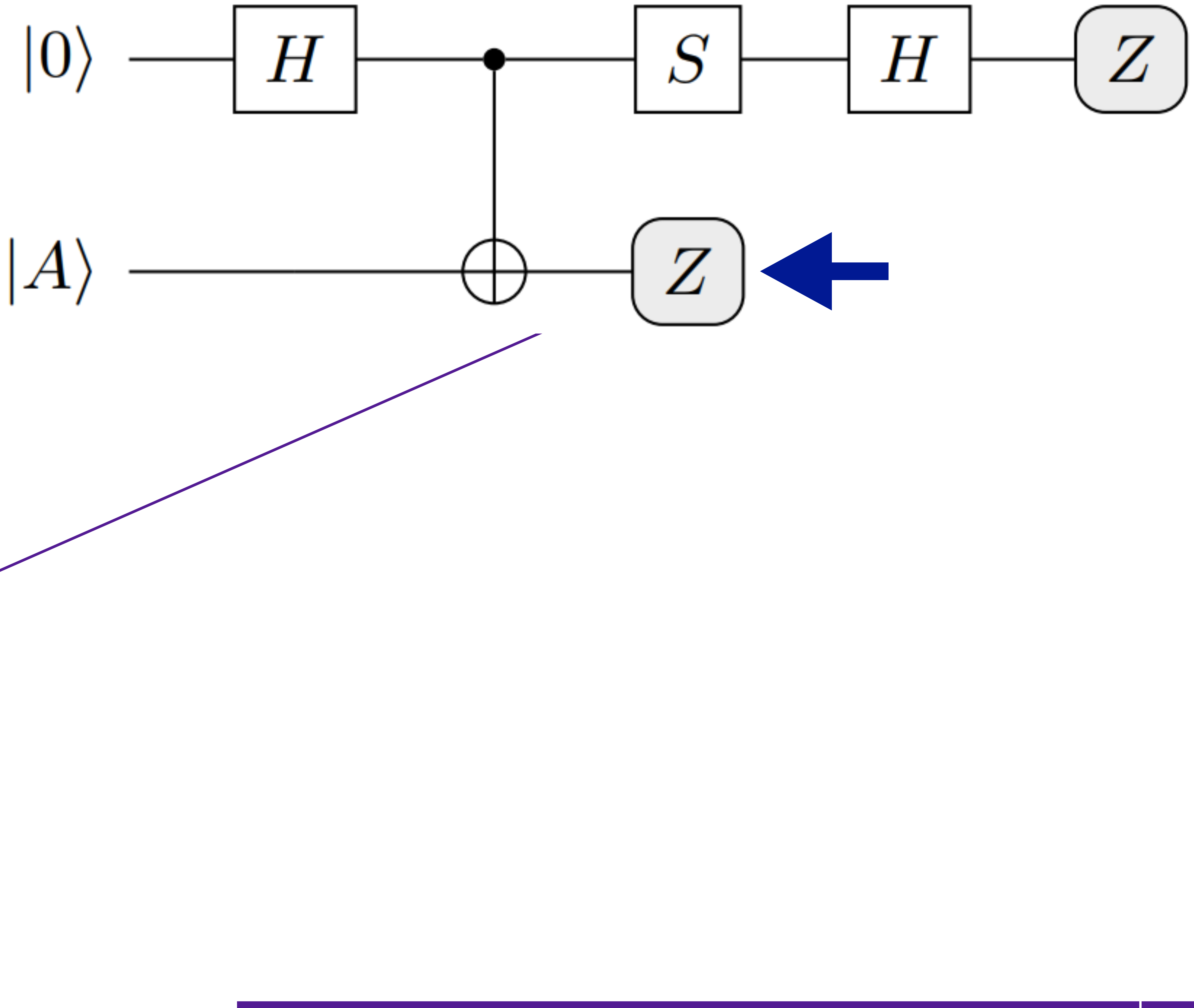


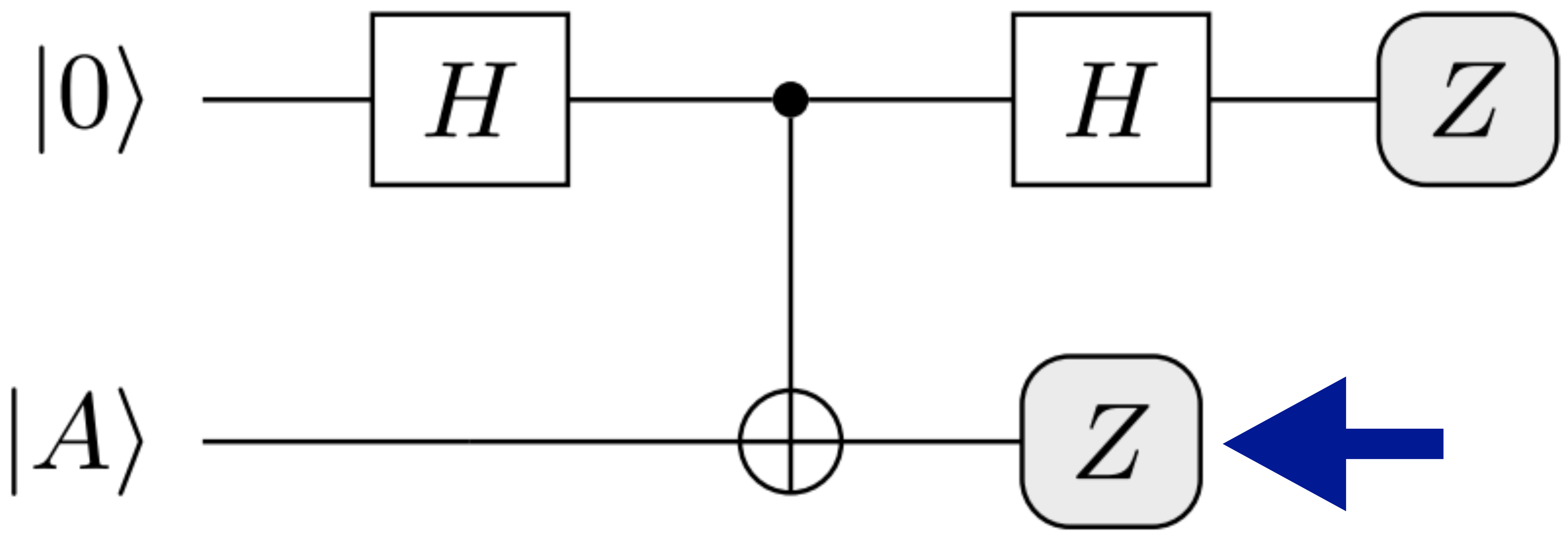
|0⟩
|A⟩
H
H
Z
Z

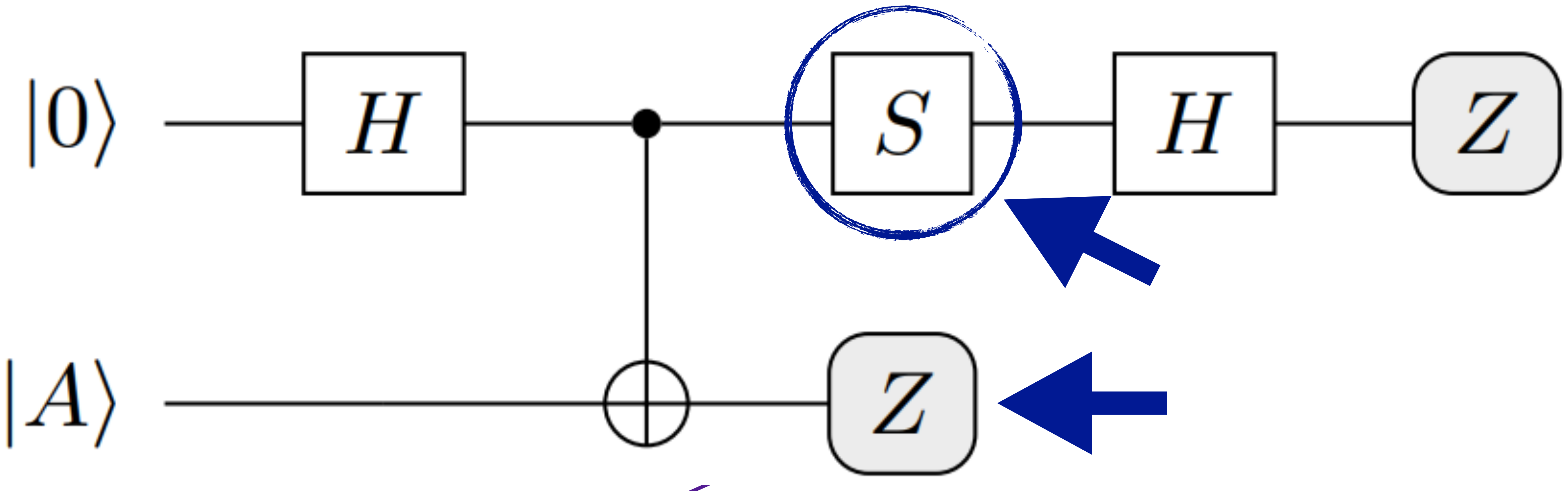


|0⟩
|A⟩
H
S
H
Z
Z


|0⟩
H
H
Z
|A⟩
Z

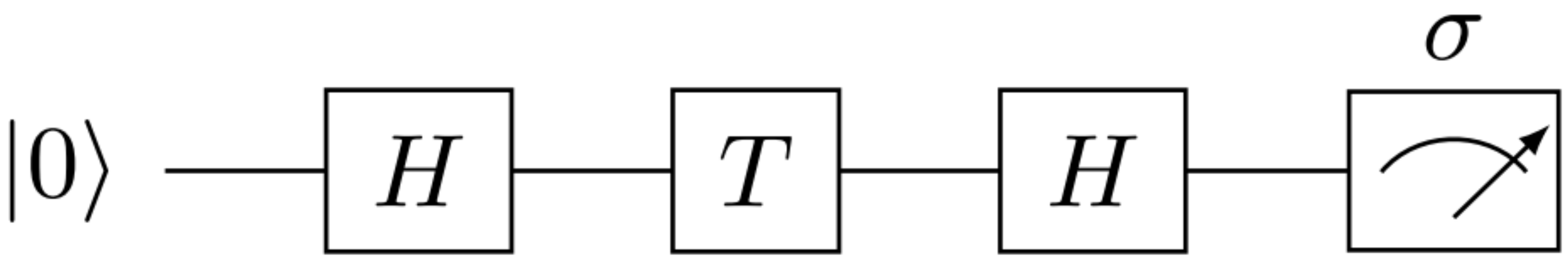

|0⟩
H
S
H
Z
|A⟩
Z

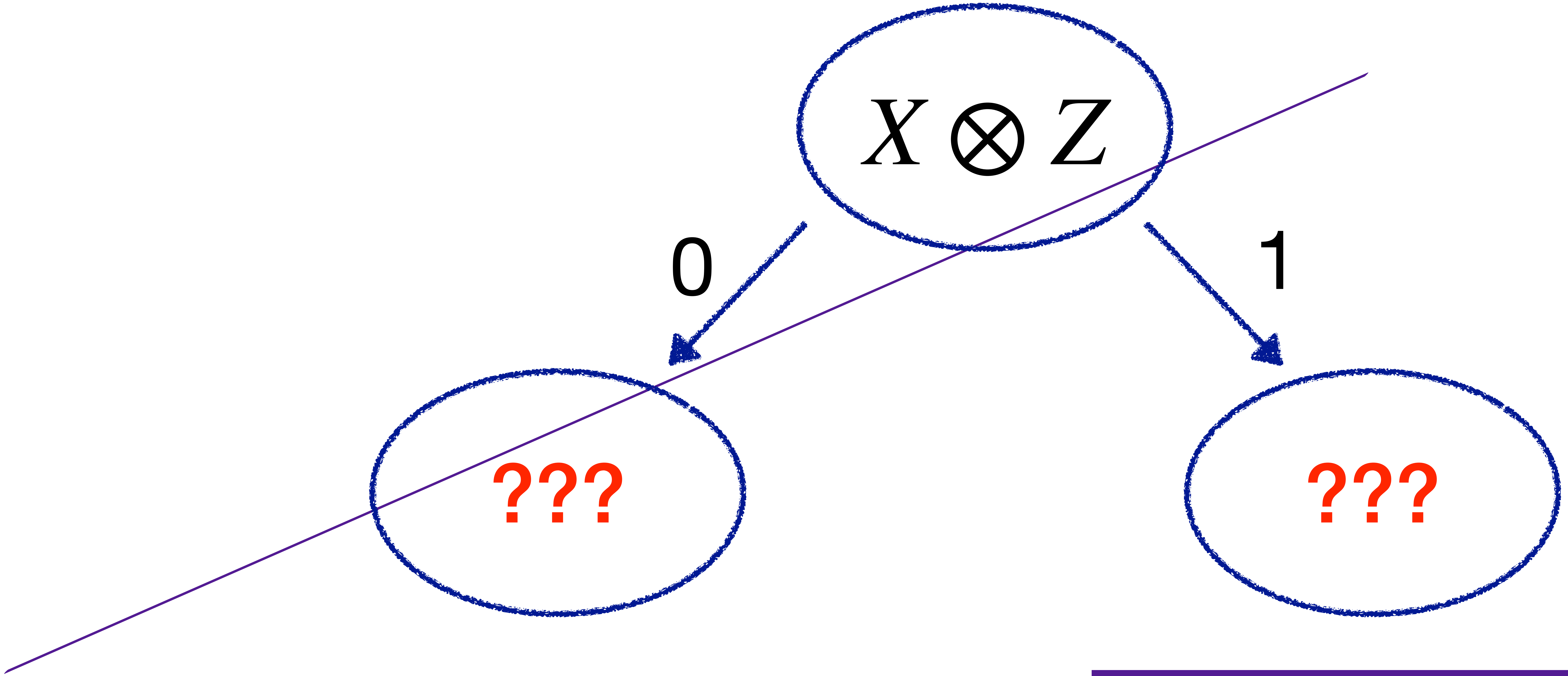

$|0\rangle$
H
H
Z
$|A\rangle$
Z

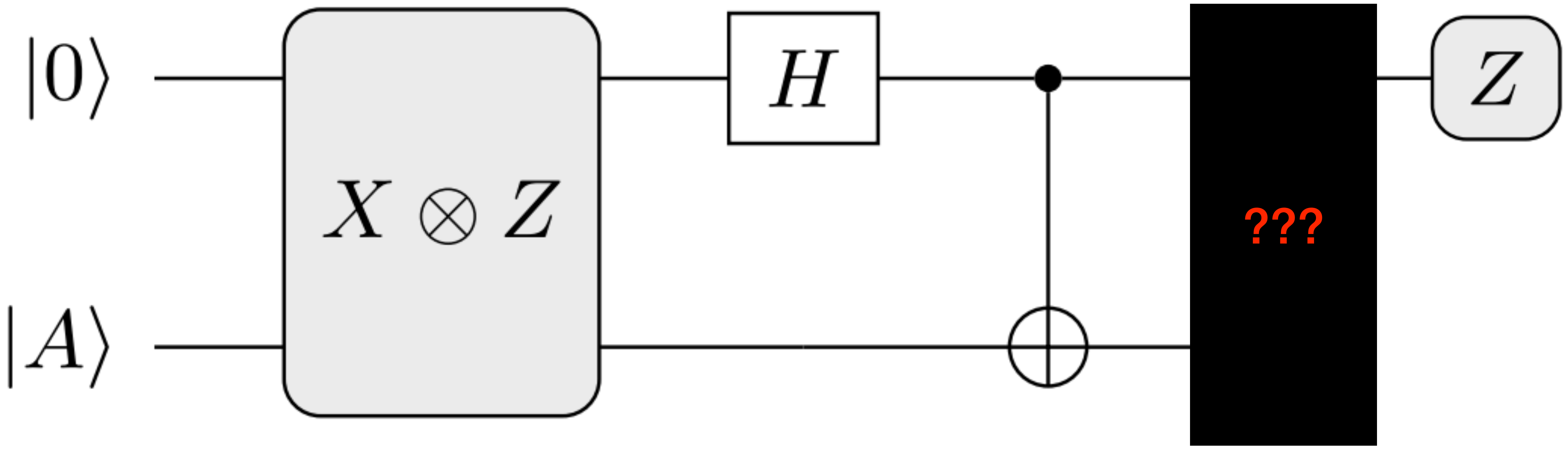

$|0\rangle$
H
S
H
Z
$|A\rangle$
Z

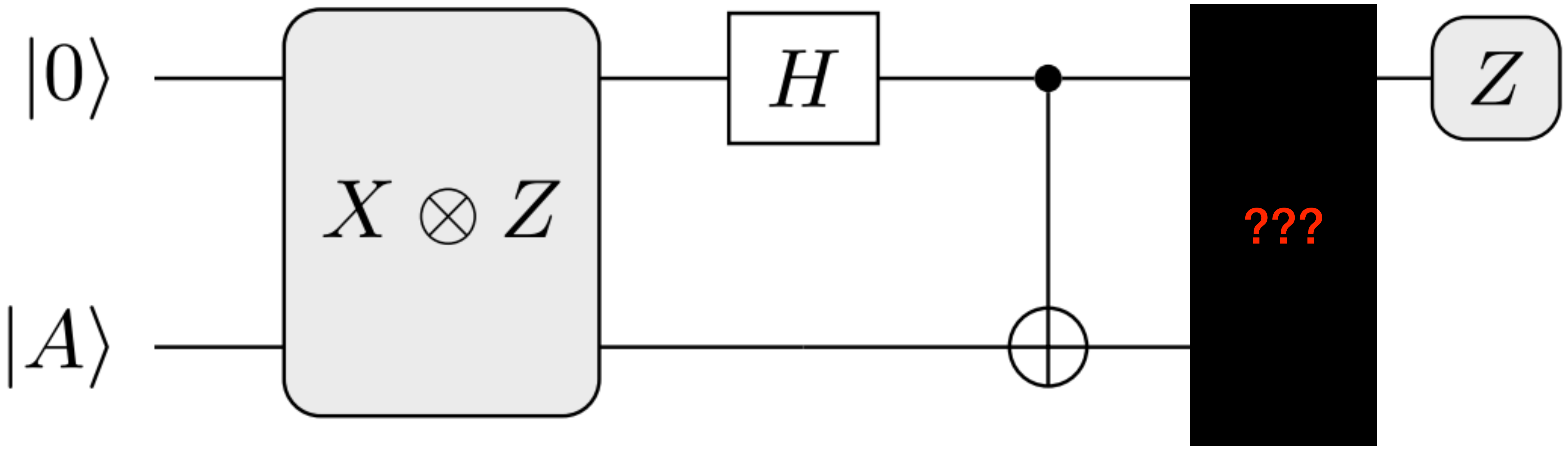

|0⟩
|A⟩
H
Z
S
Z ⊗ Z
???

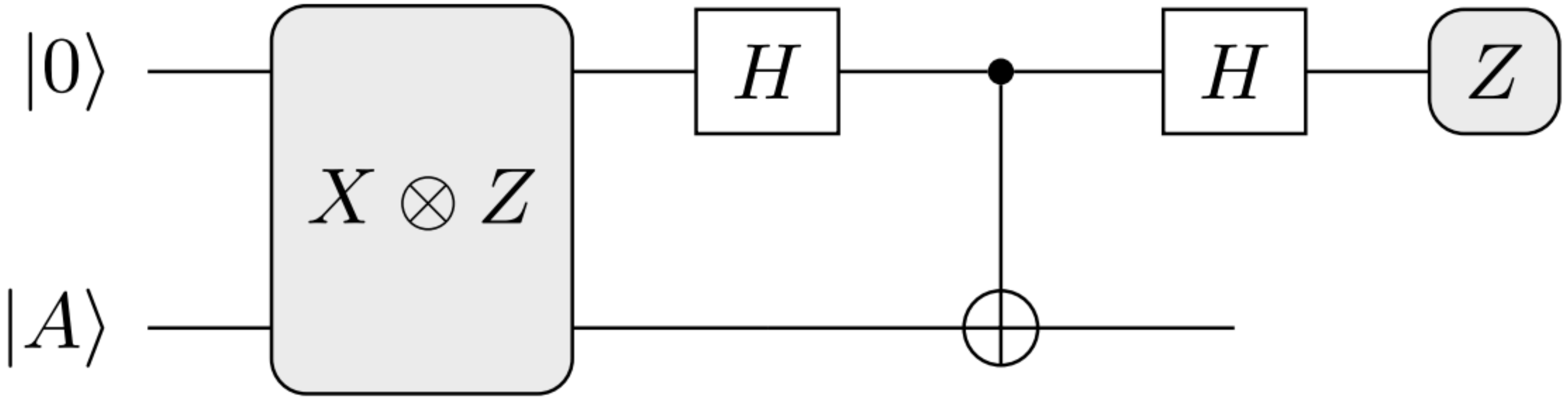

|0⟩
|A⟩
H
H
Z
Z
S
Z ⊗ Z
???
X ⊗ Z
H
???
Z

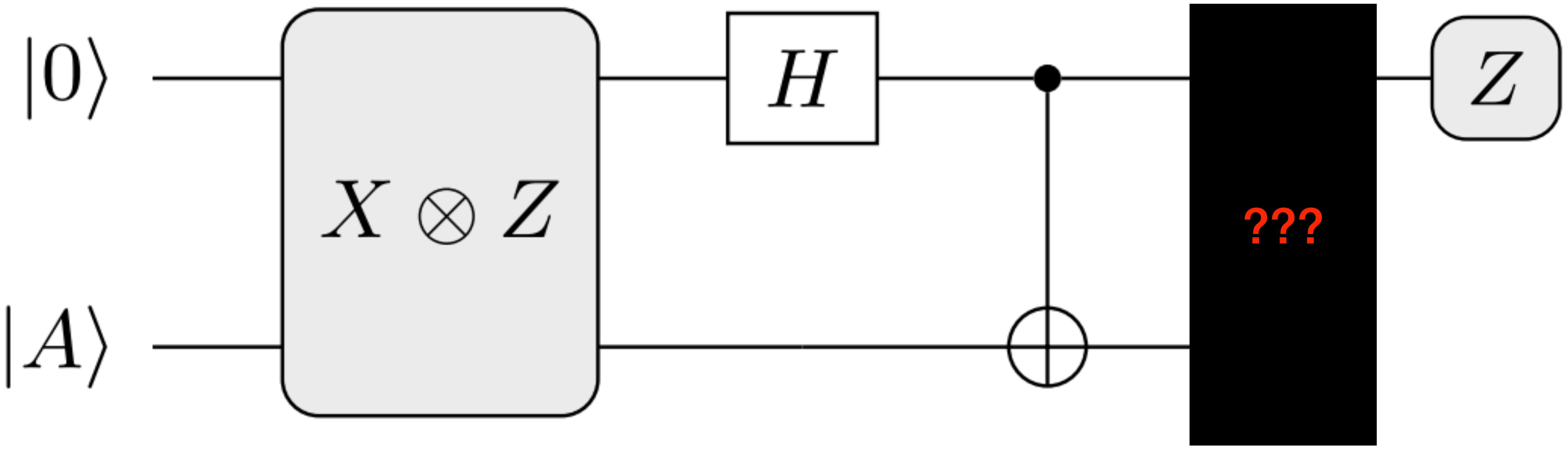

σ
|0⟩
H
T
H

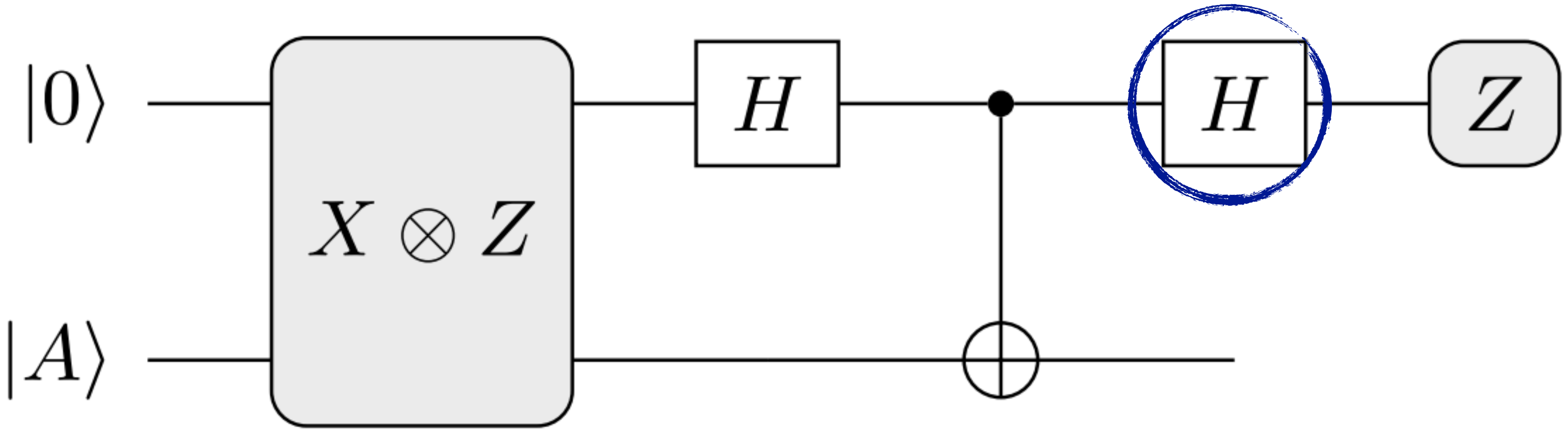

X ⊗ Z
0
1
???
???


