Estimating the entropy of shallow circuit outputs is hard

arXiv:2002.12814

Alexandru Gheorghiu   Matty J. Hoban

ETH Zürich   California Institute of Technology 1891   Goldsmiths University of London

Entropy in (quantum) information theory

For some probability distribution $p : \{0,1\}^n \to [0,1]$

Entropy in (quantum) information theory

For some probability distribution $p : \{0,1\}^n \to [0,1]$

$$S(p) = -\sum_{x\in\{0,1\}^n} p(x)\log(p(x))$$

Shannon entropy

Entropy in (quantum) information theory

For some probability distribution $p : \{0,1\}^n \to [0,1]$

$$S(p) = -\sum_{x \in \{0,1\}^n} p(x) \log(p(x))$$

Shannon entropy

For some quantum state $\rho \in \mathcal{D}(\mathbb{C}^{\otimes n})$

$$S(\rho) = -Tr(\rho \log(\rho))$$

Von Neumann entropy

Entropy in (quantum) information theory

For some probability distribution $p : \{0,1\}^n \to [0,1]$

$$S(p) = -\sum_{x \in \{0,1\}^n} p(x) \log(p(x))$$

Shannon entropy

For some quantum state $\rho \in \mathcal{D}(\mathbb{C}^{\otimes n})$

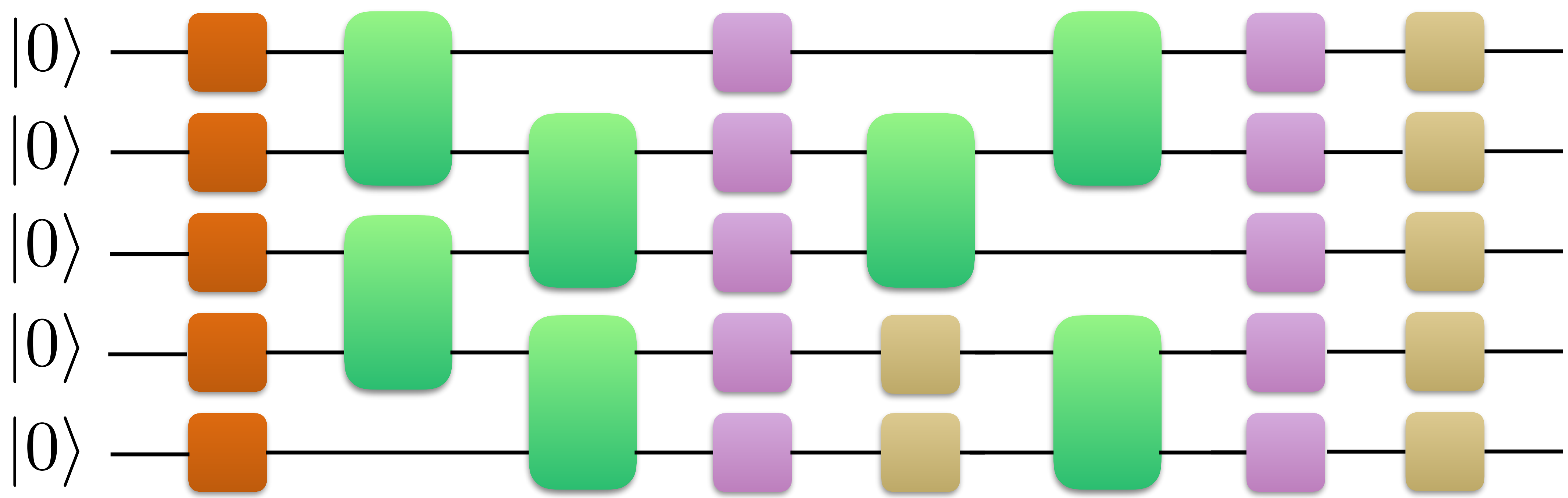
$$S(\rho) = -Tr(\rho \log(\rho))$$

Von Neumann entropy

$$0 \leq S \leq n$$

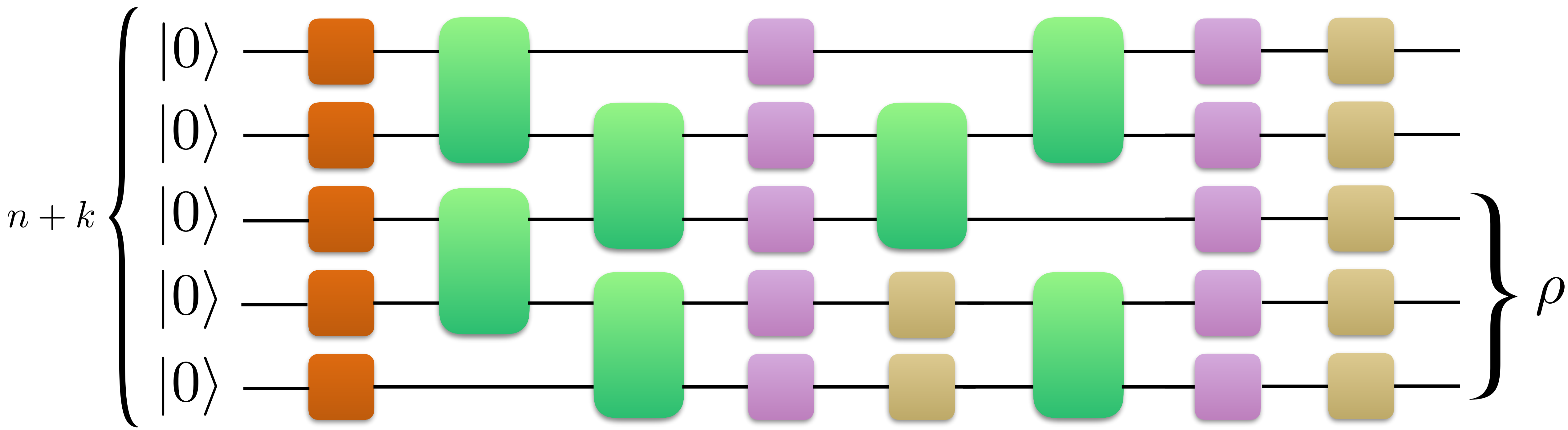
Entropy estimation

Given description of …



Entropy estimation

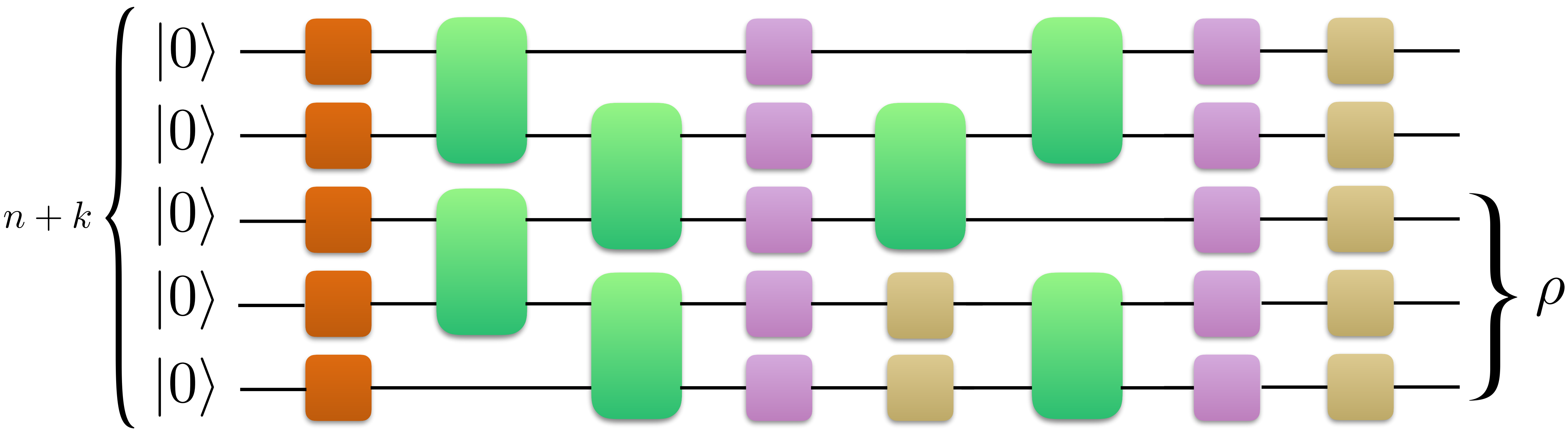
Given description of …



$$\rho \in \mathcal{D}(\mathbb{C}^{\otimes n})$$

Entropy estimation

Given description of …

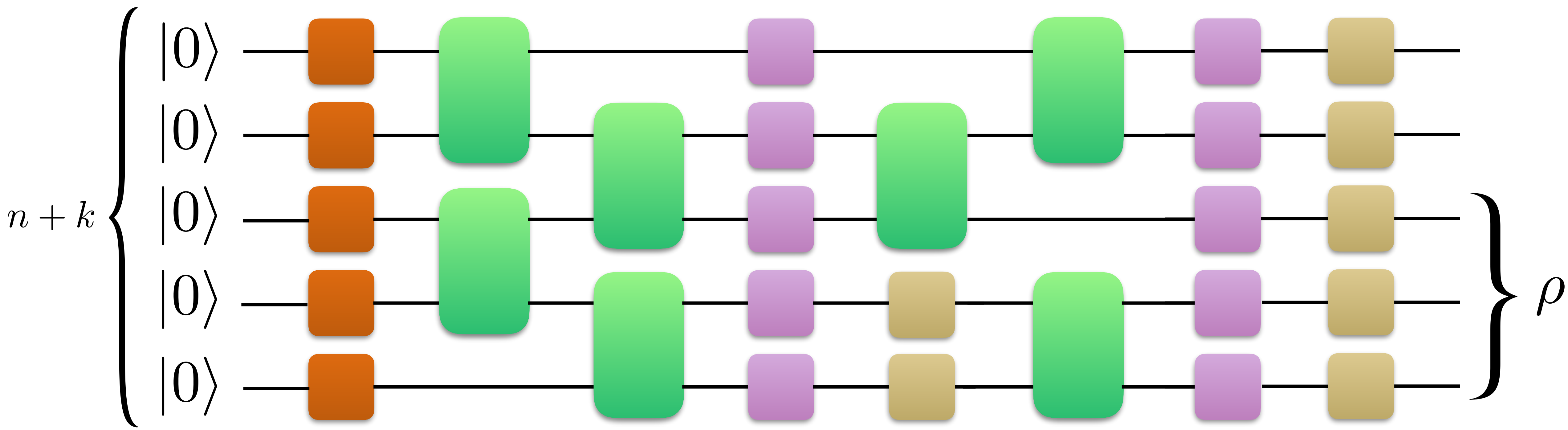


$$\rho \in \mathcal{D}(\mathbb{C}^{\otimes n})$$

(can similarly define classical case)

Entropy estimation

Given description of …



$$\rho \in \mathcal{D}(\mathbb{C}^{\otimes n})$$

(can similarly define classical case)

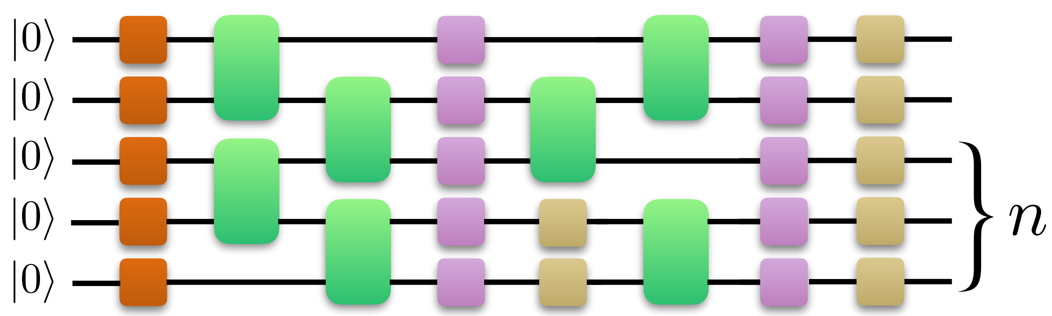
compute an entropy estimate $\hat{S}$

$$S(\rho) - 0.1 \leq \hat{S} \leq S(\rho) + 0.1$$

What is a hard problem?

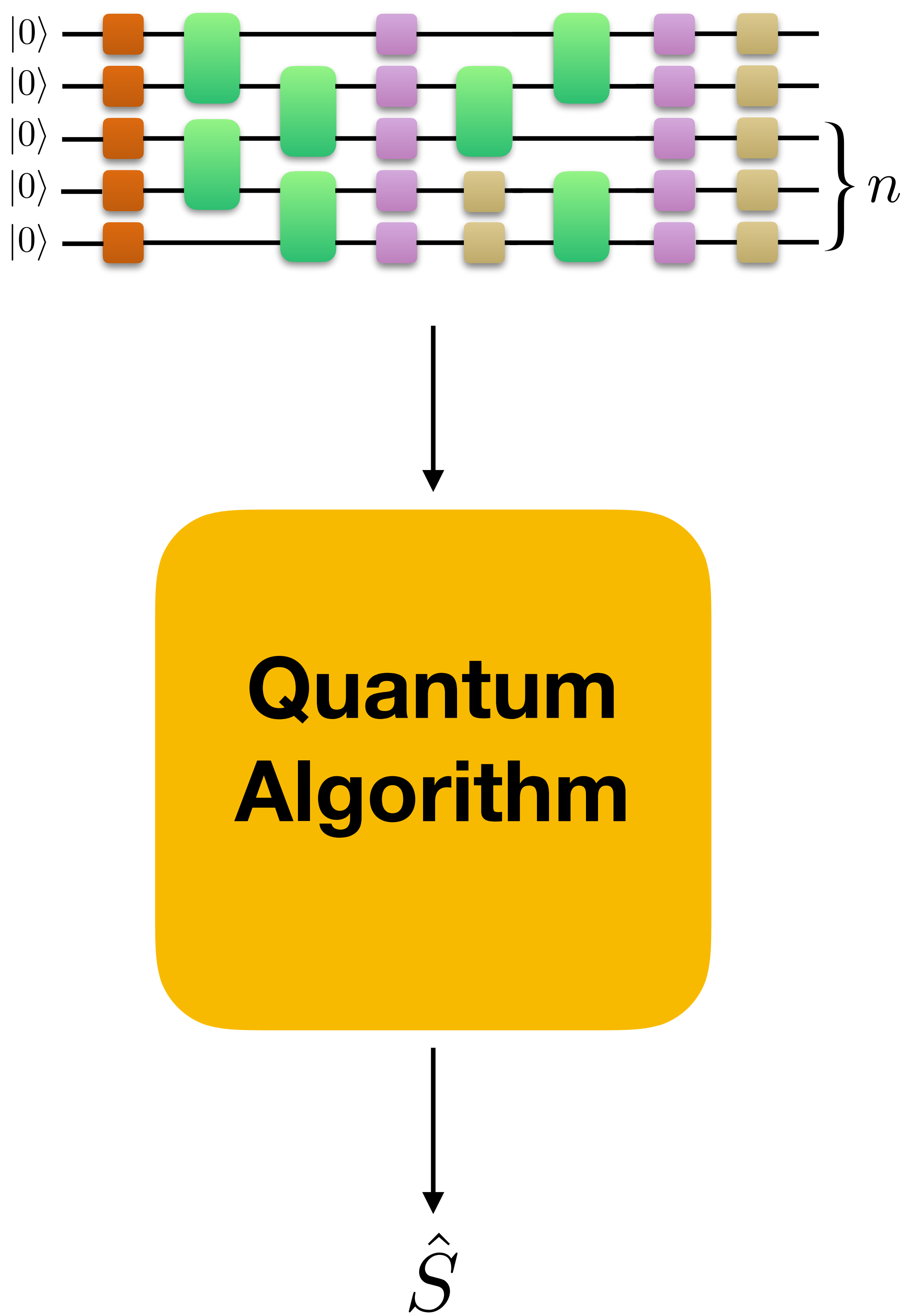
Quantum Algorithm

What is a hard problem?