|0⟩
|A⟩
X ⊗ Z
H
???
Z

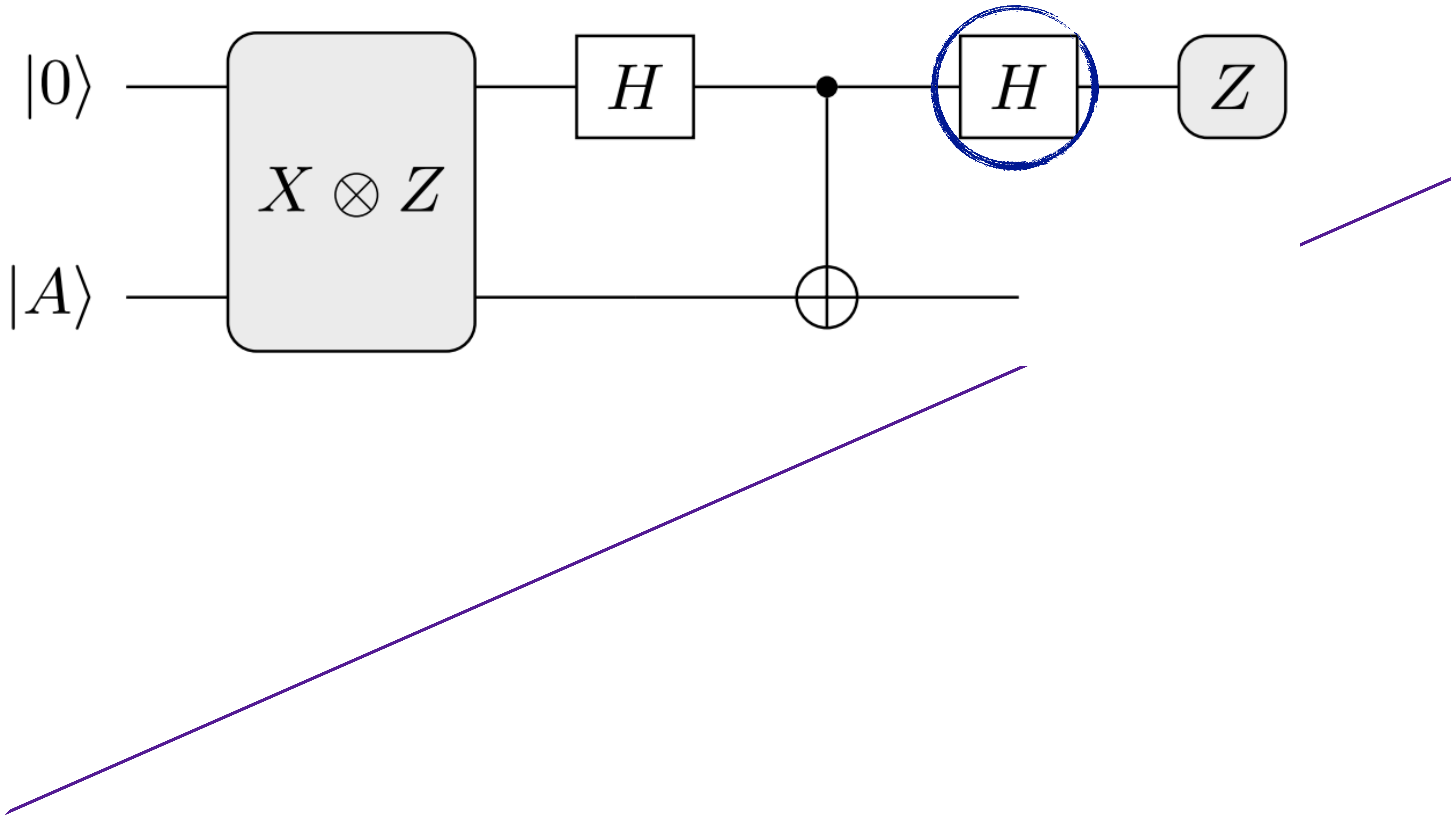

|0⟩
|A⟩
X ⊗ Z
H
???
Z

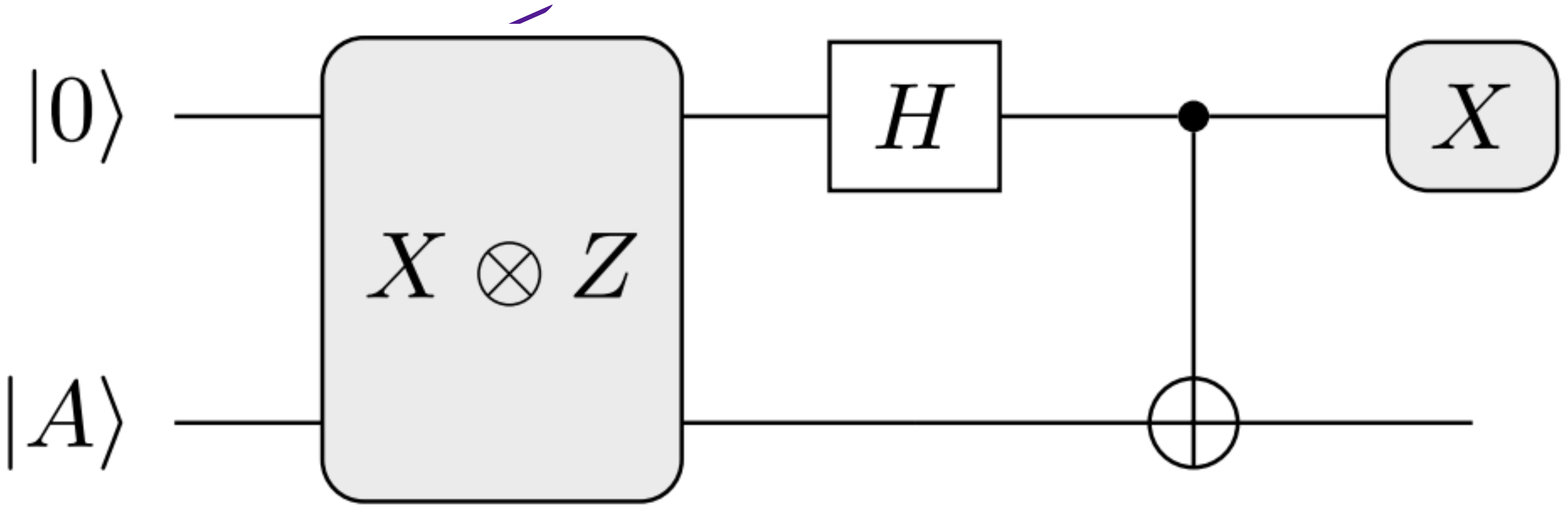

|0⟩
|A⟩
X ⊗ Z
H
H
Z

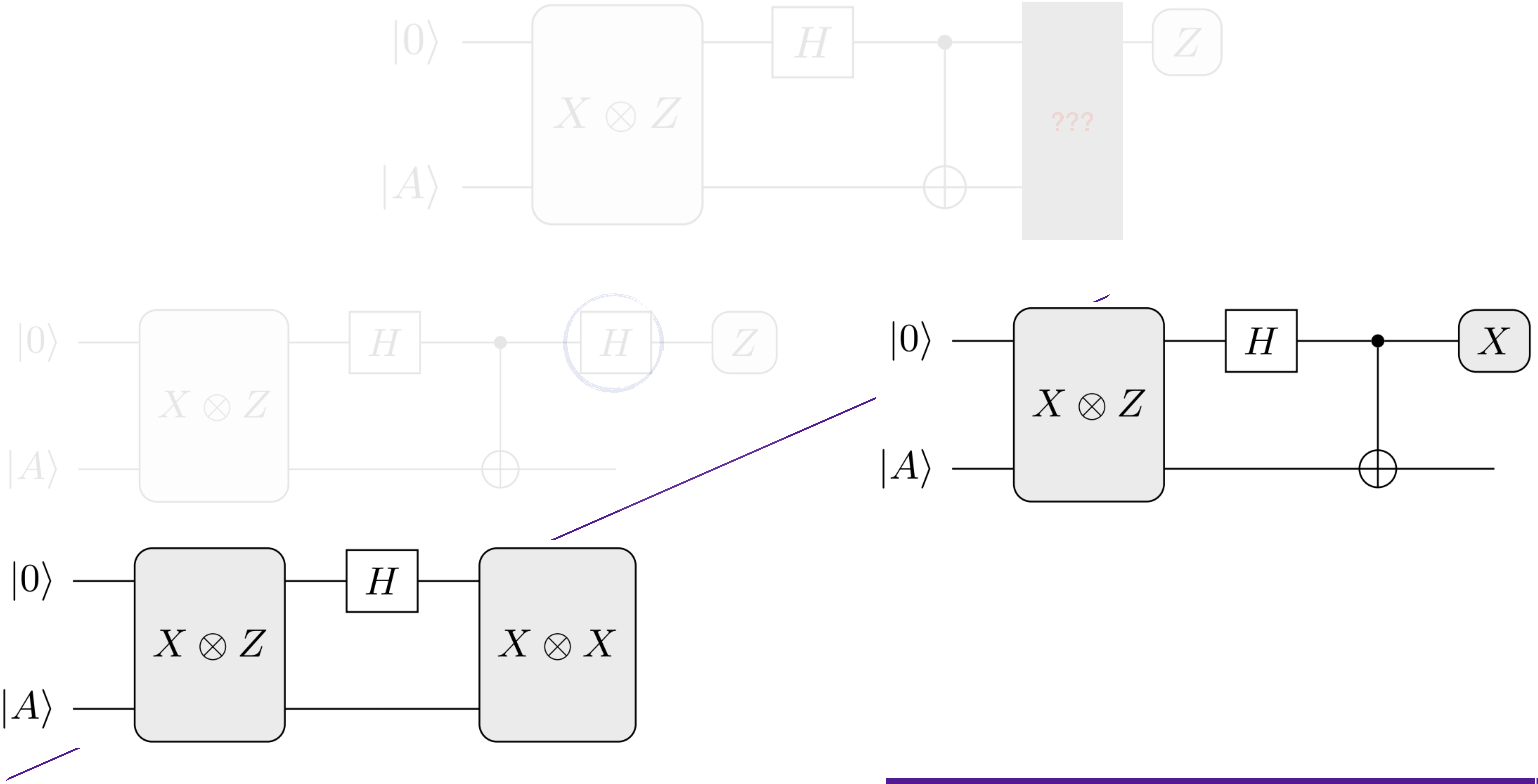

|0⟩
|A⟩
X ⊗ Z
H
???
Z

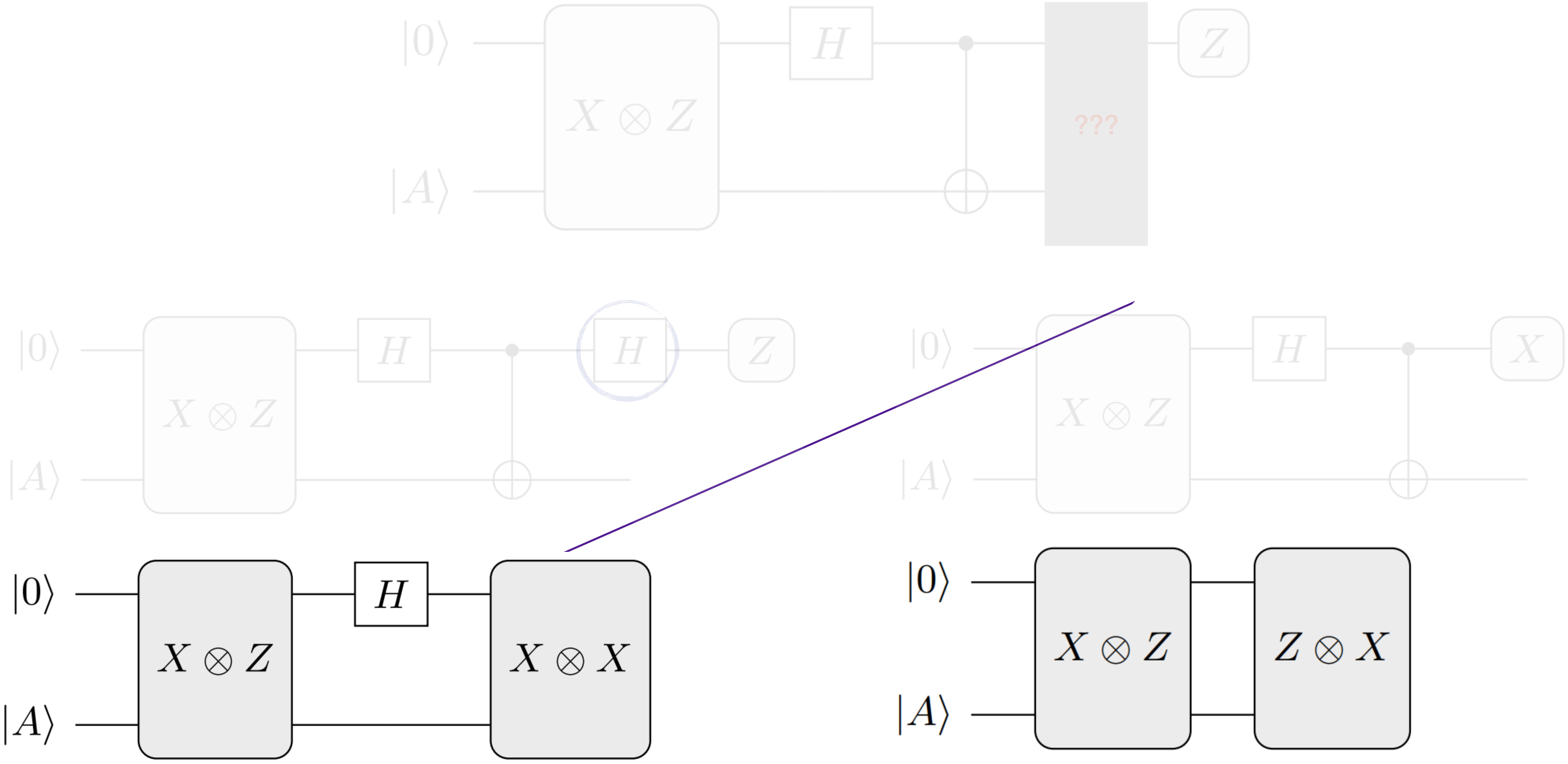

|0⟩
|A⟩
X ⊗ Z
H
H
Z

|0⟩
|A⟩
X ⊗ Z
H
???
Z

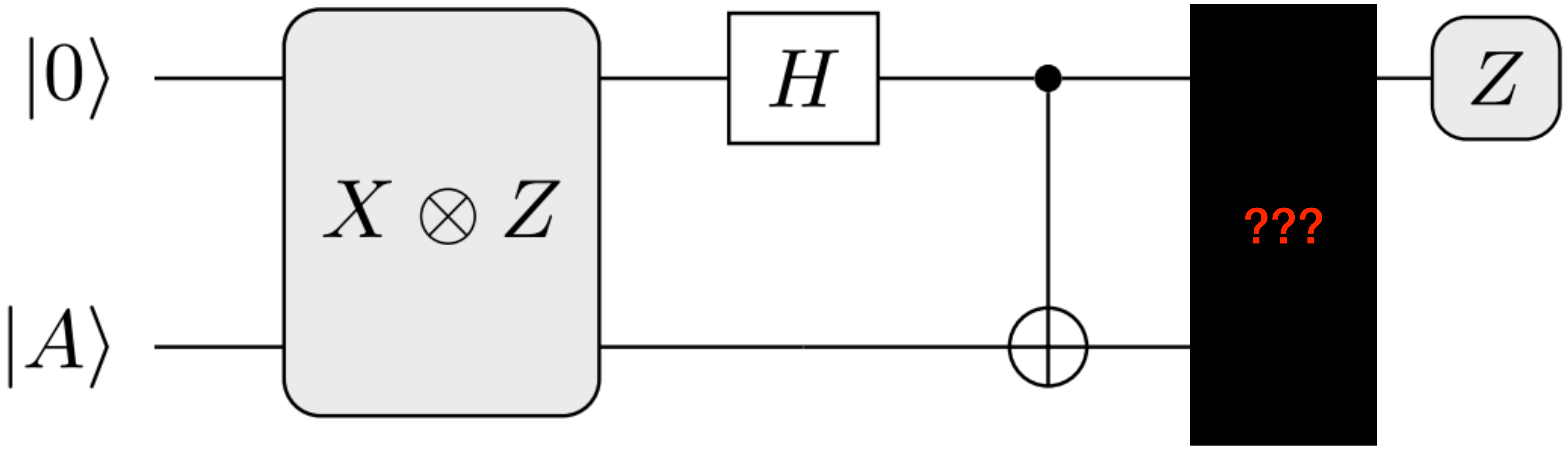

|0⟩
|A⟩
X ⊗ Z
H
H
Z

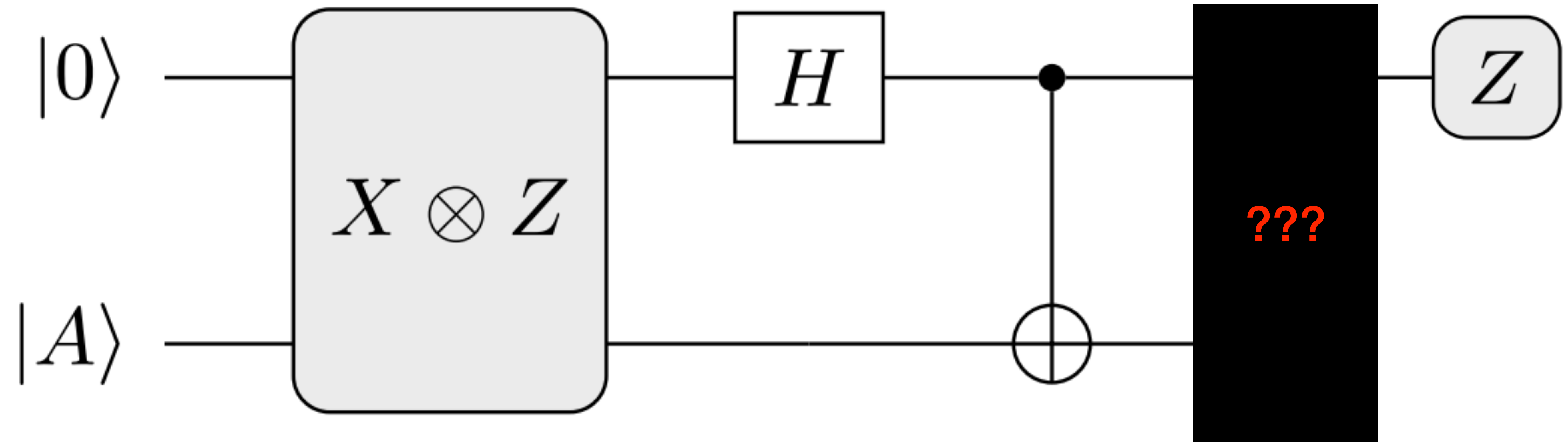

|0⟩
|A⟩
X ⊗ Z
H
X

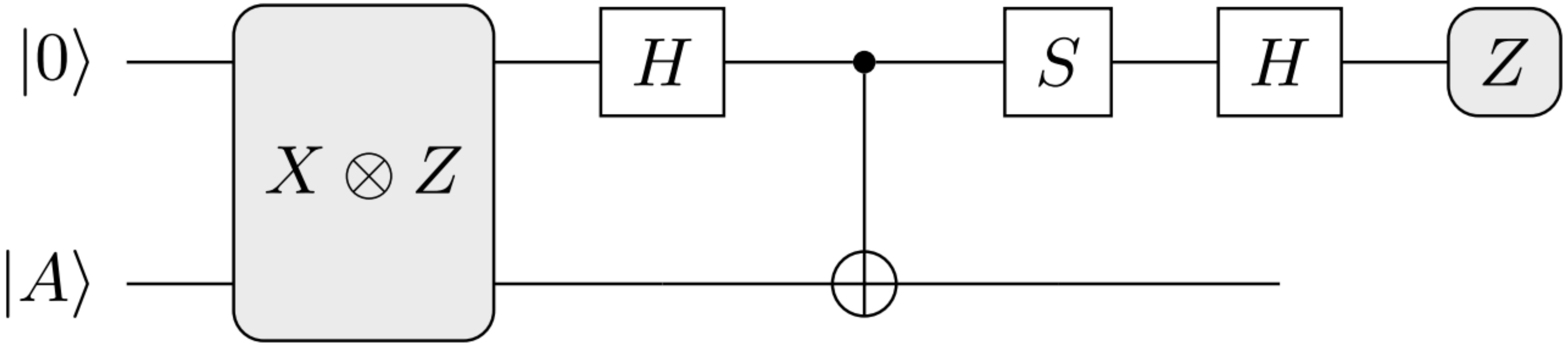

|0⟩
|A⟩
X ⊗ Z
H
???
Z
|0⟩
|A⟩
X ⊗ Z
H
H
Z
|0⟩
|A⟩
X ⊗ Z
H
X
|0⟩
|A⟩
X ⊗ Z
H
X ⊗ X

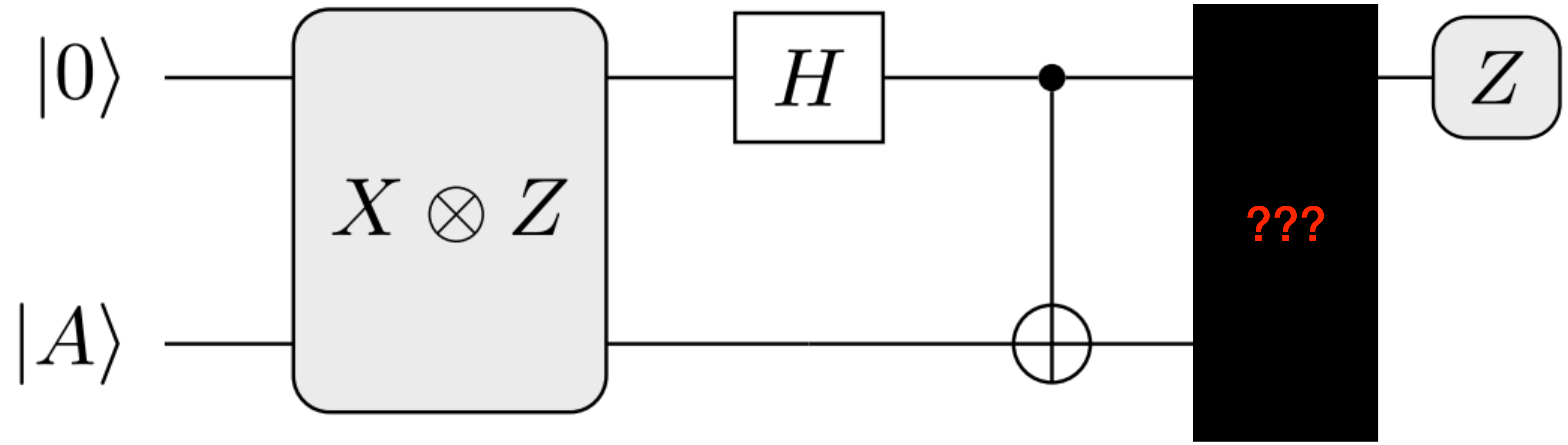


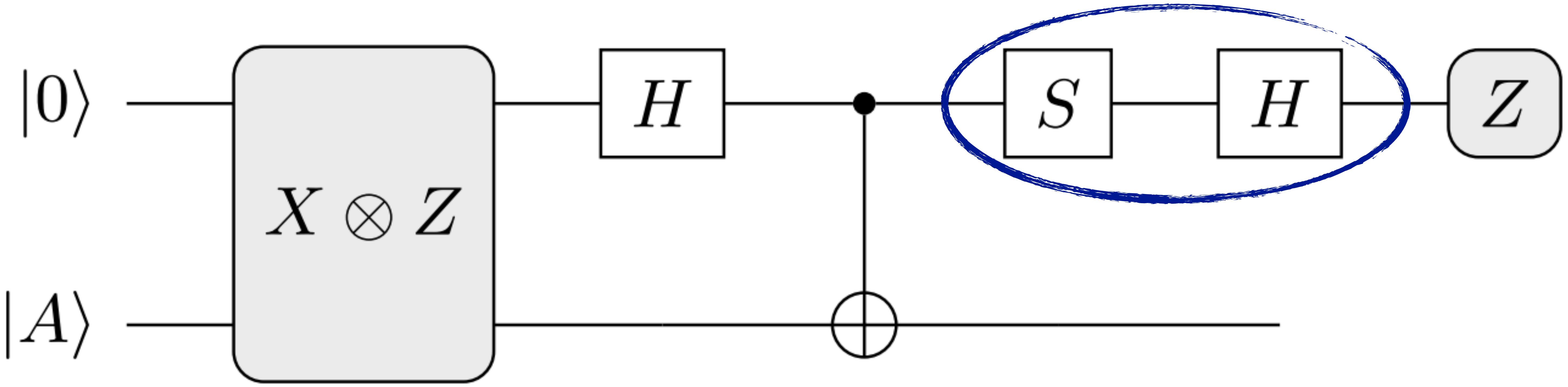
|0⟩
|A⟩
X ⊗ Z
H
???
Z
|0⟩
|A⟩
X ⊗ Z
H
H
Z
|0⟩
|A⟩
X ⊗ Z
H
X
|0⟩
|A⟩
X ⊗ Z
H
X ⊗ X
|0⟩
|A⟩
X ⊗ Z
Z ⊗ X


|0⟩
|A⟩
X ⊗ Z
H
???
Z

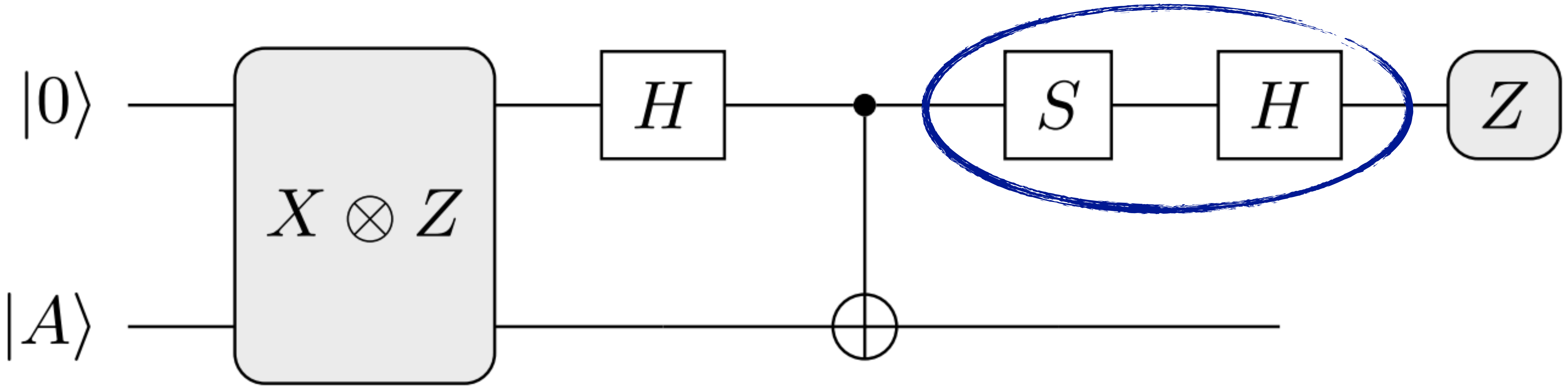

$|0\rangle$
$|A\rangle$
$X \otimes Z$
H
???
Z

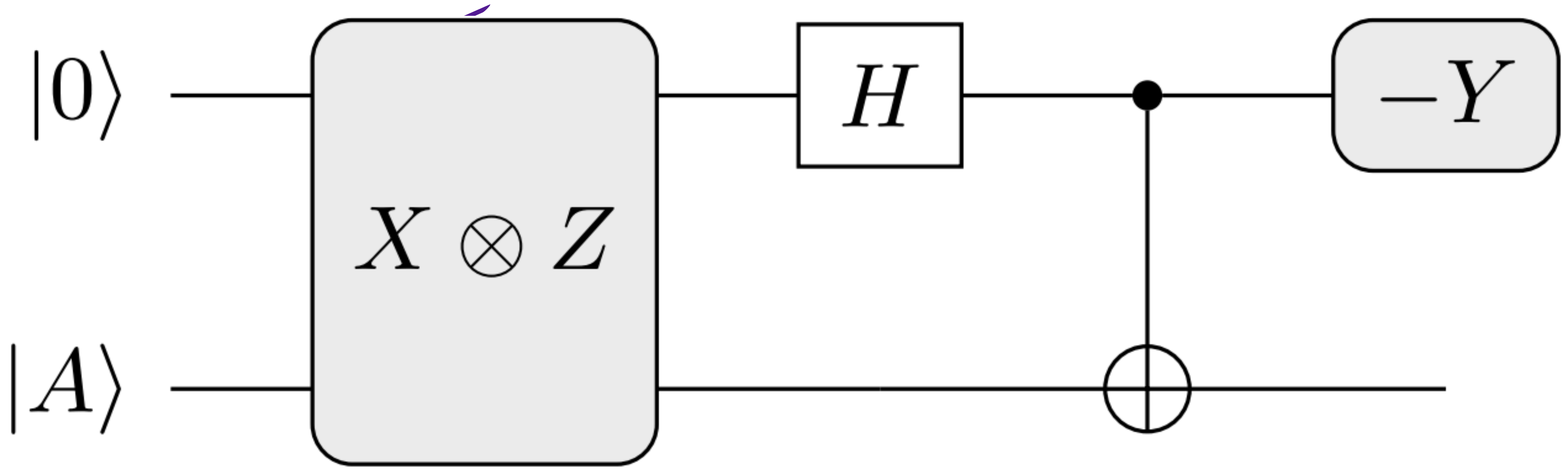

$|0\rangle$
$|A\rangle$
$X \otimes Z$
H
S
H
Z


|0⟩
|A⟩
X ⊗ Z
H
???
Z

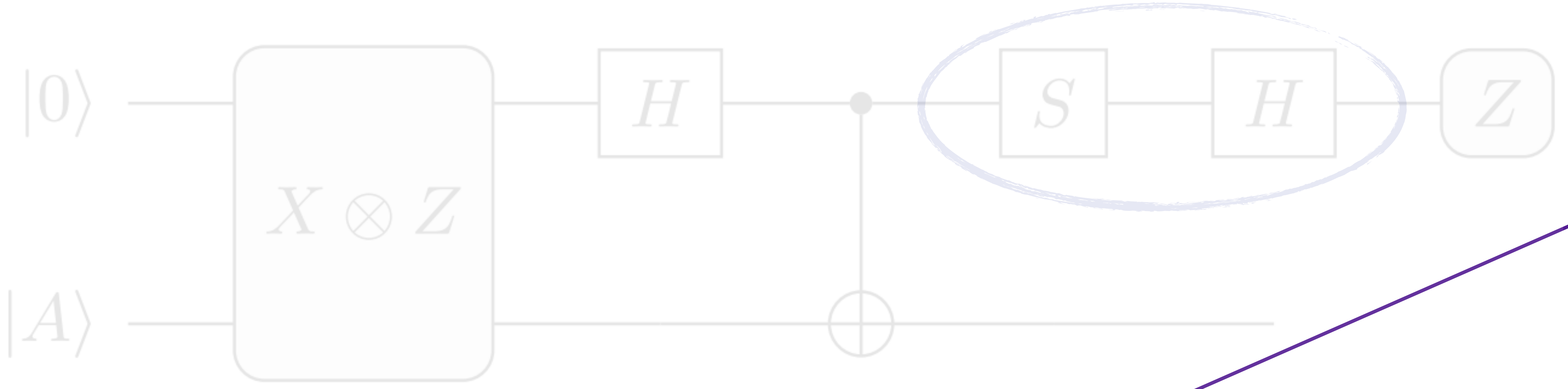

|0⟩
|A⟩
X ⊗ Z
H
S
H
Z

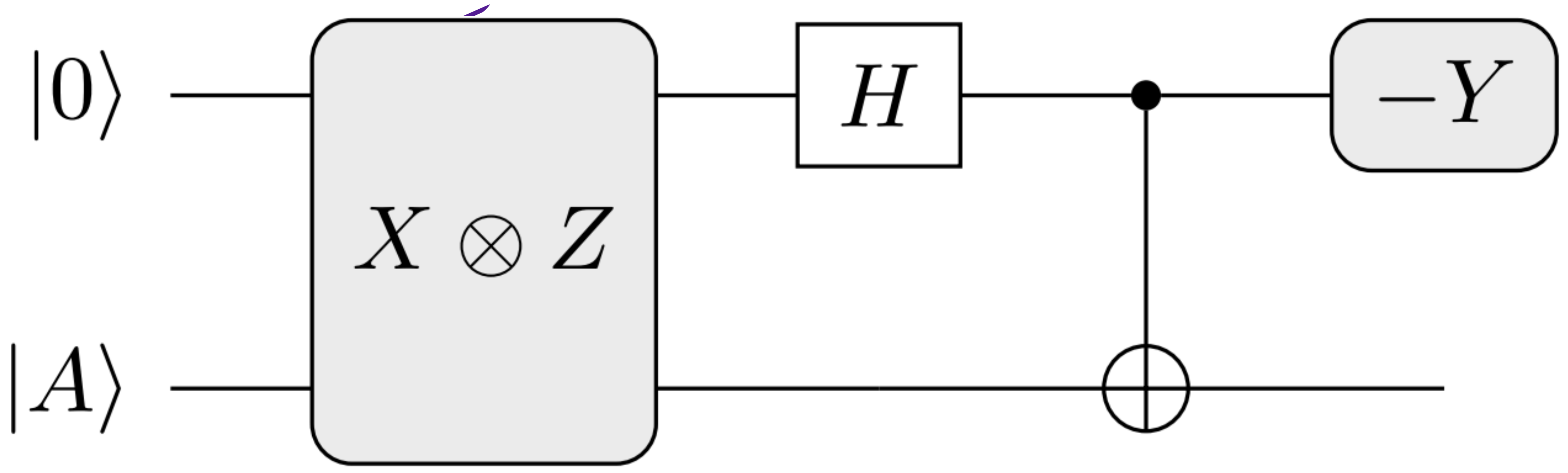
|0⟩
|A⟩
X ⊗ Z
H
???
Z

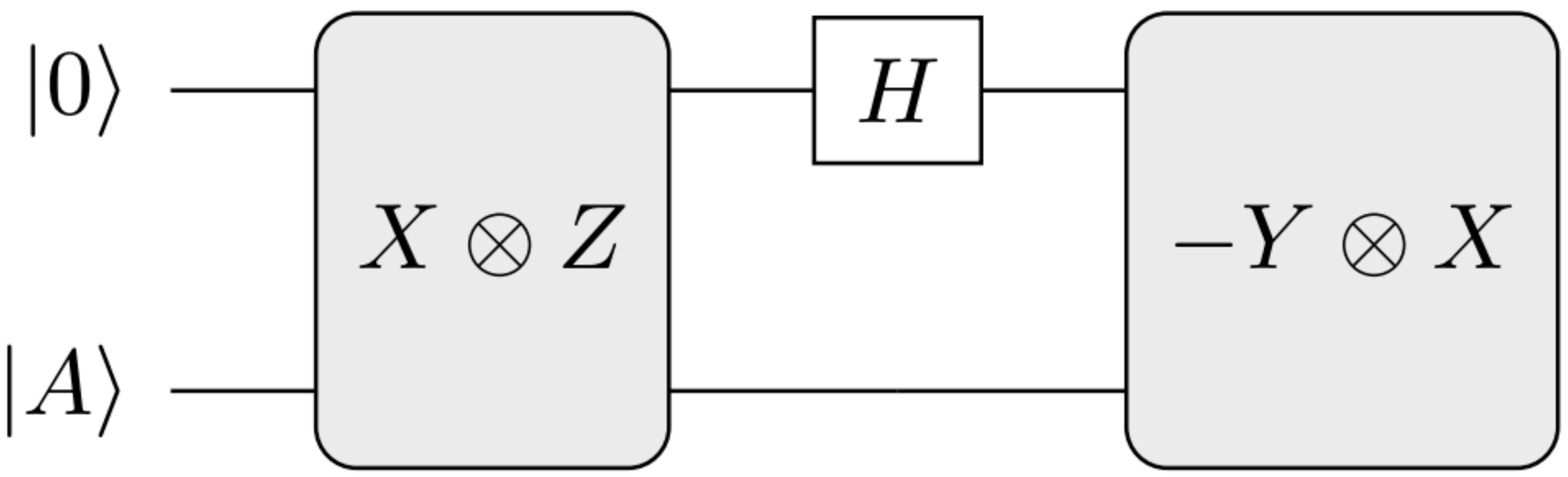

|0⟩
|A⟩
X ⊗ Z
H
S
H
Z


|0⟩
|A⟩
X ⊗ Z
H
−Y

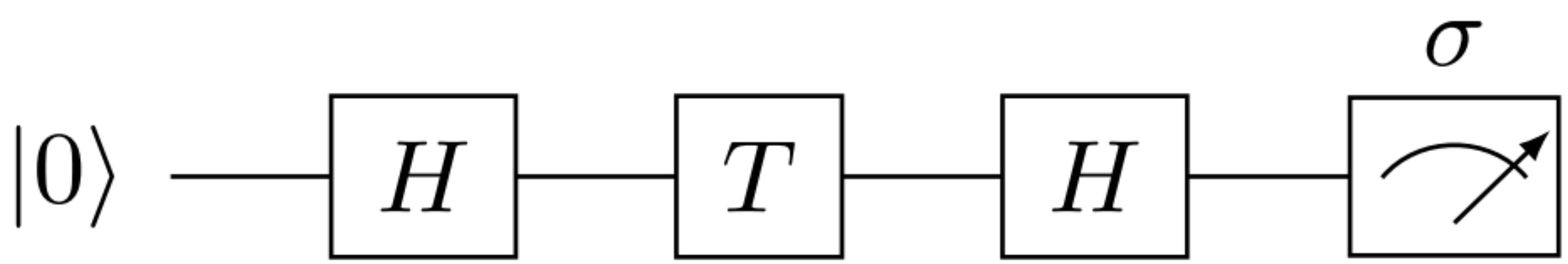
|0⟩
|A⟩
X ⊗ Z
H
???
Z

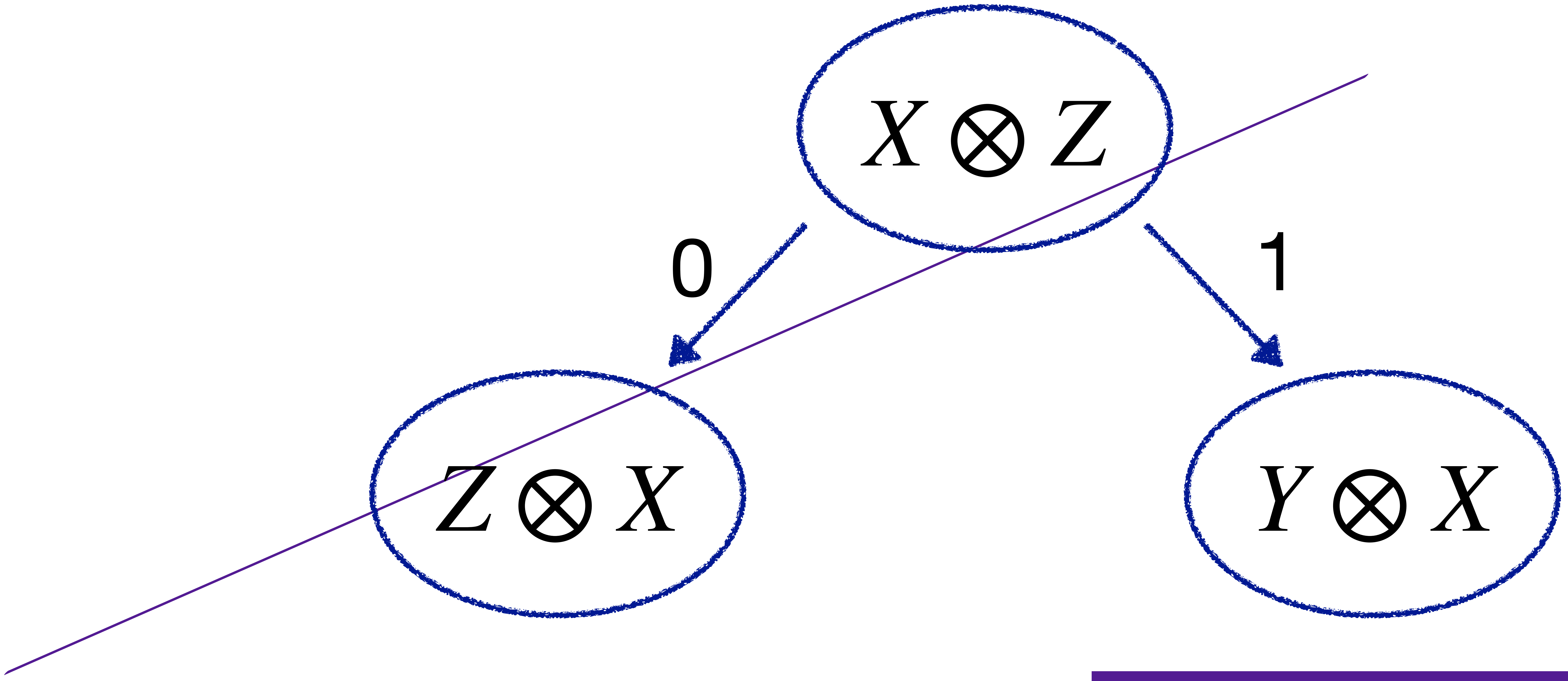

|0⟩
|A⟩
X ⊗ Z
H
S
H
Z


|0⟩
|A⟩
X ⊗ Z
H
−Y

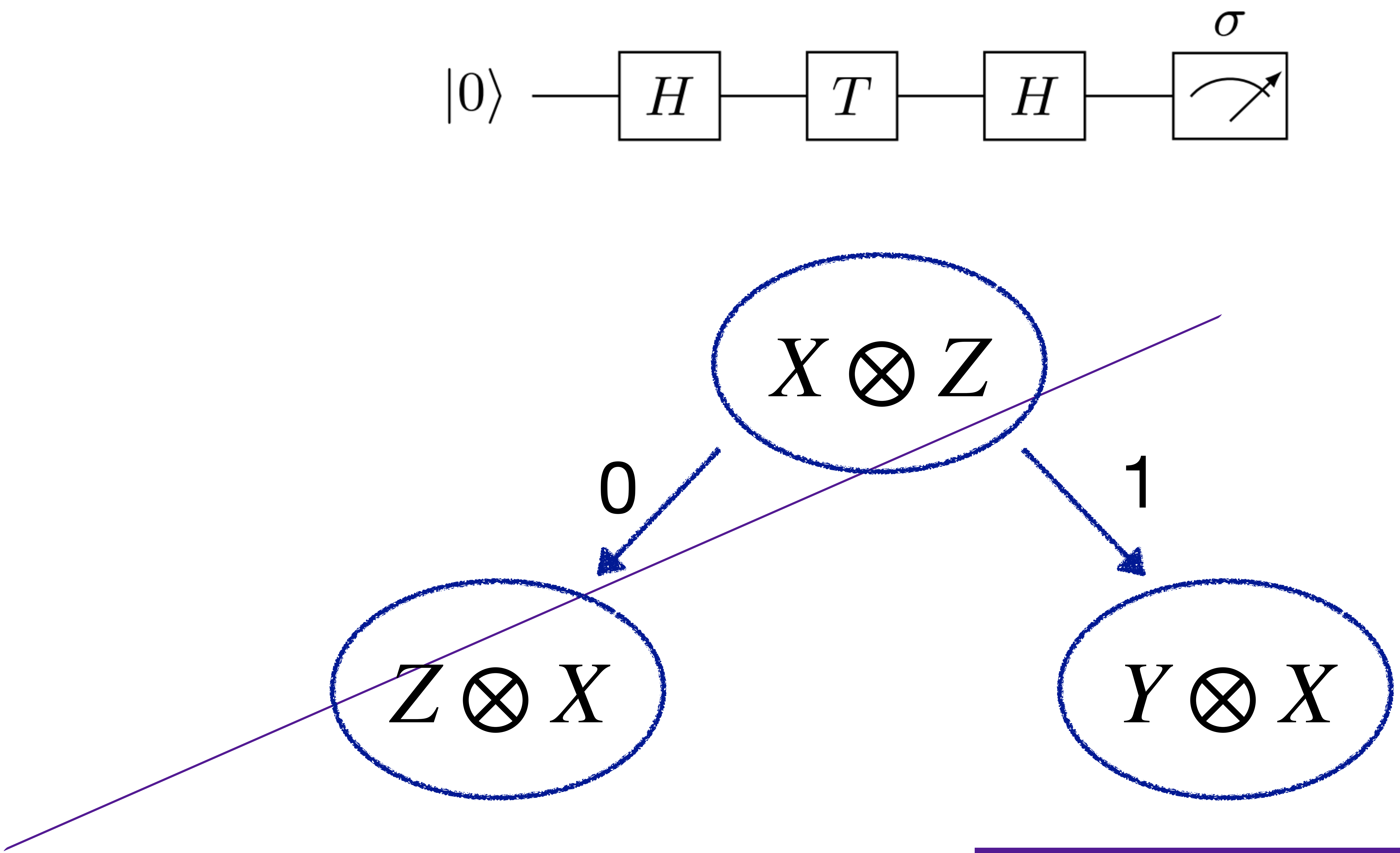

|0⟩
|A⟩
X ⊗ Z
H
−Y ⊗ X

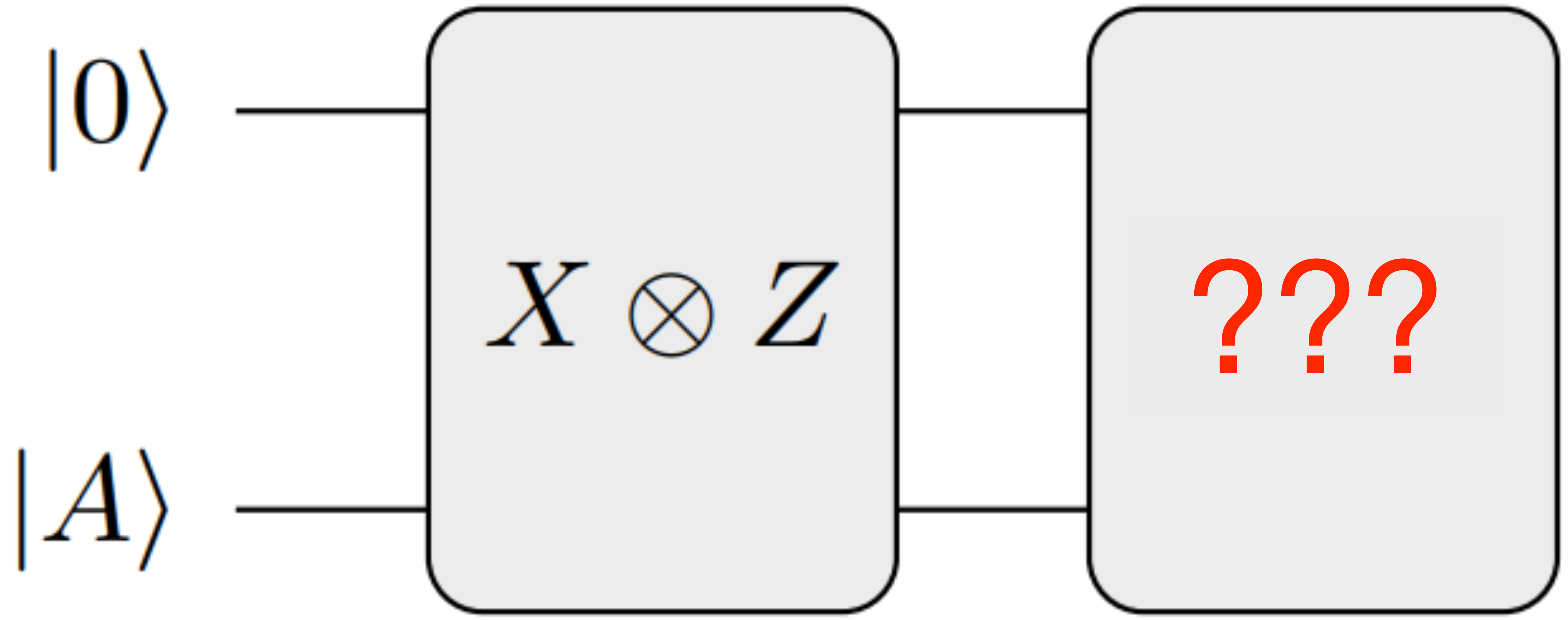

|0⟩
|A⟩
X ⊗ Z
H
???
Z
S
H
−Y
−Y ⊗ X
Y ⊗ X


$|0\rangle$
H
T
H
σ


$X \otimes Z$
0
1
$Z \otimes X$
$Y \otimes X$

For a circuit with w measurements and t gates this generalized PBC would have an associated tree with $\mathcal{O}(2^{w+t})$ paths!

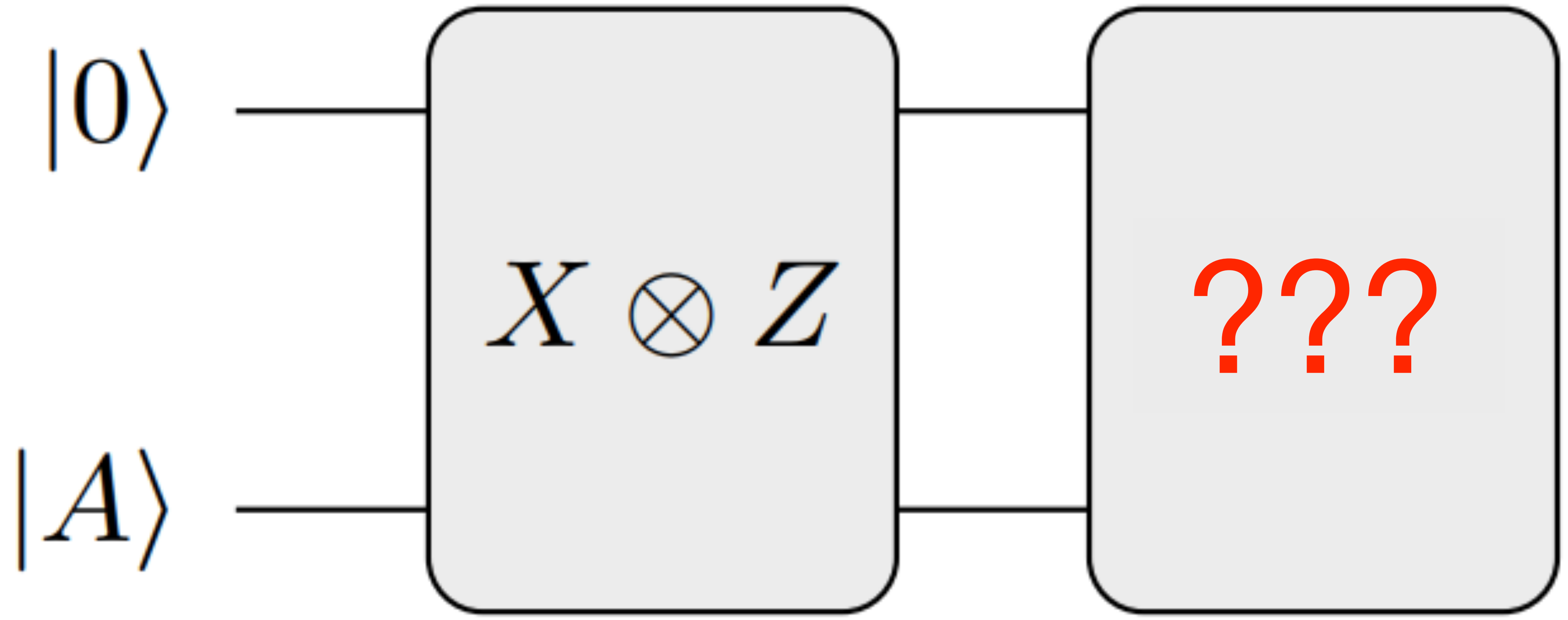

|0⟩
H
T
H
σ
X ⊗ Z
0
1
Z ⊗ X
Y ⊗ X



|0⟩
|A⟩
X ⊗ Z
???