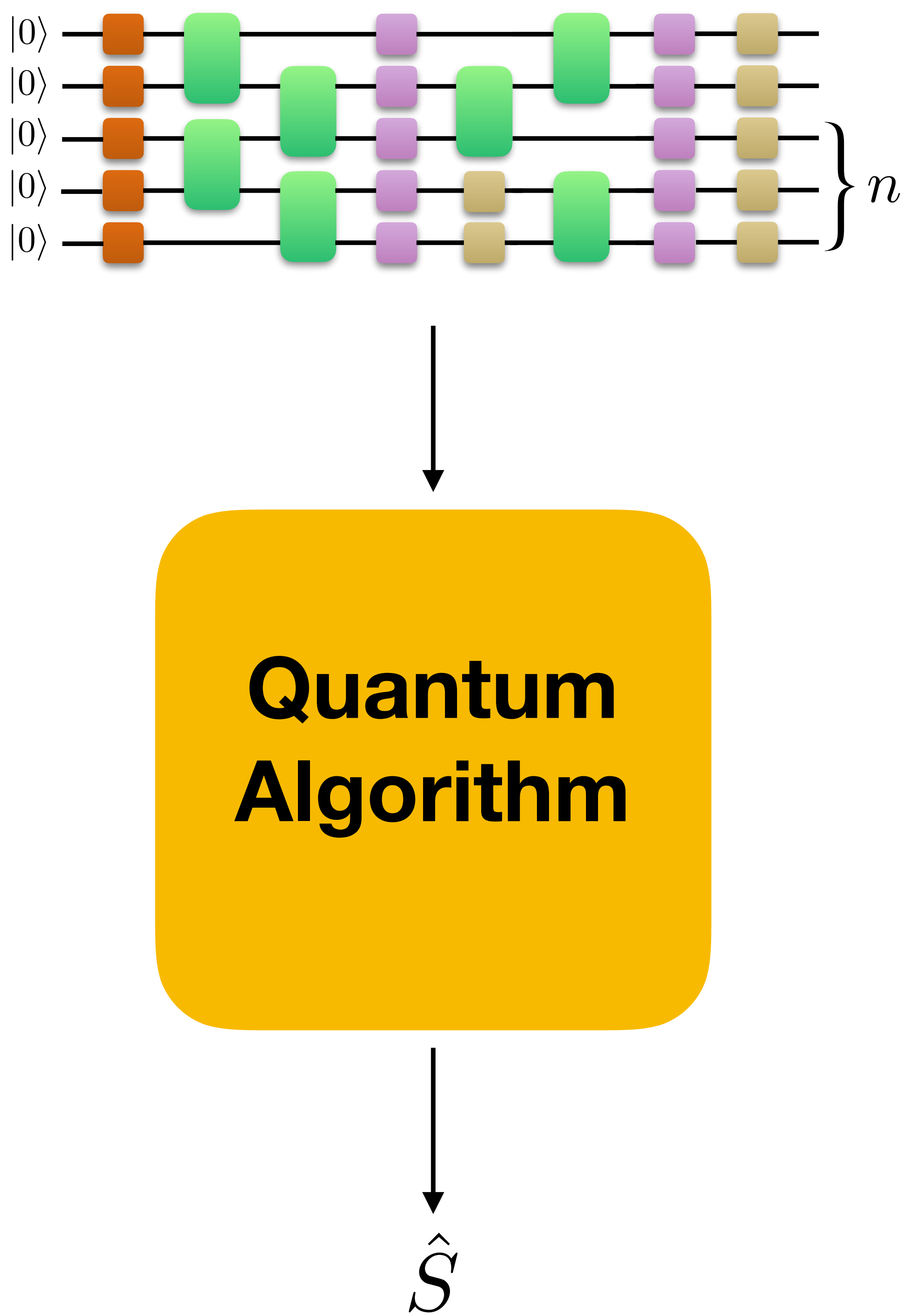


Quantum Algorithm

What is a hard problem?

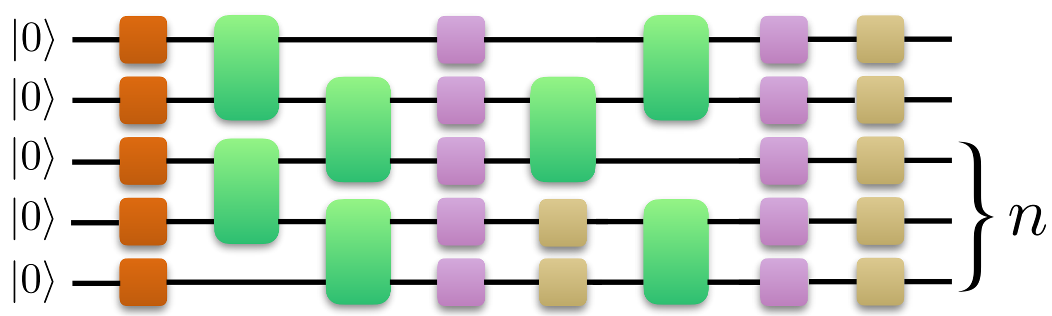


What is a hard problem?



How much time does the *fastest* algorithm require as a function of n?

What is a hard problem?



Quantum Algorithm

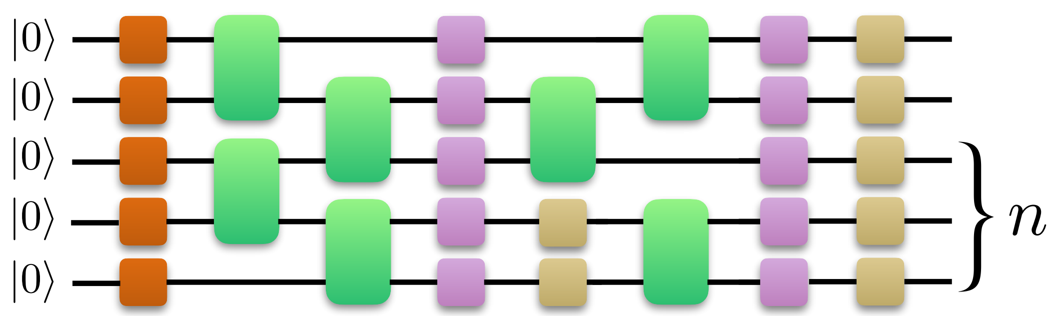
$\hat{S}$

How much time does the *fastest* algorithm require as a function of n?

$poly(n)$ ⟶ **Efficient**

Otherwise ⟶ **Inefficient**

What is a hard problem?



Quantum Algorithm

$\hat{S}$

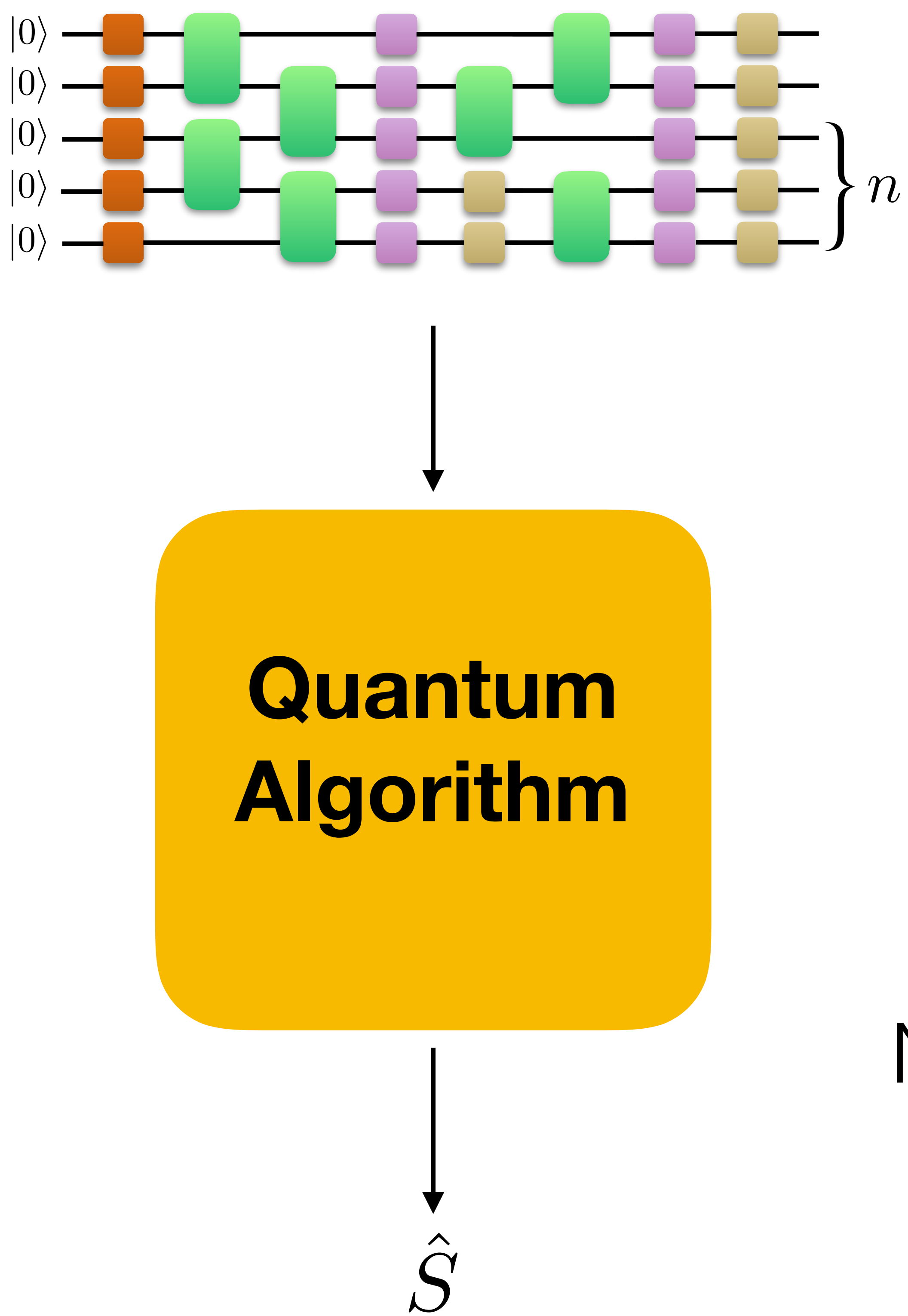
How much time does the *fastest* algorithm require as a function of n?

$poly(n)$ ⟶ **Efficient**

Otherwise ⟶ **Inefficient**

(problem is *hard*)

What is a hard problem?



How much time does the *fastest* algorithm require as a function of n?

$poly(n)$ ⟶ **Efficient**

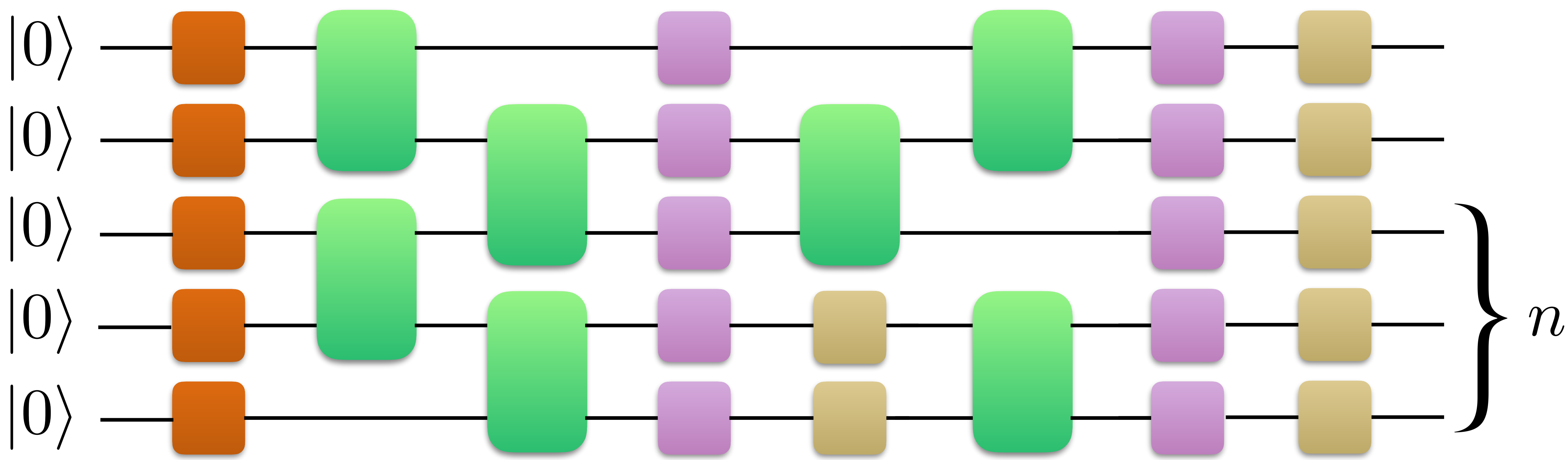
Otherwise ⟶ **Inefficient**

(problem is *hard*)