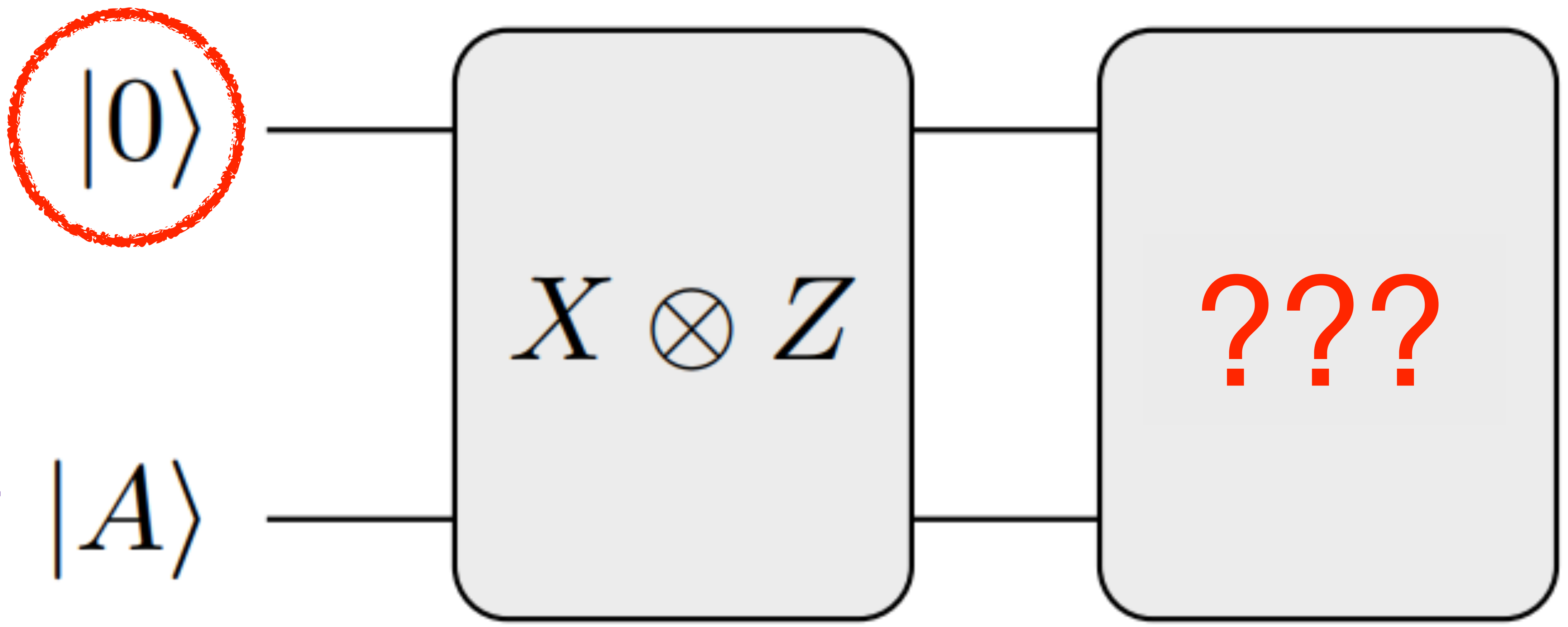
Now…

This does not fit the definition of a standard PBC!



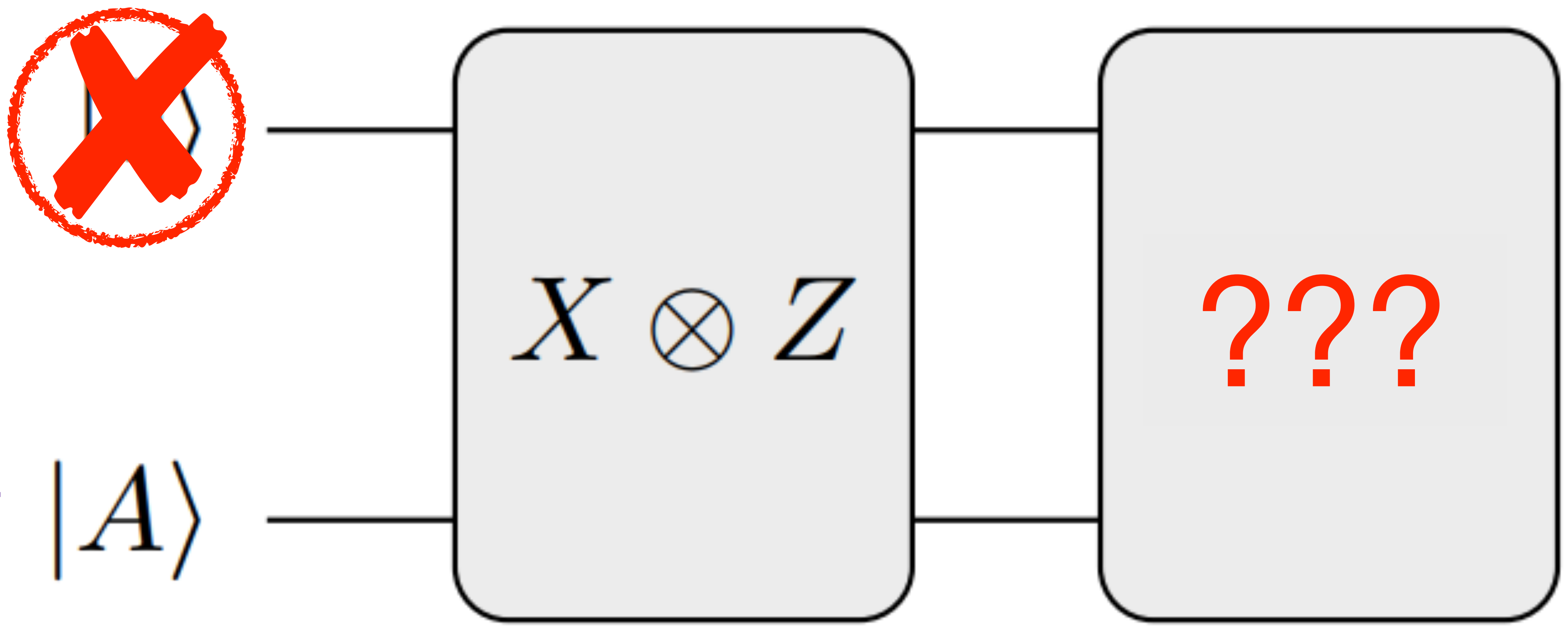
Now…

This does not fit the definition of a standard PBC!



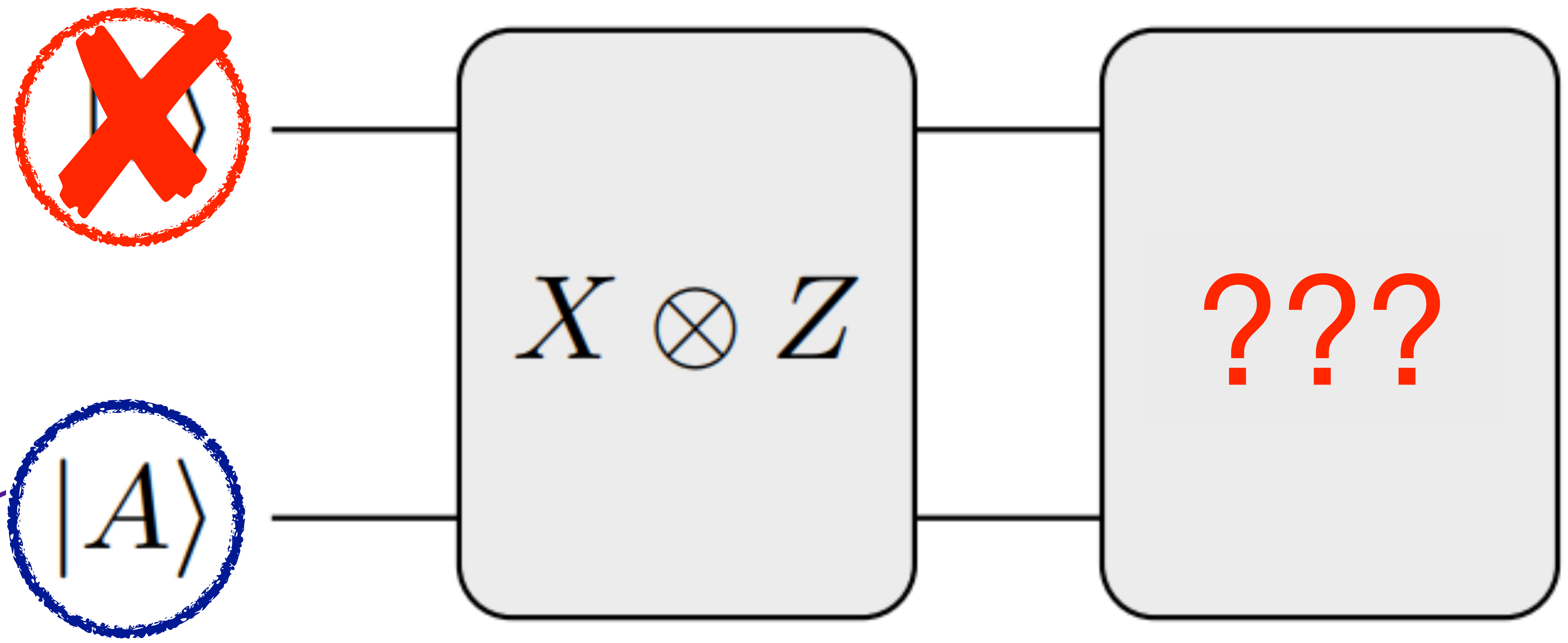
Now…

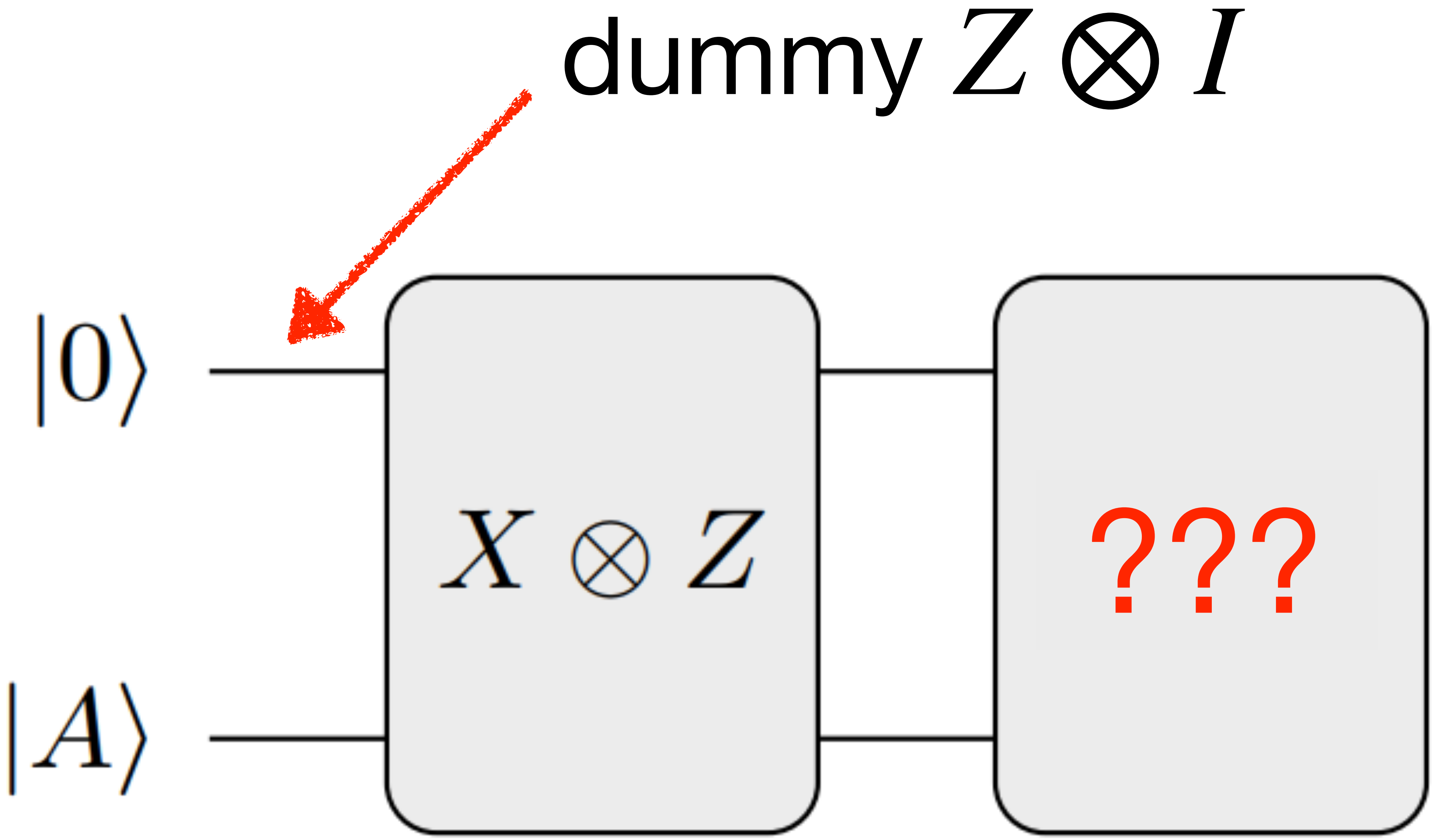
This does not fit the definition of a standard PBC!



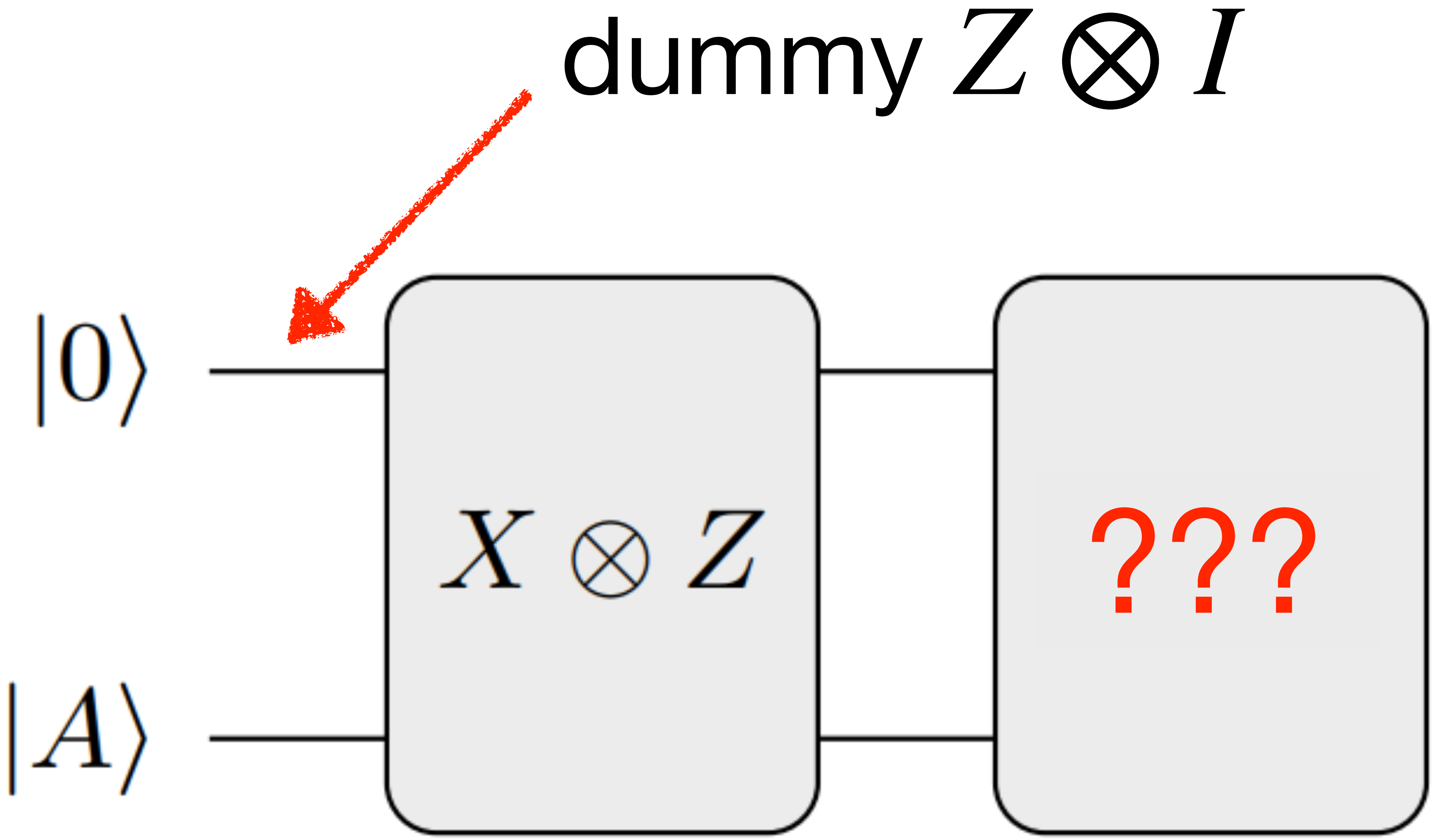
Now…

This does not fit the definition of a standard PBC!

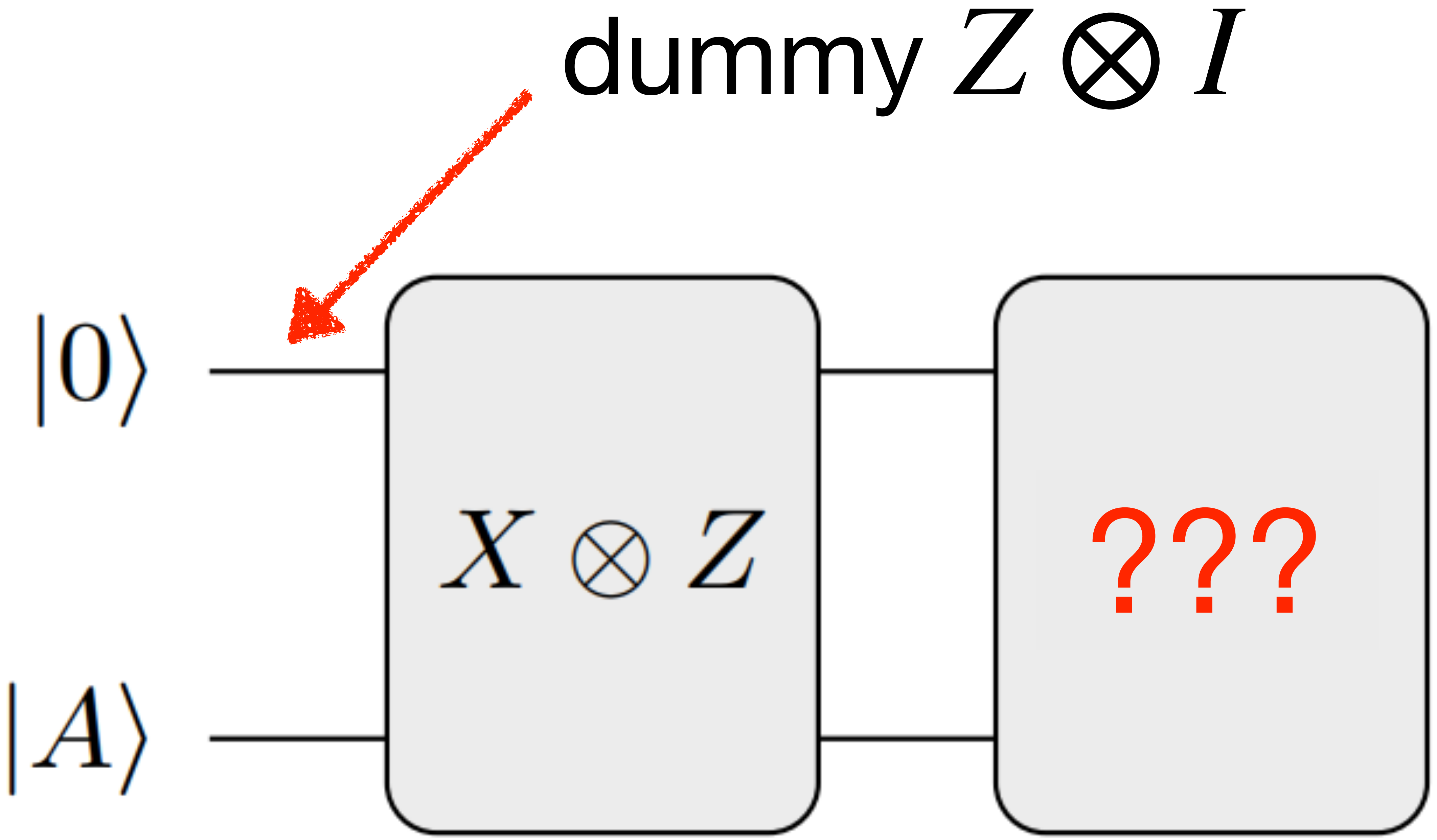




(1) Does P_i commute with all previous measurements?



a. No. P_i anti-commutes with at least one Pauli. → establish its outcome classically by coin tossing.

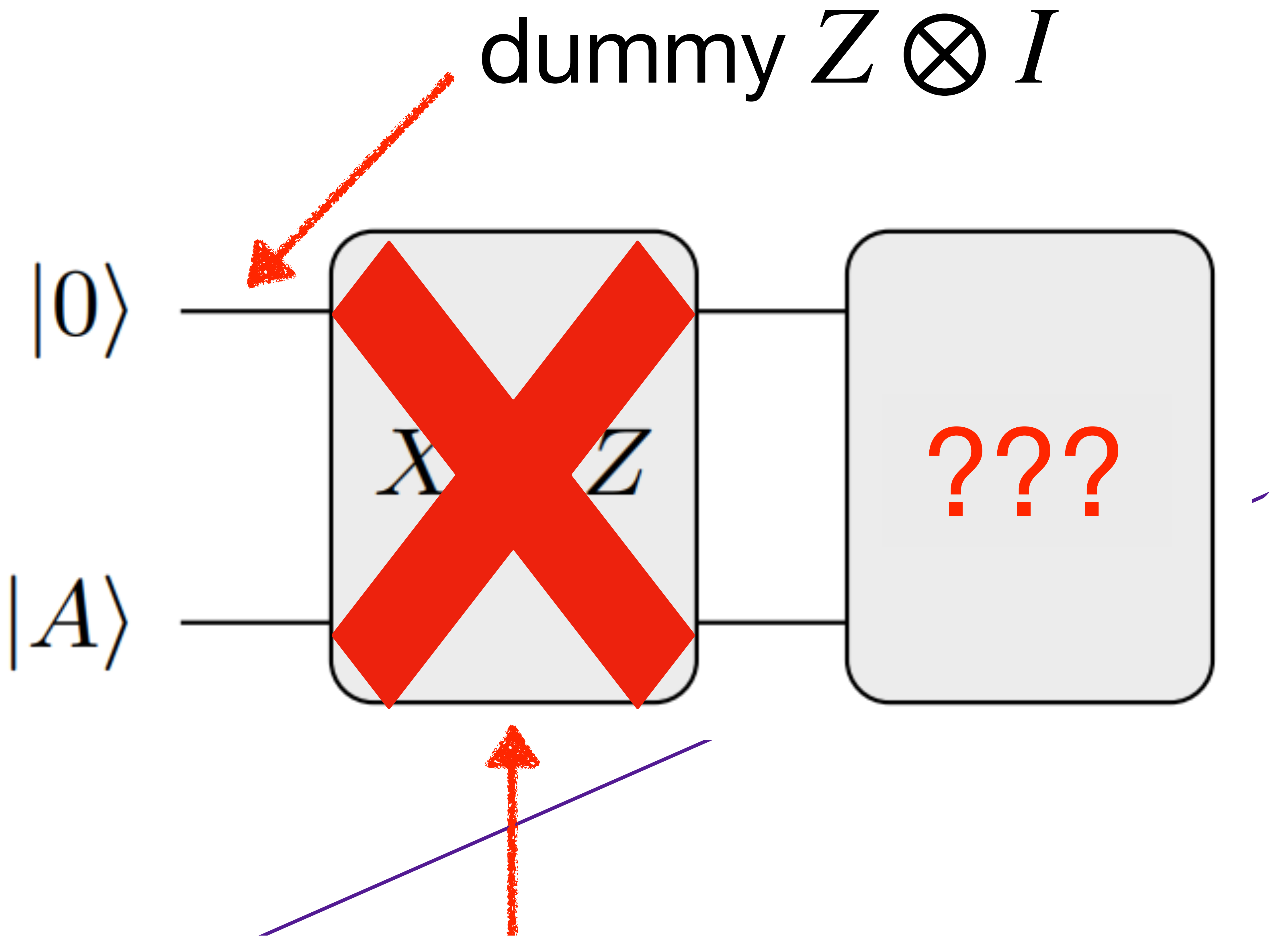


b. Yes. P_i commutes with all previously measured Paulis.

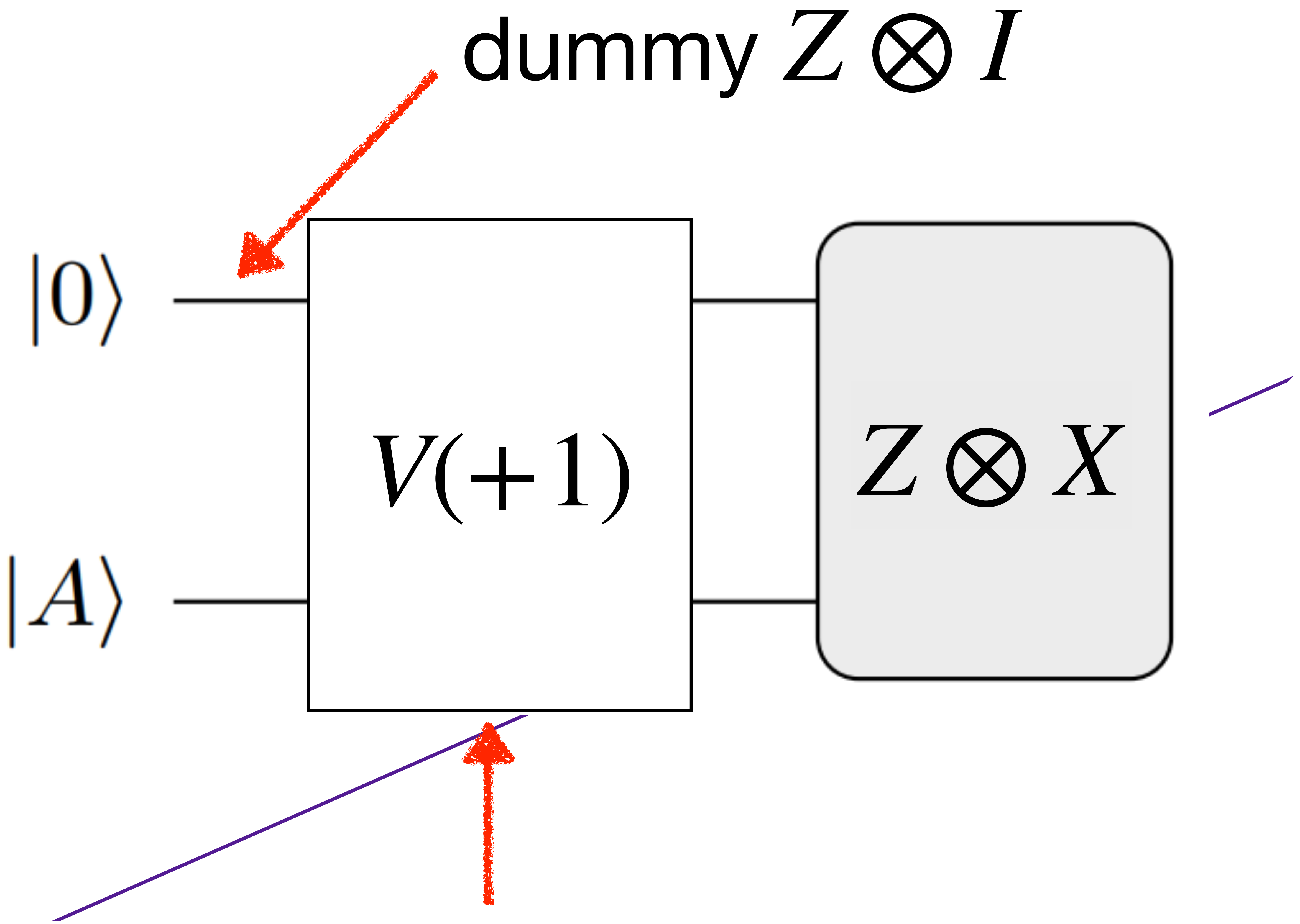
(2) Does it dependent on them?

a. Yes

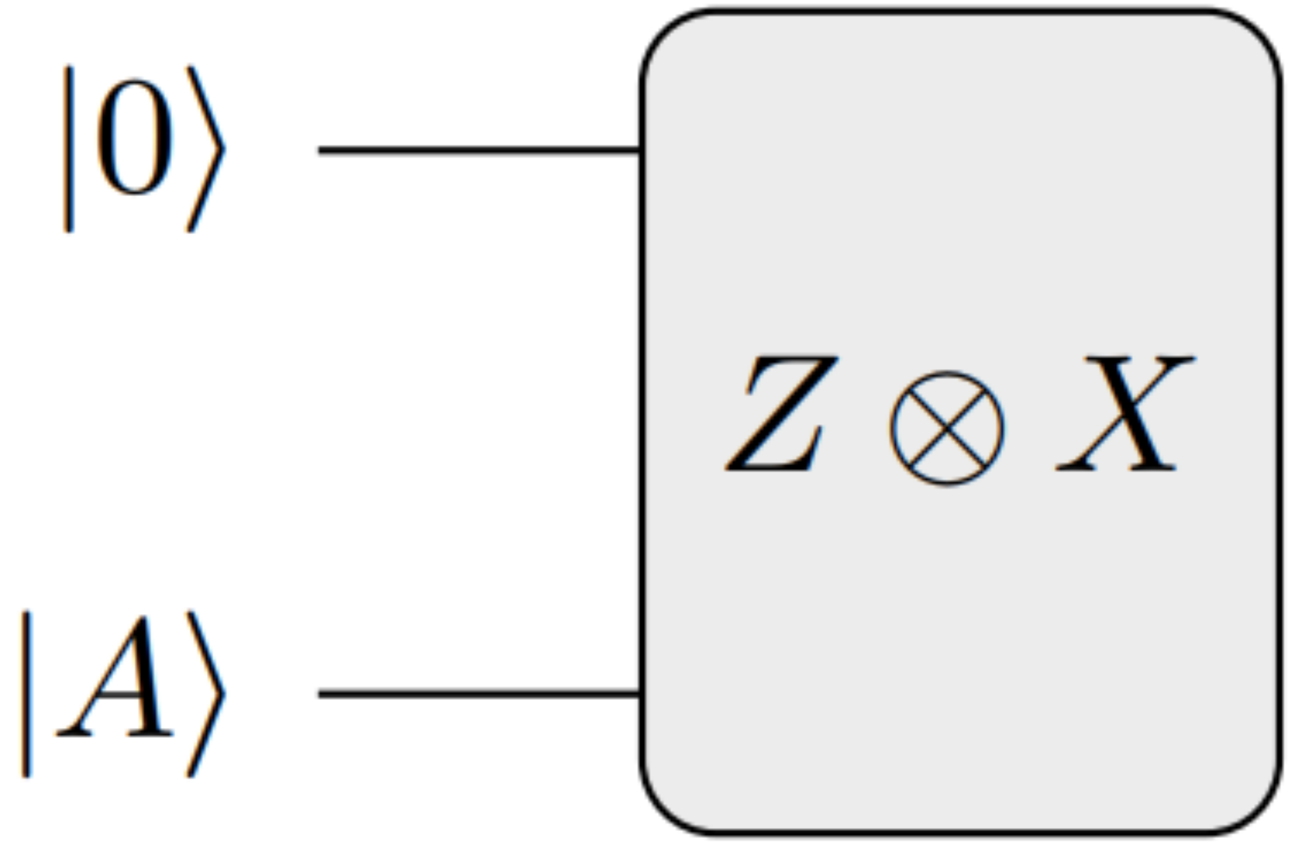
b. No

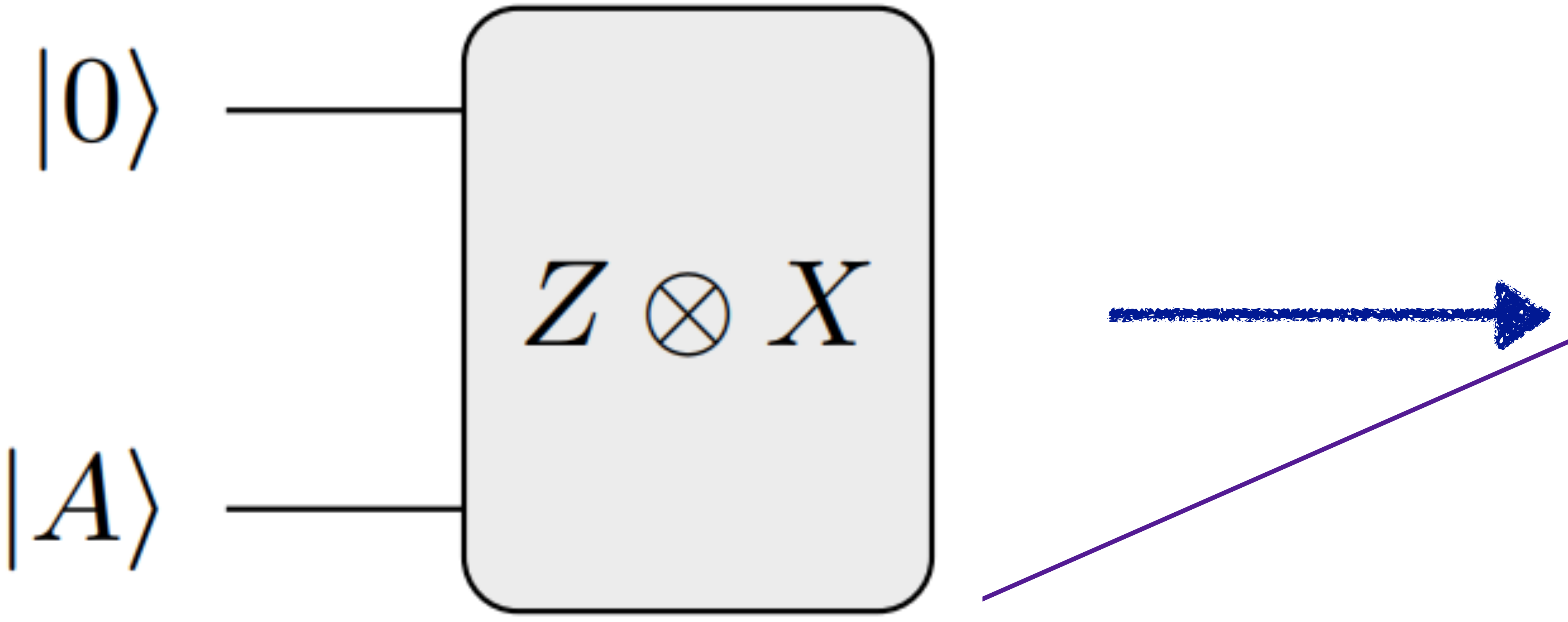


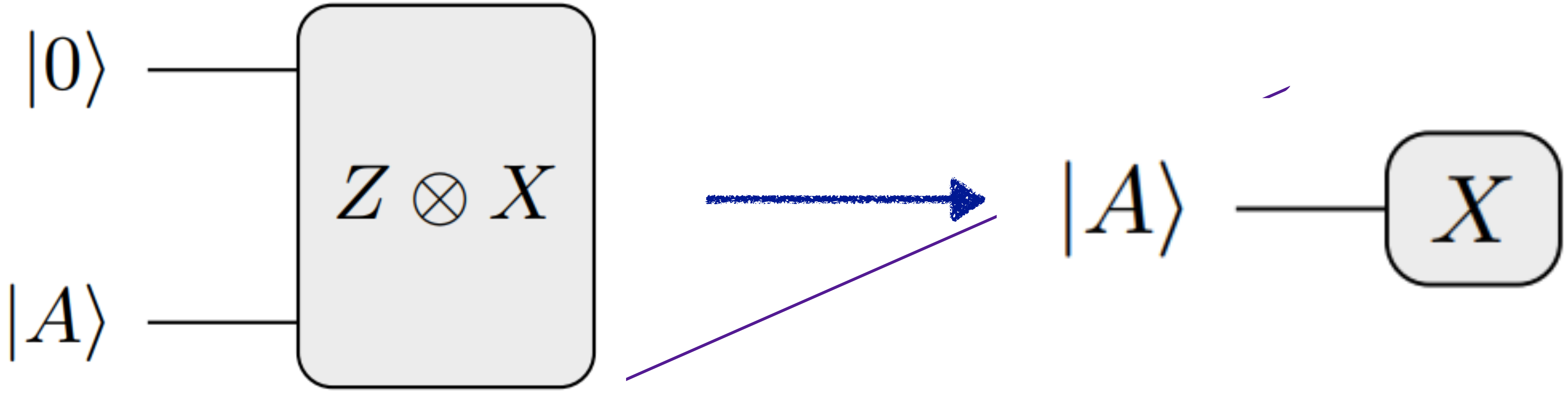
$$V(s) = \frac{Z \otimes I + sX \otimes Z}{\sqrt{2}}$$



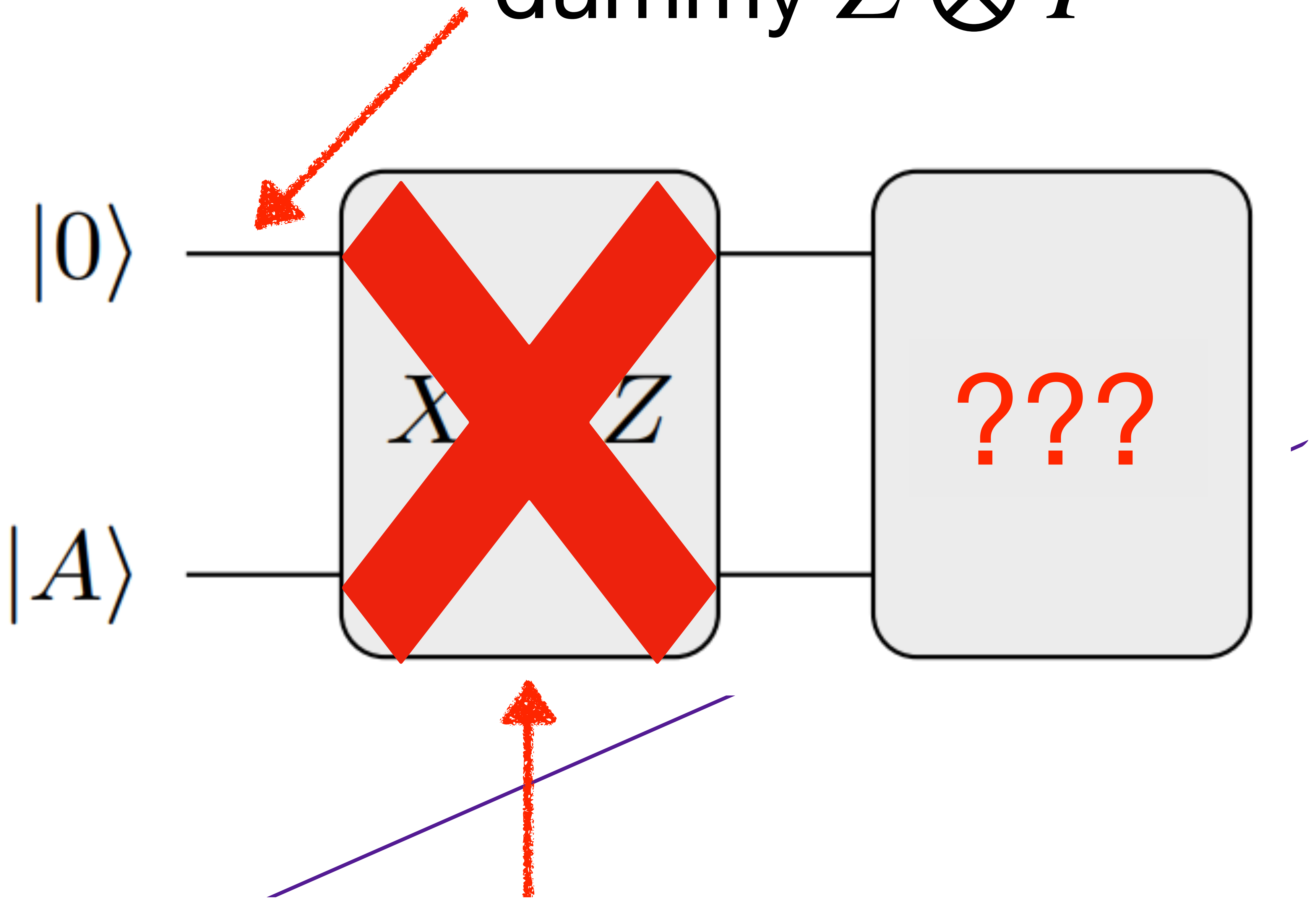
$$V(+1) = (I \otimes H) CX_{12} (H \otimes I) CX_{12} (I \otimes H)$$


$|0\rangle$
$|A\rangle$
$Z \otimes X$

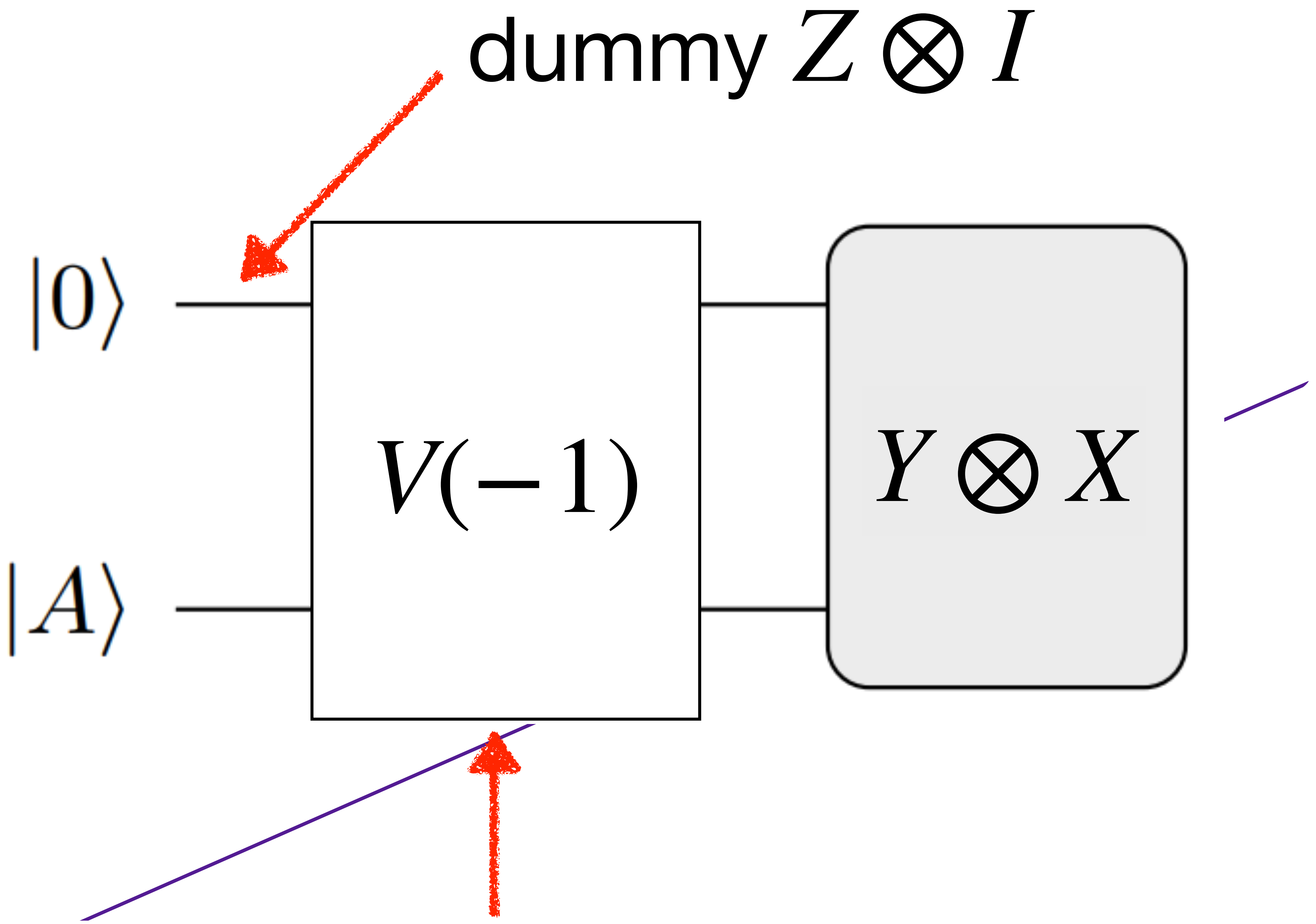

$|0\rangle$
$|A\rangle$
$Z \otimes X$


$|0\rangle$
$|A\rangle$
$Z \otimes X$
$|A\rangle$
X

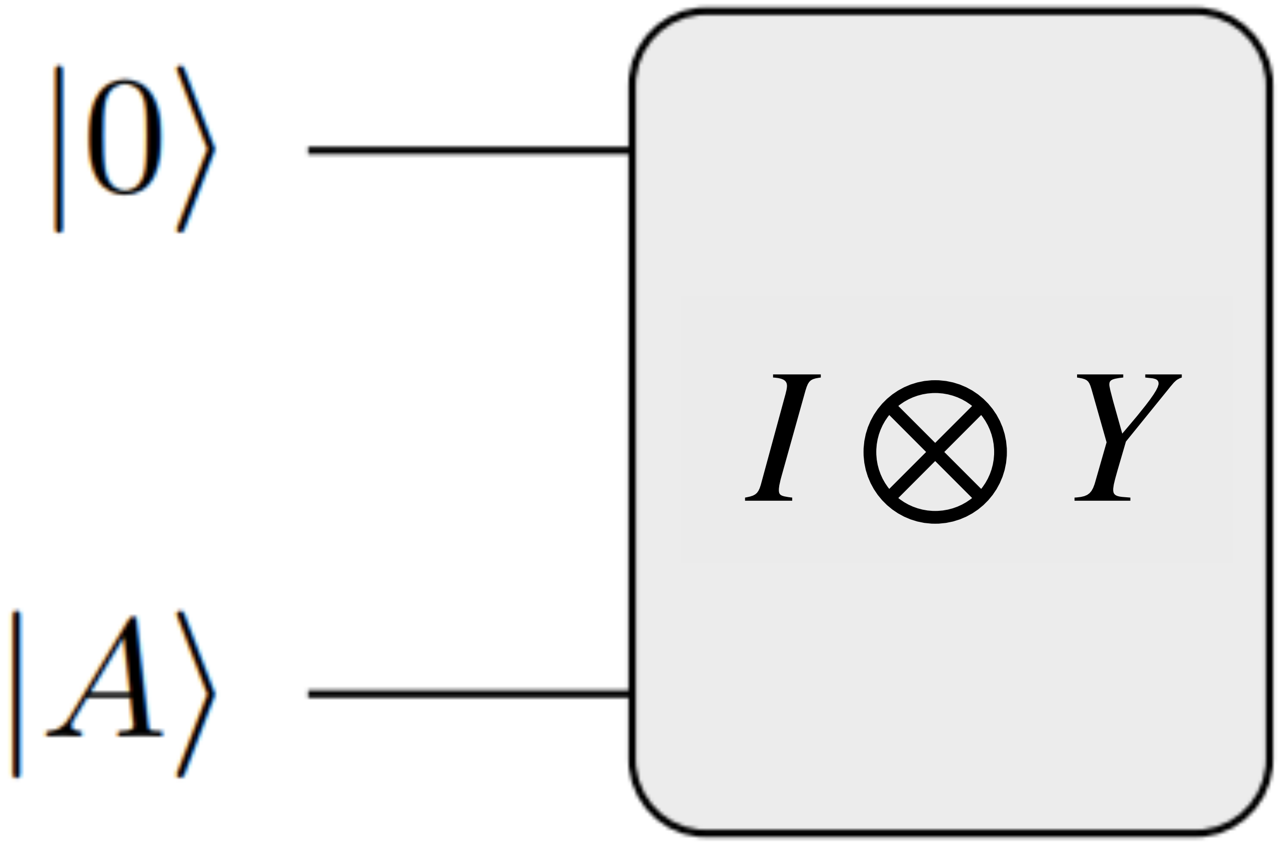
dummy $Z \otimes I$

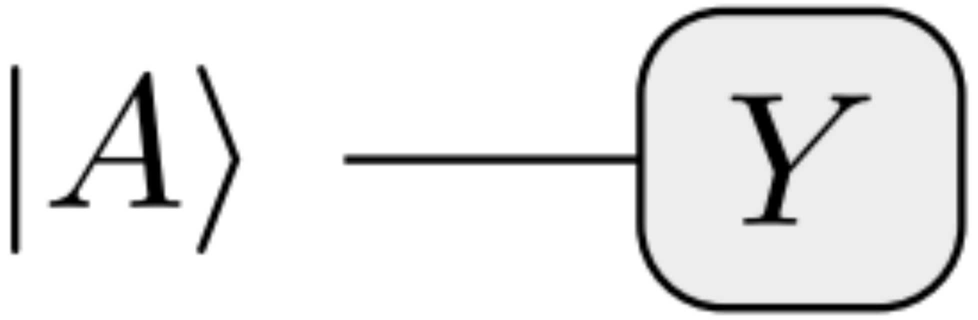


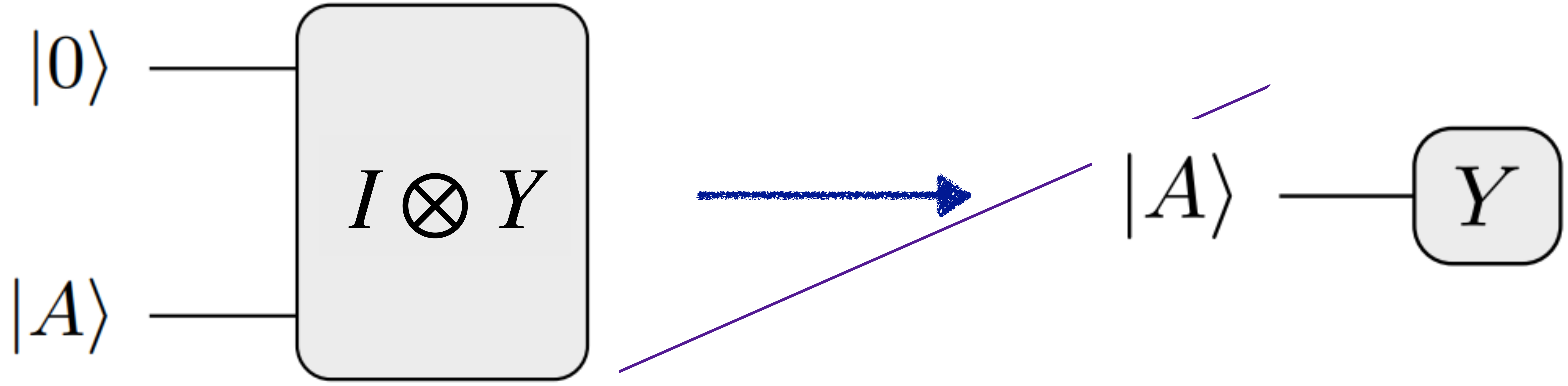
$$V(s) = \frac{Z \otimes I + sX \otimes Z}{\sqrt{2}}$$



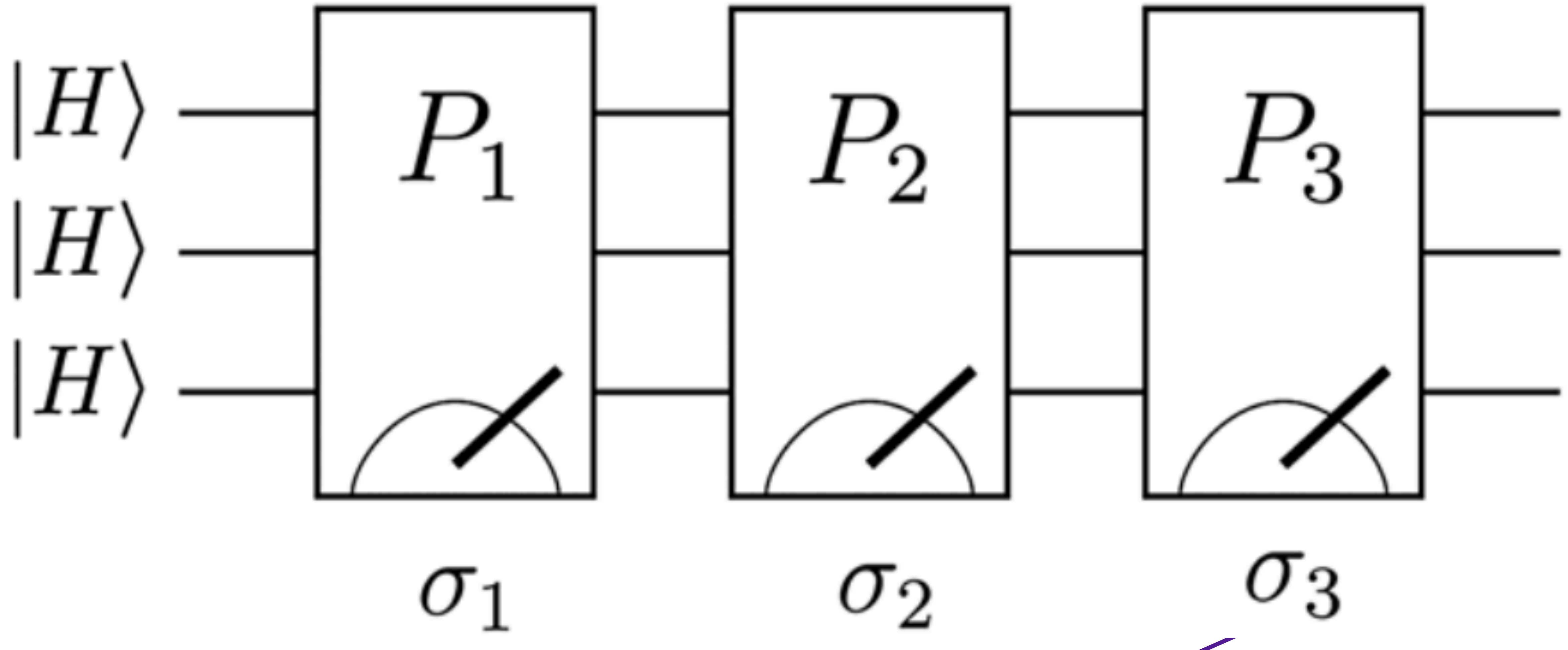
$$V(-1) = (I \otimes H) CX_{12} (ZH \otimes I) CX_{12} (Z \otimes H) .$$

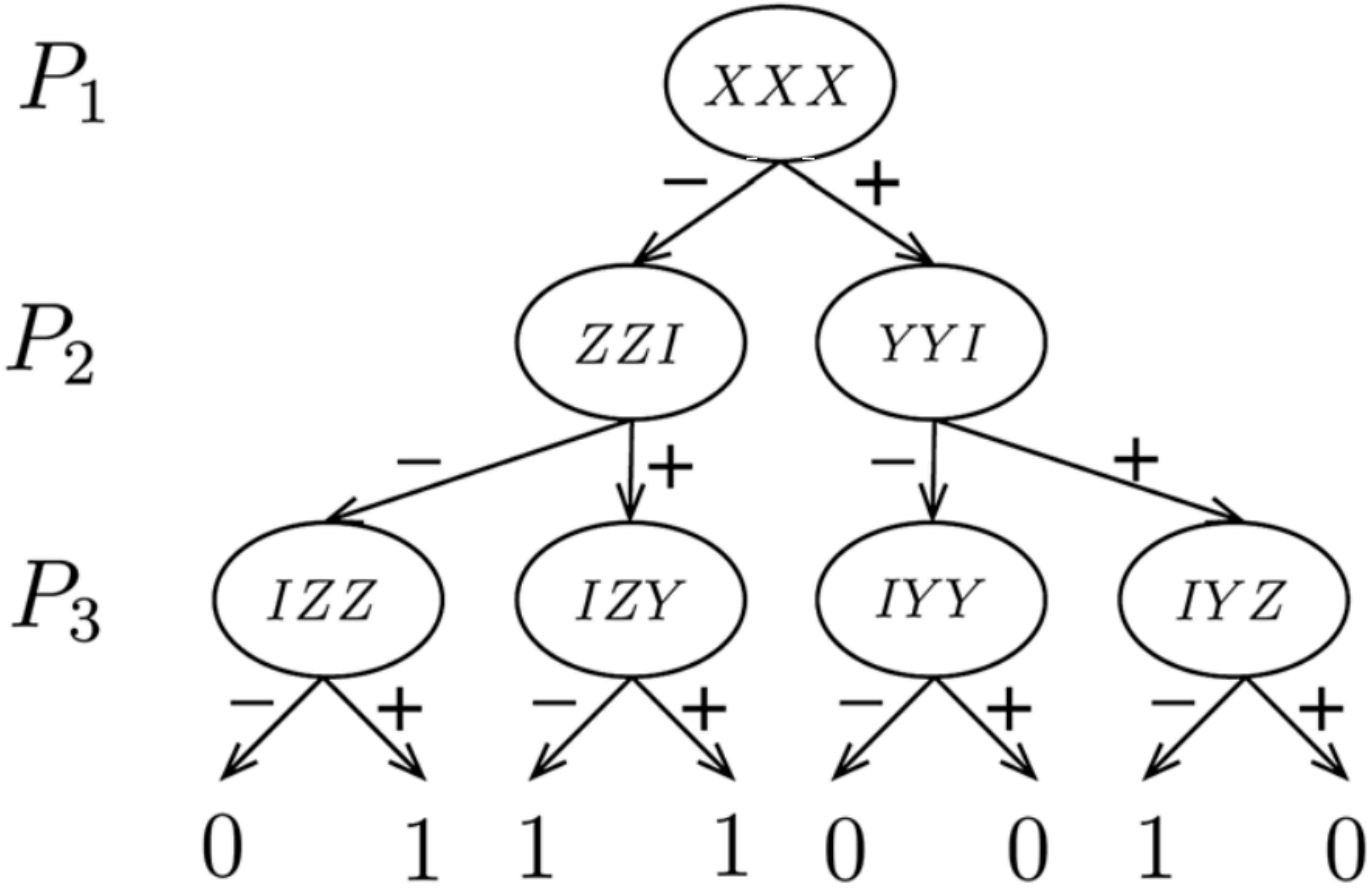

$|0\rangle$
$|A\rangle$
$I \otimes Y$


$|A\rangle$
Y

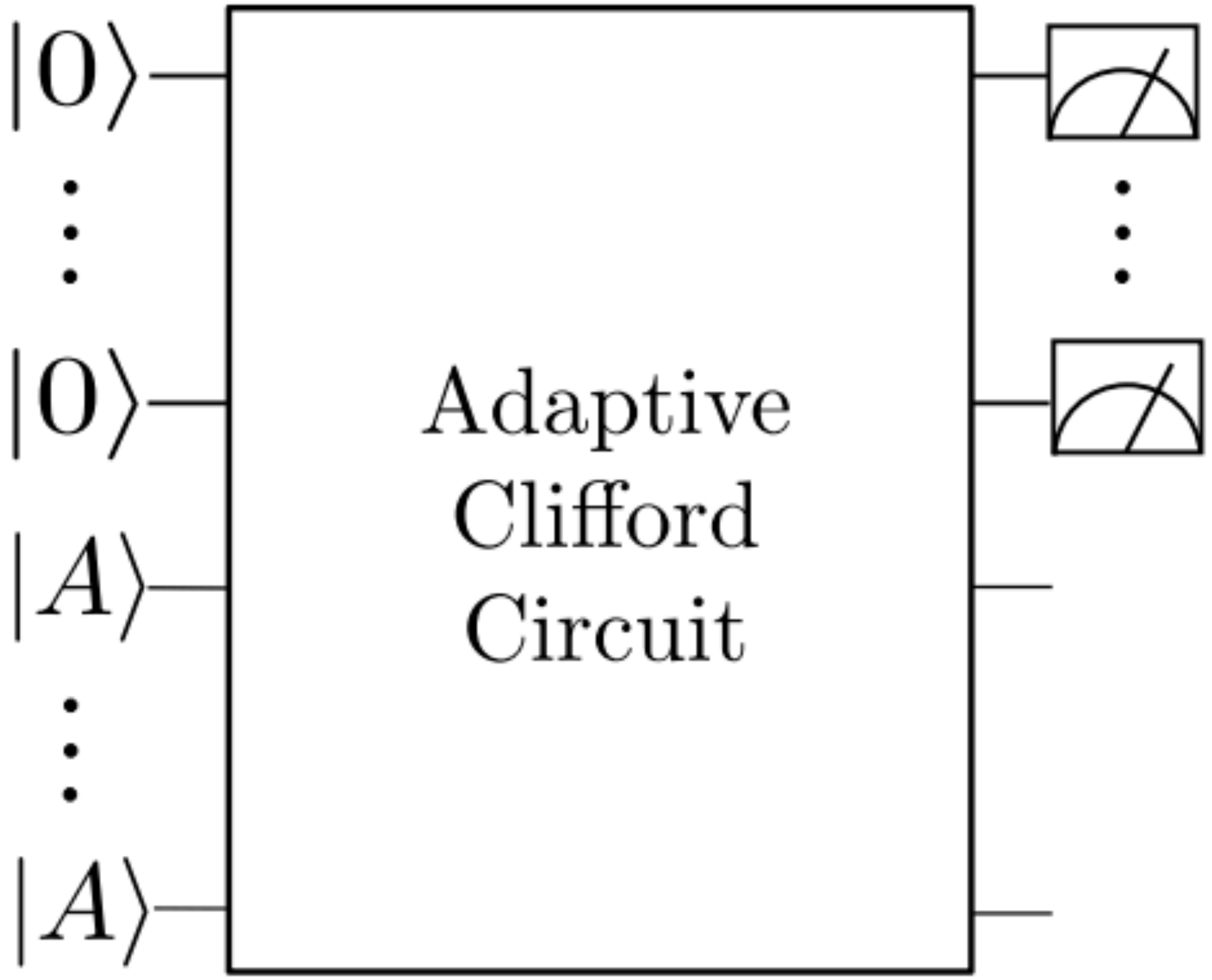


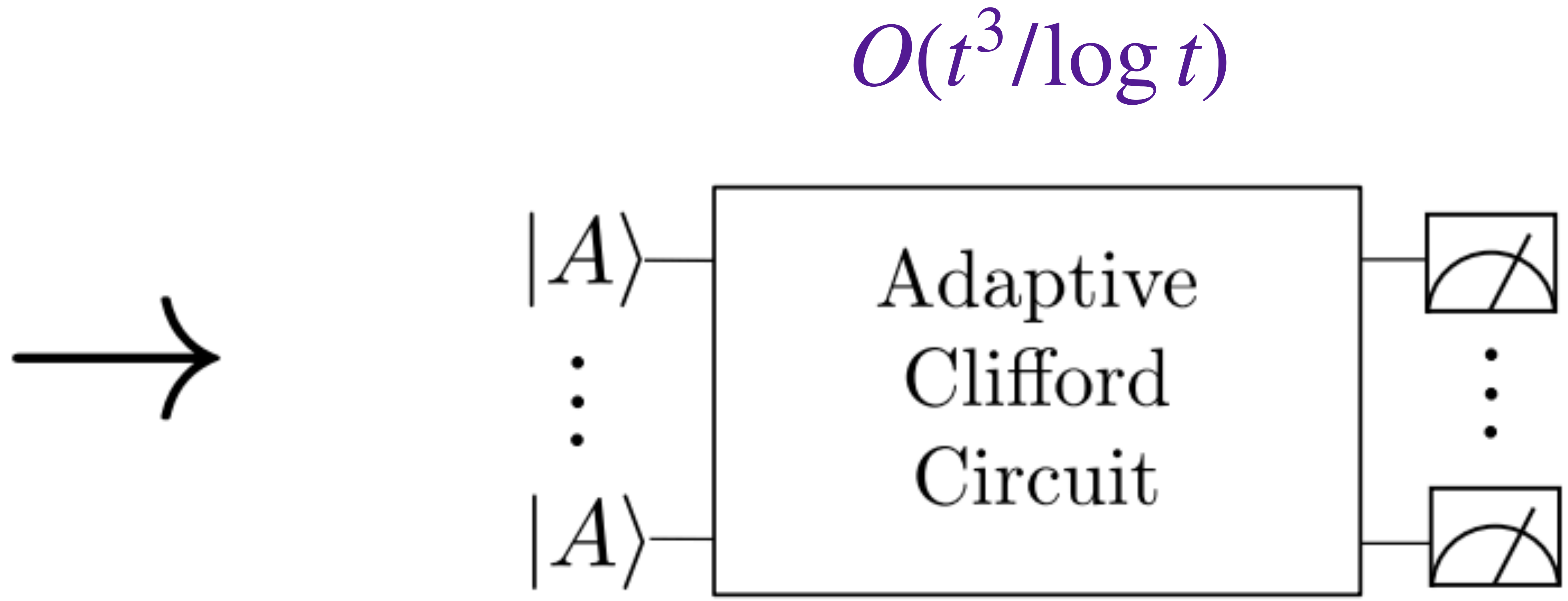
$|0\rangle$
$|A\rangle$
$I \otimes Y$
$|A\rangle$
Y


|H⟩
|H⟩
|H⟩
P_1
P_2
P_3
σ_1
σ_2
σ_3


P_1
P_2
P_3
XXX
ZZI
YYI
IZZ
IZY
IYY
IYZ
0 1 1 1 0 0 1 0

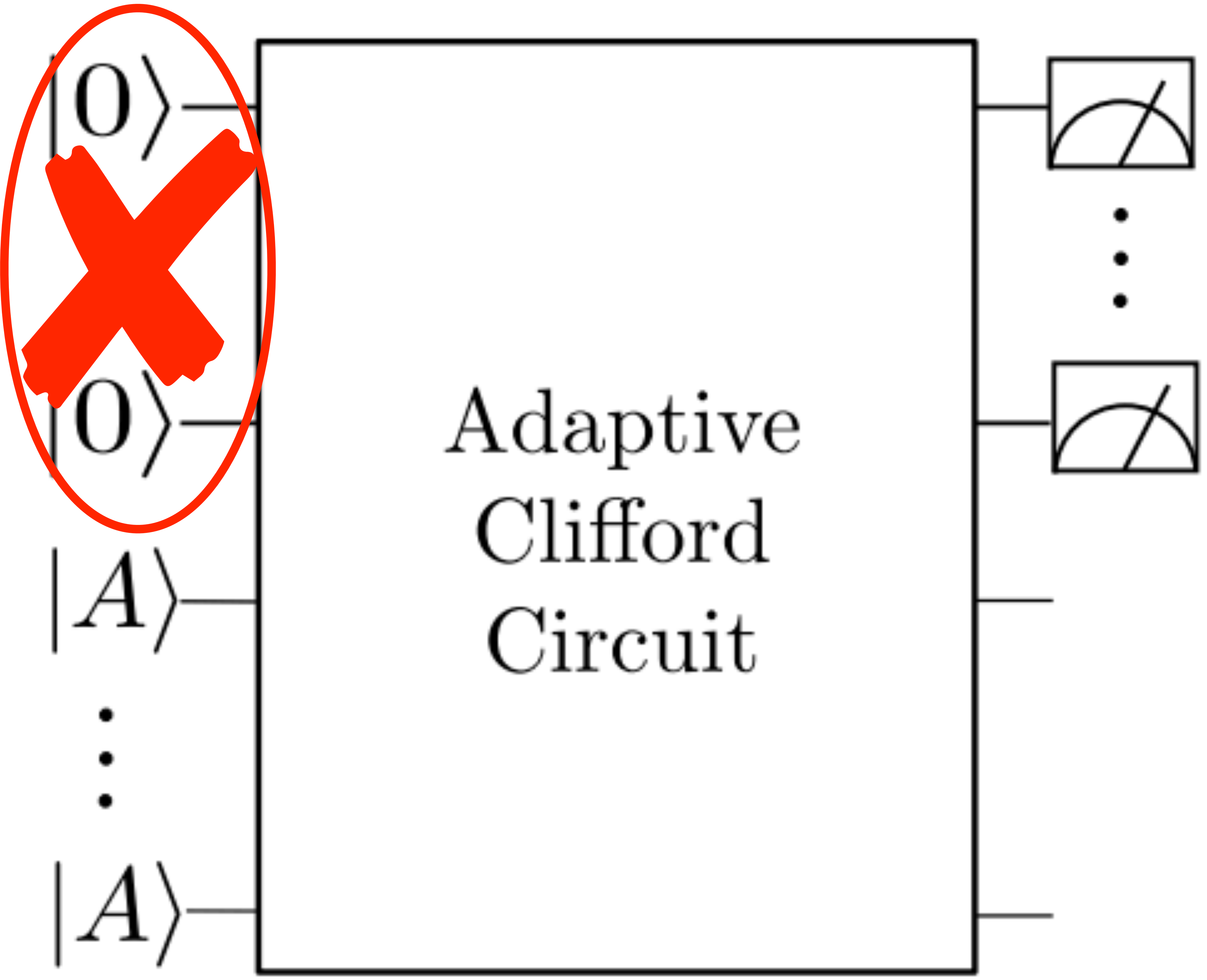
Returning to the quantum circuit model…





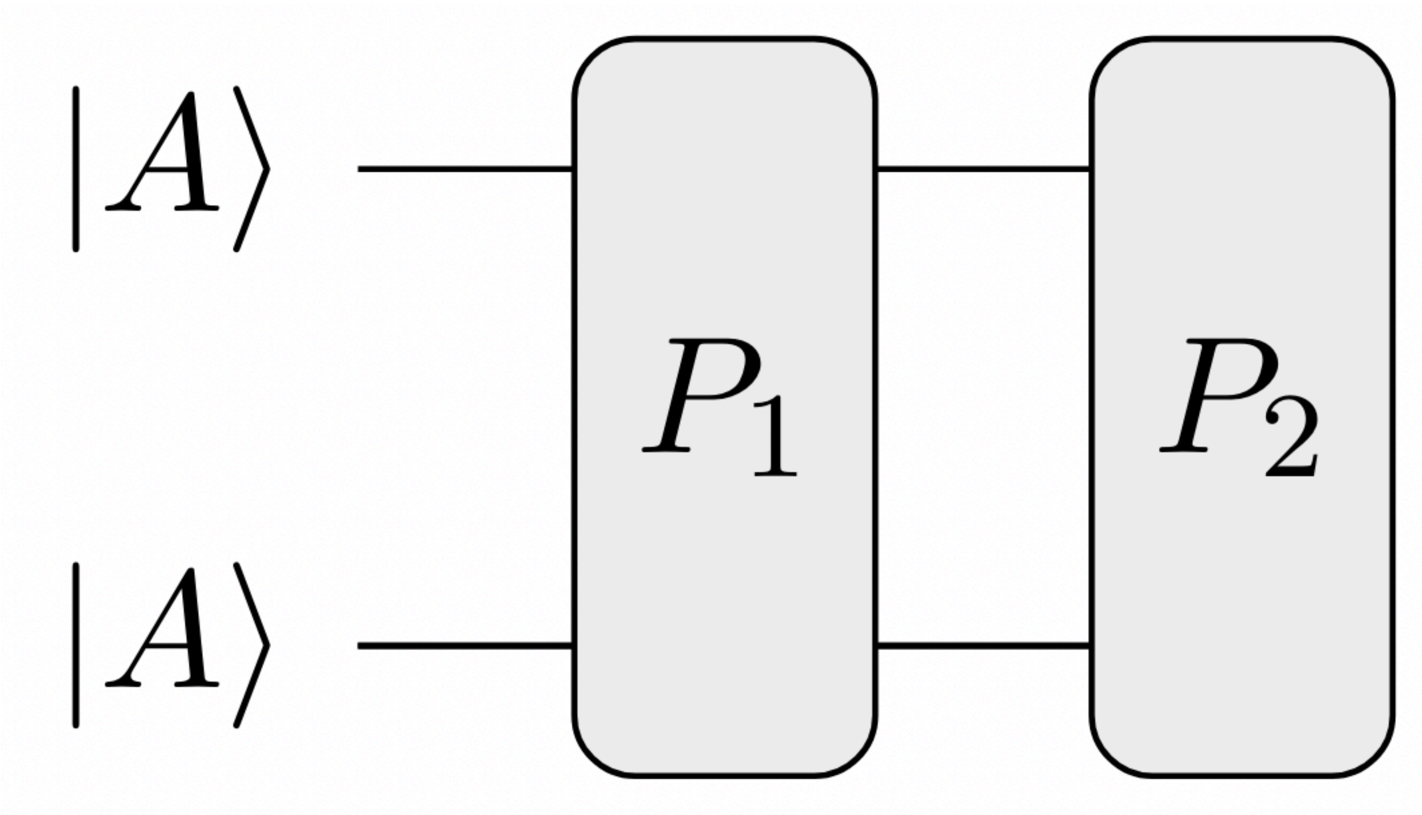
Mithuna Yoganathan, Richard Jozsa, and Sergii Strelchuk. "Quantum advantage of unitary Clifford circuits with magic state inputs". In: Proc. R. Soc. A 475 (2019)

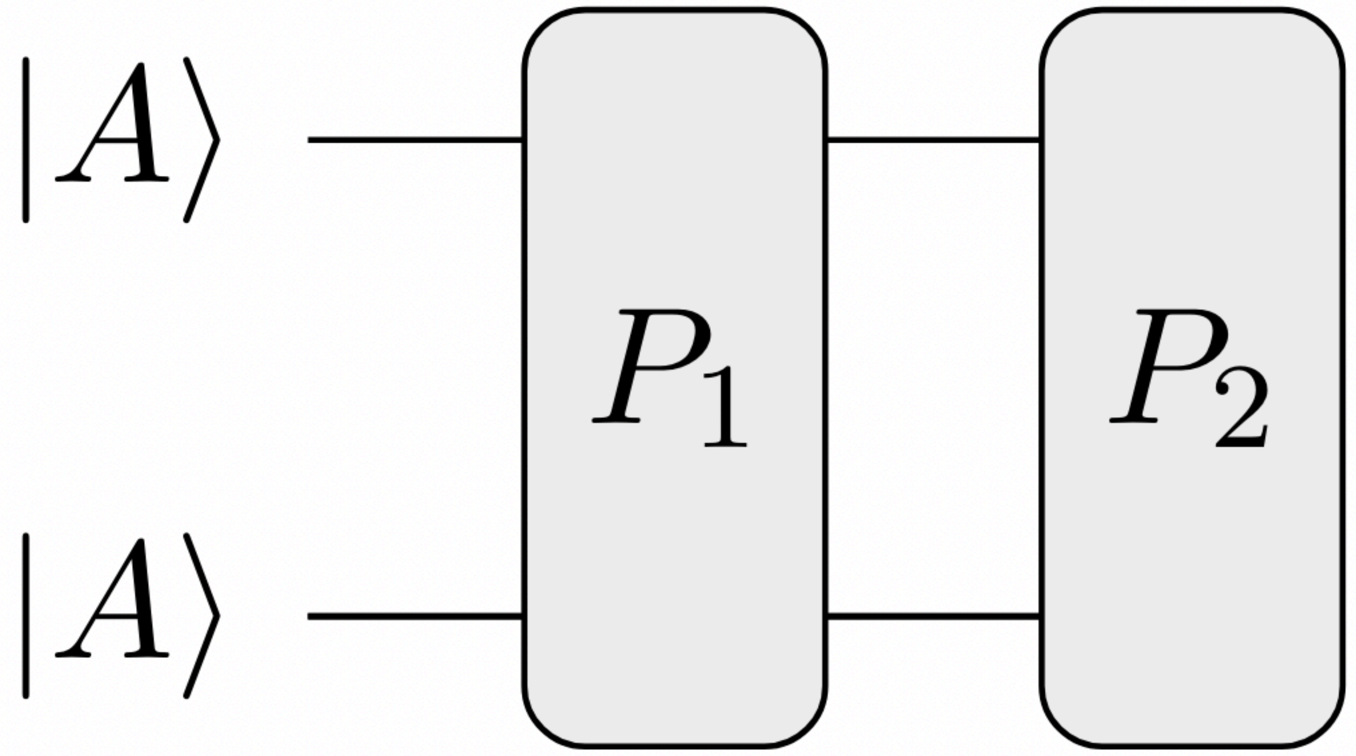
Returning to the quantum circuit model…



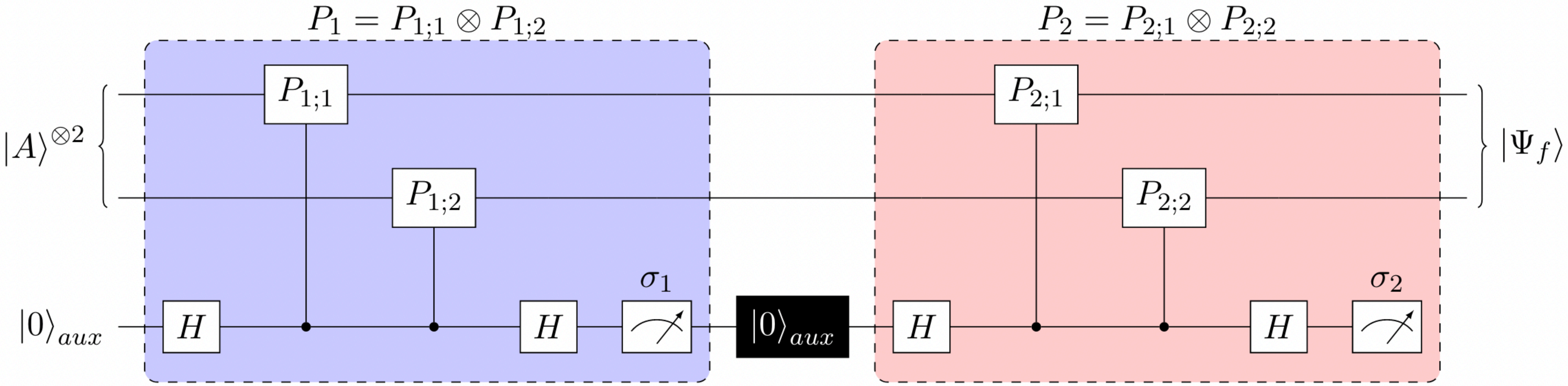
$O(t^3/\log t)$

Mithuna Yoganathan, Richard Jozsa, and Sergii Strelchuk. "Quantum advantage of unitary Clifford circuits with magic state inputs". In: Proc. R. Soc. A 475 (2019)