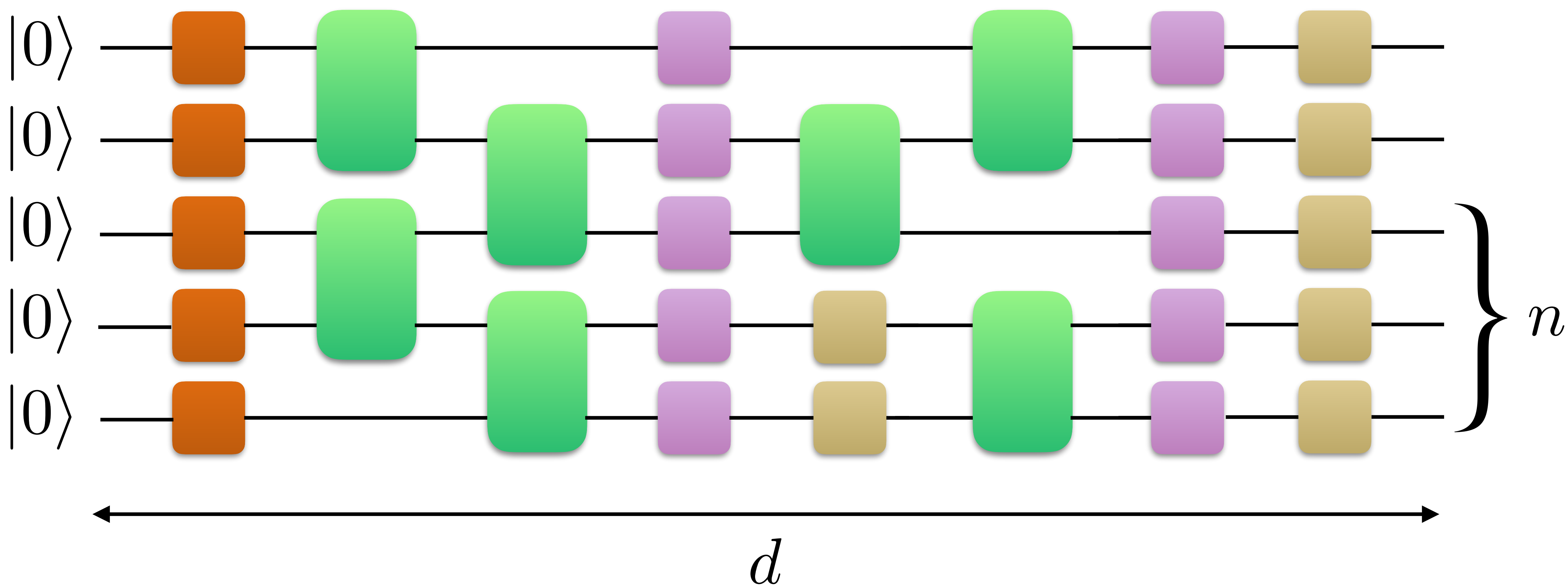
Naive approaches are inefficient

$2^{O(n)}$ time

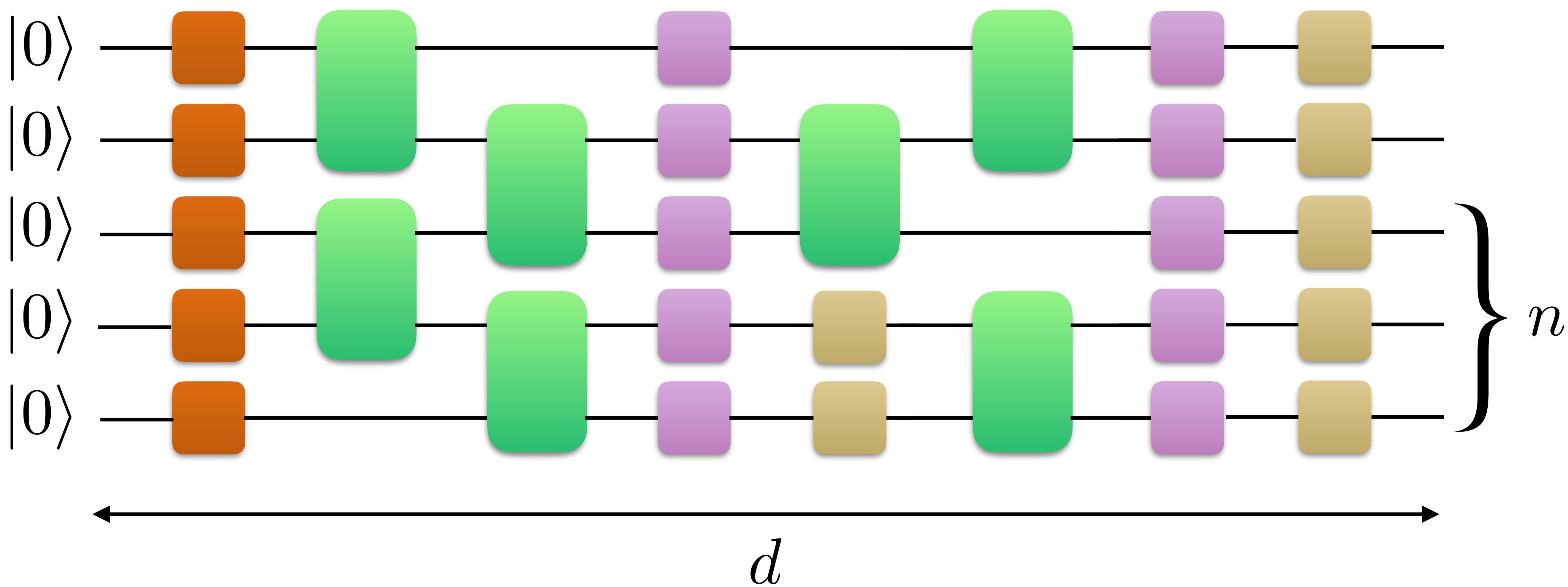
Hardness of entropy estimation



Hardness of entropy estimation

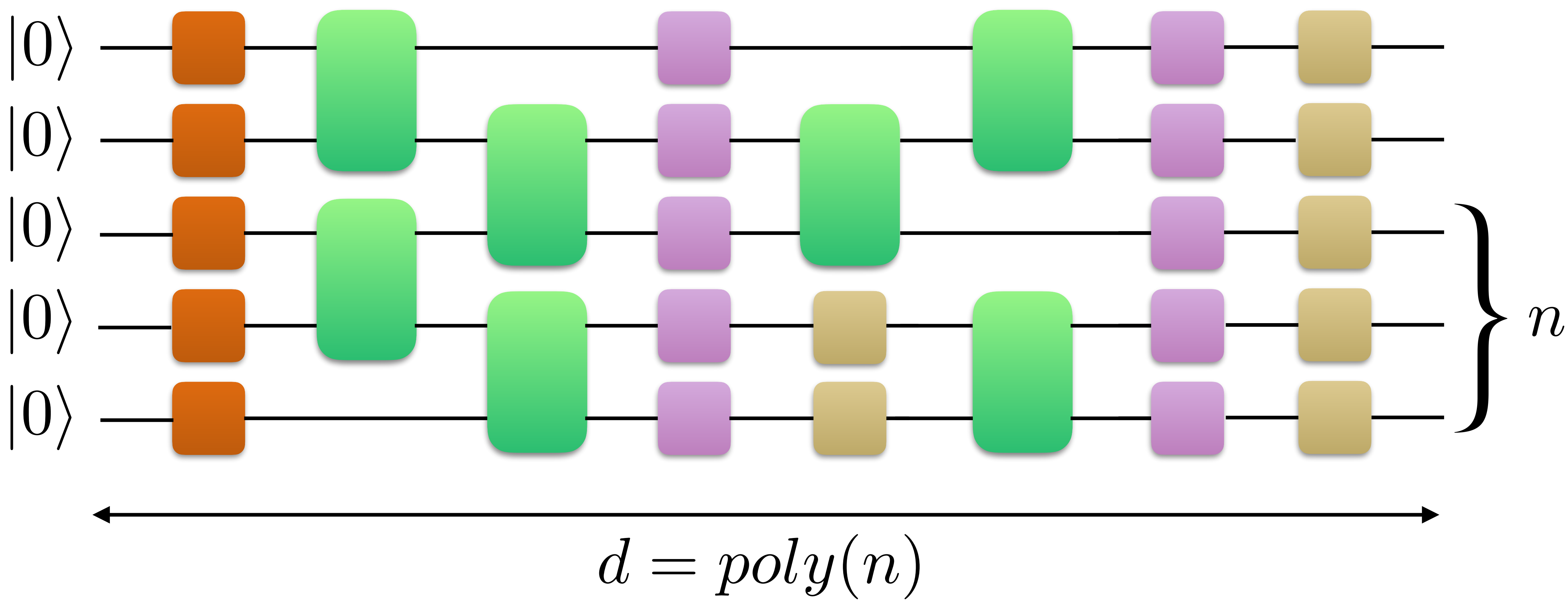


Hardness of entropy estimation

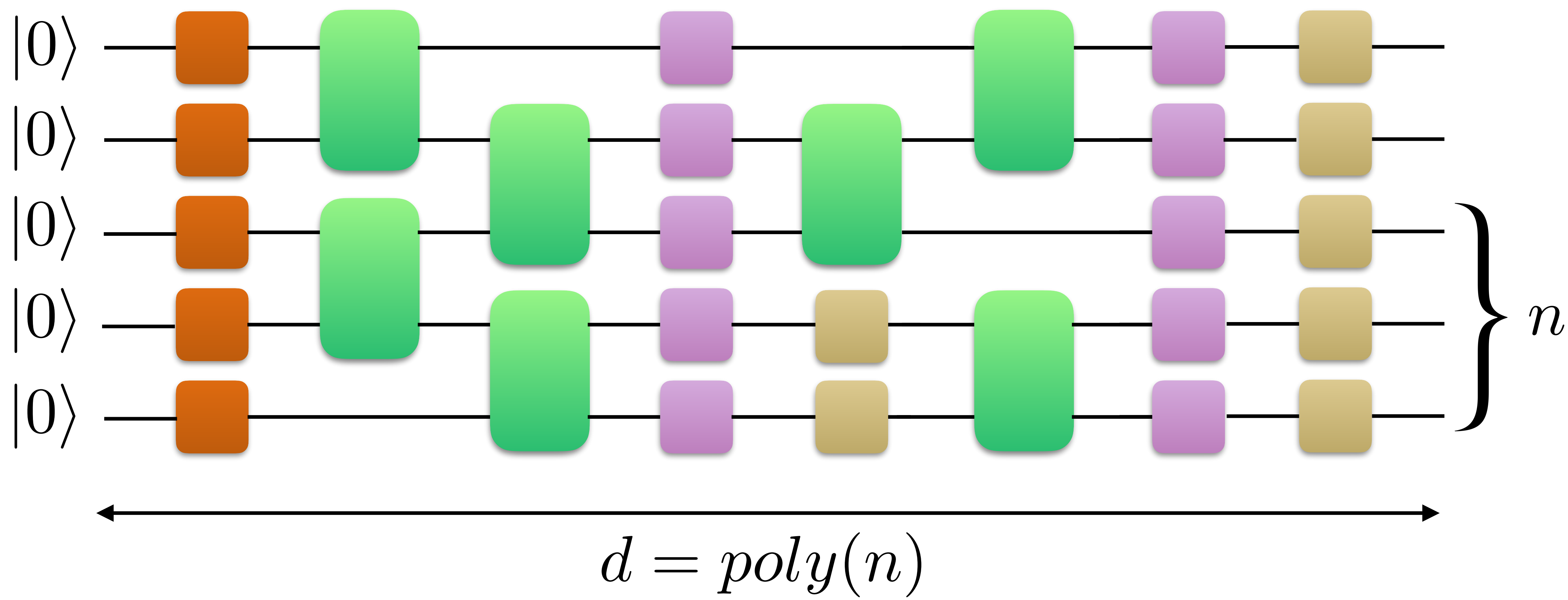


Assume circuit width is always poly(n)

Hardness of entropy estimation



Hardness of entropy estimation

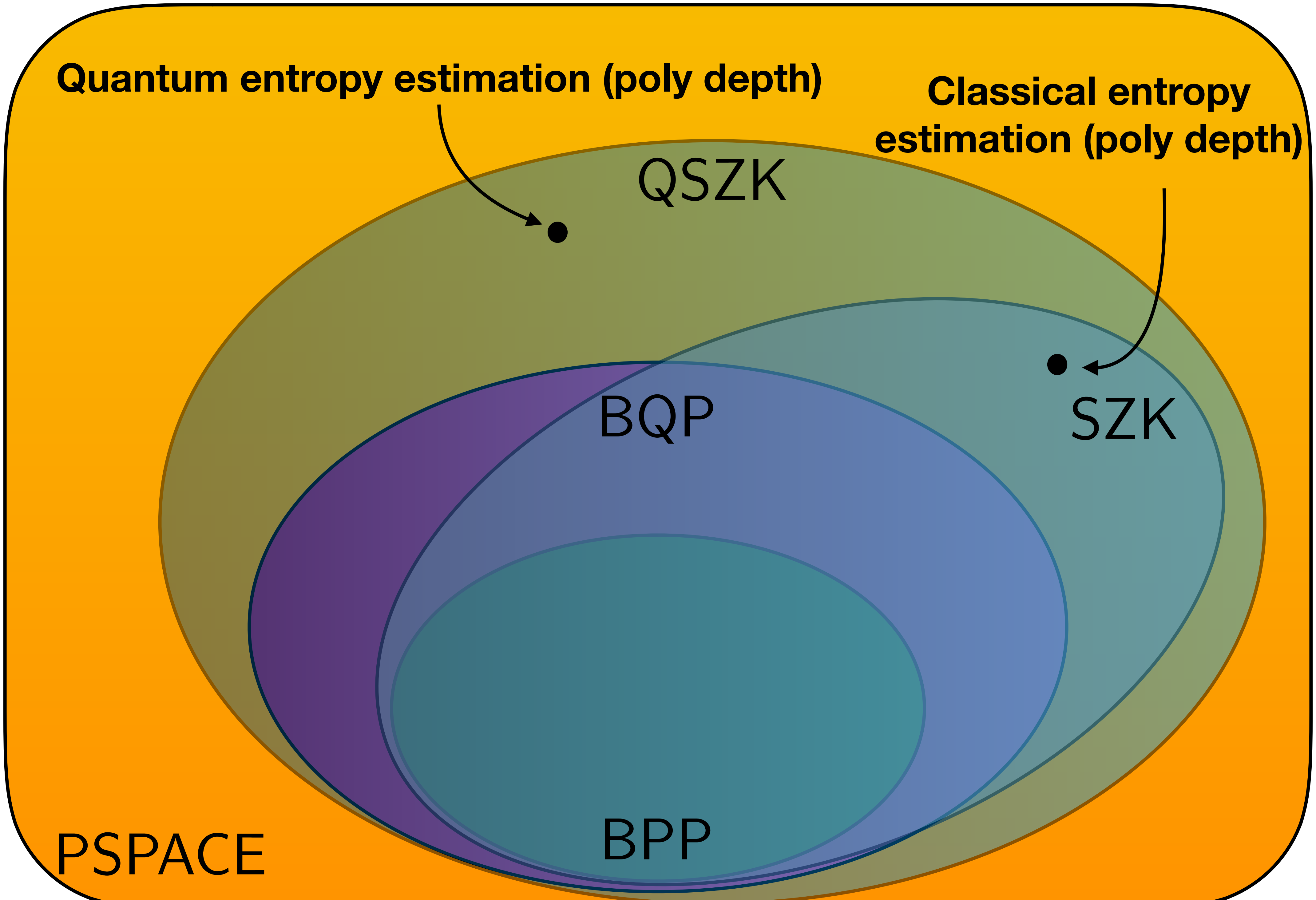


Hard based on plausible complexity-theoretic conjectures

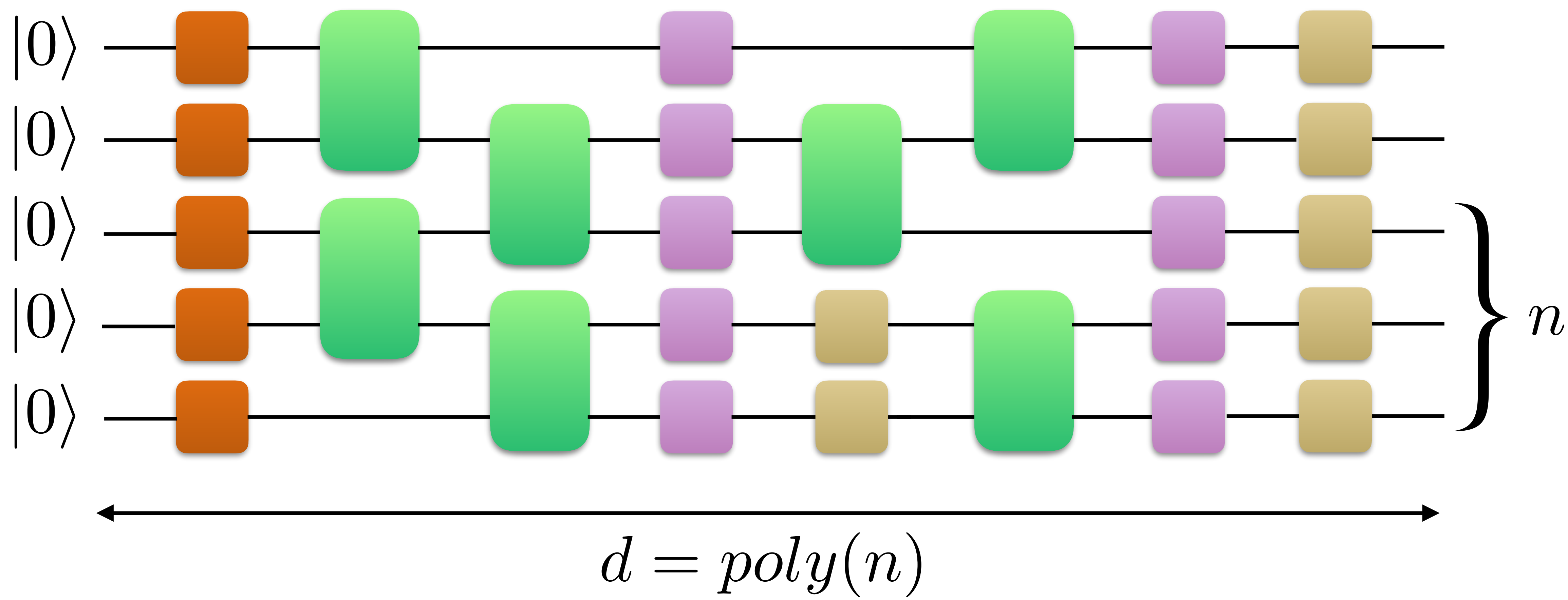
[Goldreich, Vadhan '99]

[Ben-Aroya, Schwartz, Ta-Shma '10]

Hardness of entropy estimation



Hardness of entropy estimation



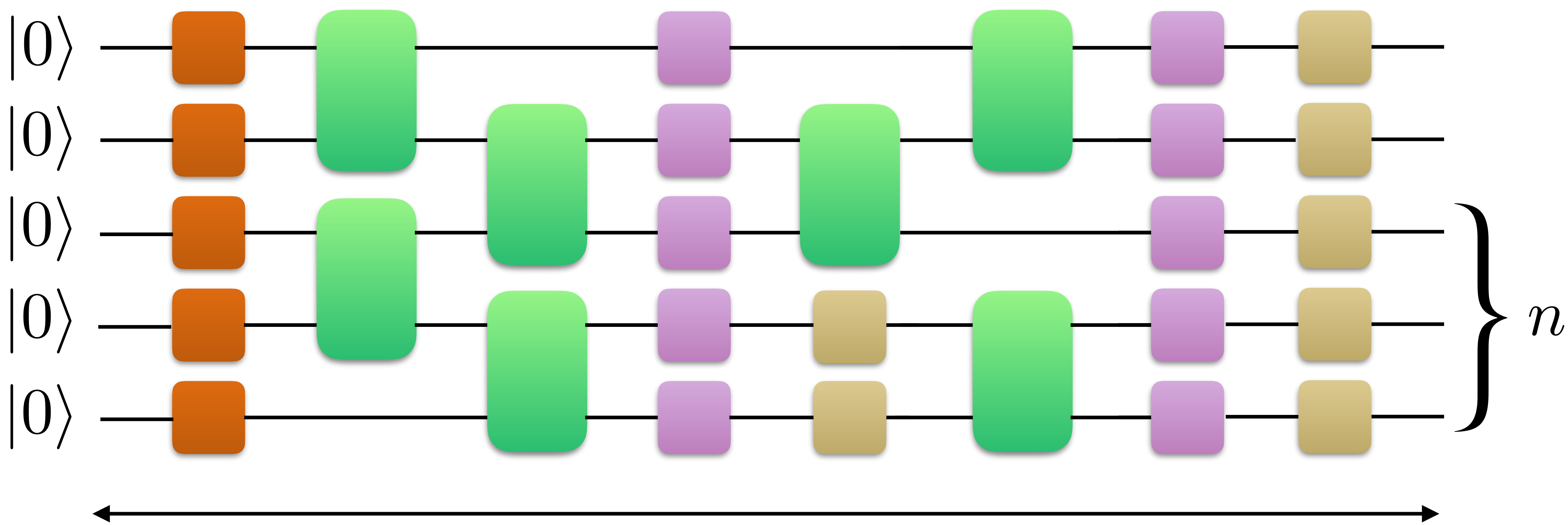
Hard based on plausible complexity-theoretic conjectures

(at least as hard as finding collisions for a function)

[Goldreich, Vadhan '99]

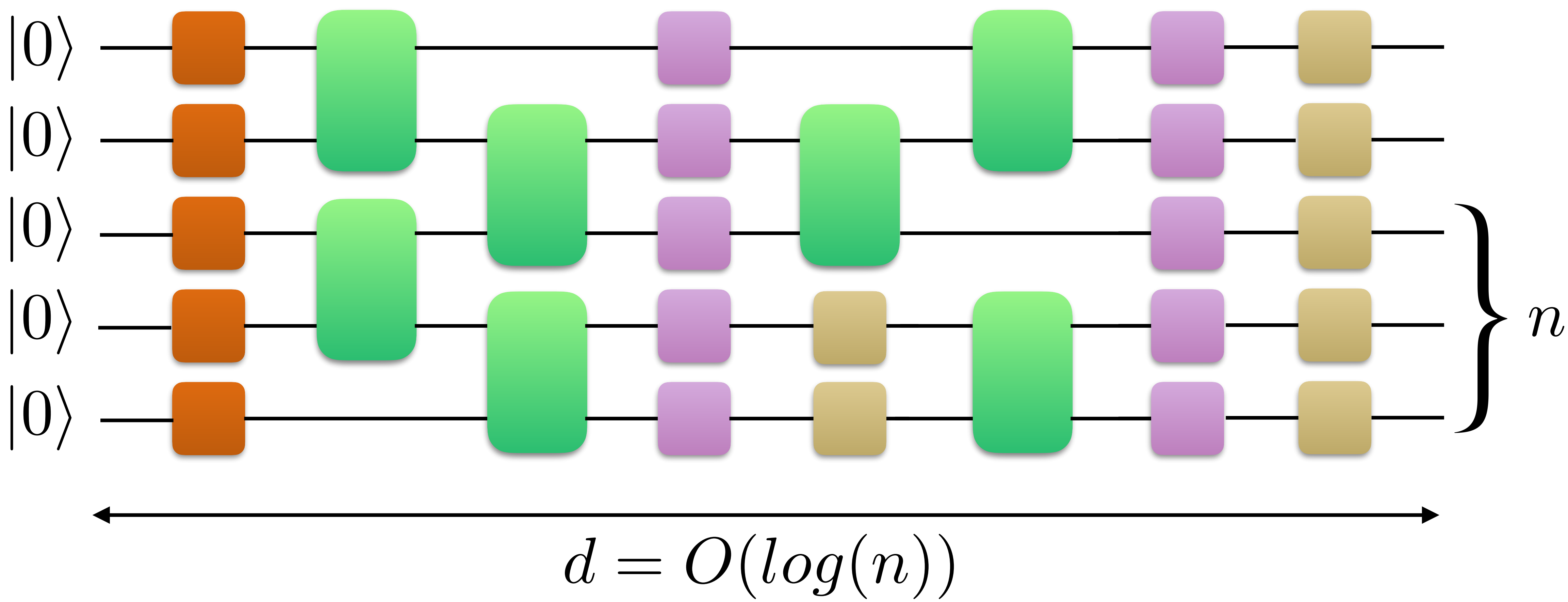
[Ben-Aroya, Schwartz, Ta-Shma '10]

Our results



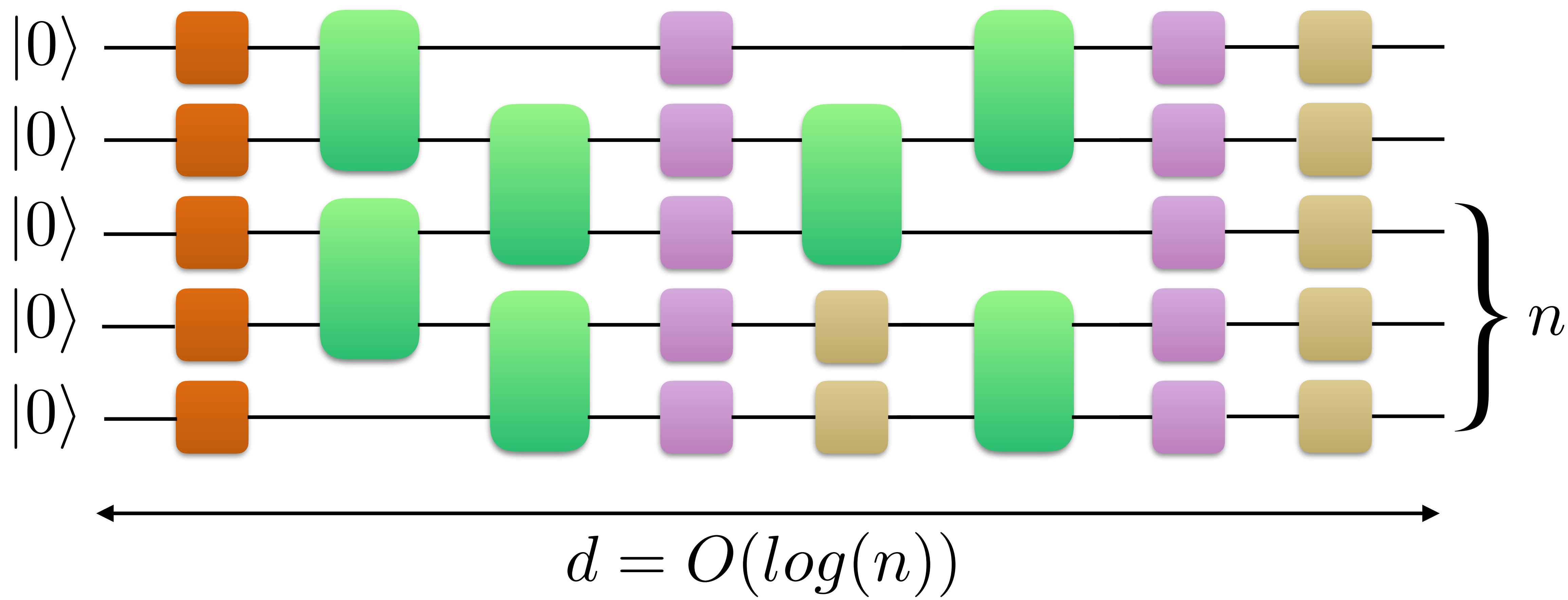
$$d = O(log(n))$$

Our results



As hard as the *Learning With Errors (LWE)* problem

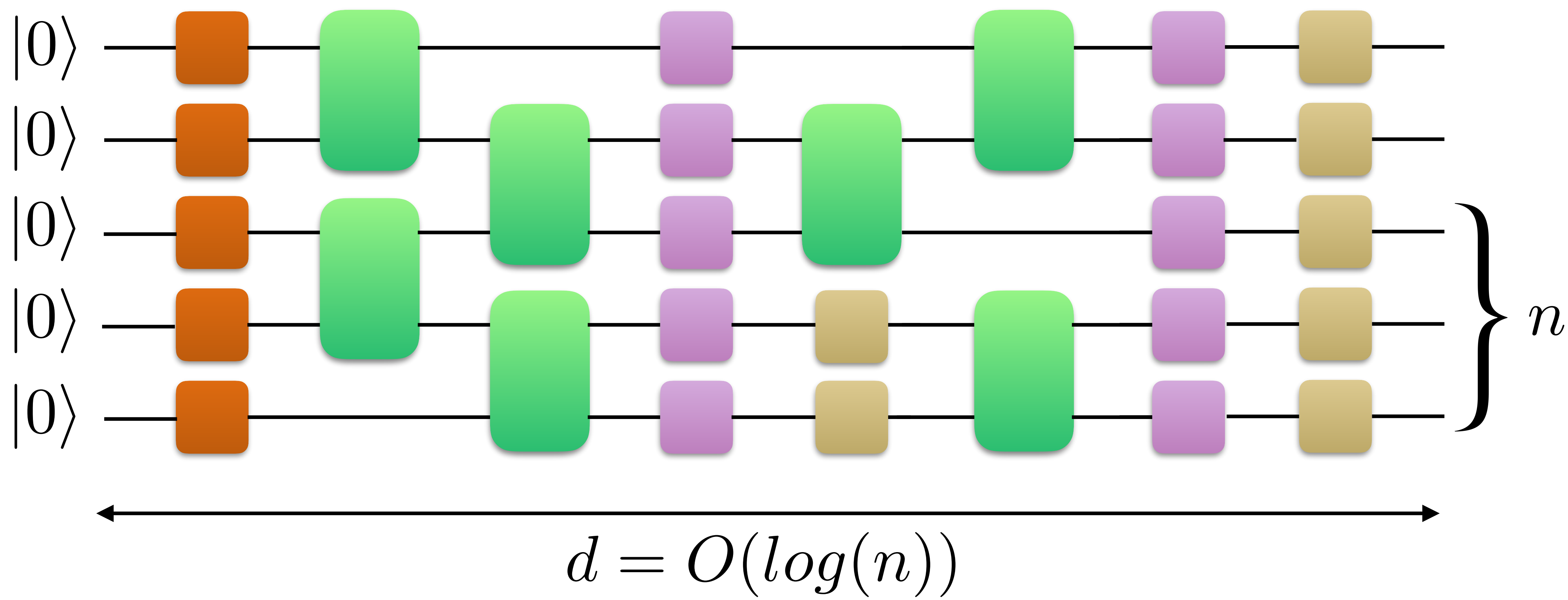
Our results



As hard as the *Learning With Errors (LWE)* problem

LWE is a candidate problem for post-quantum cryptographic protocols

Our results

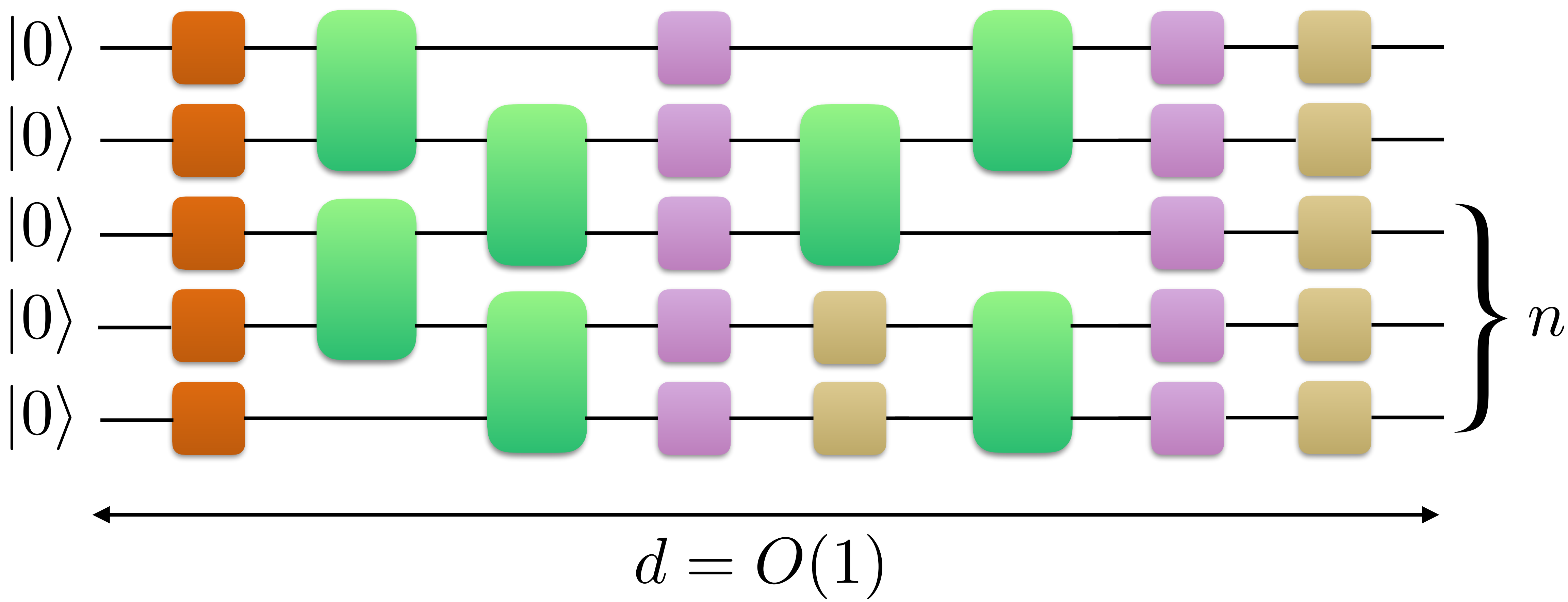


As hard as the *Learning With Errors (LWE)* problem

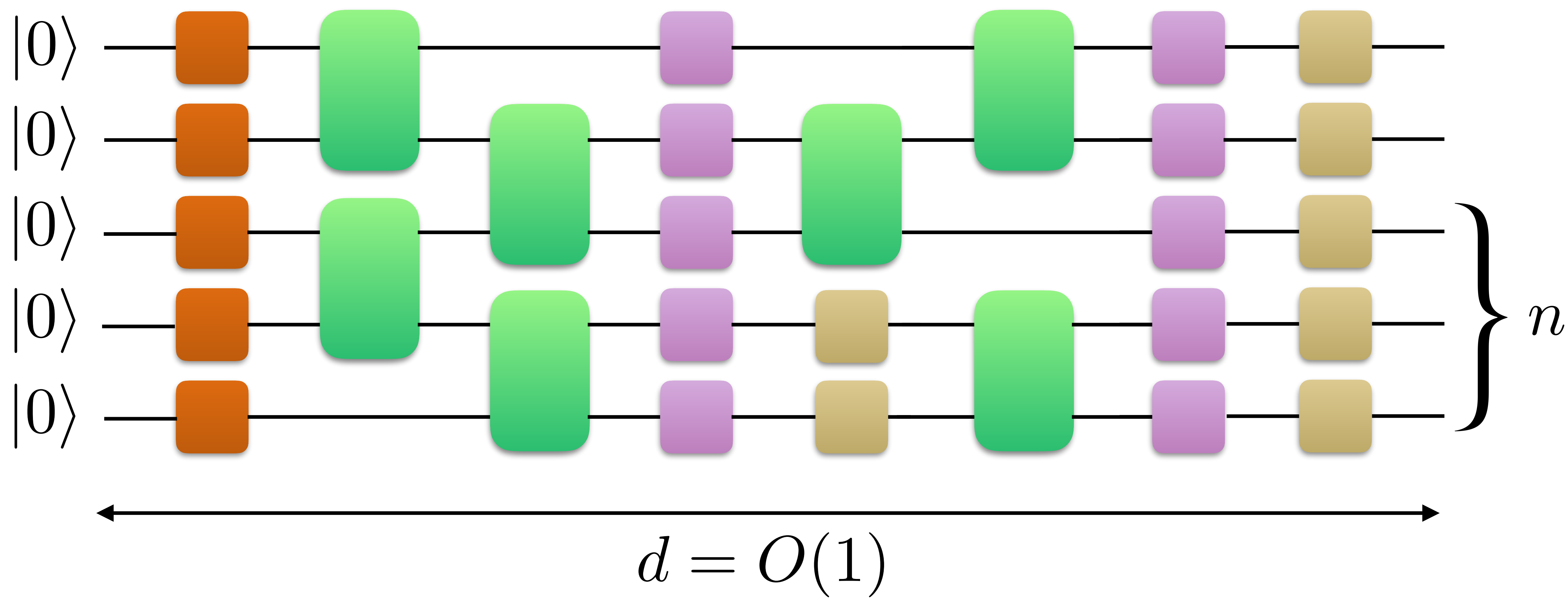
LWE is a candidate problem for post-quantum cryptographic protocols