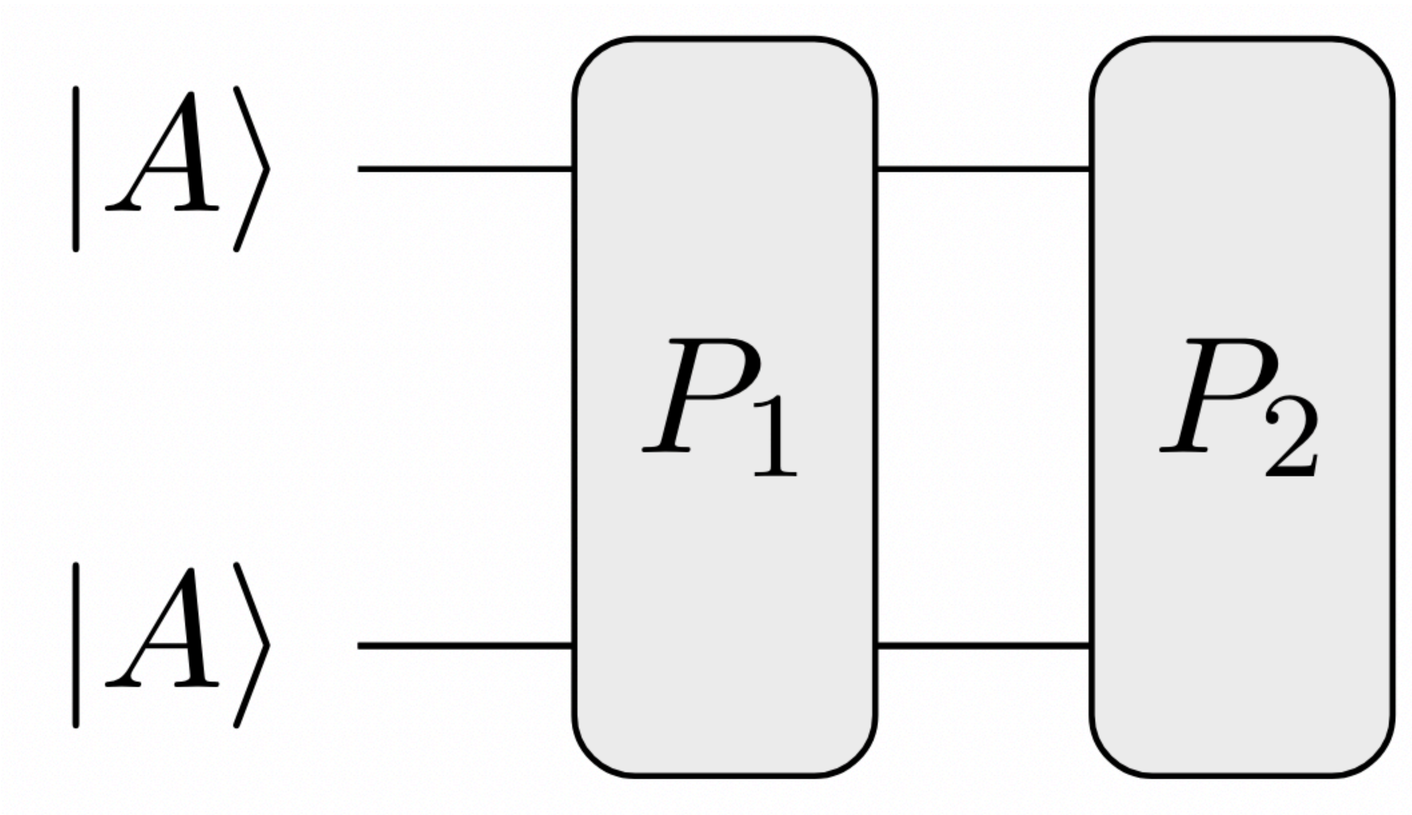

$|A\rangle$
$|A\rangle$
P_1
P_2

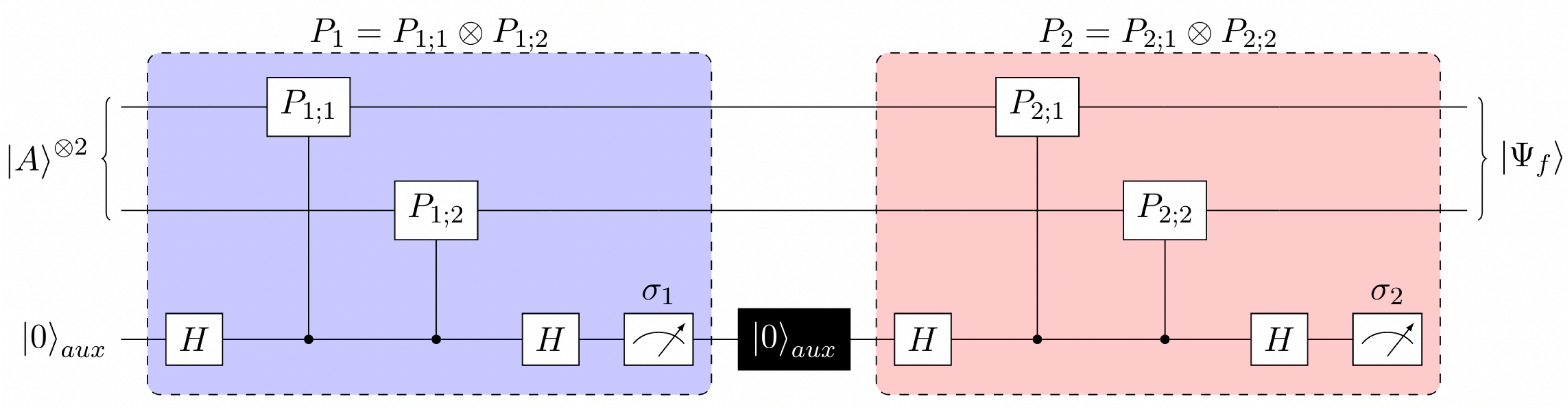


$|A\rangle$
$|A\rangle$
P_1
P_2

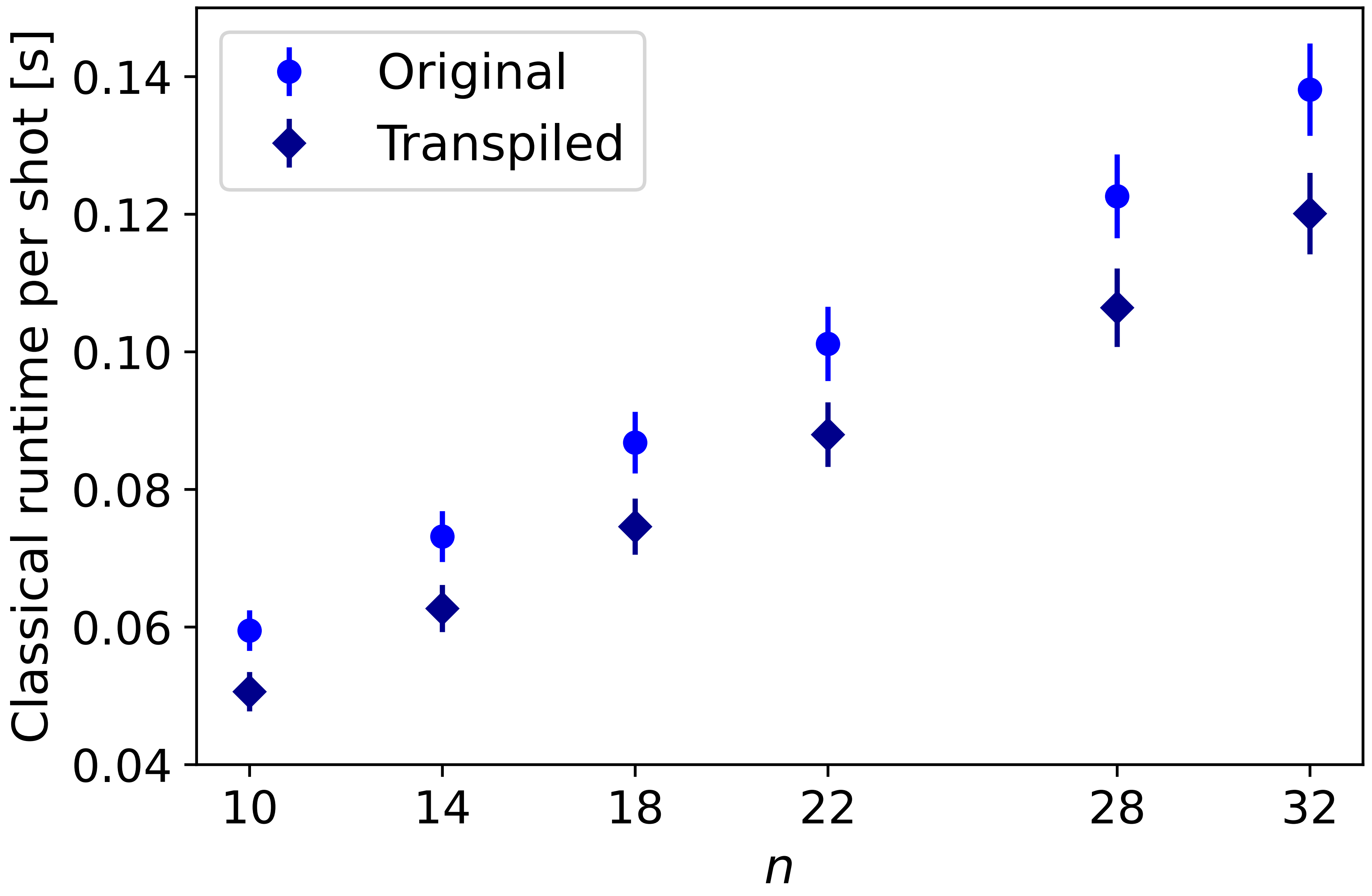


$P_1 = P_{1;1} \otimes P_{1;2}$
$P_2 = P_{2;1} \otimes P_{2;2}$
$|A\rangle^{\otimes 2}$
$|\Psi_f\rangle$
$|0\rangle_{aux}$
$P_{1;1}$
$P_{1;2}$
$P_{2;1}$
$P_{2;2}$
H
σ_1
σ_2
$|0\rangle_{aux}$

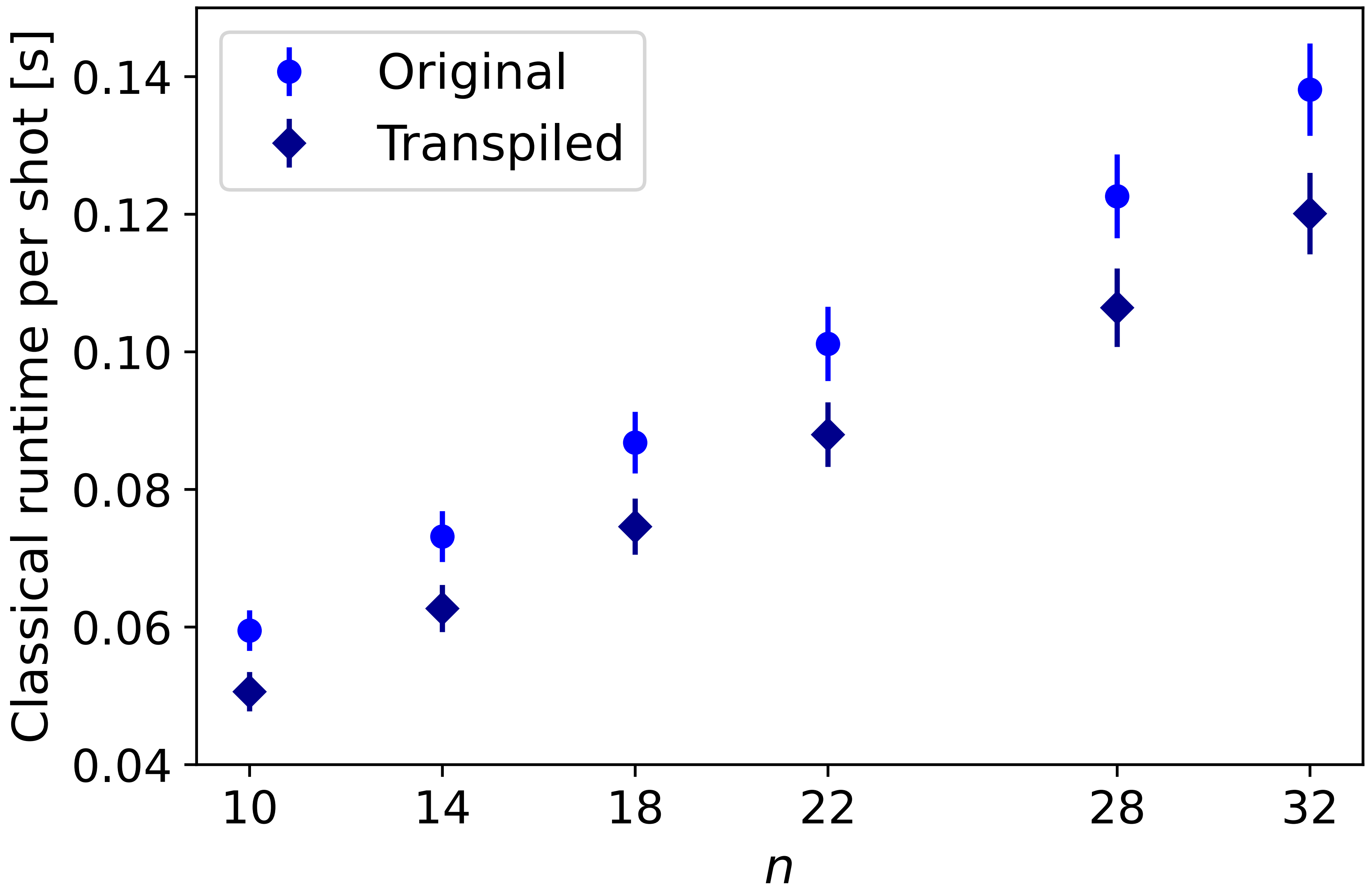

$|A\rangle$
$|A\rangle$
P_1
P_2

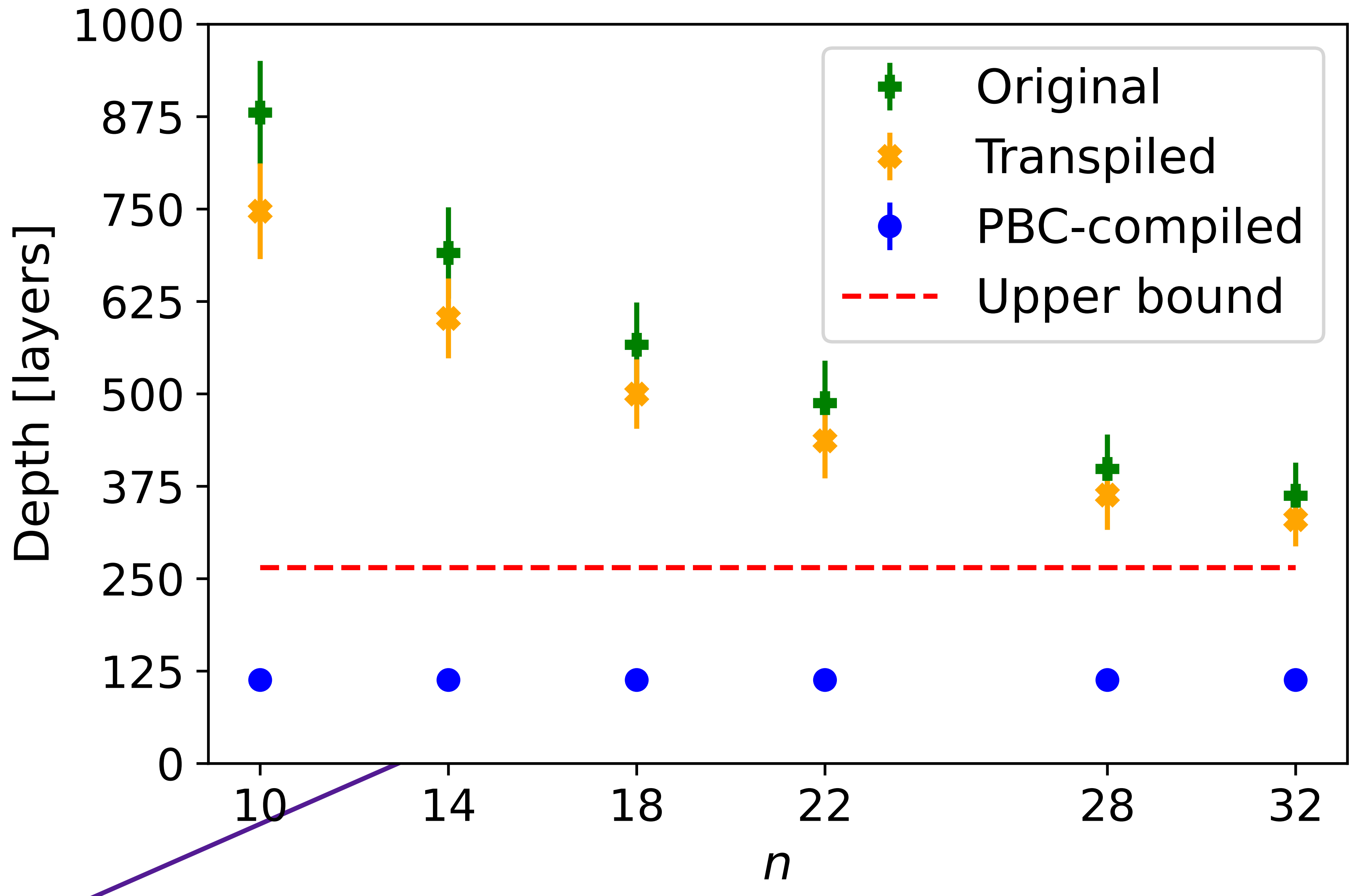

$P_1 = P_{1;1} \otimes P_{1;2}$
$P_2 = P_{2;1} \otimes P_{2;2}$
$|A\rangle^{\otimes 2}$
$|0\rangle_{aux}$
H
$P_{1;1}$
$P_{1;2}$
H
σ_1
$|0\rangle_{aux}$
H
$P_{2;1}$
$P_{2;2}$
H
σ_2
$|\Psi_f\rangle$