Best known (quantum) algorithms require exponential time

Our results

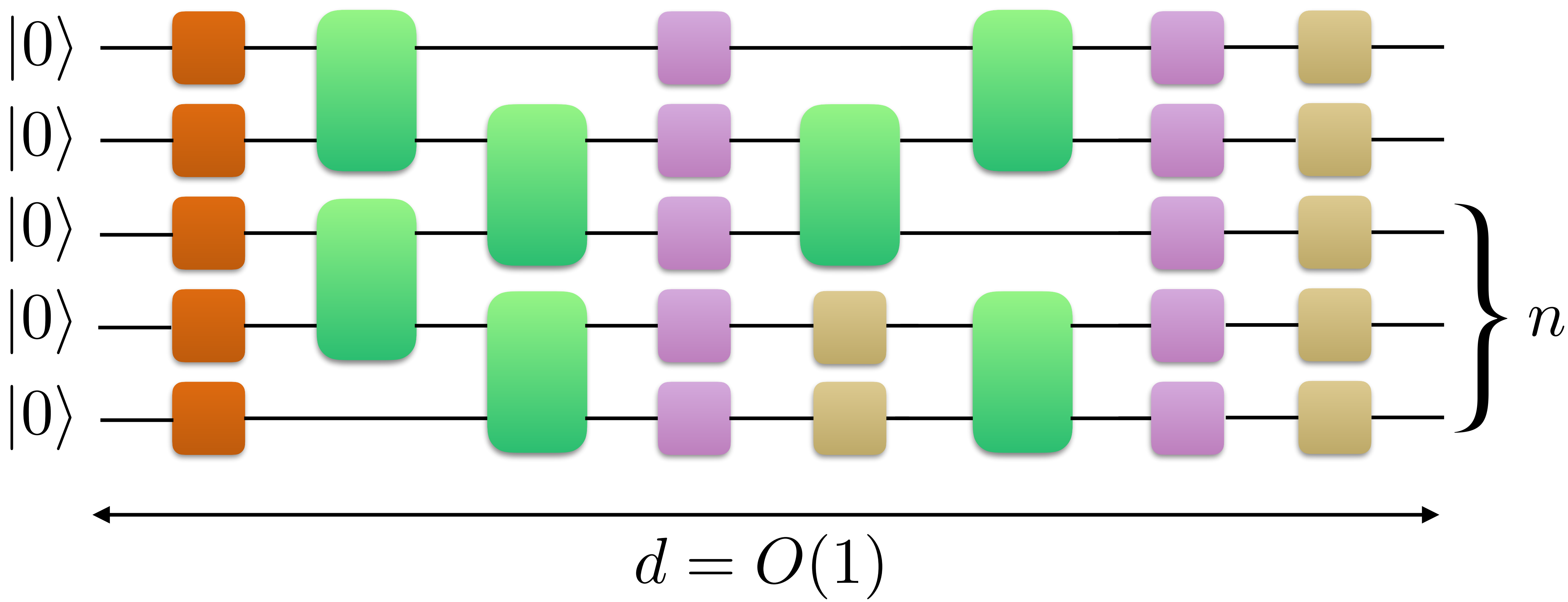


Our results



Classical circuit case is easy!

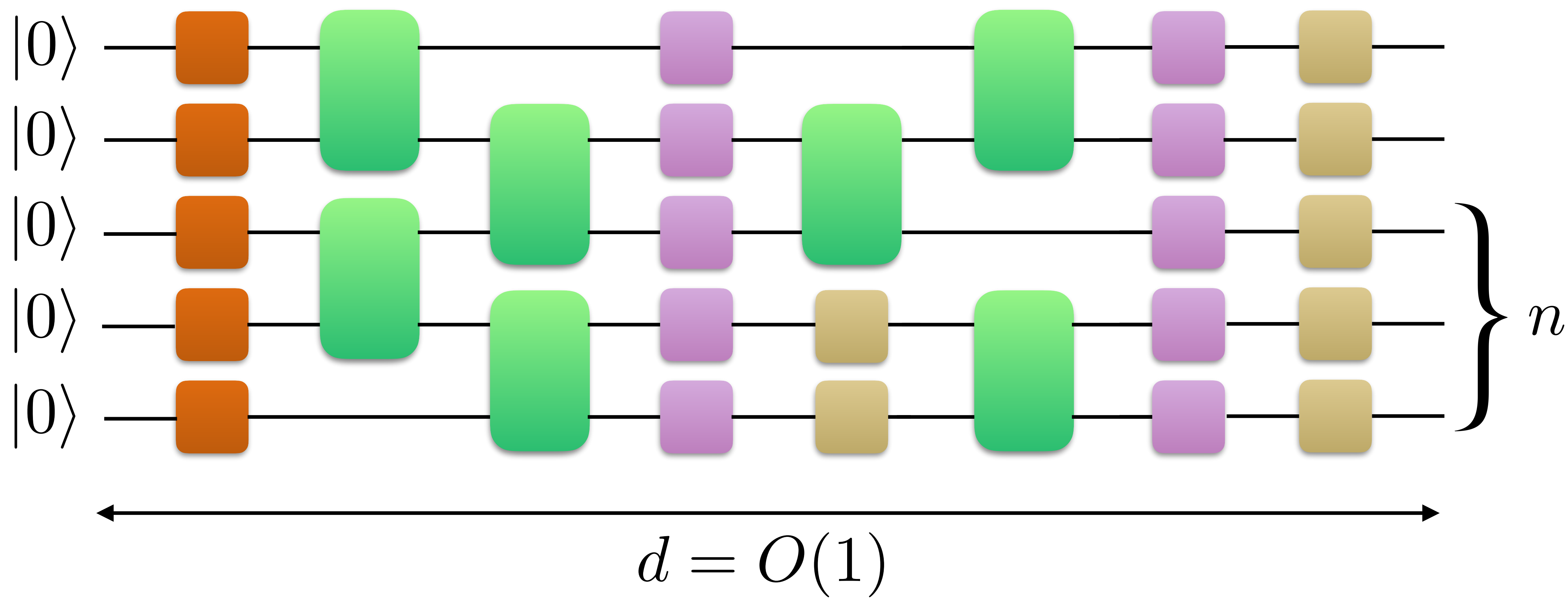
Our results



Classical circuit case is easy!

Quantum circuit case remains as hard as LWE

Our results

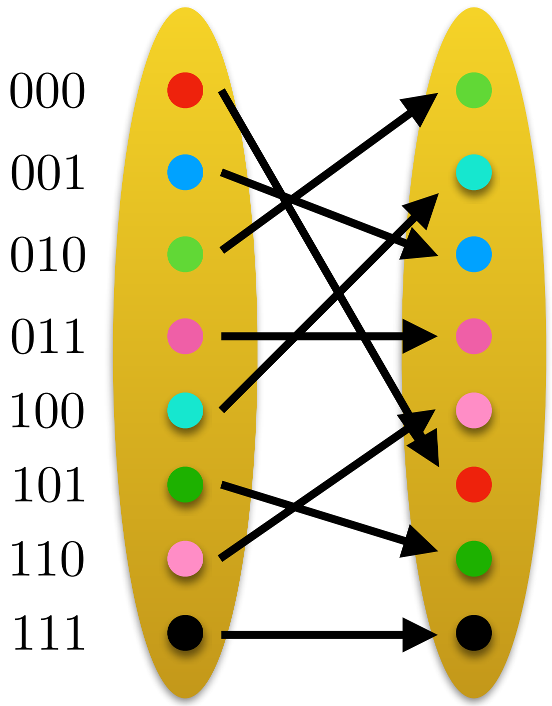


Classical circuit case is easy!

Quantum circuit case remains as hard as LWE

(requires arbitrary rotation gates)