$O(t^2)$

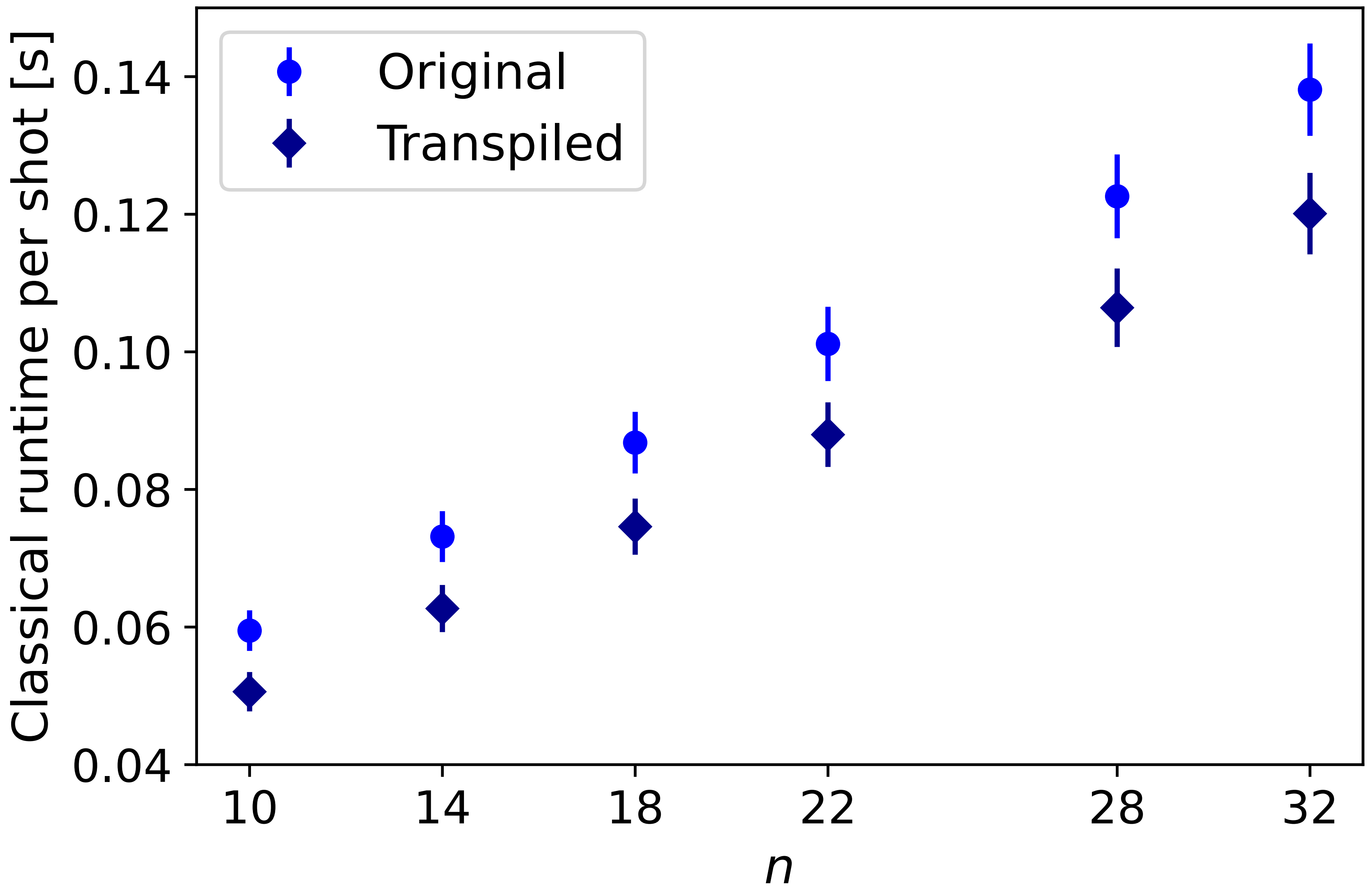


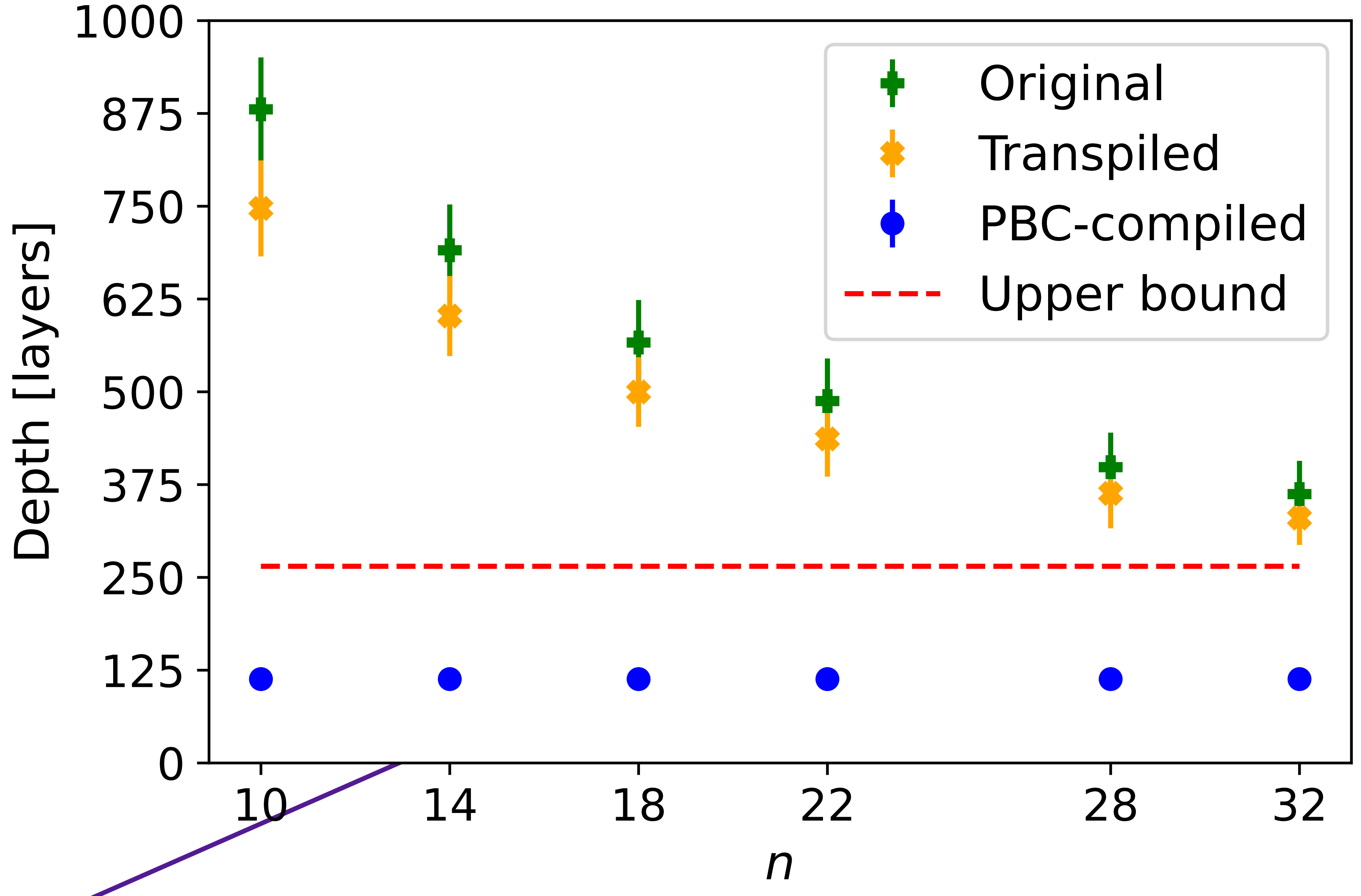
Hidden shift circuits



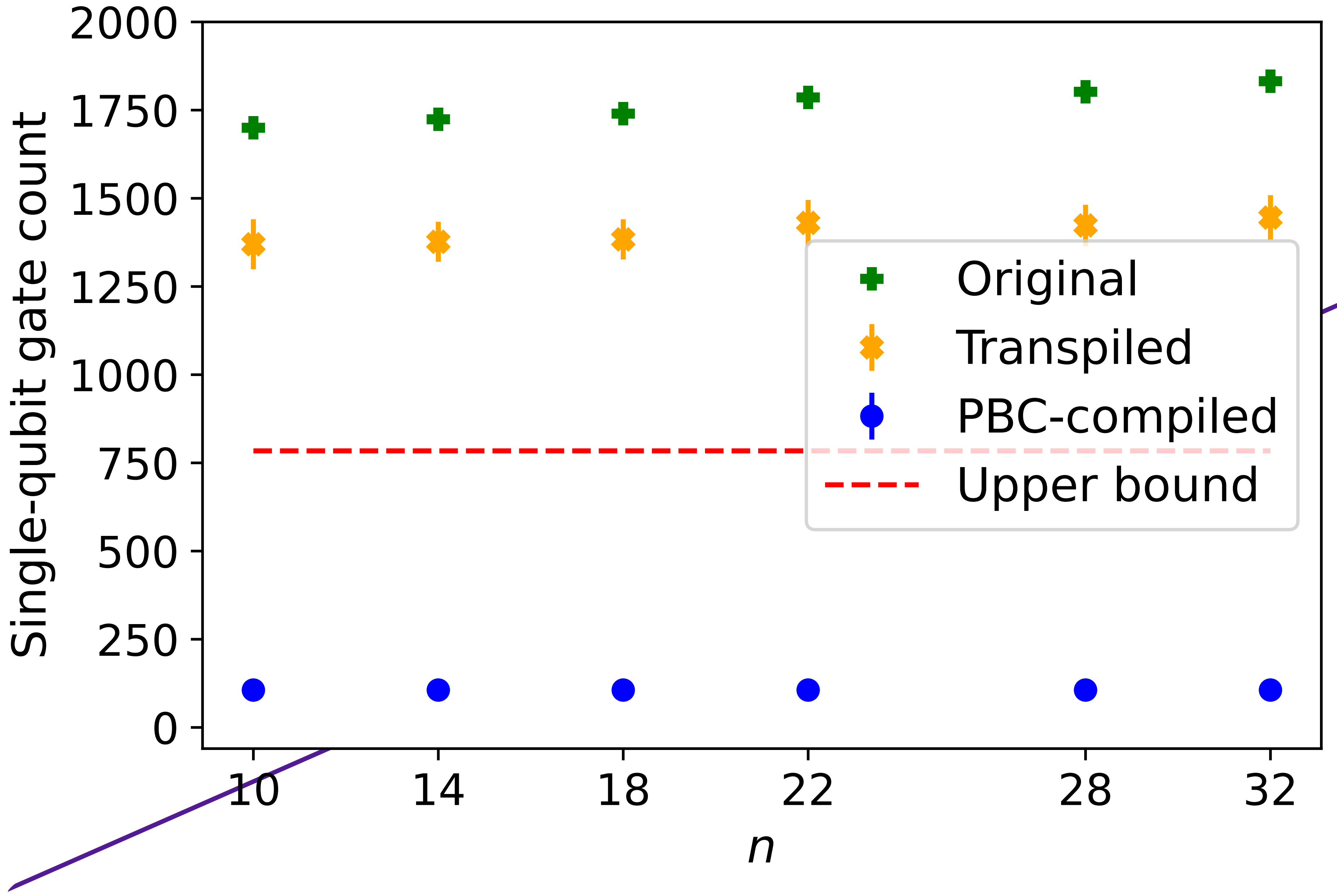


Hidden shift circuits

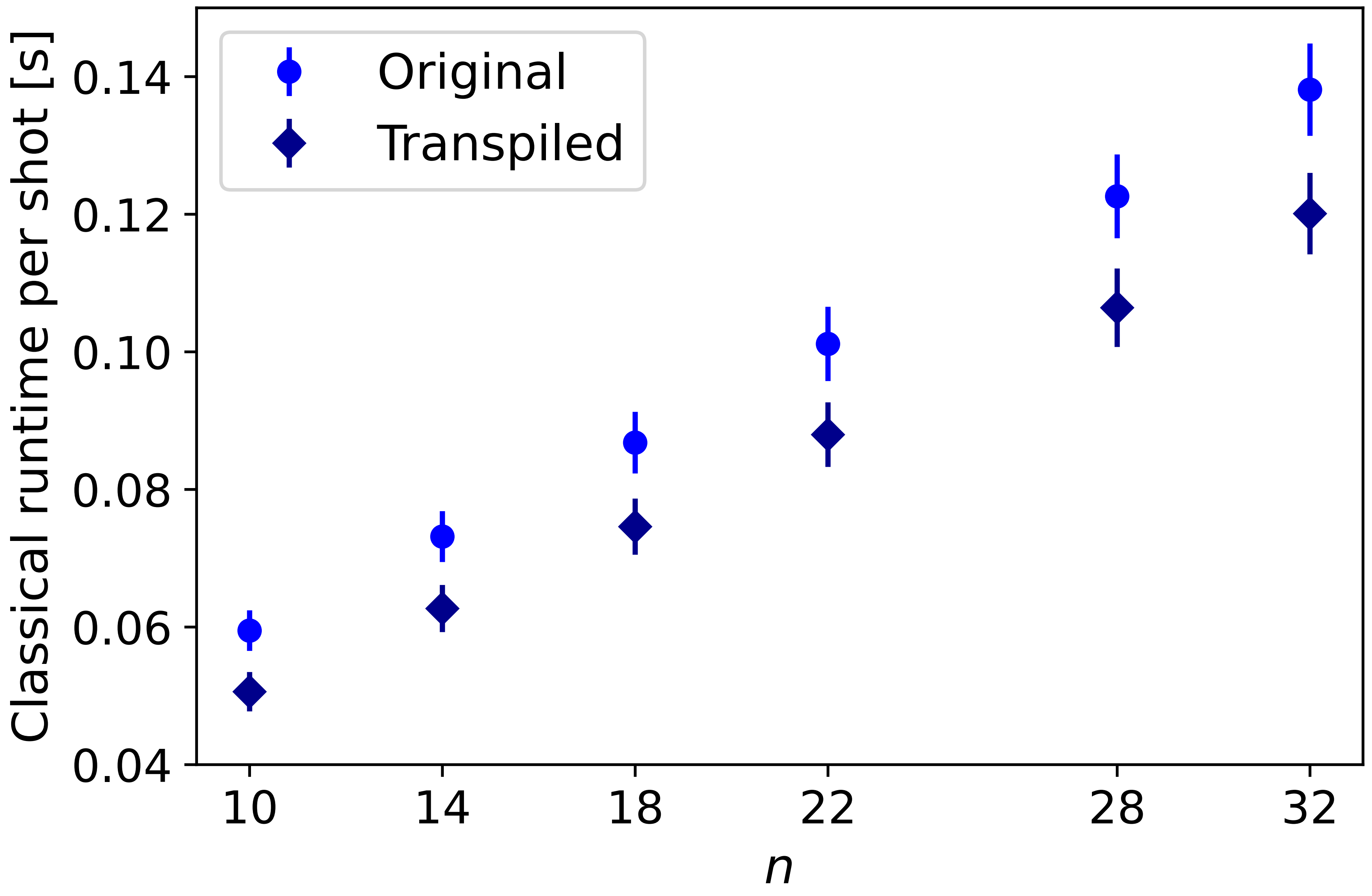


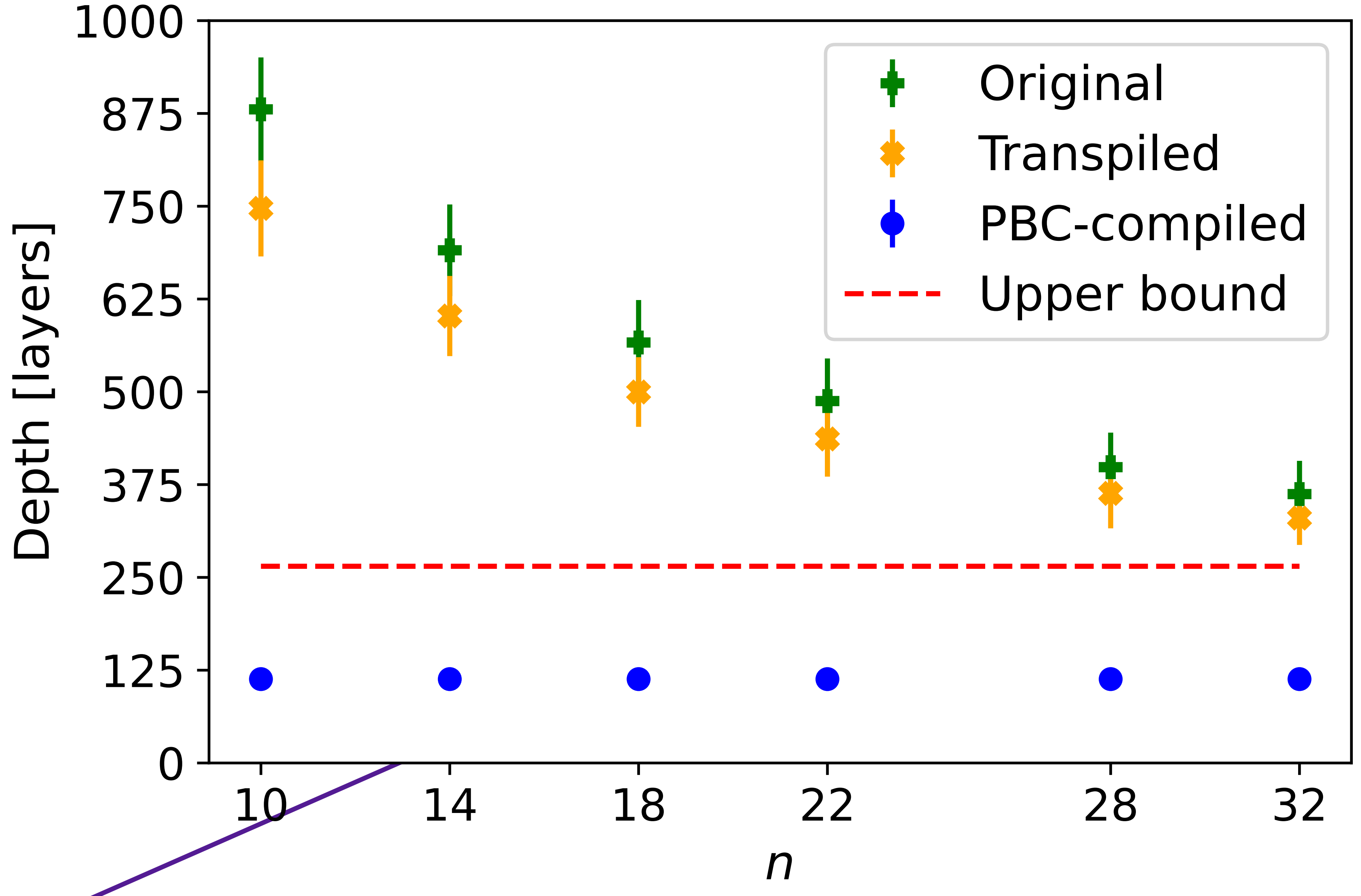


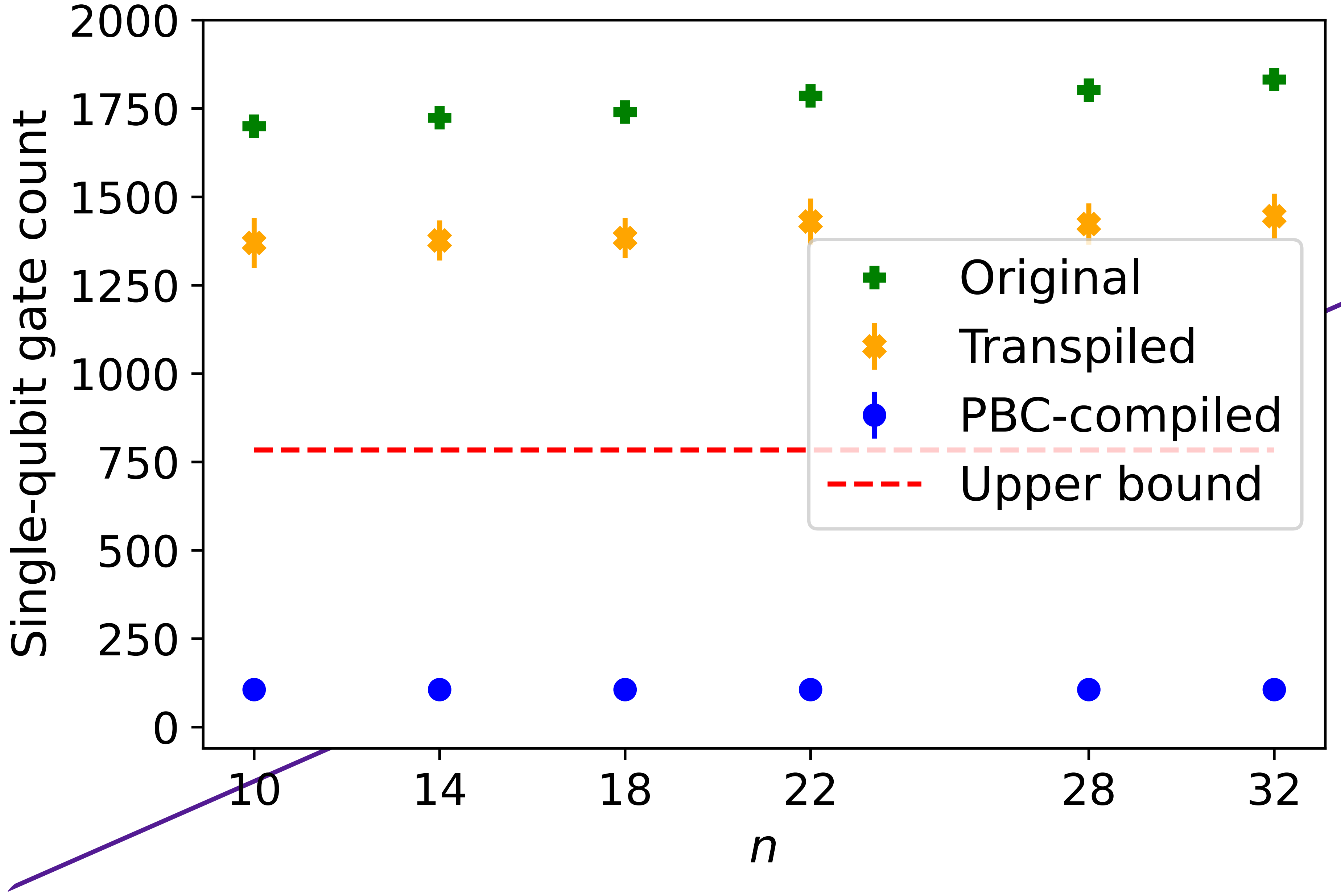
Hidden shift circuits

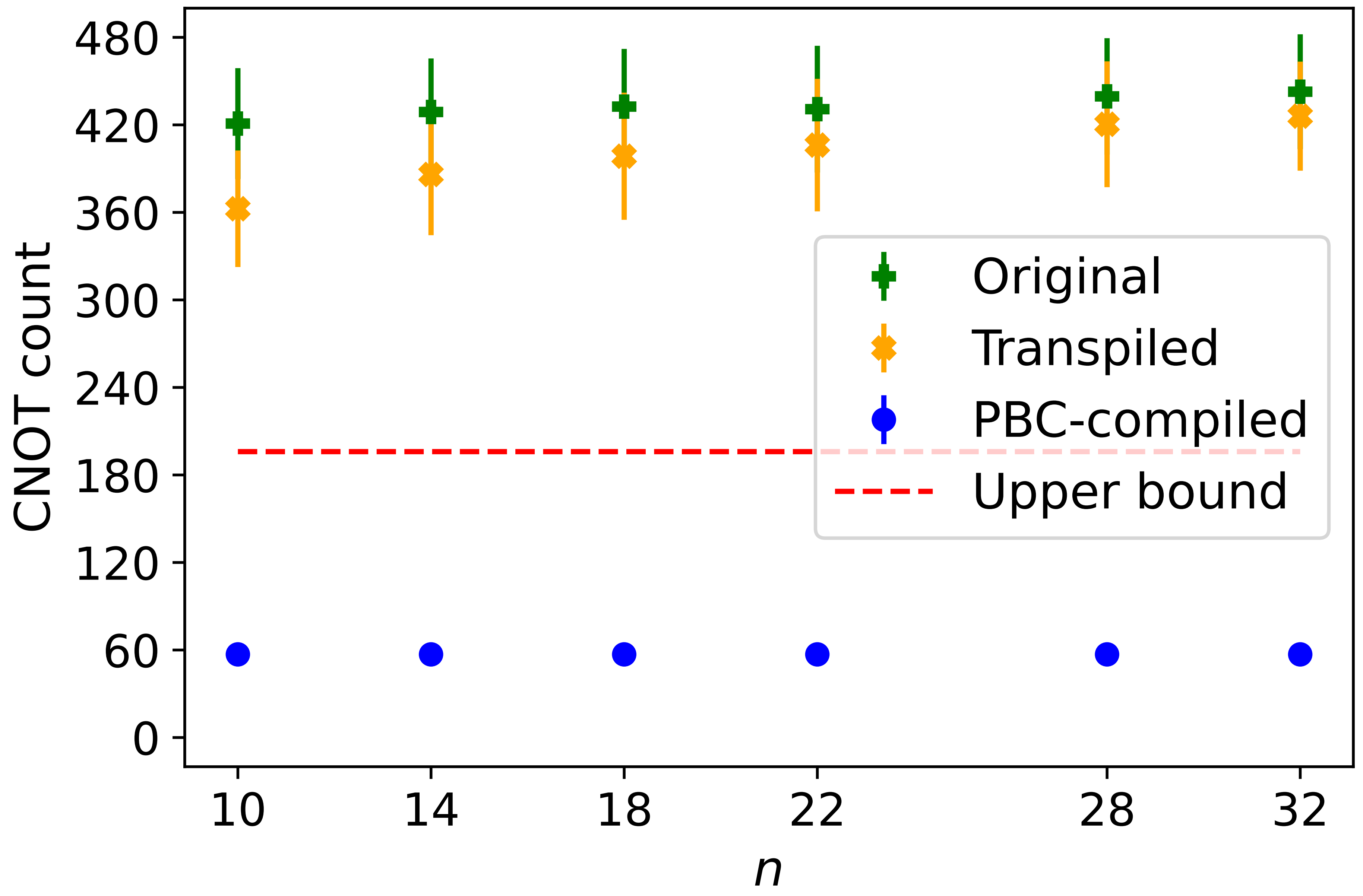


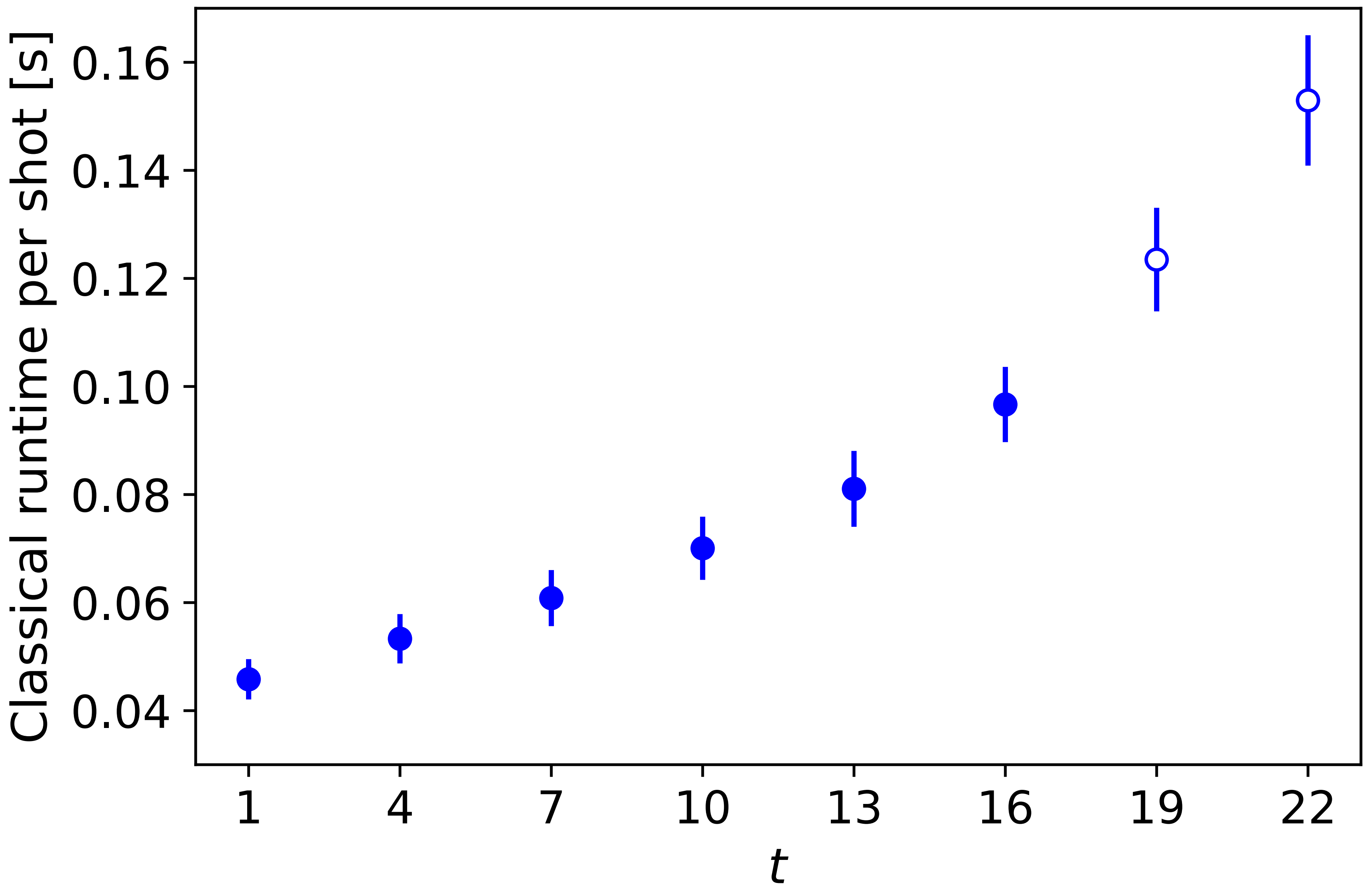
Hidden shift circuits



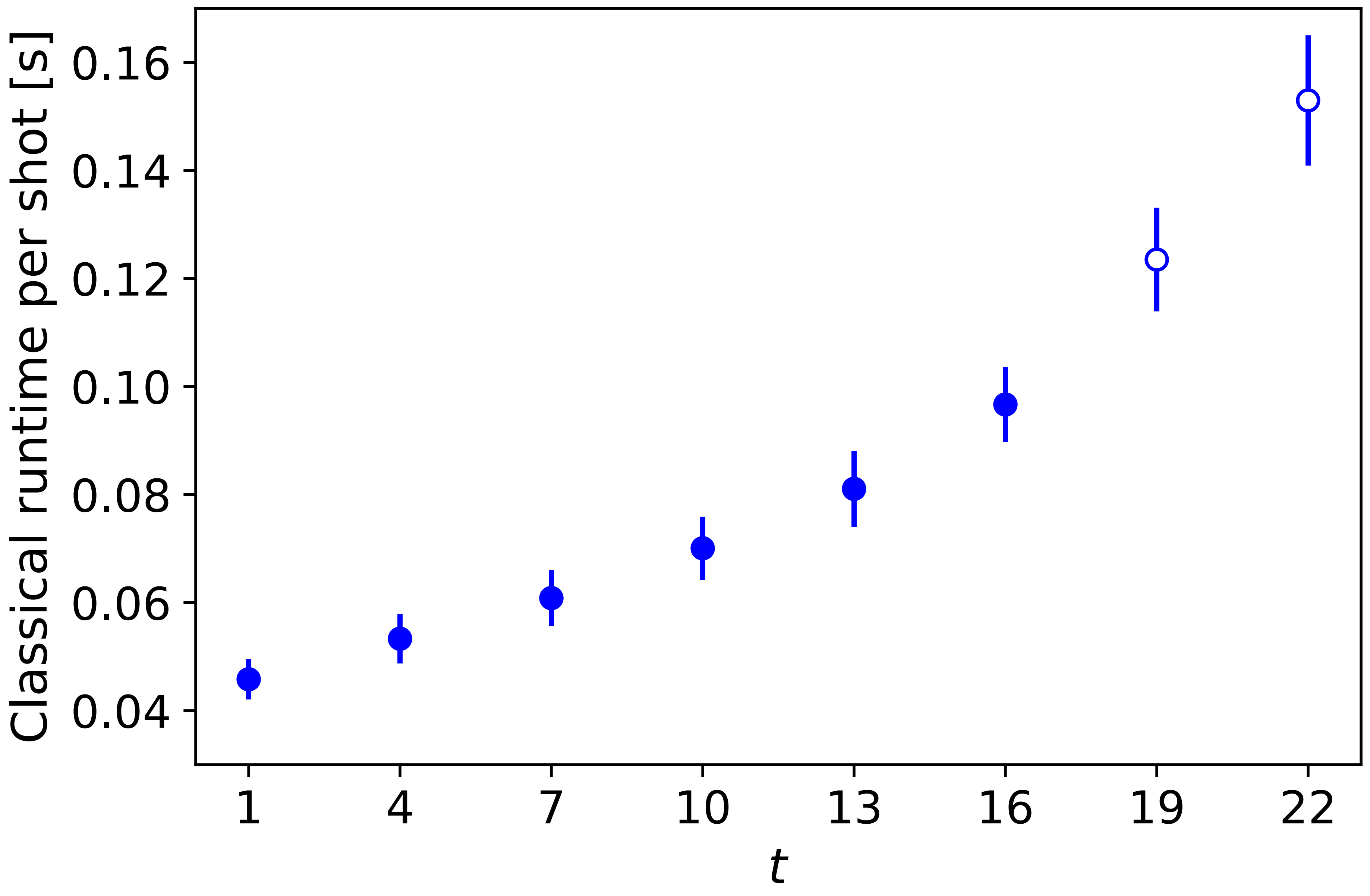


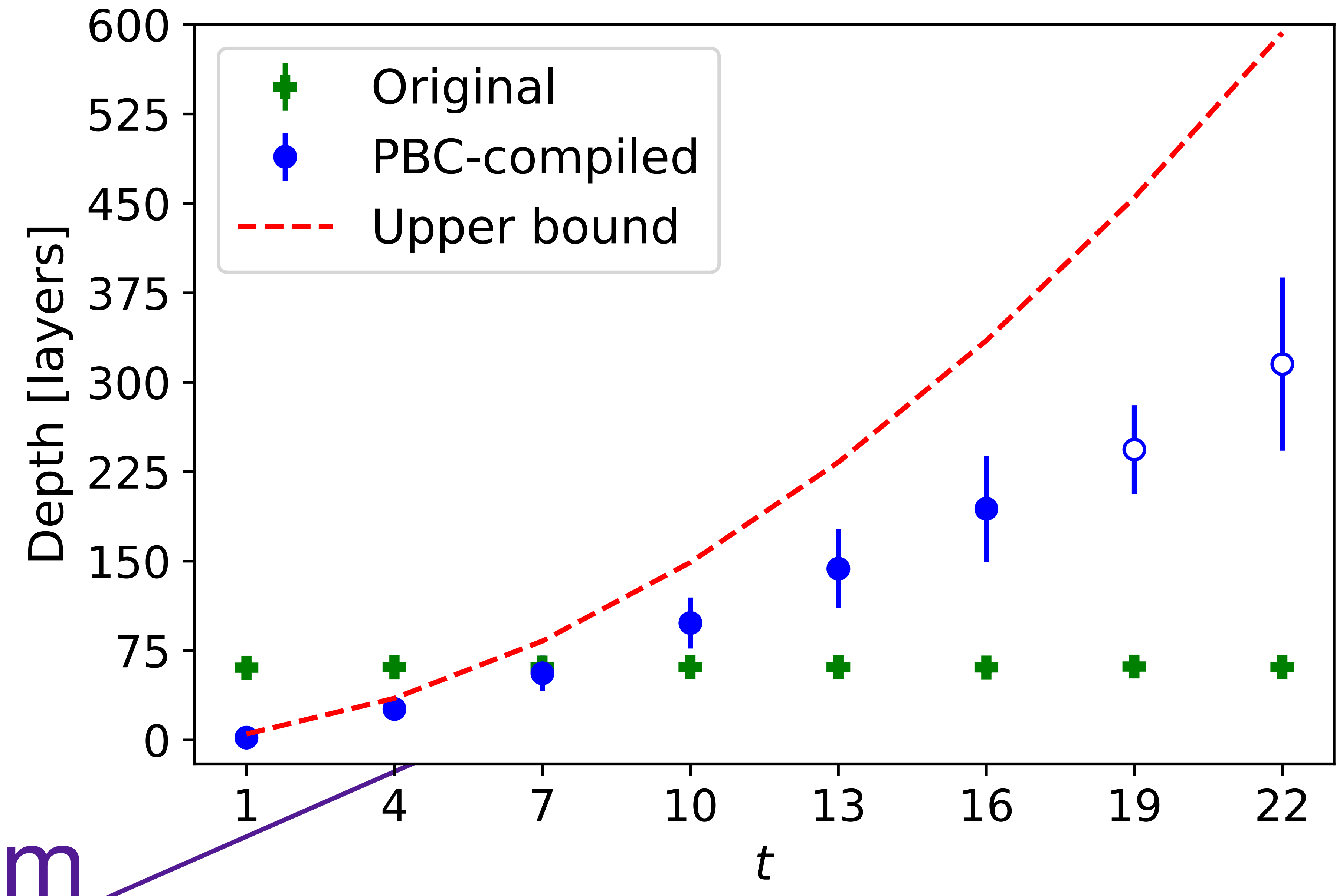




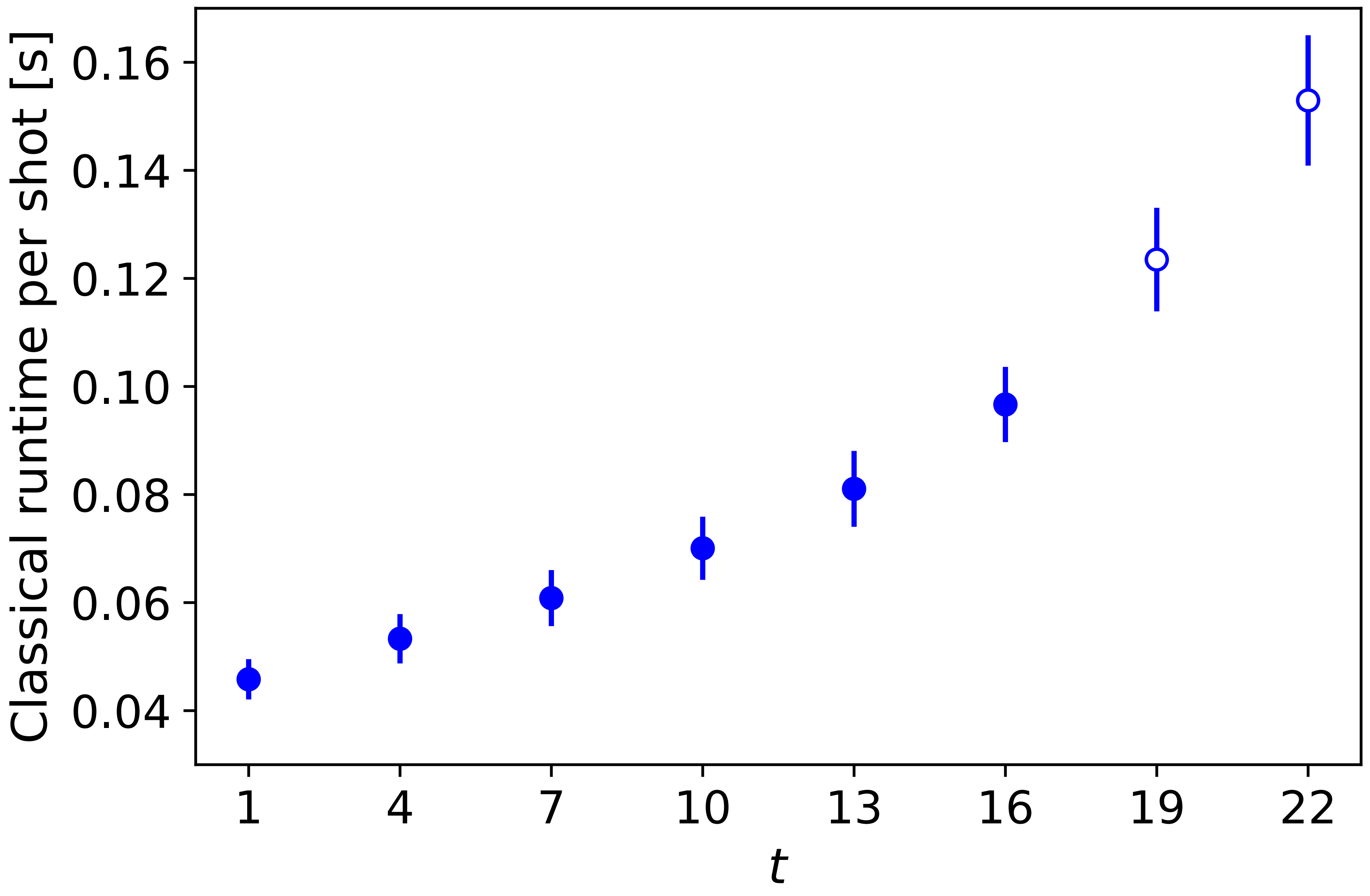


Random quantum circuits

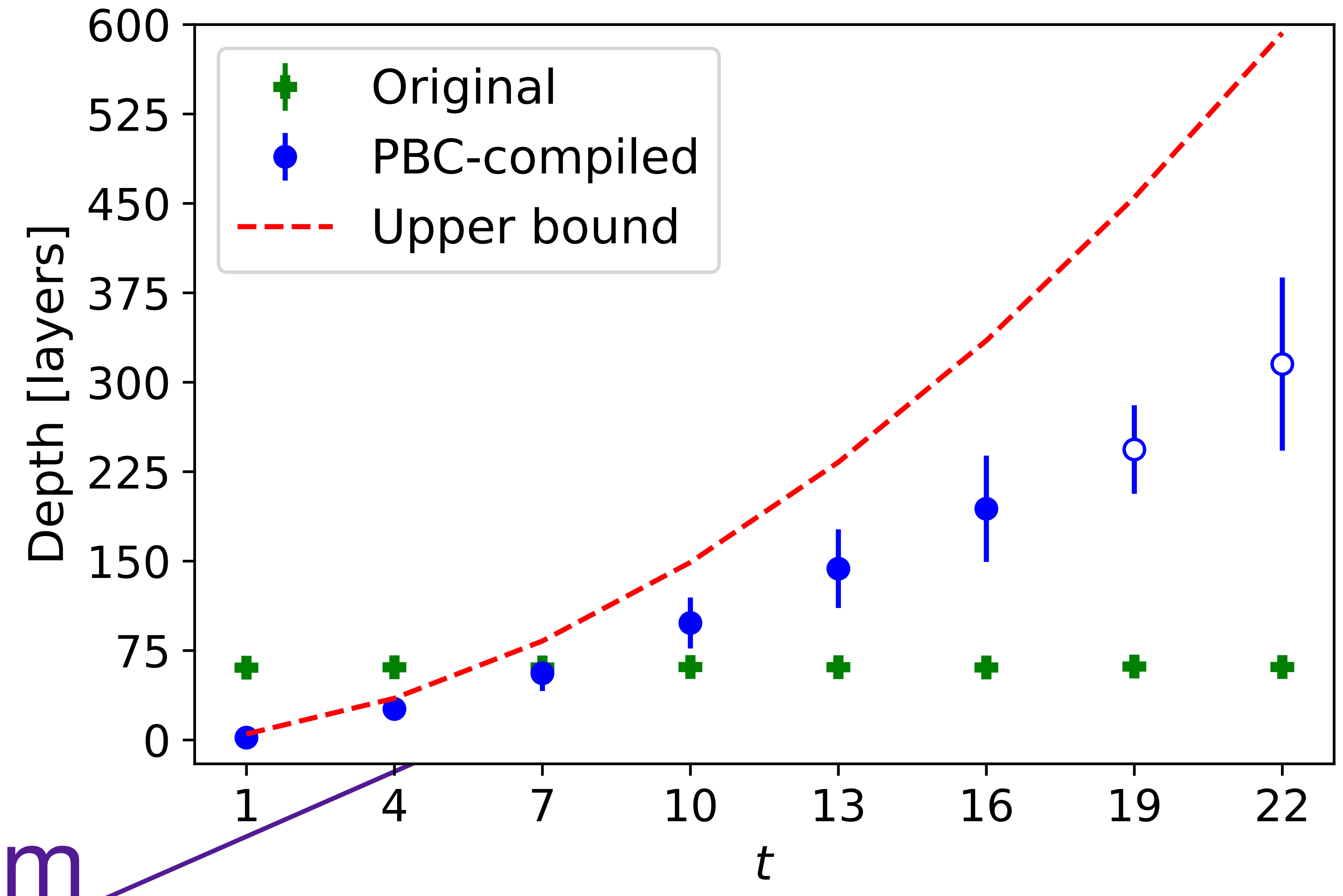


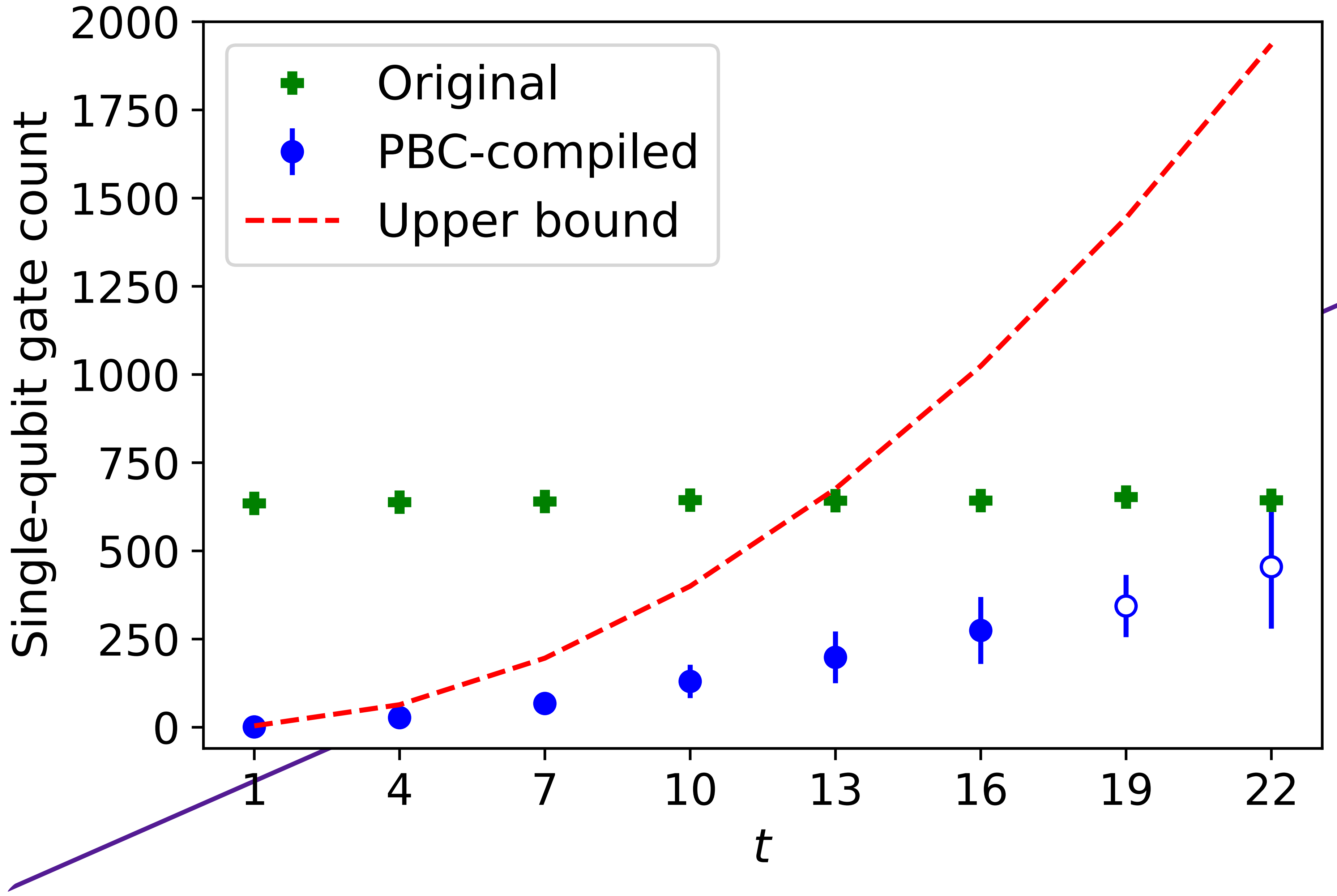


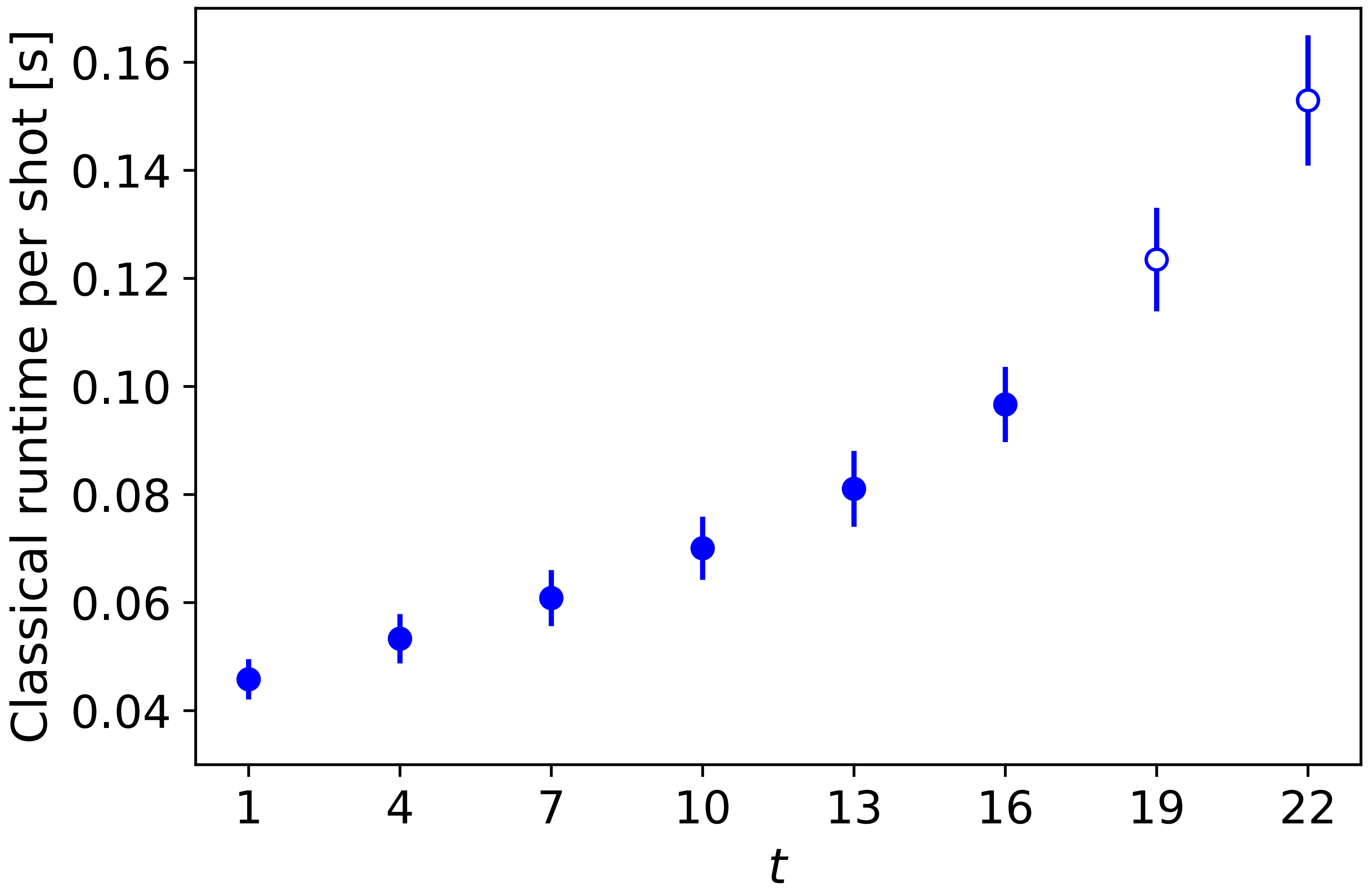
Random quantum circuits

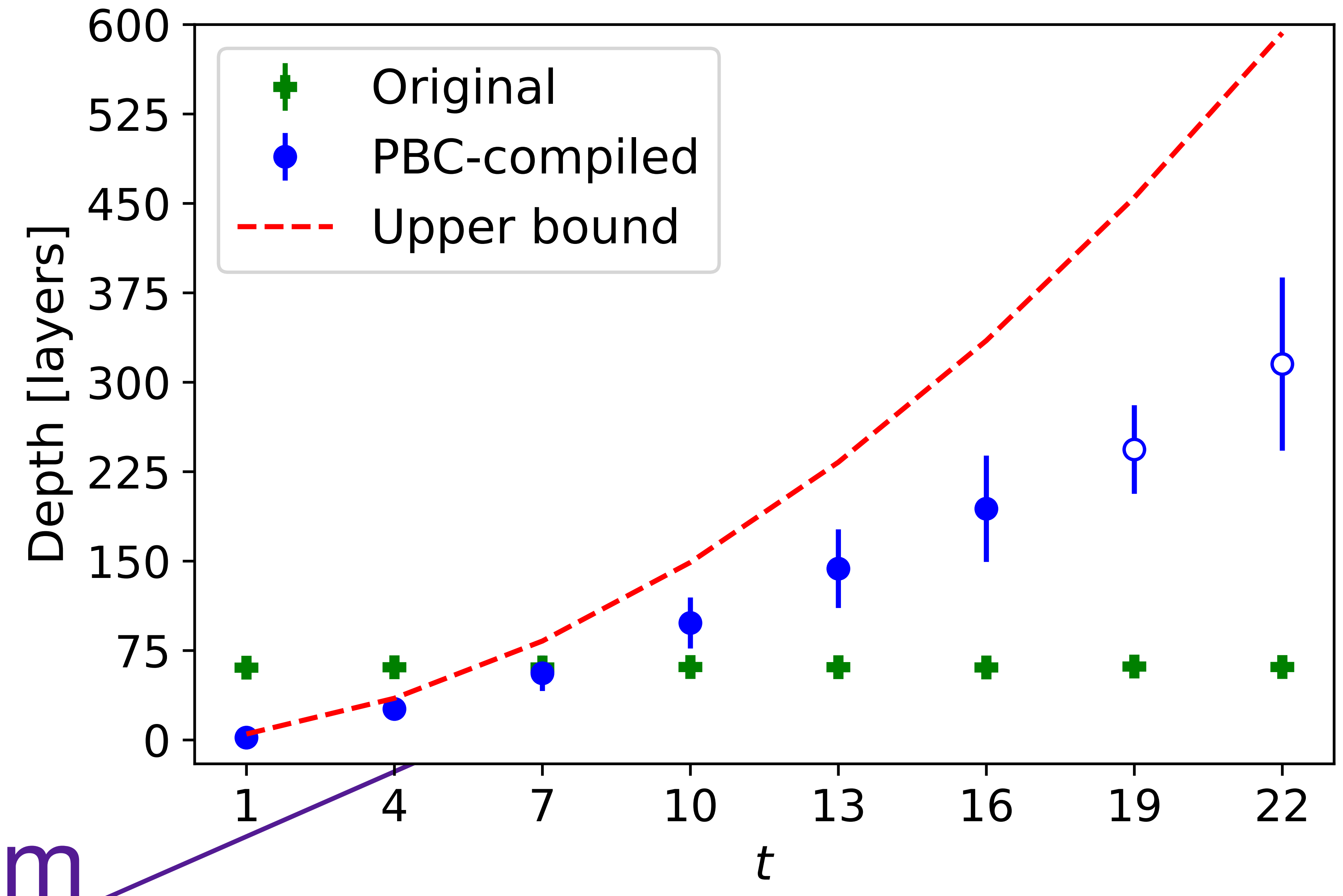


Random quantum circuits

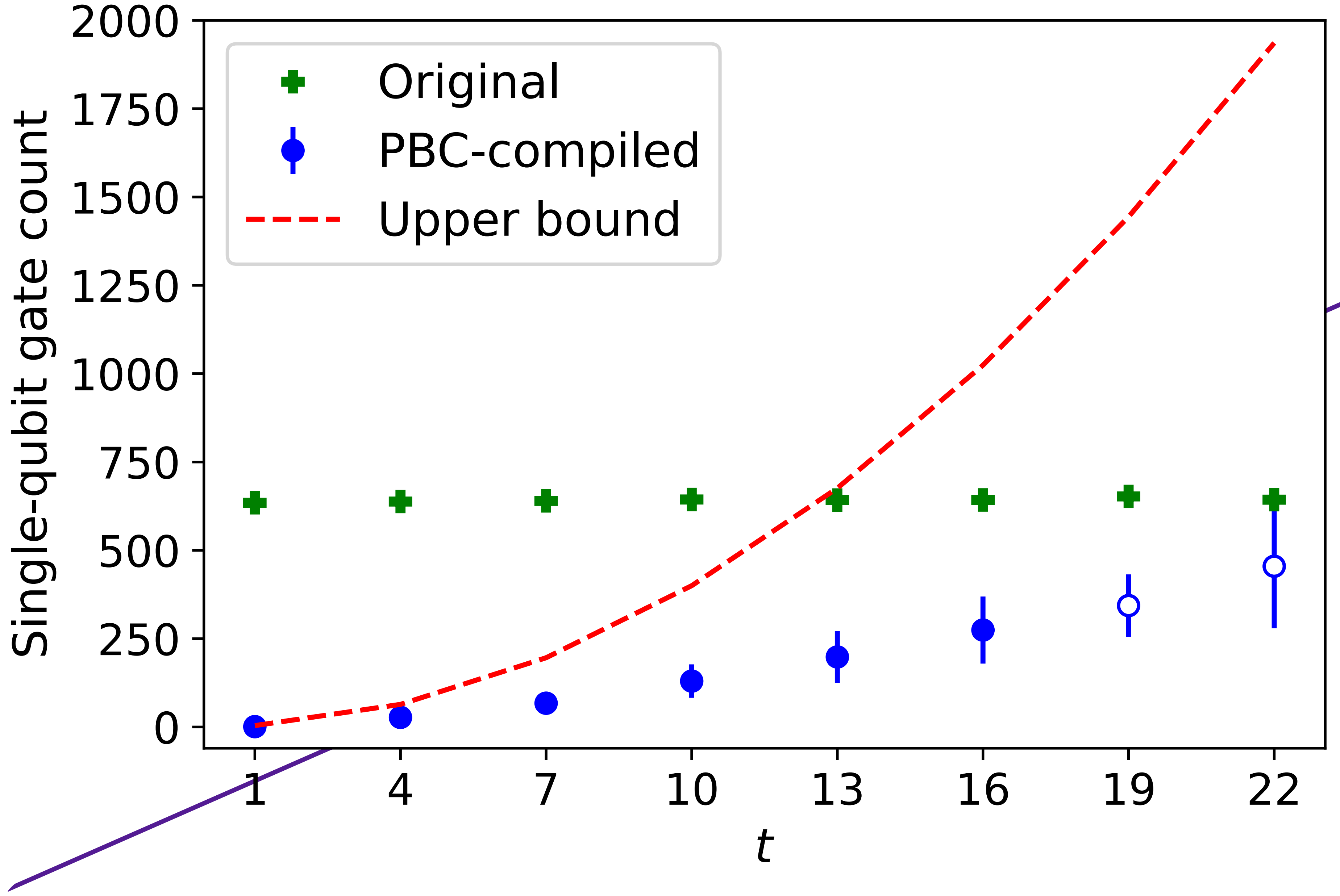


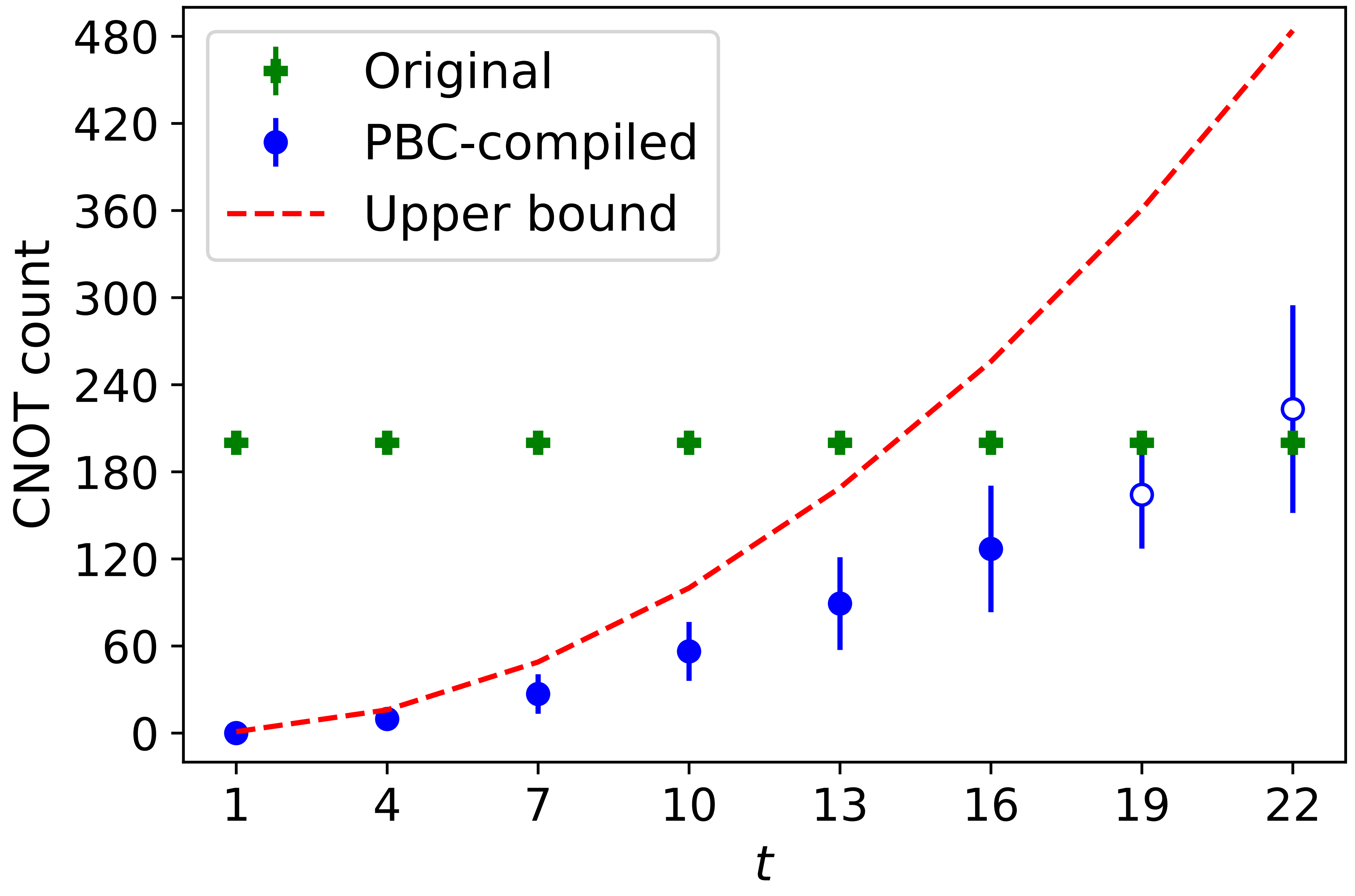






Random quantum circuits



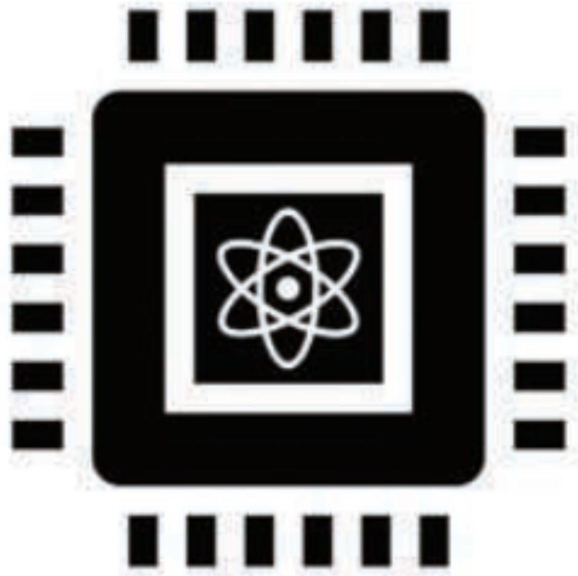


Computation

$n + l$ qubits

$\Downarrow$

n qubits



Concept: [STABILIZER PSEUDOMIXTURES]

$$\left|\psi\right\rangle\left\langle\psi\right| = \sum_{i=1}^{M} c_i' \left|\varphi_i\right\rangle\left\langle\varphi_i\right|$$

Concept: [STABILIZER PSEUDOMIXTURES]

$$|\psi\rangle\langle\psi| = \sum_{i=1}^{M} c_i' |\varphi_i\rangle\langle\varphi_i|$$

non-stabilizer state

Concept: [Stabilizer pseudomixtures]

$$\left|\psi\right\rangle\left\langle\psi\right| = \sum_{i=1}^{M} c_i' \left|\varphi_i\right\rangle\left\langle\varphi_i\right|$$

non-stabilizer state

stabilizer states

Concept: [STABILIZER PSEUDOMIXTURES]

real coefficients

$$|\psi\rangle\langle\psi| = \sum_{i=1}^{M} c'_i |\varphi_i\rangle\langle\varphi_i|$$