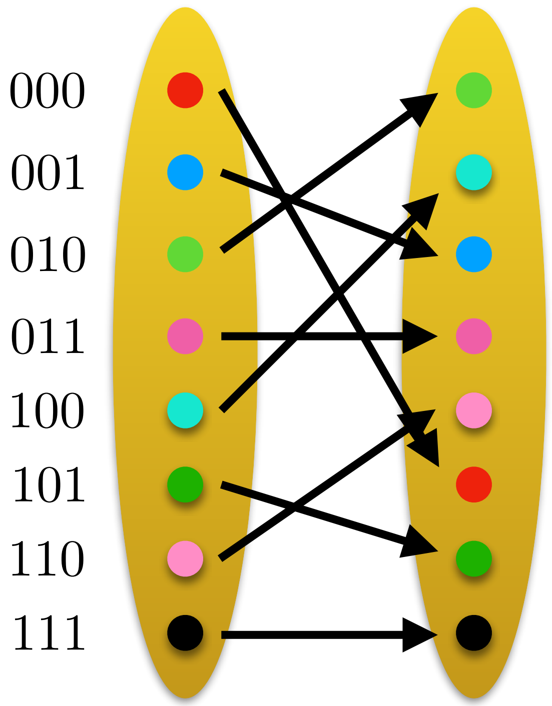
Idea



$$f : \{0,1\}^n \to \{0,1\}^n$$

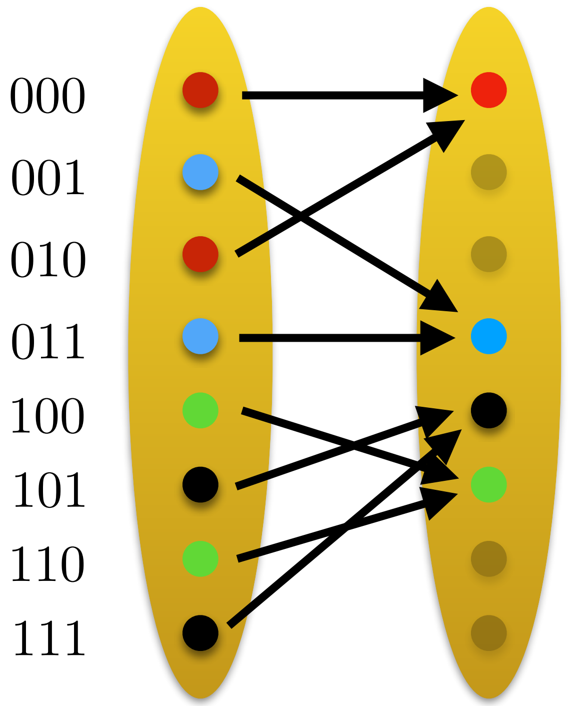
1-to-1

Idea



$$f : \{0,1\}^n \to \{0,1\}^n$$

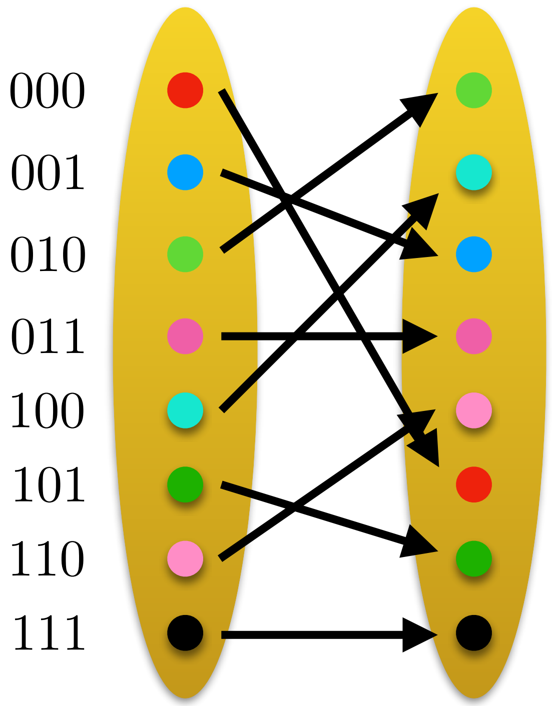
1-to-1



$$g : \{0,1\}^n \to \{0,1\}^n$$

2-to-1

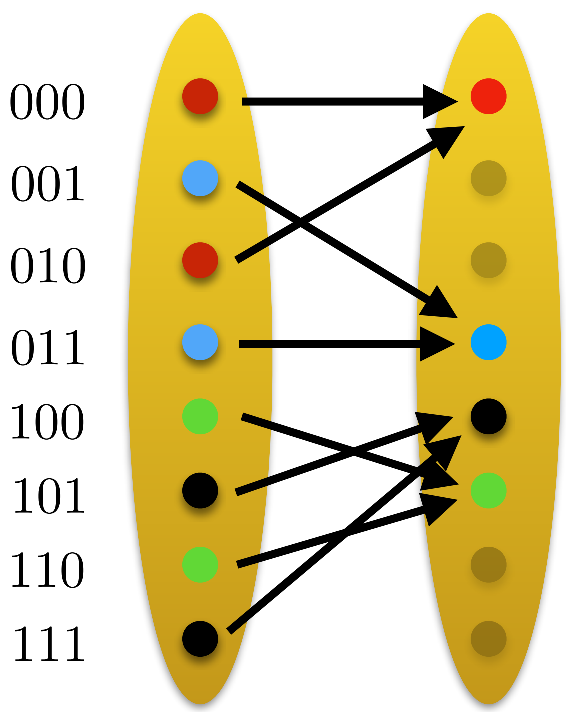
Idea



$$f : \{0,1\}^n \to \{0,1\}^n$$

1-to-1

$$x \leftarrow_U \{0,1\}^n$$

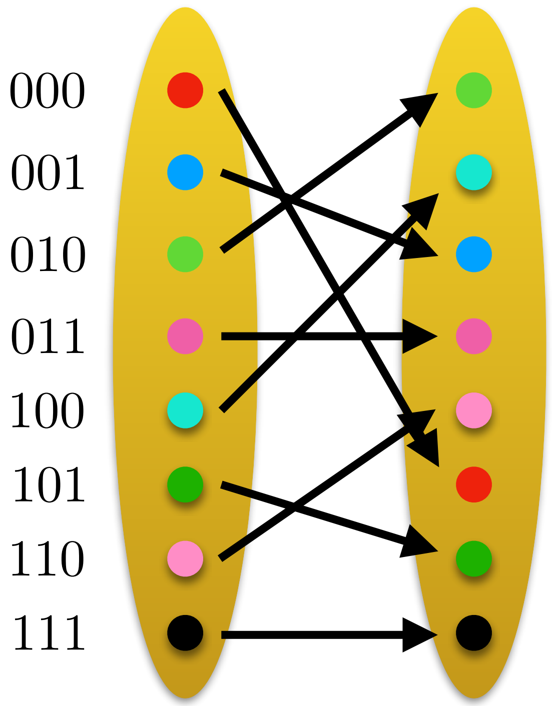


$$g : \{0,1\}^n \to \{0,1\}^n$$

2-to-1

$$x \leftarrow_U \{0,1\}^n$$

Idea

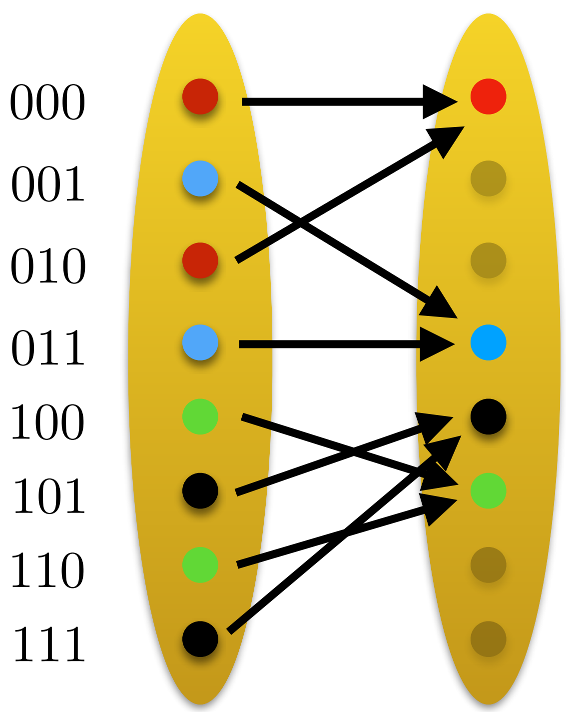


$$f : \{0,1\}^n \to \{0,1\}^n$$

1-to-1

$$x \leftarrow_U \{0,1\}^n$$

$$S(f(x)) = n$$



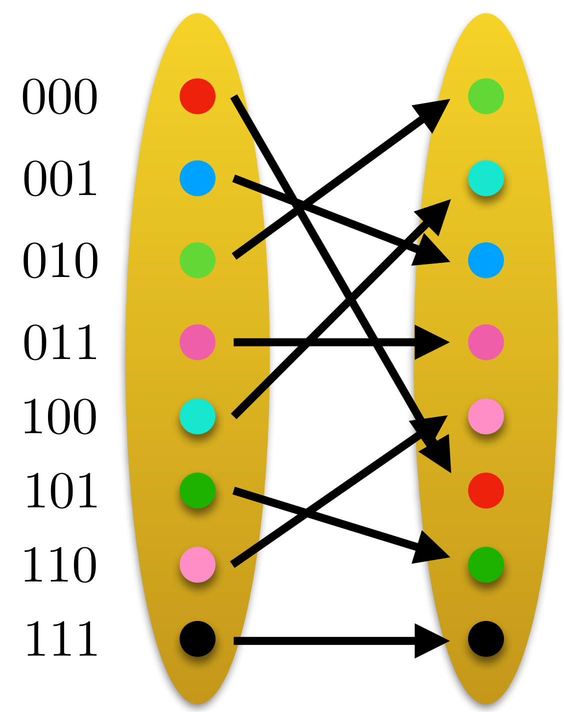
$$g : \{0,1\}^n \to \{0,1\}^n$$

2-to-1

$$x \leftarrow_U \{0,1\}^n$$

$$S(g(x)) = n - 1$$

Idea

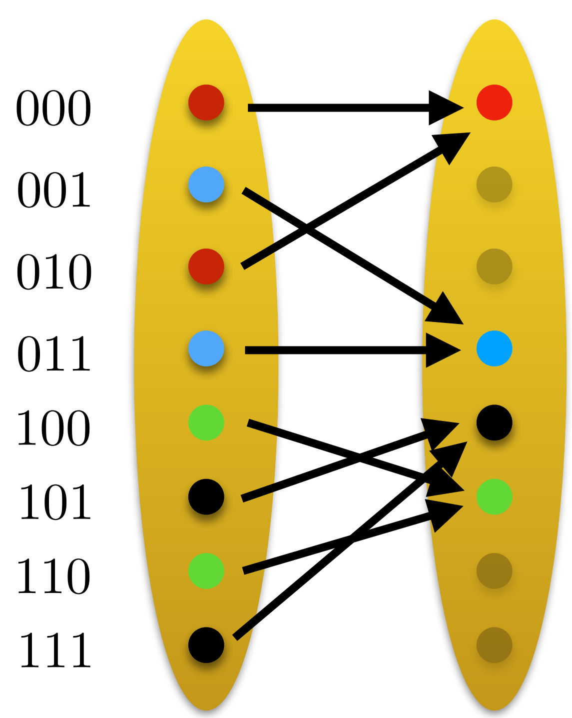


$$f : \{0,1\}^n \to \{0,1\}^n$$

1-to-1

$$\sum_{x \in \{0,1\}^n} |x\rangle |f(x)\rangle$$

$$S(\rho_f) = n$$



$$g : \{0,1\}^n \to \{0,1\}^n$$

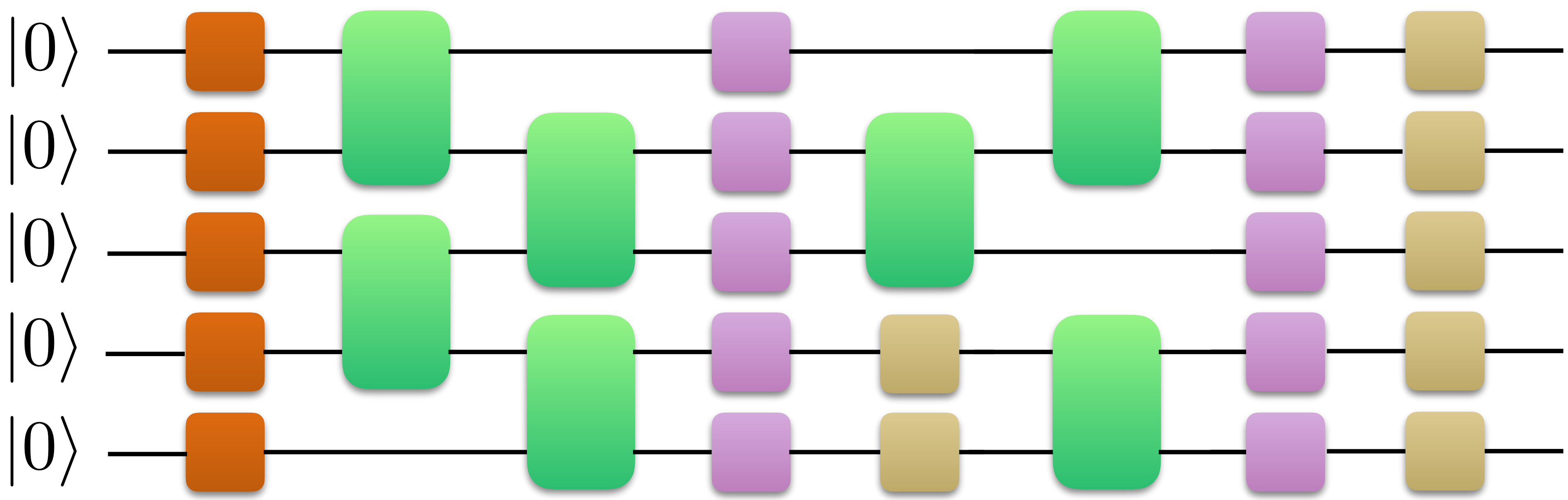
2-to-1

$$\sum_{x \in \{0,1\}^n} |x\rangle |g(x)\rangle$$

$$S(\rho_g) = n - 1$$

Idea

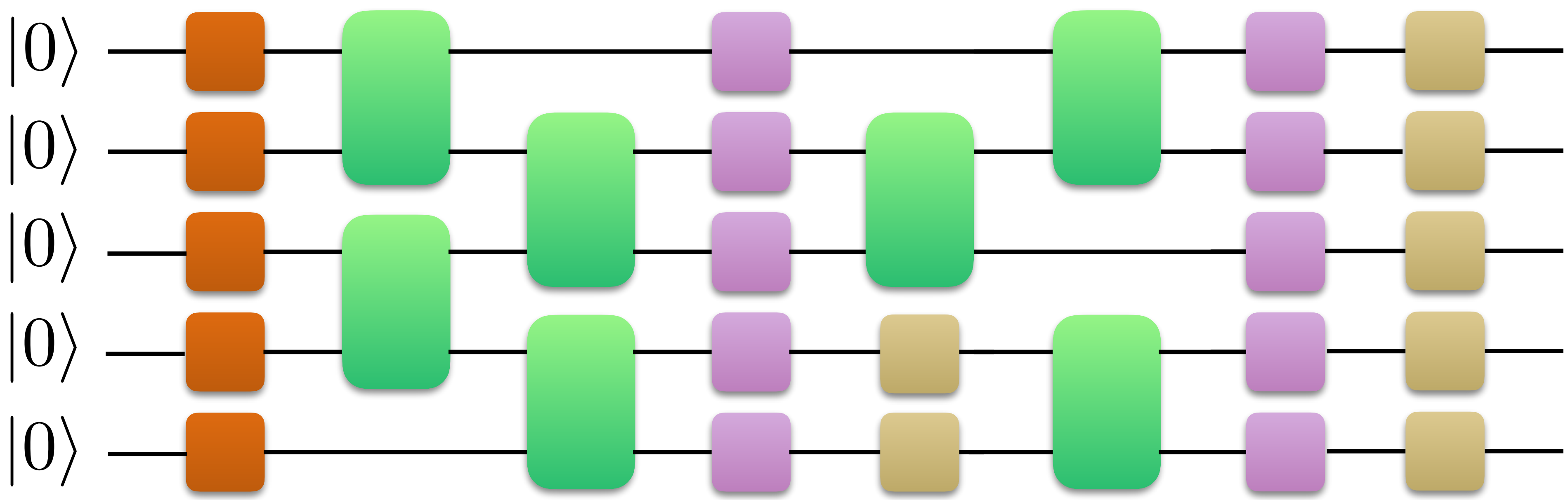
Given…



$$\sum_{x\in\{0,1\}^n} |x\rangle|h(x)\rangle$$

Idea

Given…

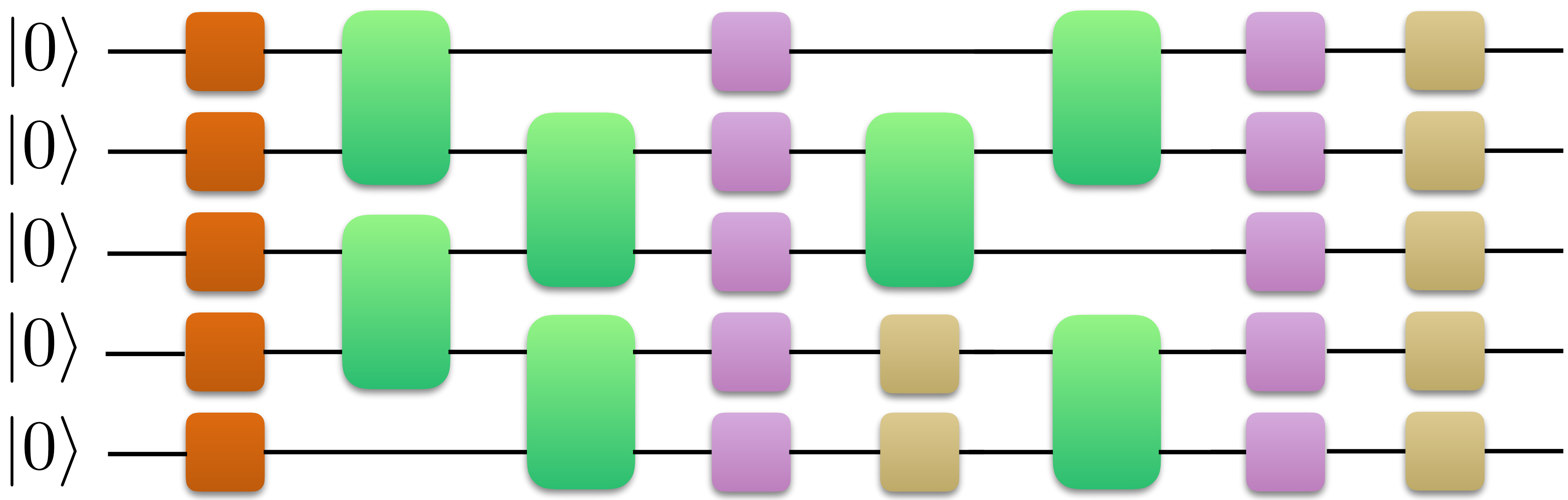


$$\sum_{x\in\{0,1\}^n} |x\rangle|h(x)\rangle$$

is h a 1-to-1 or a 2-to-1 function?

Idea

Given…



$$\sum_{x\in\{0,1\}^n} |x\rangle|h(x)\rangle$$

is h a 1-to-1 or a 2-to-1 function?

If we could estimate entropy, we could answer this question!

Idea

Can consider…

Idea

[Mahadev '18]

Can consider…

$$f(b,x) = Ax + b \cdot u + e \ (mod\ q)$$
$$g(b,x) = Ax + b \cdot (As + e') + e \ (mod\ q)$$

$$A \in \mathbb{Z}_q^{m \times n},\ x, s \in \mathbb{Z}_q^n,\ u, e, e' \in \mathbb{Z}_q^m$$

Idea

[Mahadev '18]

Can consider…

$$f(b,x) = Ax + b \cdot u + e \ (mod\ q)$$
$$g(b,x) = Ax + b \cdot (As + e') + e \ (mod\ q)$$

$$A \in \mathbb{Z}_q^{m \times n},\ x, s \in \mathbb{Z}_q^n,\ u, e, e' \in \mathbb{Z}_q^m$$

such that, determining which is the 2-to-1 function is as hard as LWE

Idea

[Mahadev ’18]

Can consider…

$$f(b,x) = Ax + b \cdot u + e \ (mod \ q)$$
$$g(b,x) = Ax + b \cdot (As + e') + e \ (mod \ q)$$

$$A \in \mathbb{Z}_q^{m \times n}, \ x, s \in \mathbb{Z}_q^n, \ u, e, e' \in \mathbb{Z}_q^m$$

such that, determining which is the 2-to-1 function is as hard as LWE

Functions involve only linear-algebraic operations

Idea

[Mahadev '18]

Can consider…

$$f(b,x) = Ax + b \cdot u + e \ (mod\ q)$$
$$g(b,x) = Ax + b \cdot (As + e') + e \ (mod\ q)$$

$$A \in \mathbb{Z}_q^{m \times n},\ x, s \in \mathbb{Z}_q^n,\ u, e, e' \in \mathbb{Z}_q^m$$

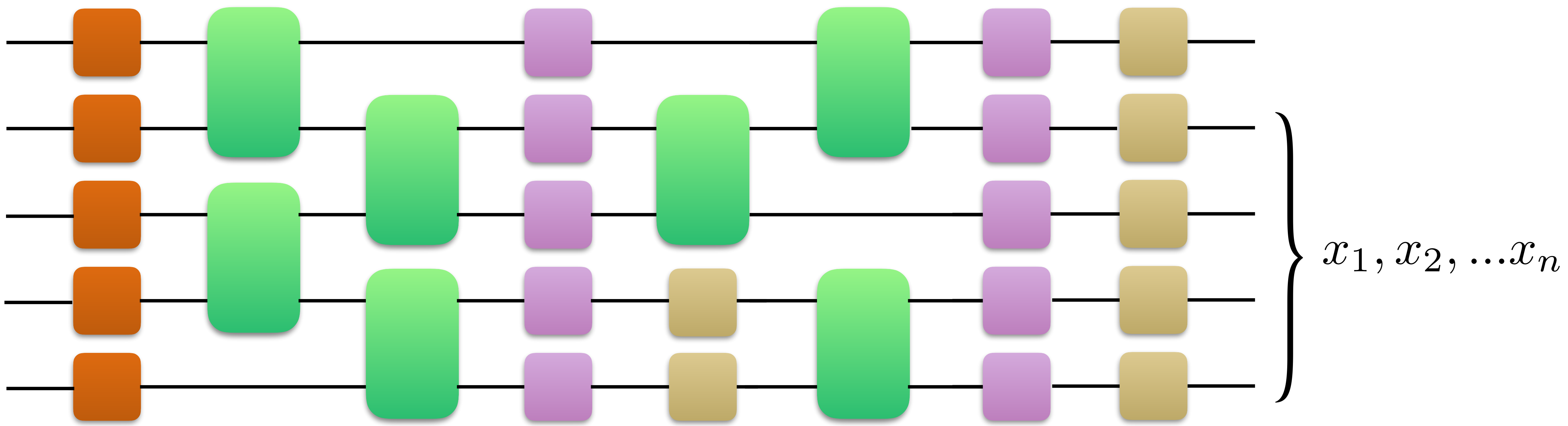
such that, determining which is the 2-to-1 function is as hard as LWE

Functions involve only linear-algebraic operations

Can be performed in logarithmic depth!

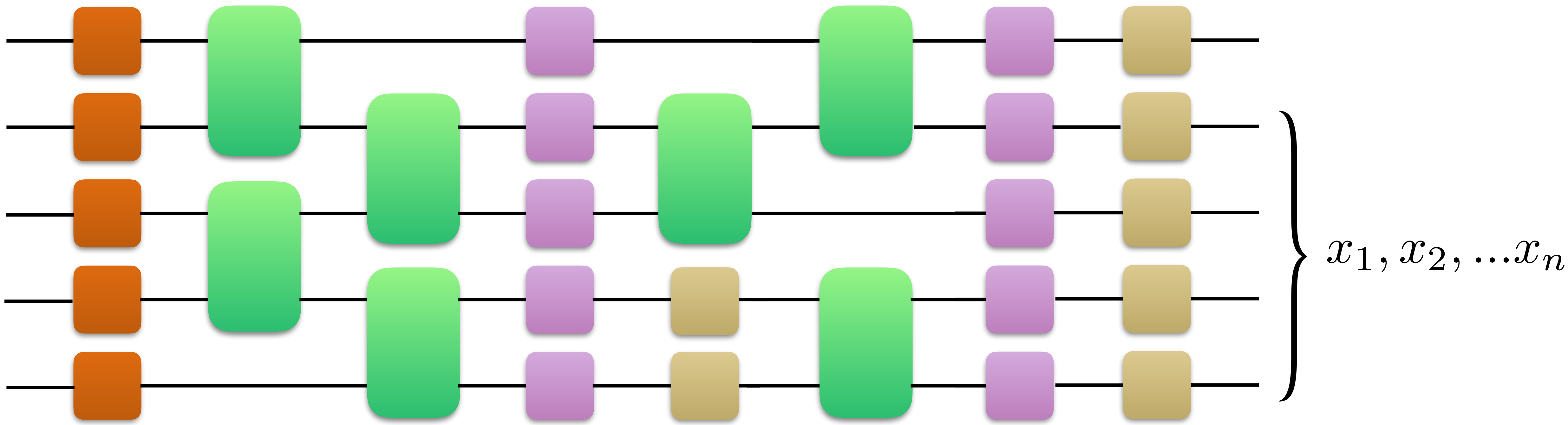
Constant depth case

The classical case



Constant depth case

The classical case

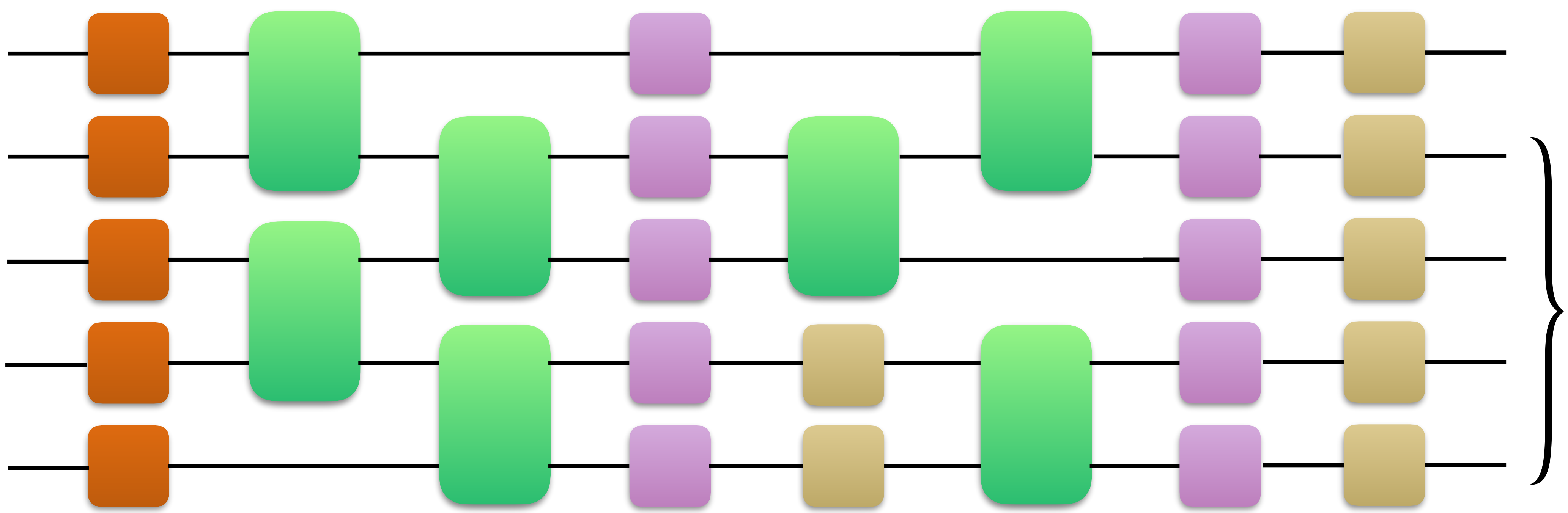


Use entropy chain rule

$$S(x_1, x_2, \ldots x_n) = \sum_i S(x_i | x_{i+1}, \ldots x_n)$$

Constant depth case

The classical case



$x_1, x_2, \ldots x_n$

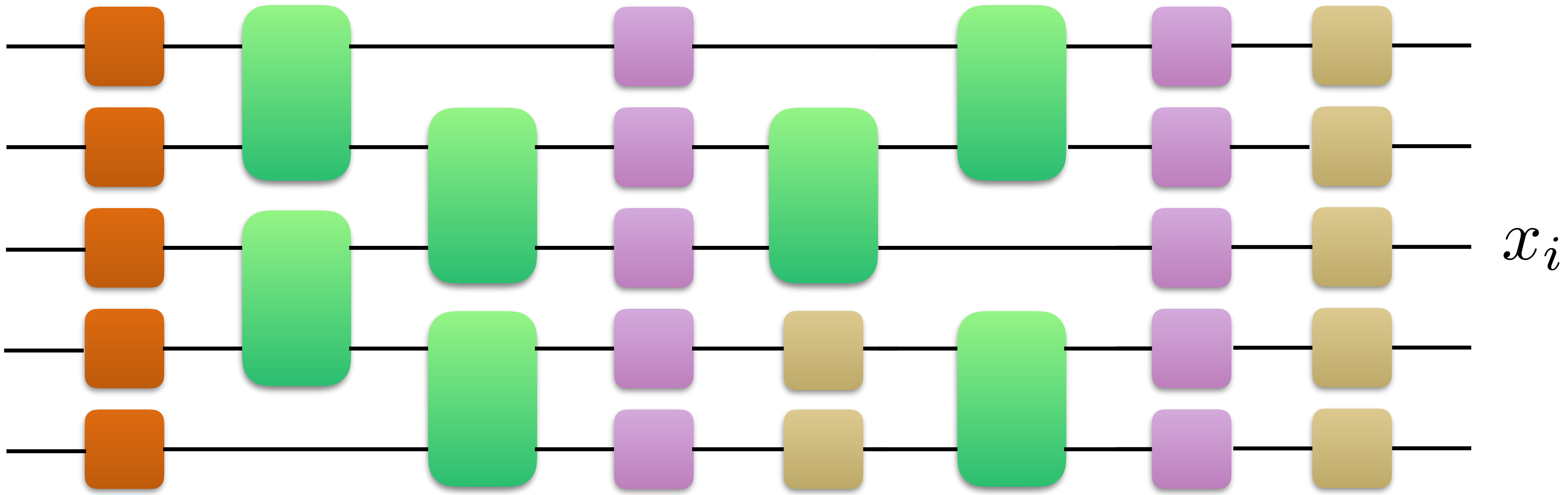
Use entropy chain rule

$$S(x_1, x_2, \ldots x_n) = \sum_i S(x_i | x_{i+1}, \ldots x_n)$$

$$S(x_i | x_j) = S(x_i) \; if \; x_i \; indep \; x_j$$

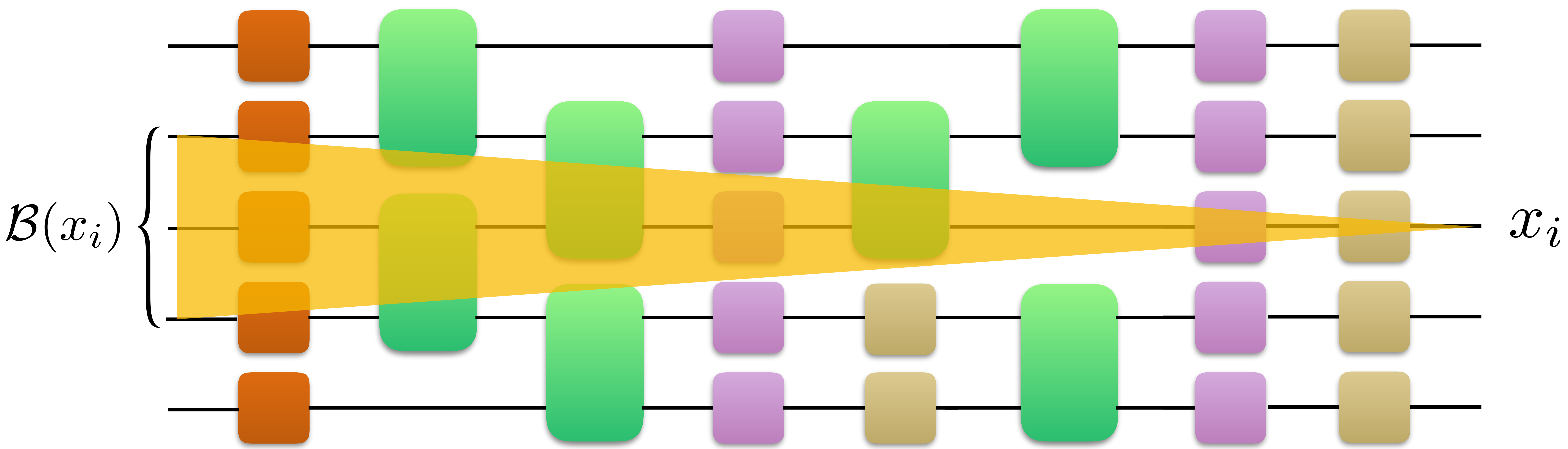
Constant depth case

The classical case



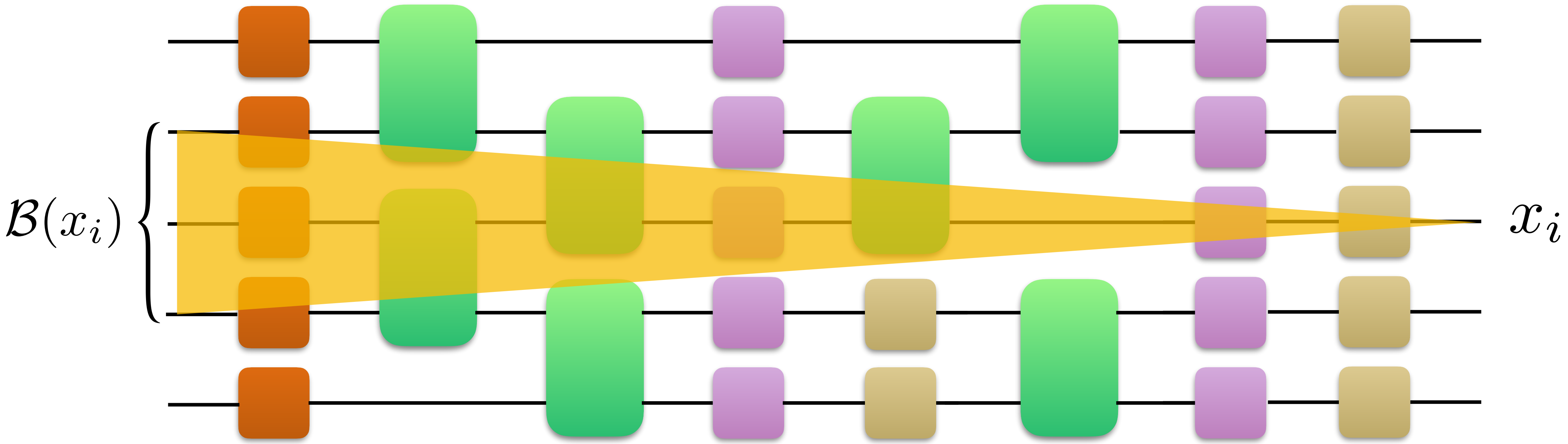
Constant depth case

The classical case



Constant depth case

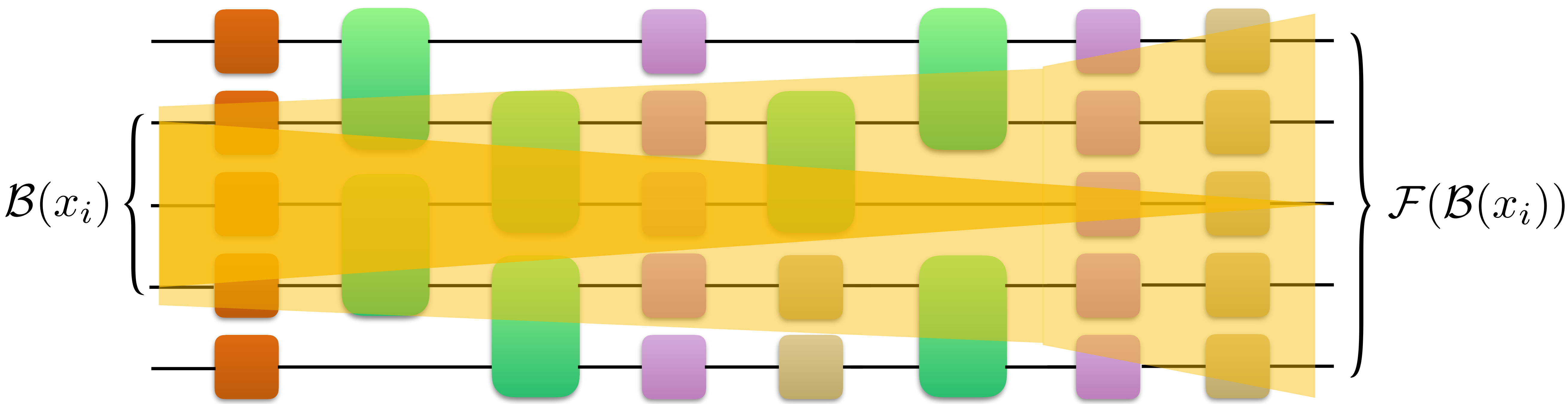
The classical case



$$|\mathcal{B}(x_i)| \leq f_{in}^{d}$$

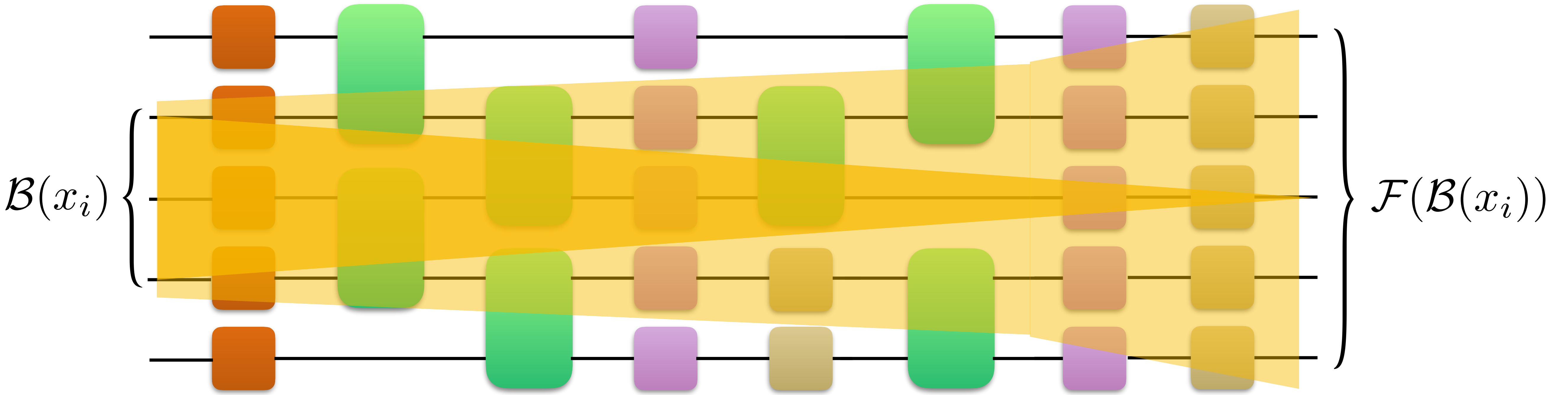
Constant depth case

The classical case



Constant depth case

The classical case

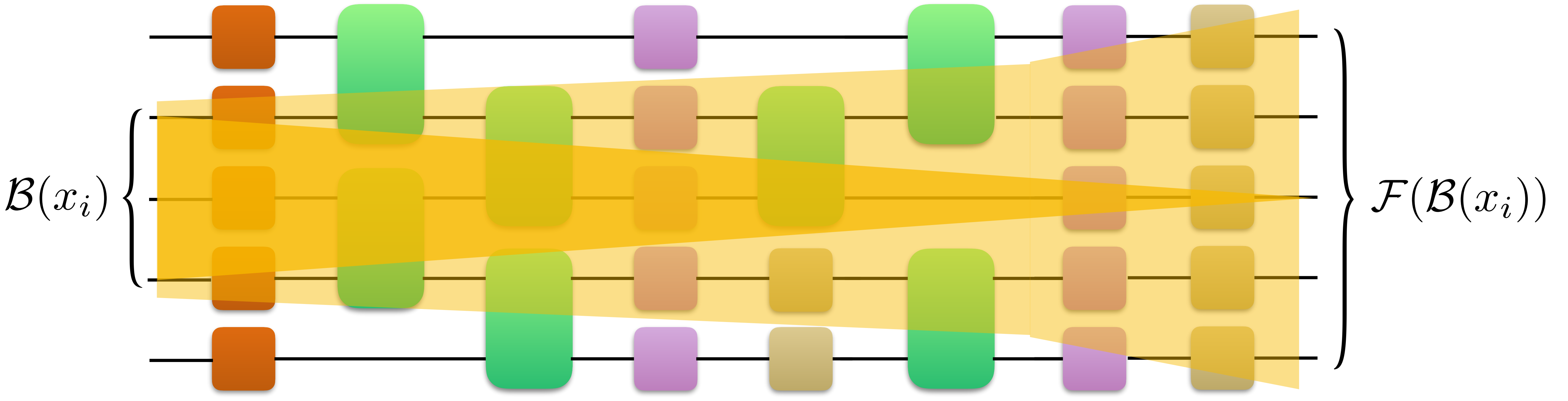


$$|\mathcal{F}(\mathcal{B}(x_i))| \leq (f_{in} f_{out})^d$$

$$|\mathcal{F}(\mathcal{B}(x_i))| = O(1)$$

Constant depth case

The classical case



$$|\mathcal{F}(\mathcal{B}(x_i))| \leq (f_{in} f_{out})^d$$

$$|\mathcal{F}(\mathcal{B}(x_i))| = O(1)$$

$$x_j \notin \mathcal{F}(\mathcal{B}(x_i)) \implies x_i \; indep \; x_j$$

Constant depth case

The classical case

$$S(x_1, x_2, ...x_n) = \sum_i S(x_i|x_{i+1}, ...x_n)$$

Constant depth case

The classical case

$$S(x_1, x_2, ...x_n) = \sum_i S(x_i | x_{i+1}, ...x_n)$$

$$S(x_1, x_2, ...x_n) = \sum_i S(x_i | \mathcal{F}(\mathcal{B}(x_i)) \setminus \{x_i\})$$