non-stabilizer state

stabilizer states

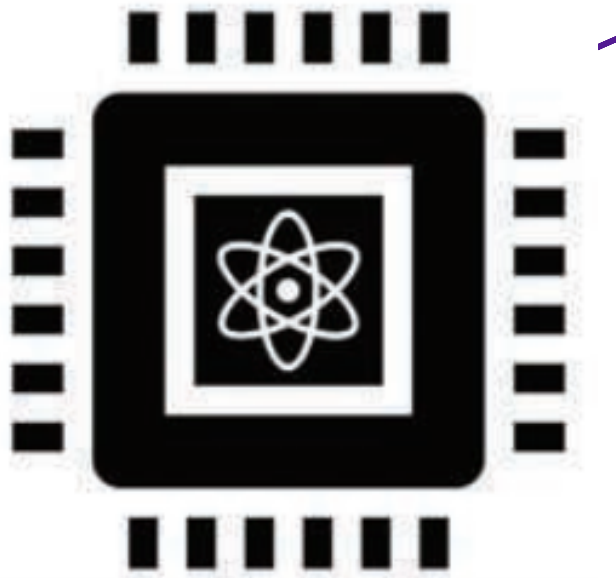
Concept: [STABILIZER PSEUDOMIXTURES]

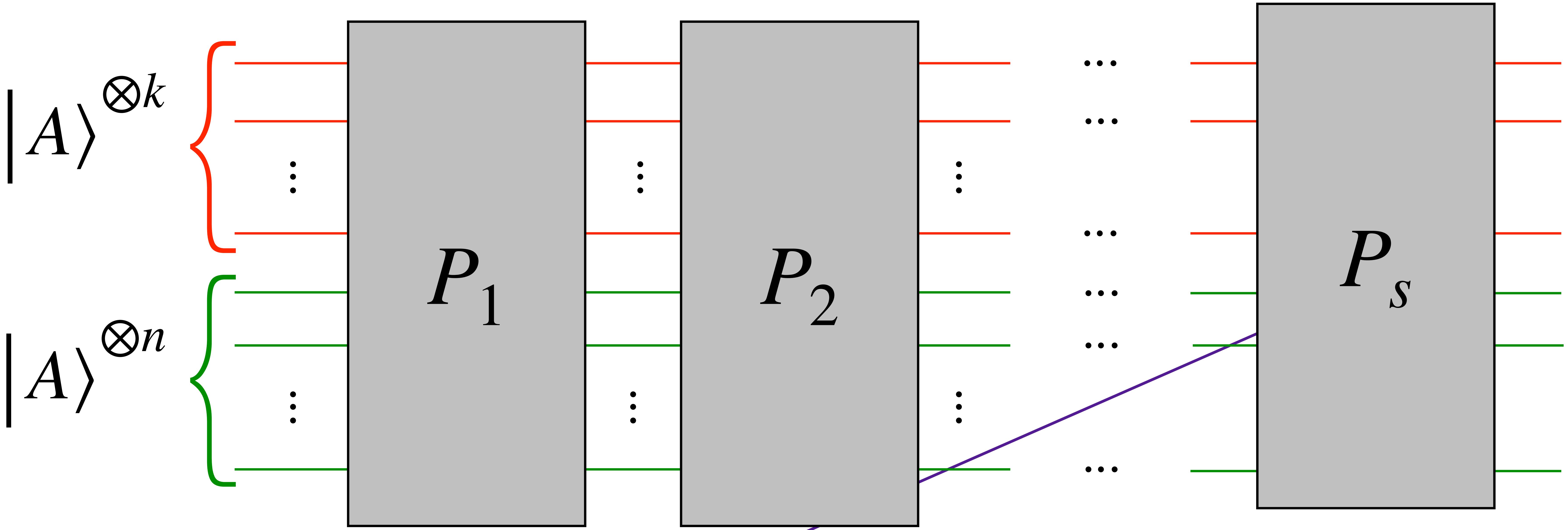
$$|A\rangle\langle A| = \frac{1}{2}|+\rangle\langle+| + \frac{1-\sqrt{2}}{2}|-\rangle\langle-| + \frac{\sqrt{2}}{2}|+_i\rangle\langle+_i|$$

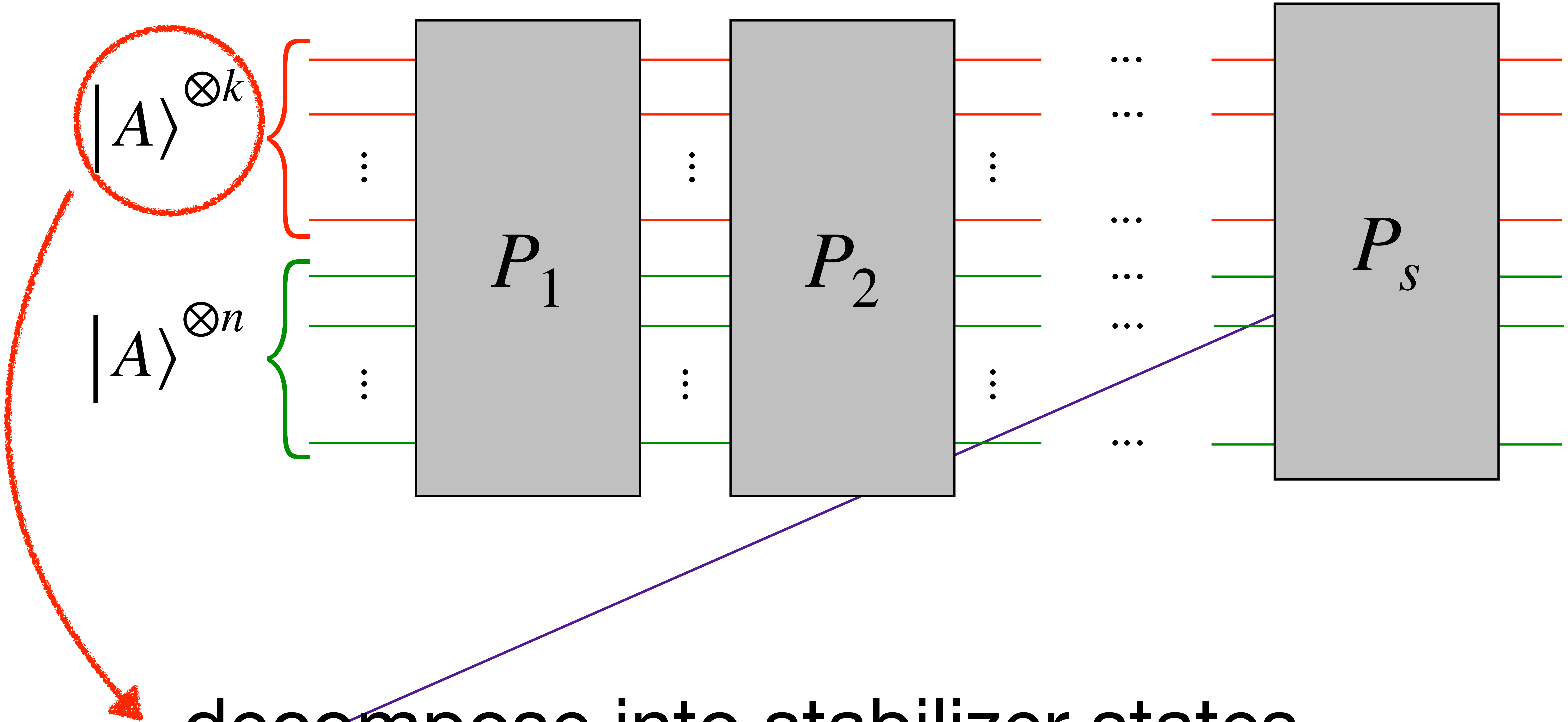
$$M = 3$$

Computation
$n + k$ qubits

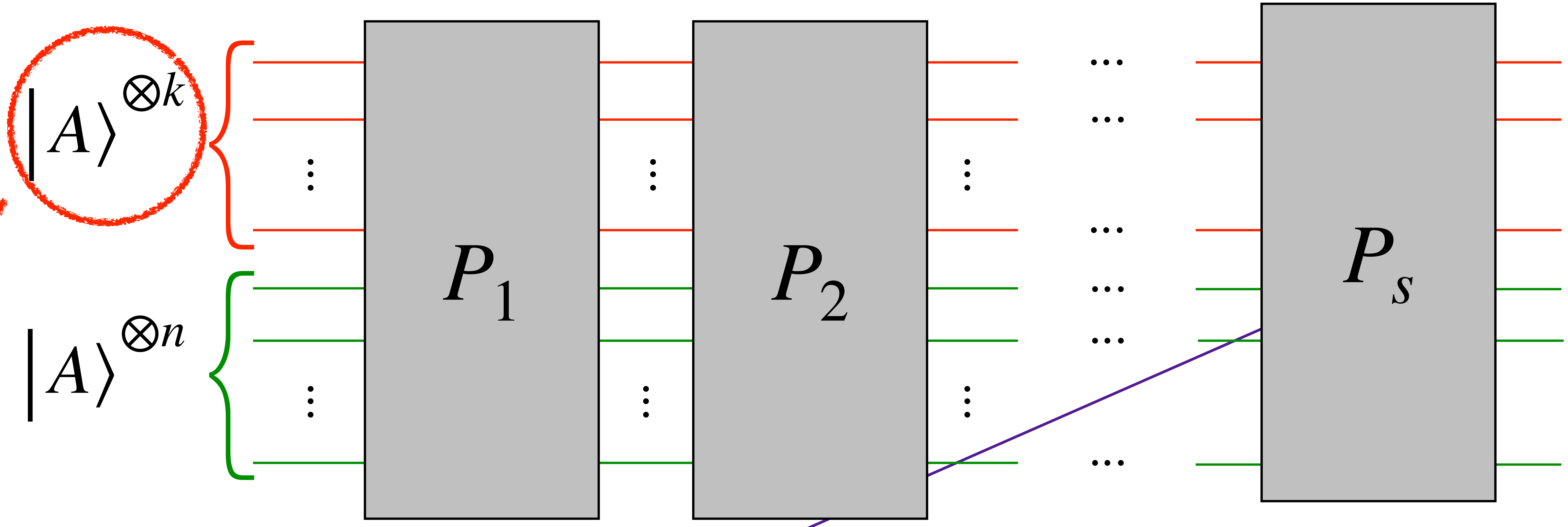
n qubits



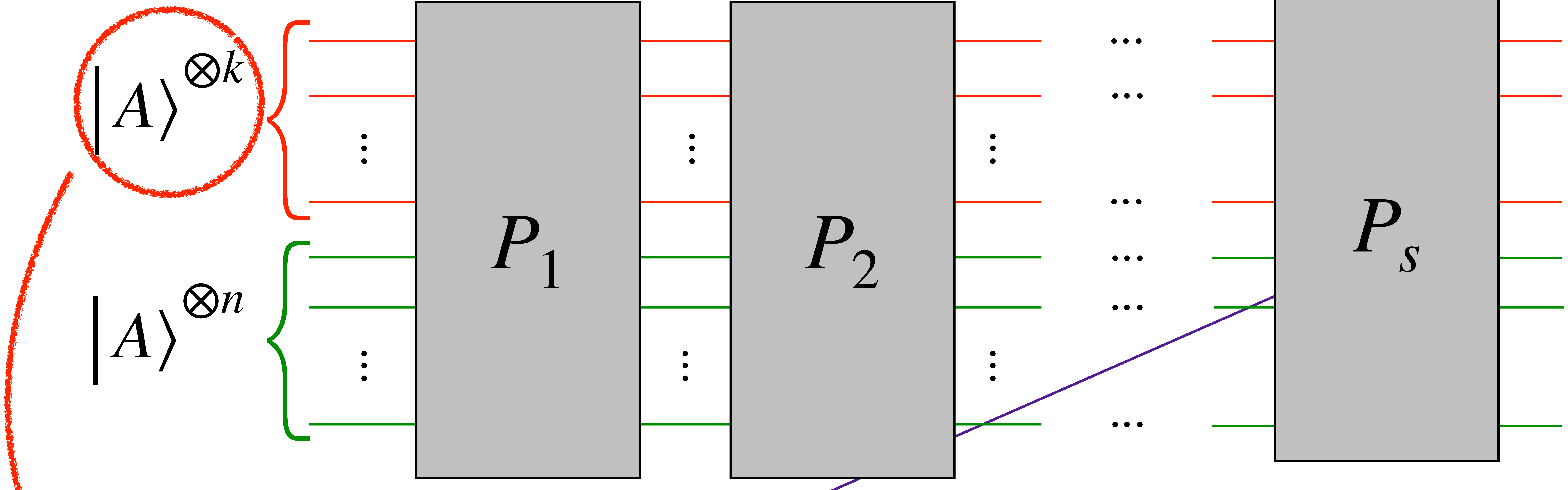

$|A\rangle^{\otimes k}$
$|A\rangle^{\otimes n}$
P_1
P_2
P_s



decompose into stabilizer states

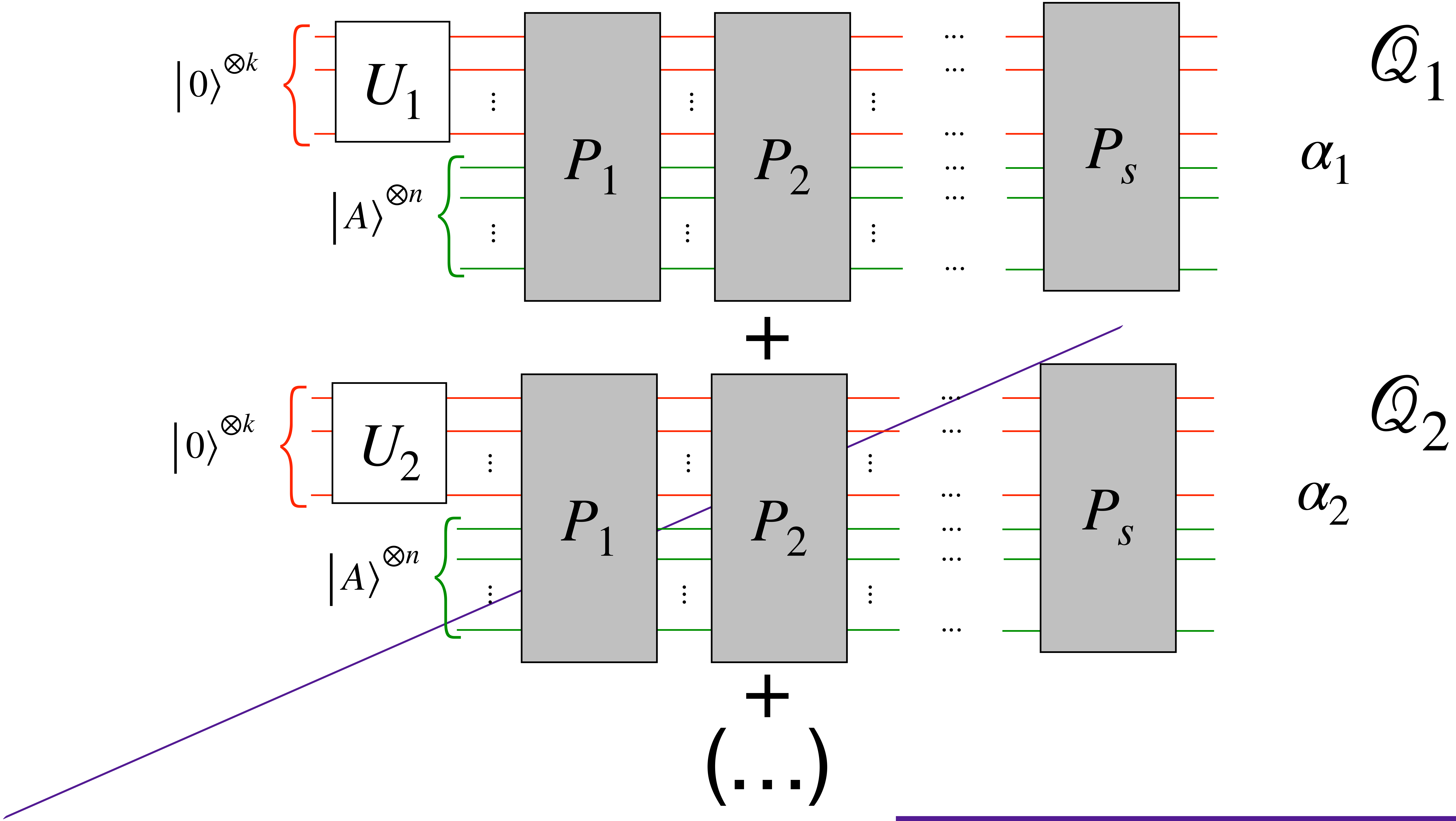


$$|A\rangle\langle A|^{\otimes k} = \sum_{i=1}^{M} \alpha_i \, |\varphi_i\rangle\langle\varphi_i|$$



$$|A\rangle\langle A|^{\otimes k} = \sum_{i=1}^{M} \alpha_i |\varphi_i\rangle\langle\varphi_i|;$$

$$|\varphi_i\rangle = U_i |0\rangle^{\otimes k}$$


$|0\rangle^{\otimes k}$
U_1
$|A\rangle^{\otimes n}$
P_1
P_2
P_s
$\mathcal{Q}_1$
α_1
+
$|0\rangle^{\otimes k}$
U_2
$|A\rangle^{\otimes n}$
P_1
P_2
P_s
$\mathcal{Q}_2$
α_2
+
(...)

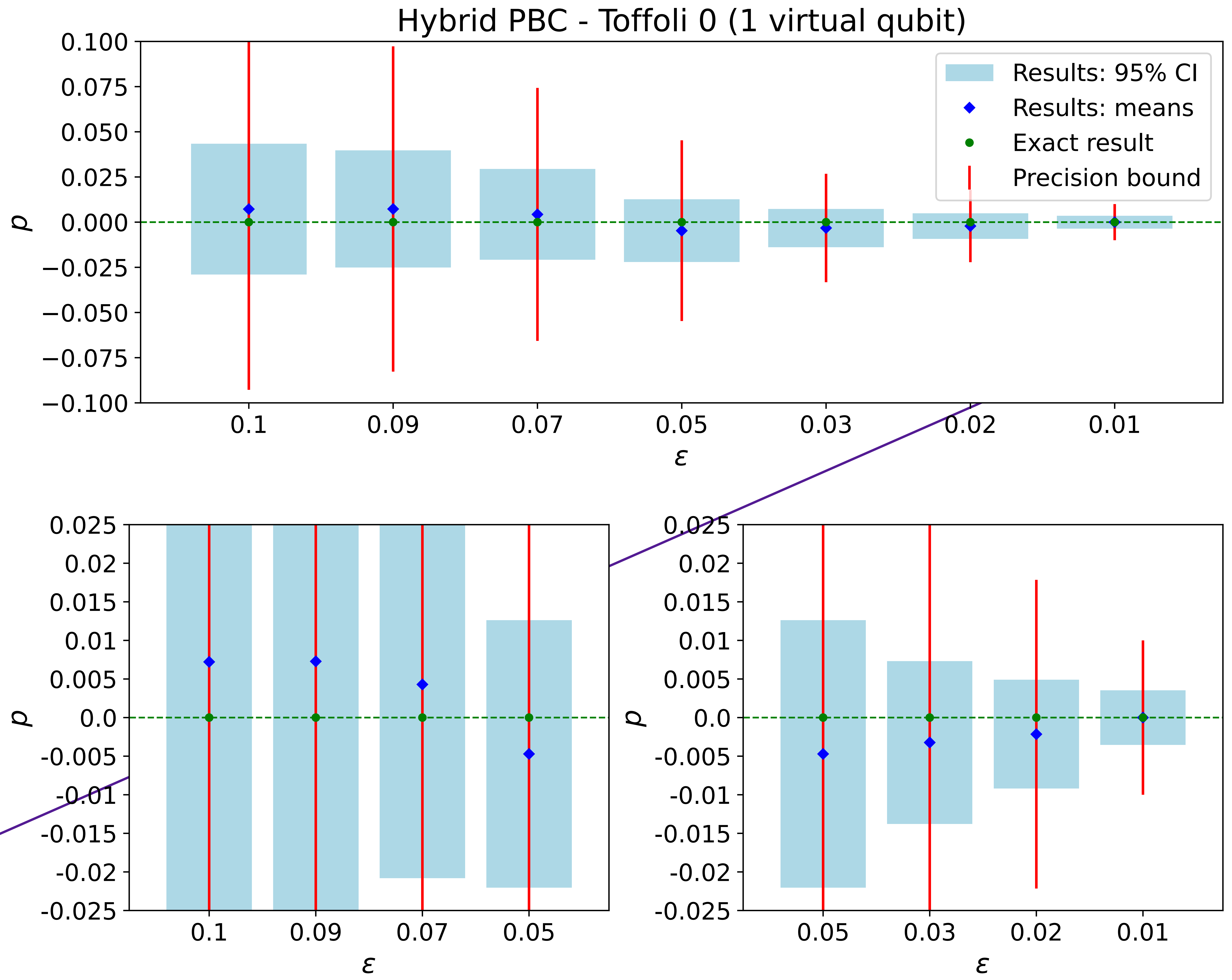
$$\text{Linearity} \Rightarrow p(\mathcal{Q}) = \sum_{i=1}^{M} \alpha_i p(\mathcal{Q}_i)$$

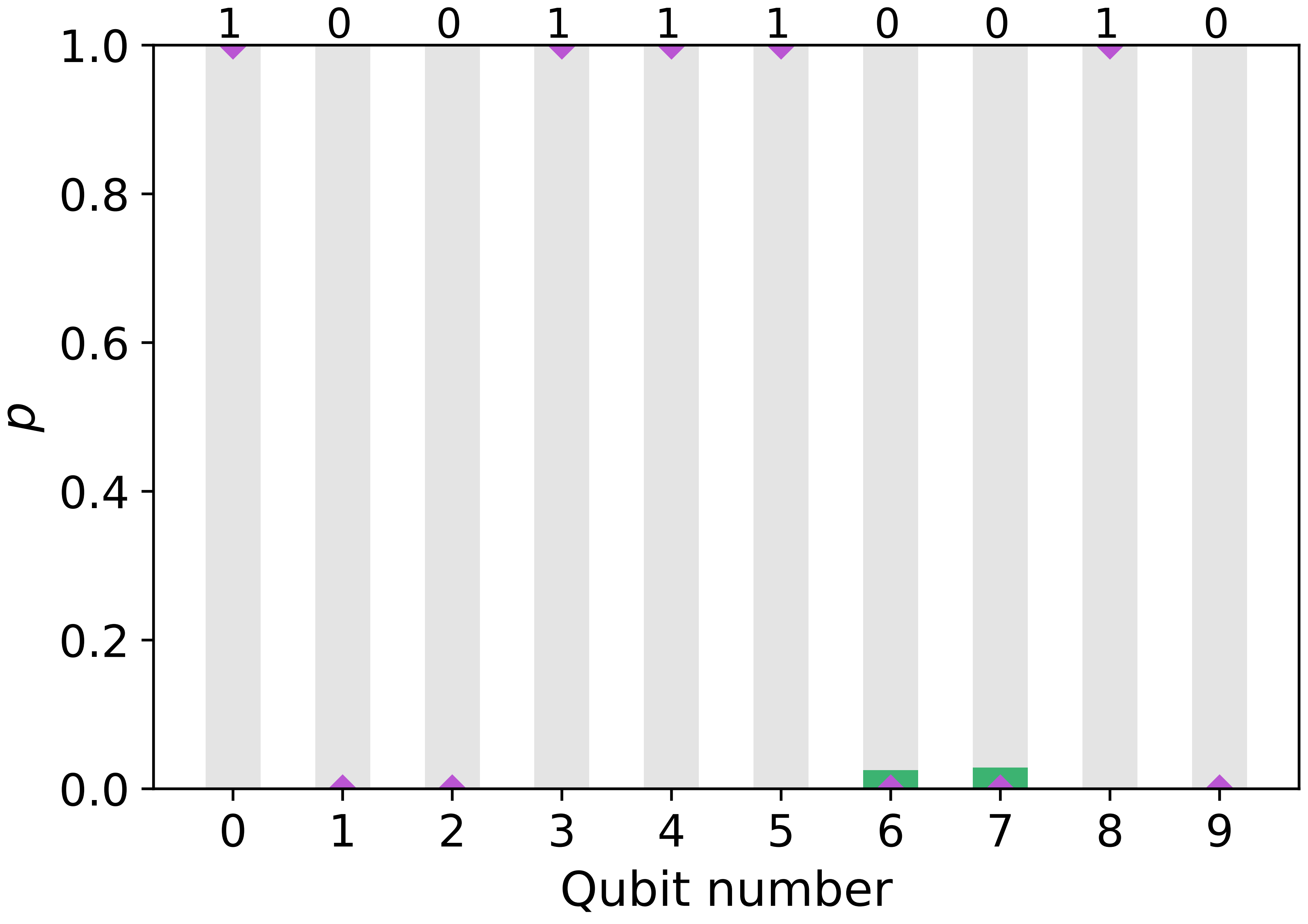
$$\text{Unbiased estimator} \Rightarrow \xi = \sum_{i=1}^{M} \alpha_i b_i$$

Theorem: A PBC on $n + k$ qubits can be simulated by $M = 2^{\mathcal{O}(k)}$ PBCs on n qubits, and a classical processing that takes time $2^{\mathcal{O}(k)} poly(n)$.

Theorem: A PBC on $n + k$ qubits can be simulated by $M = 2^{\mathcal{O}(k)}$ PBCs on n qubits, and a classical processing that takes time $2^{\mathcal{O}(k)} poly(n)$.

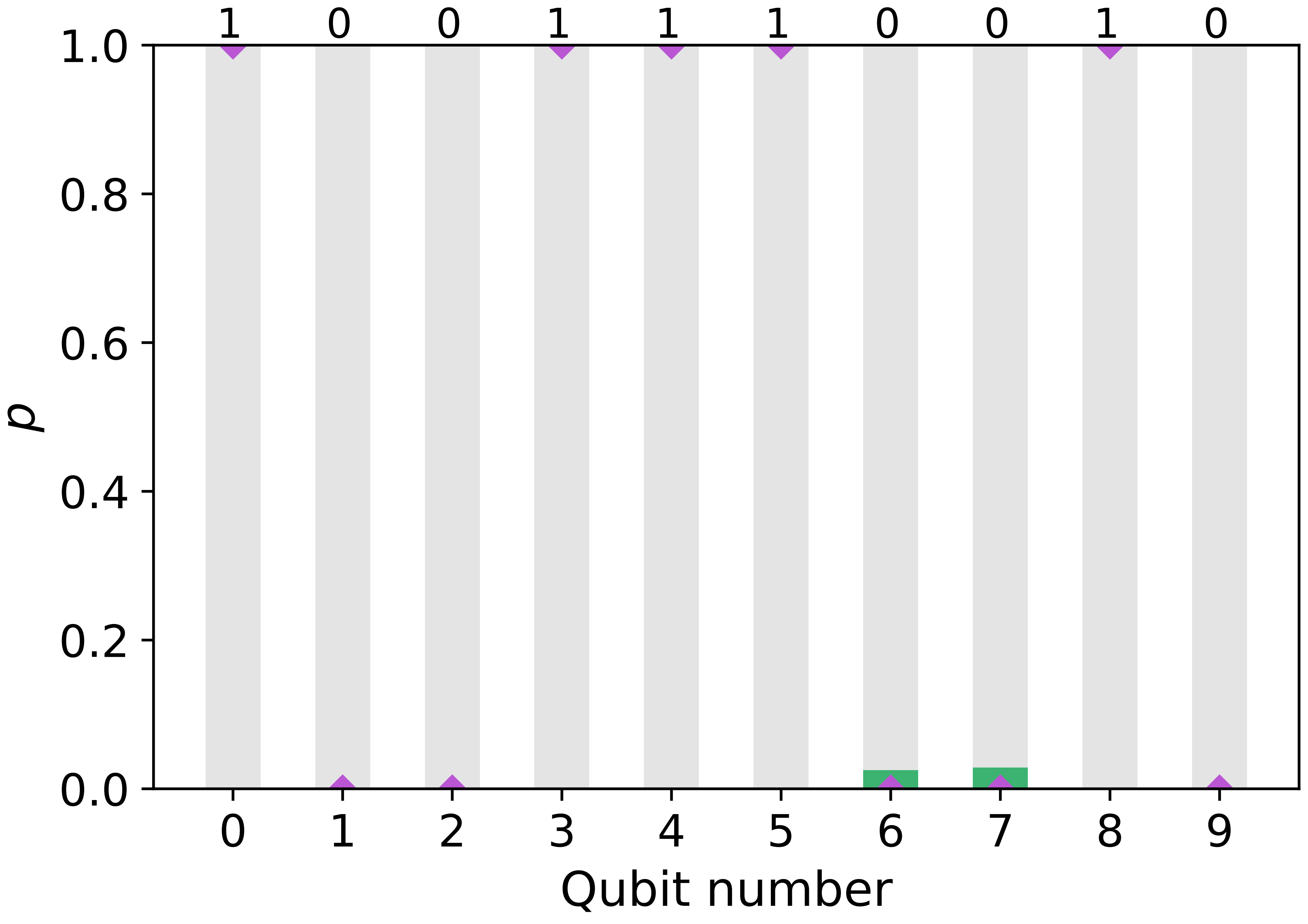
3^k


Hybrid PBC - Toffoli 0 (1 virtual qubit)
Results: 95% CI
Results: means
Exact result
Precision bound
p
ε
0.100
0.075
0.050
0.025
0.000
−0.025
−0.050
−0.075
−0.100
0.1
0.09
0.07
0.05
0.03
0.02
0.01
0.025
0.02
0.015
0.01
0.005
0.0
-0.005
-0.01
-0.015
-0.02
-0.025



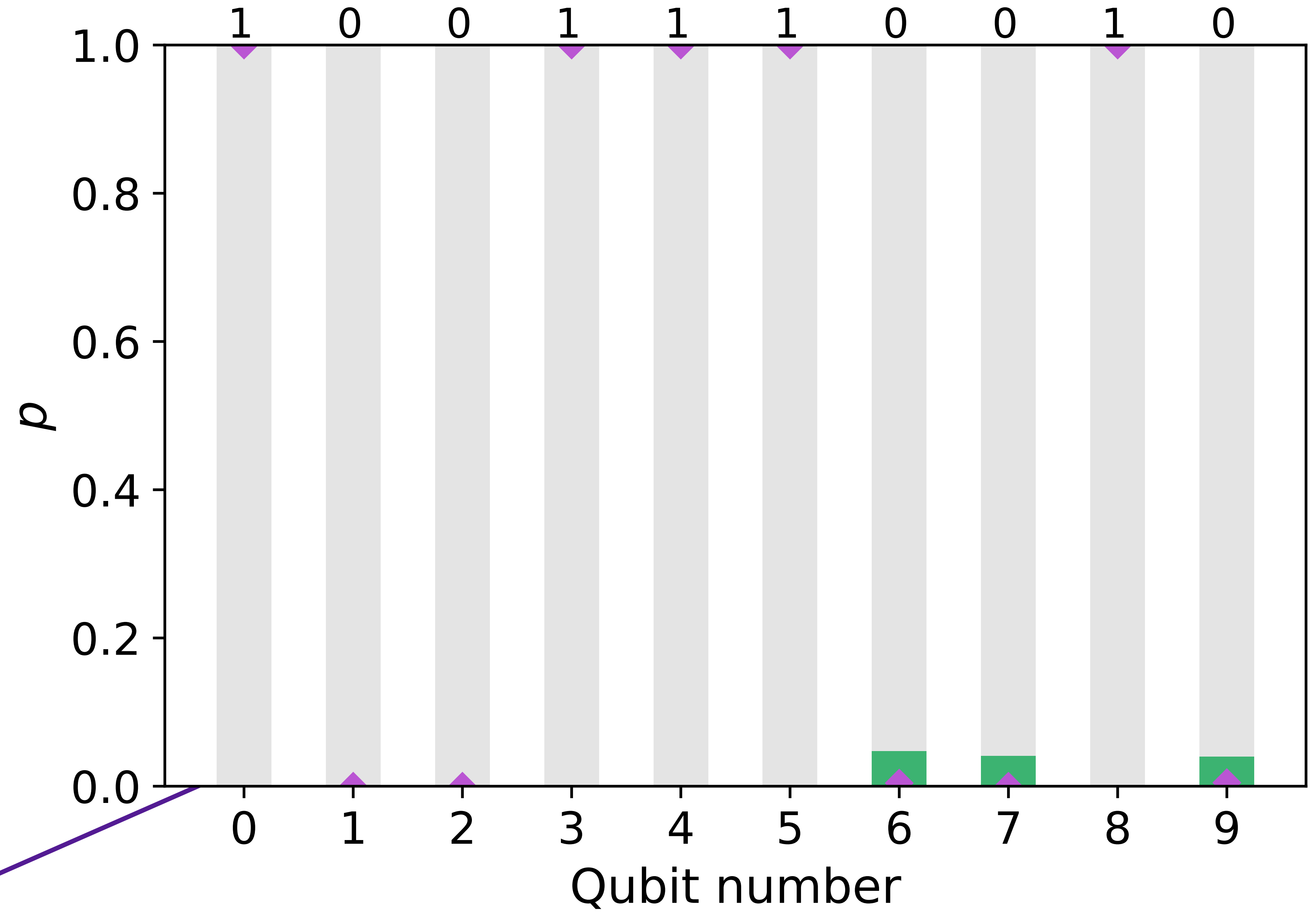
$\epsilon = 0.1$

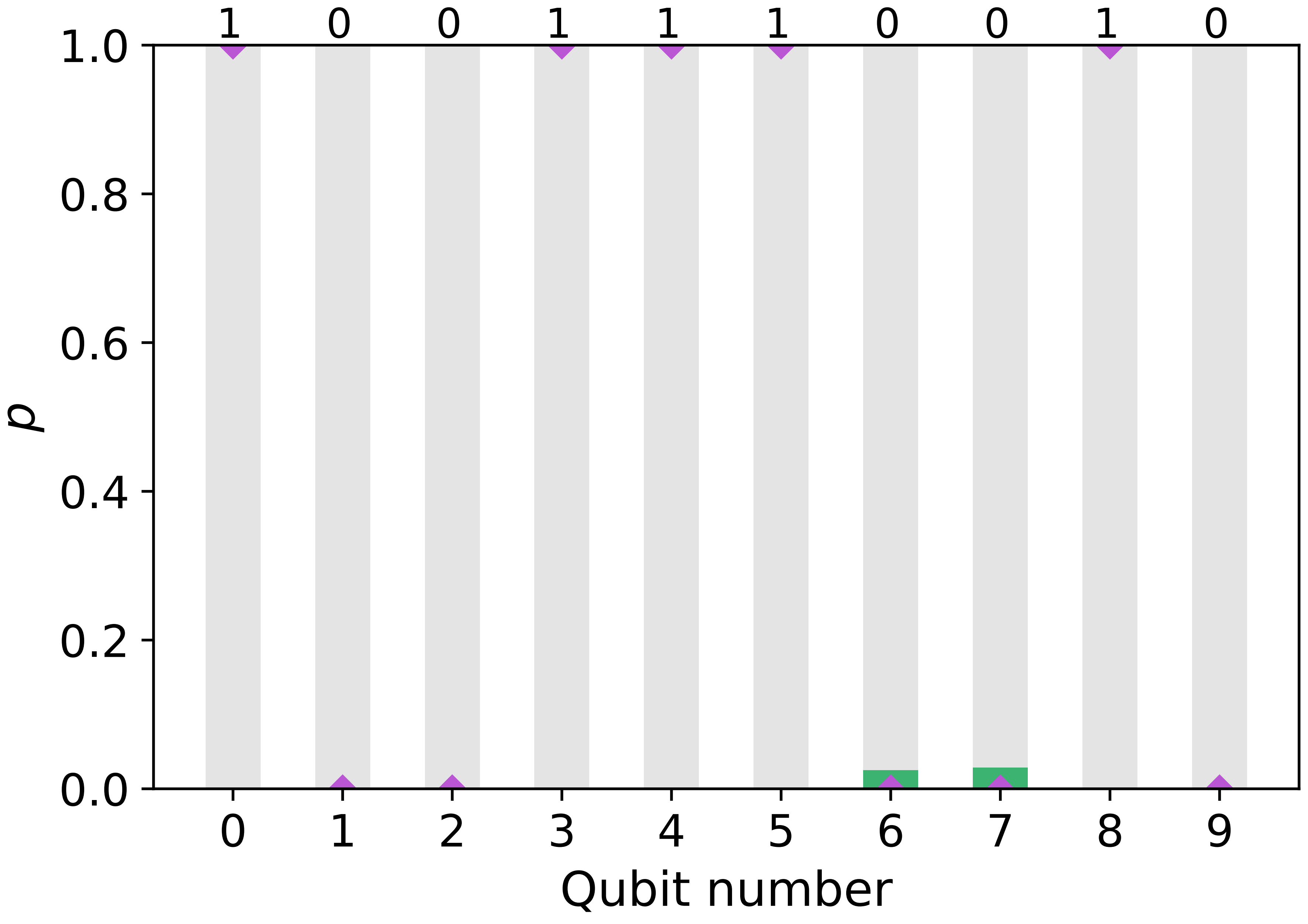
Hidden shift circuit



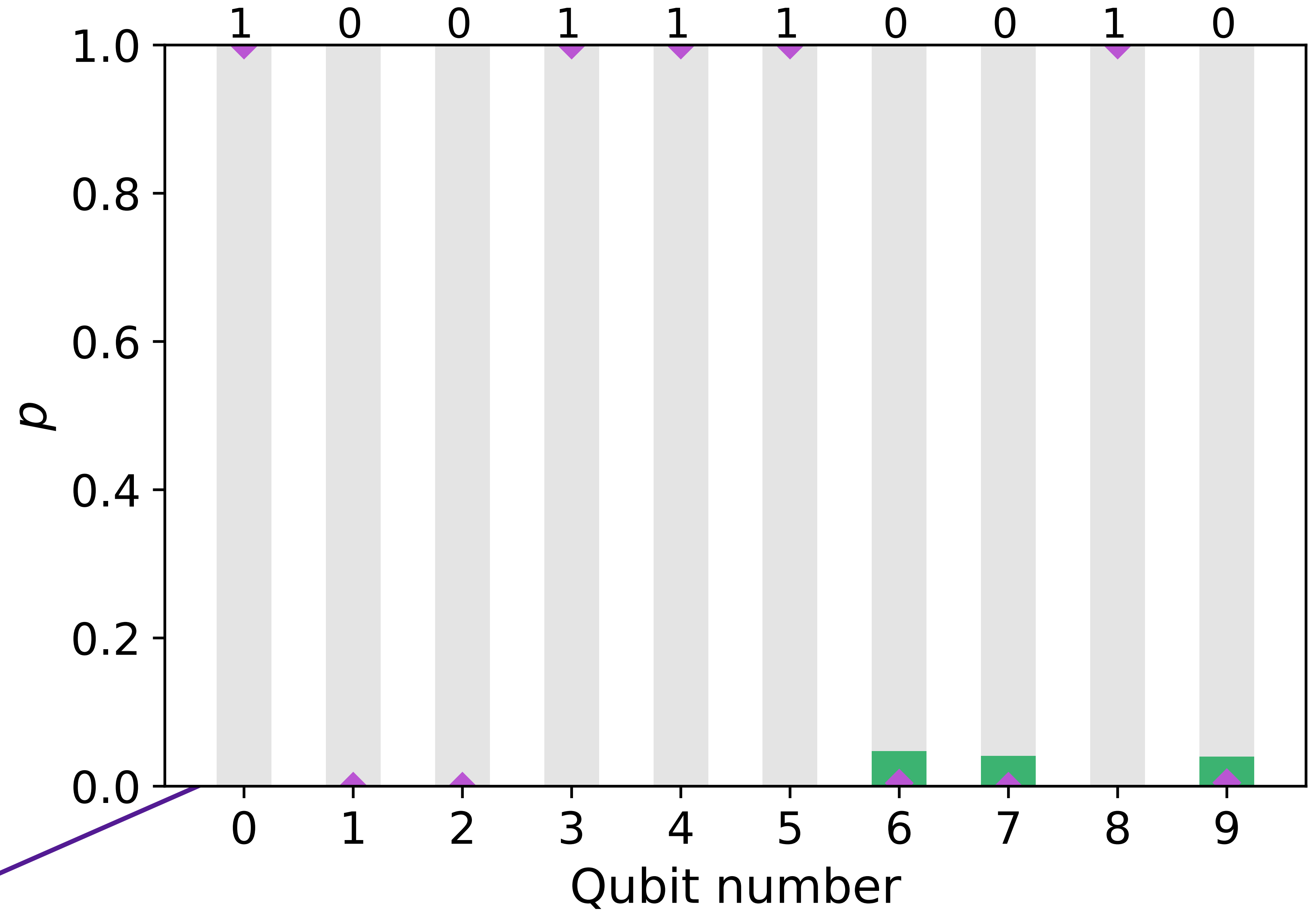
$\epsilon = 0.1$

Hidden shift circuit

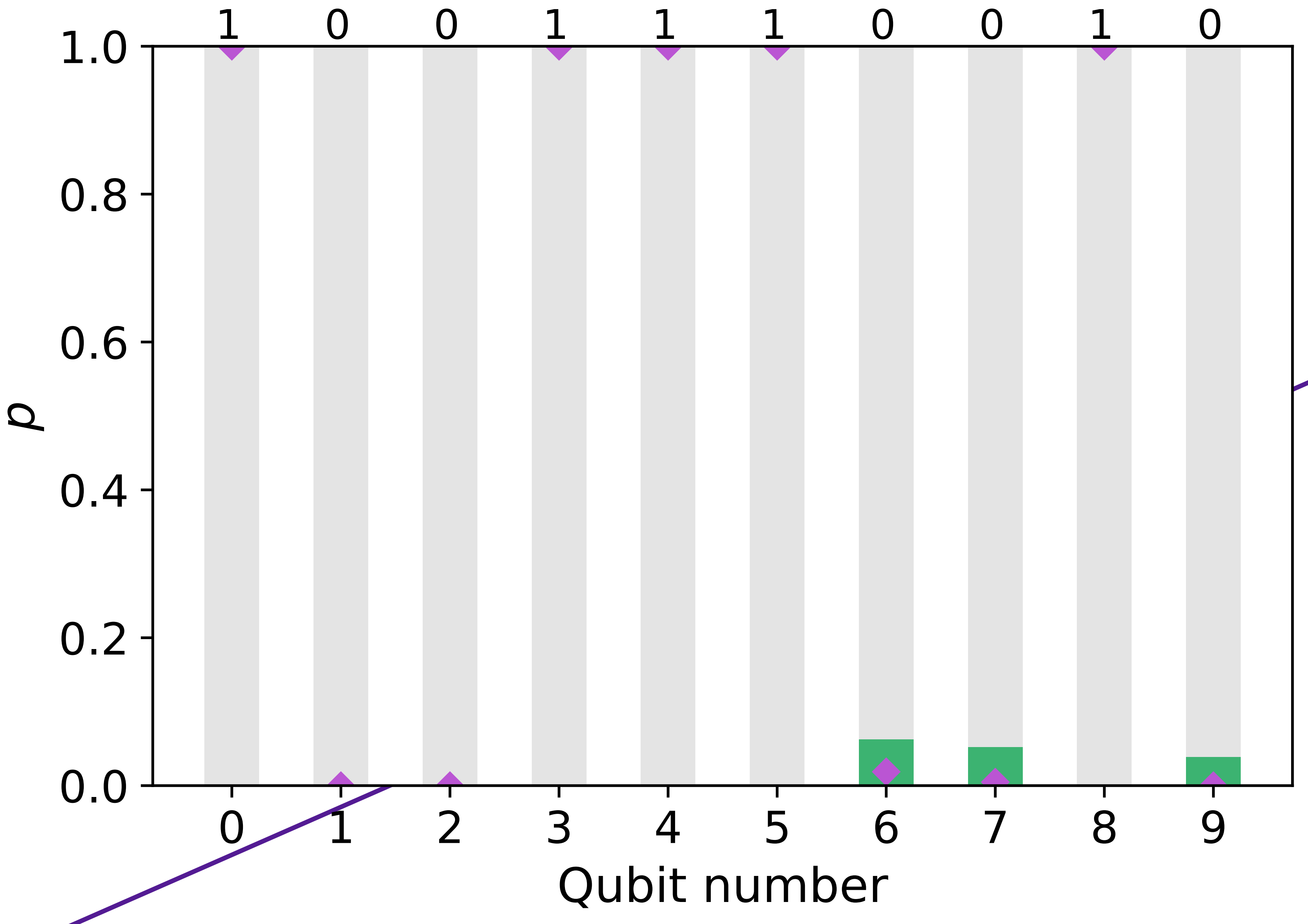




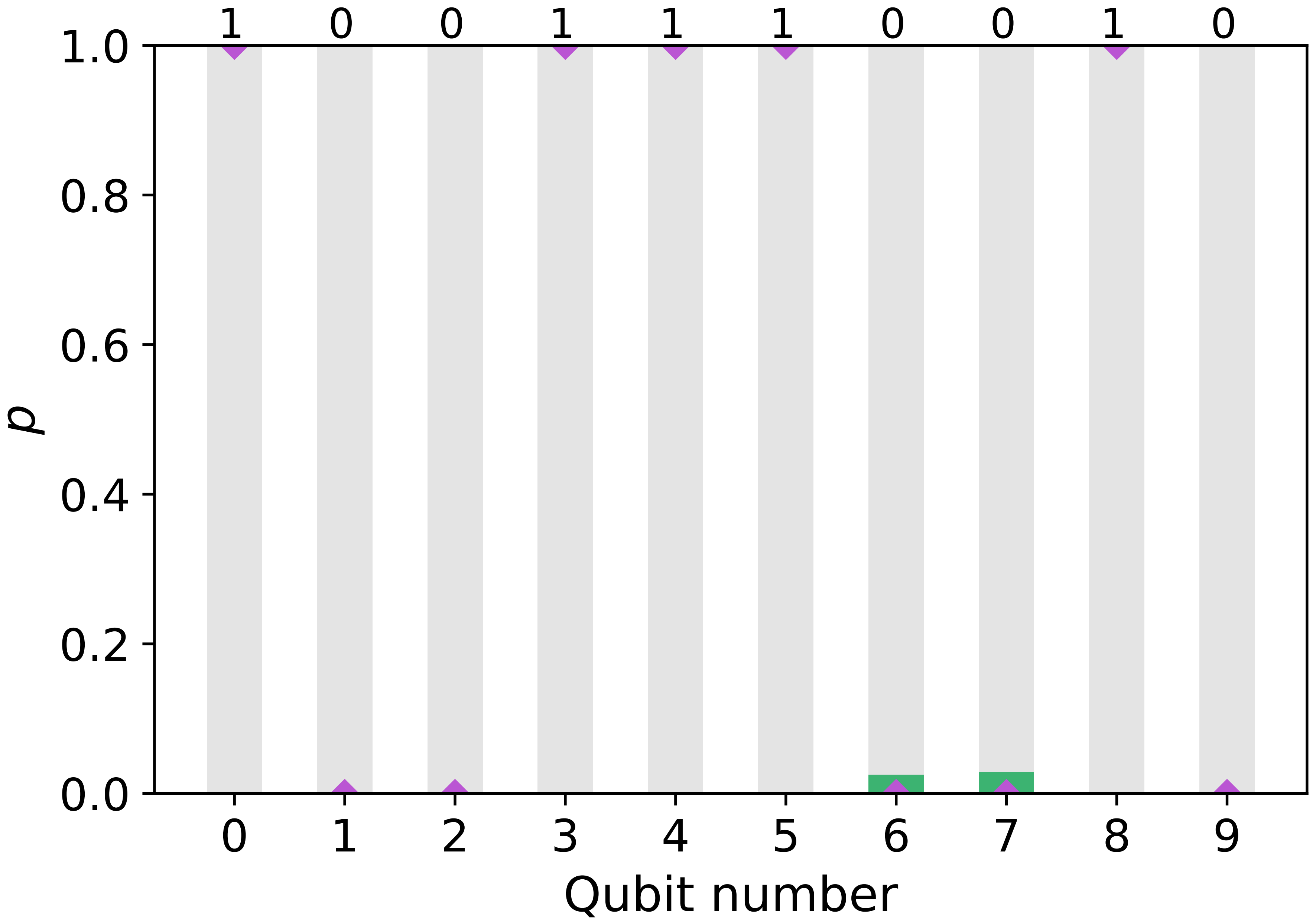
$\epsilon = 0.1$

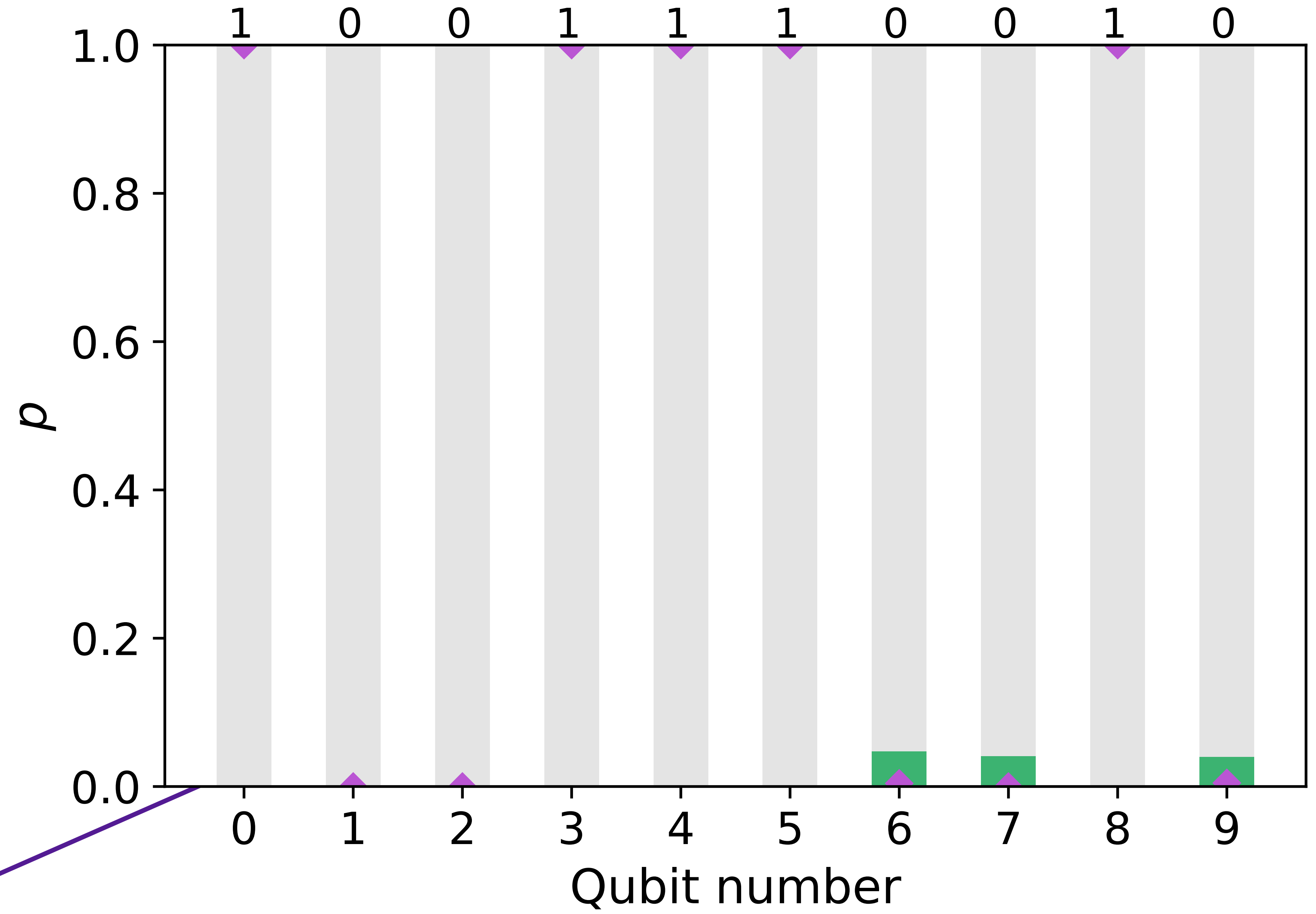


Hidden shift circuit

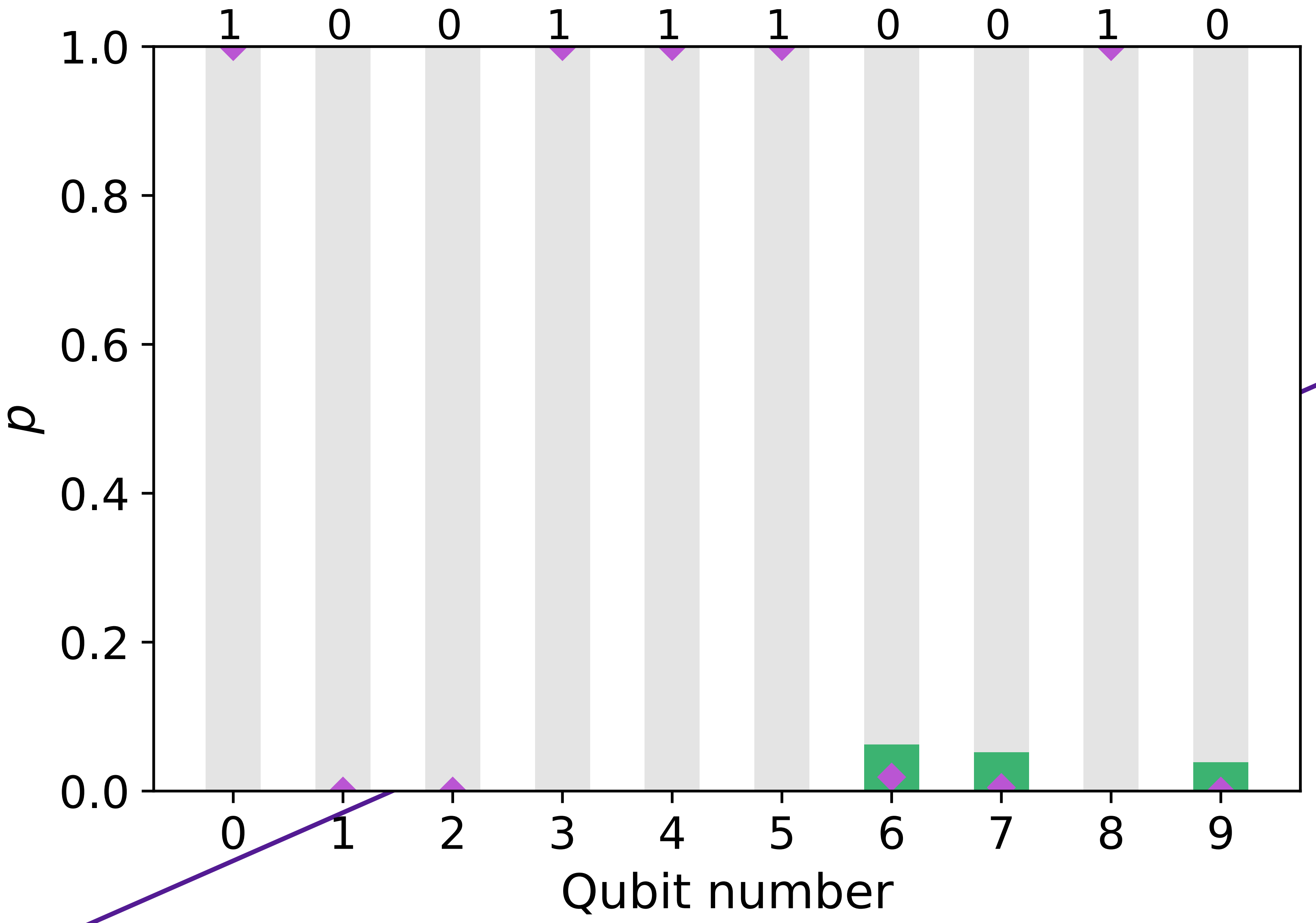


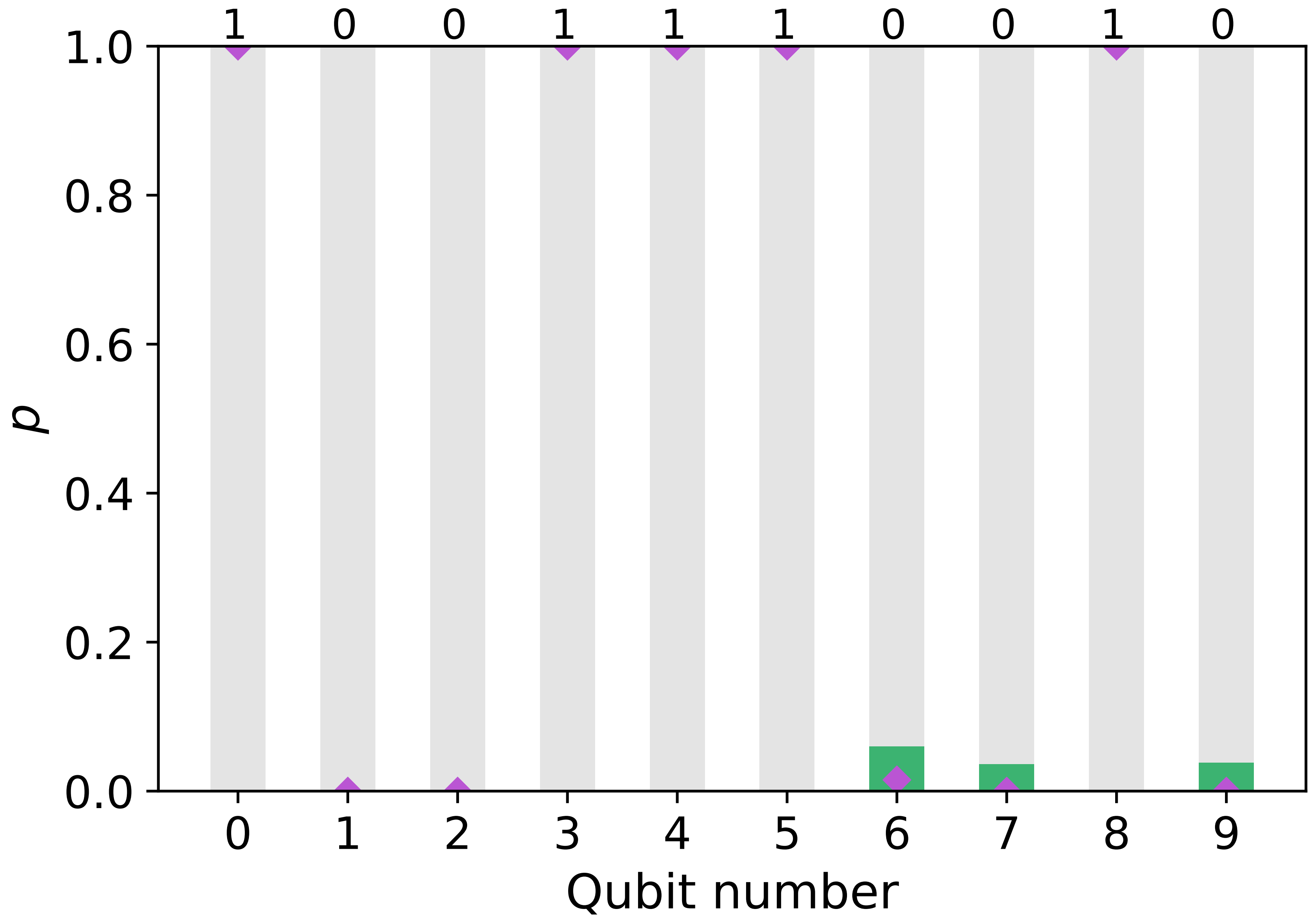
$$\epsilon = 0.1$$



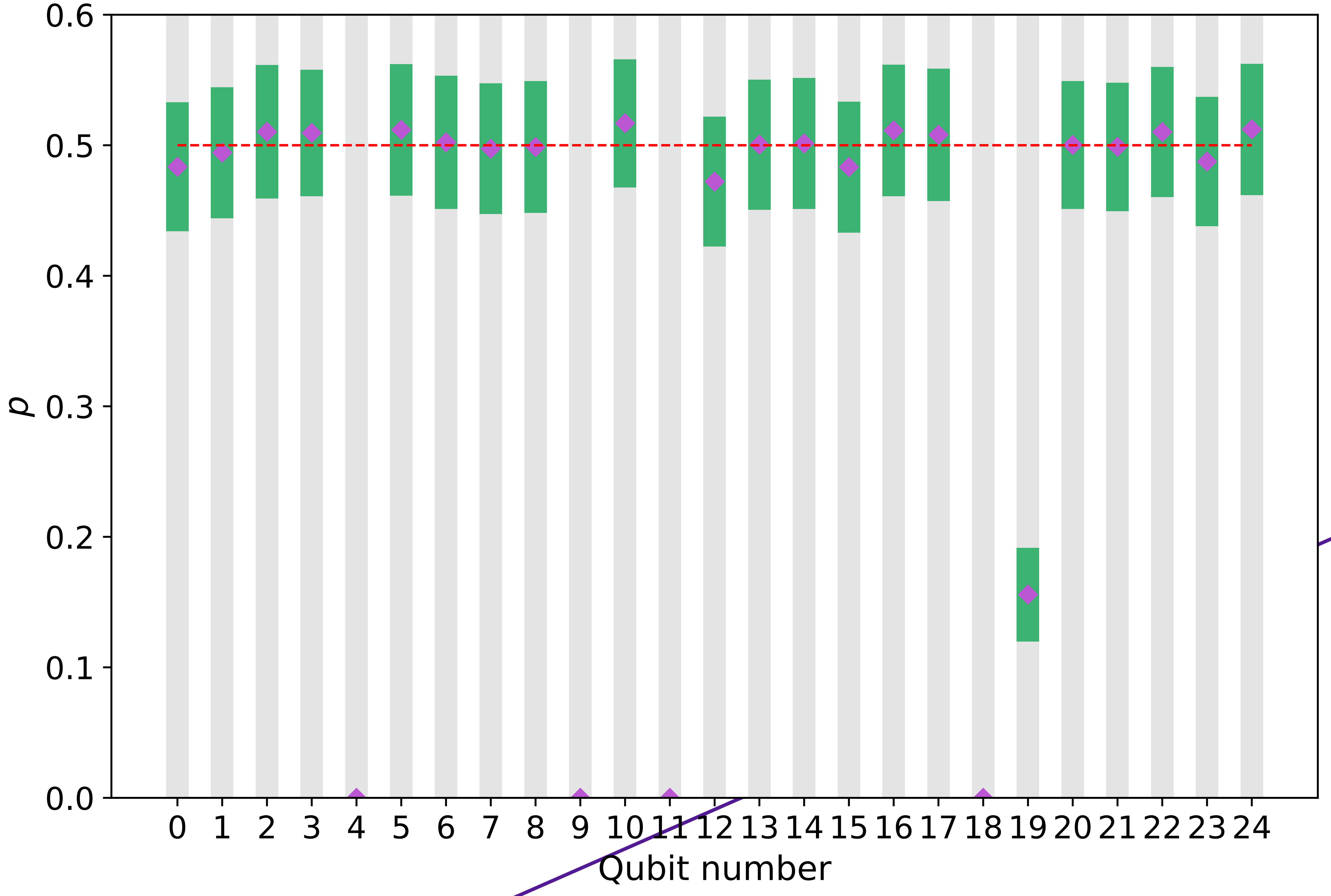


Hidden shift circuit



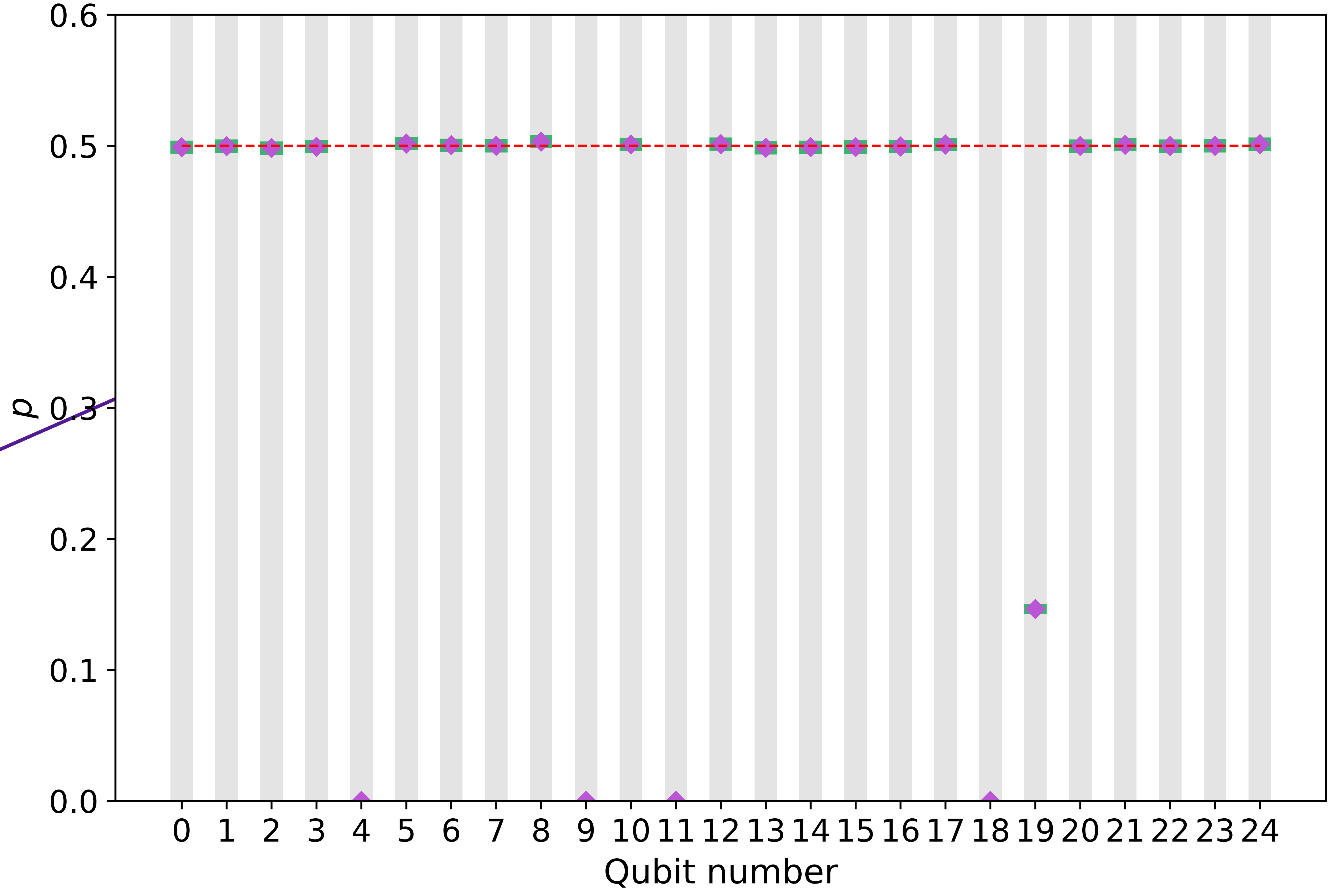


$\epsilon = 0.1$



$N(\epsilon = 0.1, k = 1) = 1\,586 \rightarrow \mathcal{N} = 4\,758$

$\epsilon = 0.01$

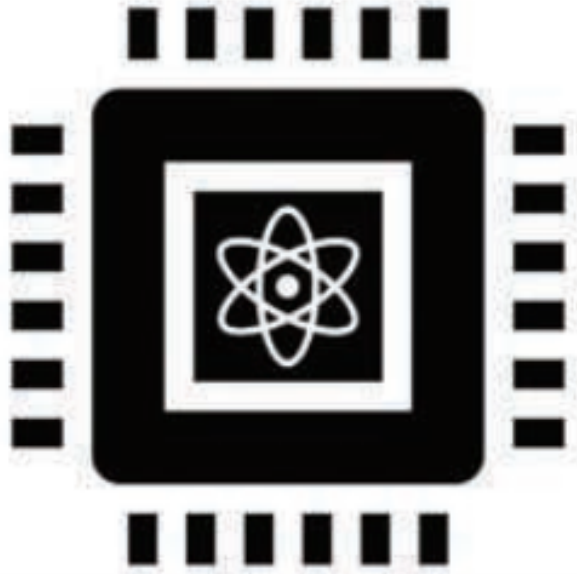


$N(\epsilon = 0.01, k = 1) = 158\,579 \rightarrow \mathcal{N} = 475\,737$

Computation

$n + k$ qubits

n qubits



Thank you for your attention!