Constant depth case

The classical case

$$S(x_1, x_2, ...x_n) = \sum_i S(x_i | x_{i+1}, ...x_n)$$

$$S(x_1, x_2, ...x_n) = \sum_i S(x_i | \mathcal{F}(\mathcal{B}(x_i)) \setminus \{x_i\})$$

$$S(x_i | \mathcal{F}(\mathcal{B}(x_i)) \setminus \{x_i\}) = S(\mathcal{F}(\mathcal{B}(x_i))) - S(\mathcal{F}(\mathcal{B}(x_i)) \setminus \{x_i\})$$

Constant depth case

The classical case

$$S(x_1, x_2, ...x_n) = \sum_i S(x_i | x_{i+1}, ...x_n)$$

$$S(x_1, x_2, ...x_n) = \sum_i S(x_i | \mathcal{F}(\mathcal{B}(x_i)) \setminus \{x_i\})$$

$$S(x_i | \mathcal{F}(\mathcal{B}(x_i)) \setminus \{x_i\}) = S(\mathcal{F}(\mathcal{B}(x_i))) - S(\mathcal{F}(\mathcal{B}(x_i)) \setminus \{x_i\})$$

Completely determined by $\mathcal{B}(\mathcal{F}(\mathcal{B}(x_i)))$

Constant depth case

The classical case

$$S(x_1, x_2, \ldots x_n) = \sum_i S(x_i | x_{i+1}, \ldots x_n)$$

$$S(x_1, x_2, \ldots x_n) = \sum_i S(x_i | \mathcal{F}(\mathcal{B}(x_i)) \setminus \{x_i\})$$

$$S(x_i | \mathcal{F}(\mathcal{B}(x_i)) \setminus \{x_i\}) = S(\mathcal{F}(\mathcal{B}(x_i))) - S(\mathcal{F}(\mathcal{B}(x_i)) \setminus \{x_i\})$$

Completely determined by $\mathcal{B}(\mathcal{F}(\mathcal{B}(x_i)))$

Can be computed in O(1) time

Constant depth case

The classical case

$$S(x_1, x_2, ...x_n) = \sum_i S(x_i | x_{i+1}, ...x_n)$$

$$S(x_1, x_2, ...x_n) = \sum_i S(x_i | \mathcal{F}(\mathcal{B}(x_i)) \setminus \{x_i\})$$

$$S(x_i | \mathcal{F}(\mathcal{B}(x_i)) \setminus \{x_i\}) = S(\mathcal{F}(\mathcal{B}(x_i))) - S(\mathcal{F}(\mathcal{B}(x_i)) \setminus \{x_i\})$$

Completely determined by $\mathcal{B}(\mathcal{F}(\mathcal{B}(x_i)))$

Can be computed in O(1) time

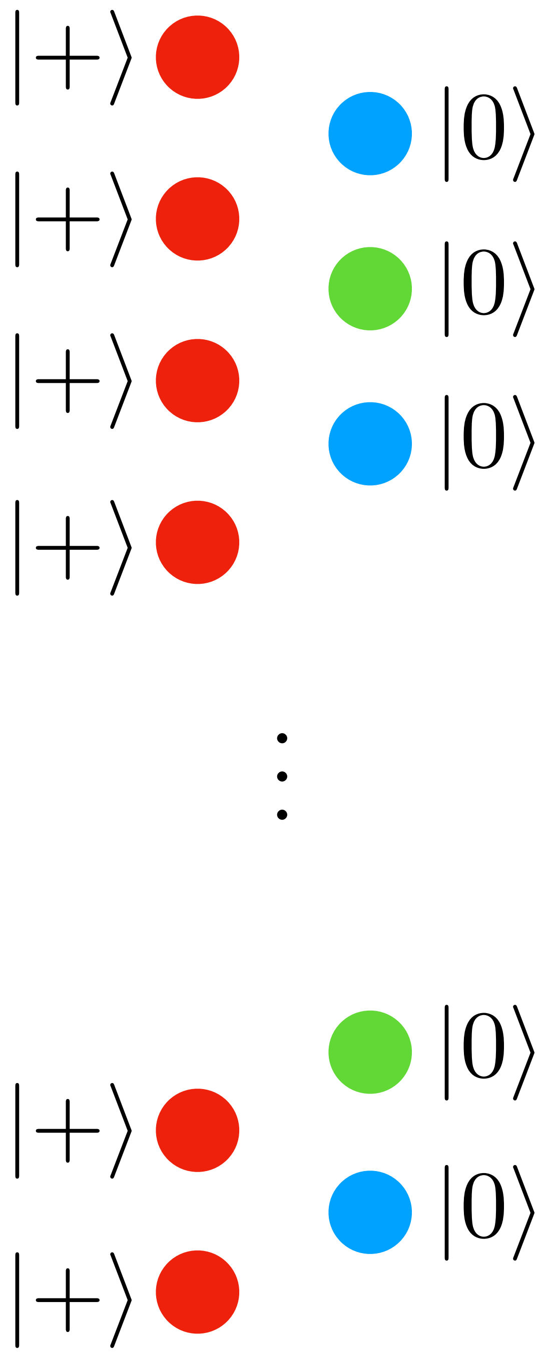
Whole sum can be computed in O(n) time!

Constant depth case

In the quantum case this argument breaks down!

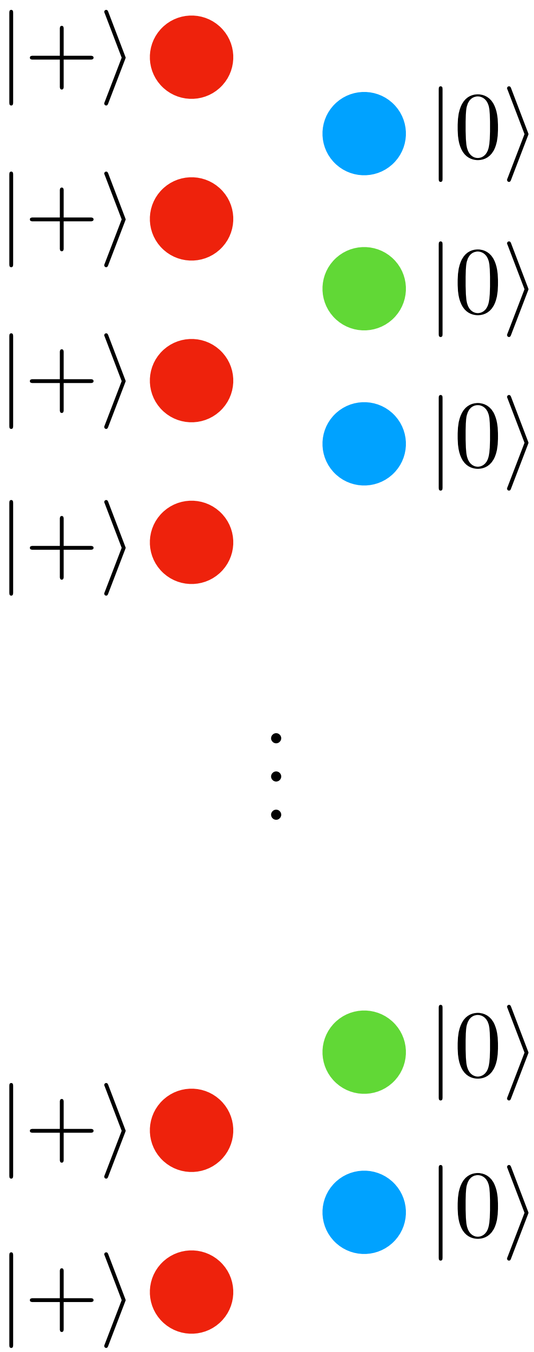
Constant depth case

In the quantum case this argument breaks down!



Constant depth case

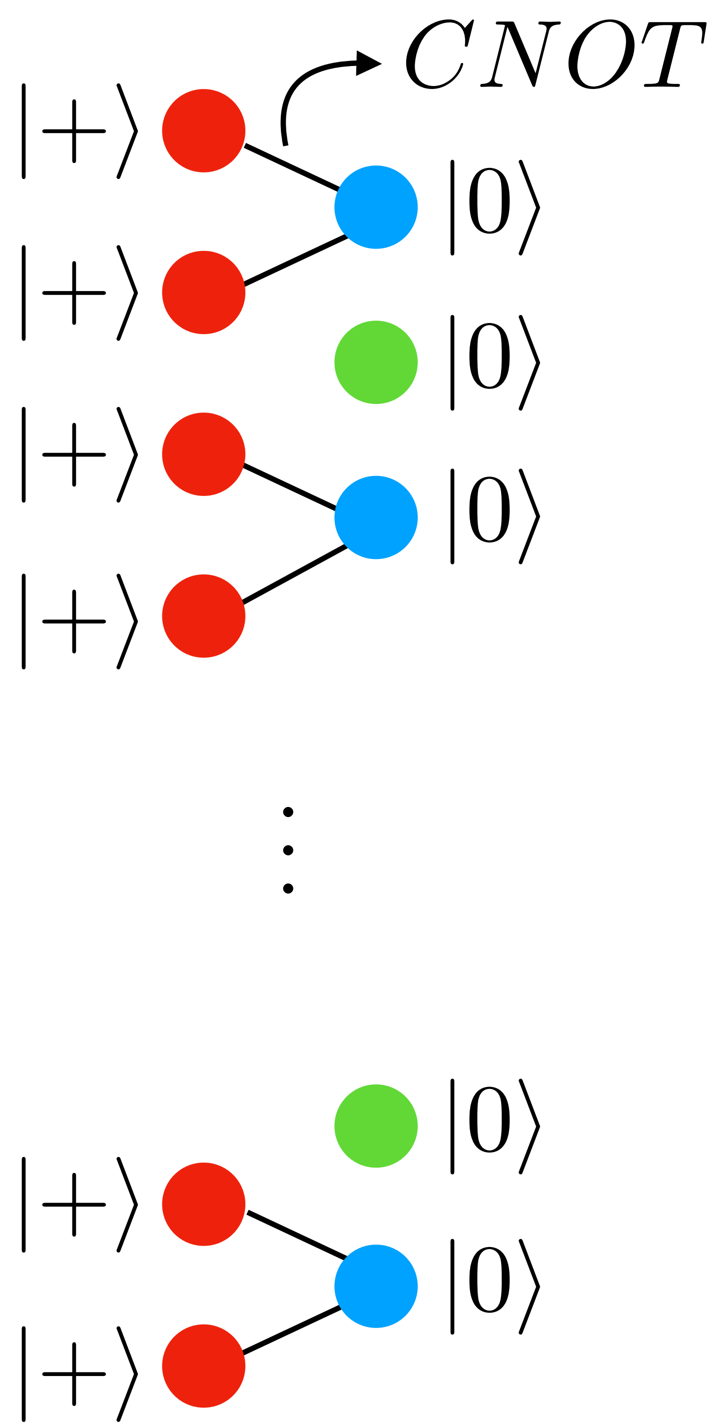
In the quantum case this argument breaks down!



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

Constant depth case

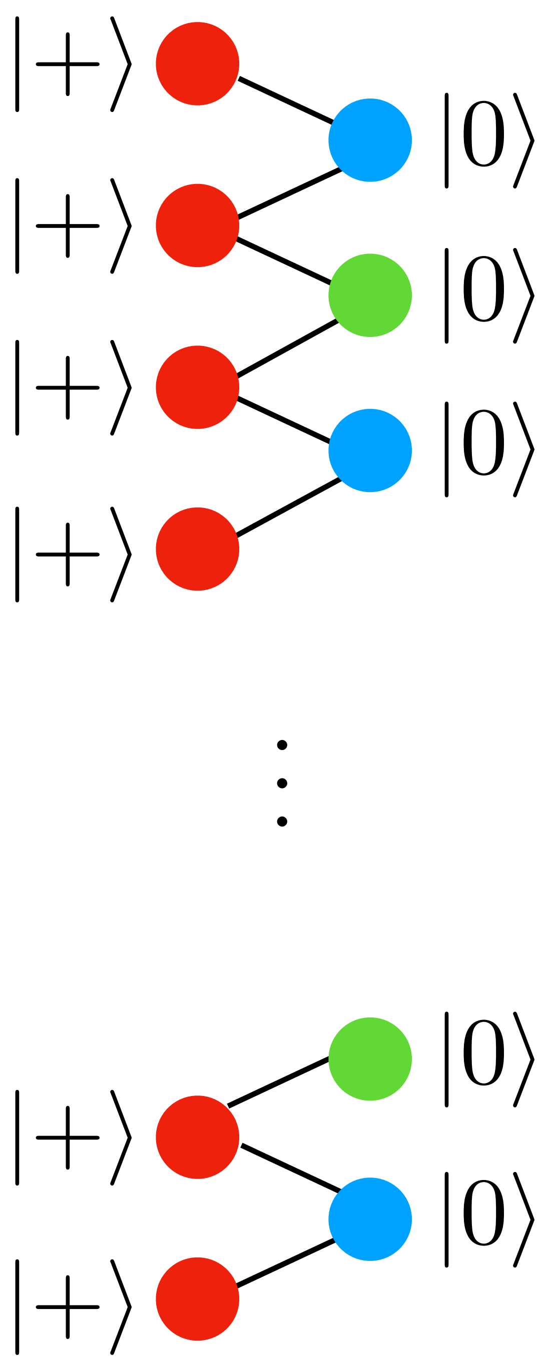
In the quantum case this argument breaks down!



$$CNOT = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$$

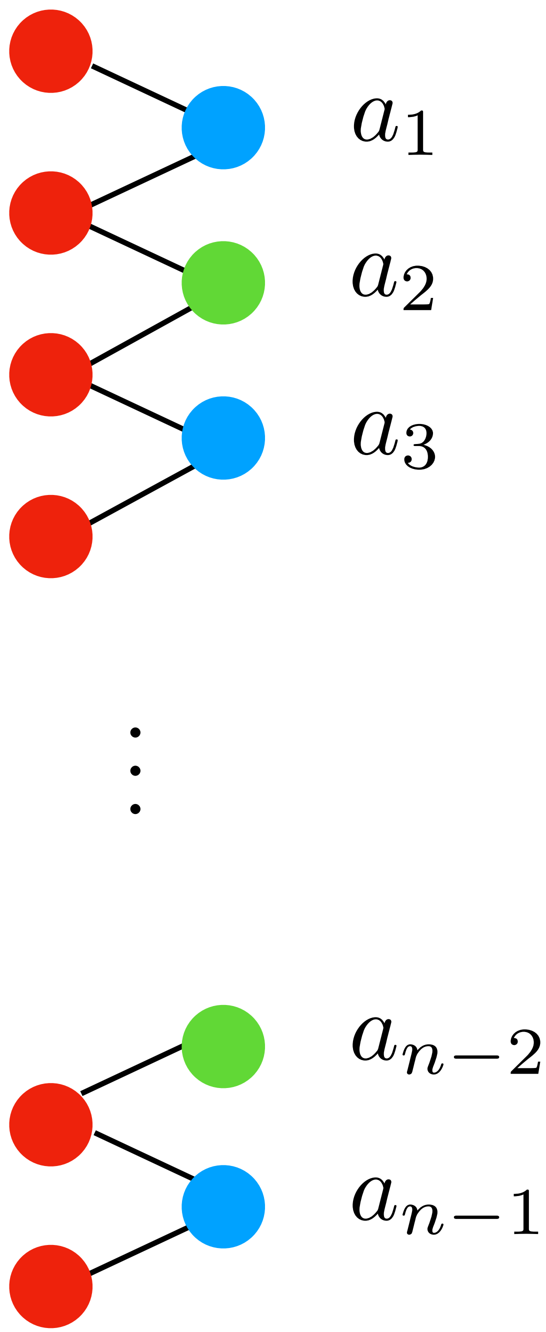
Constant depth case

In the quantum case this argument breaks down!



Constant depth case

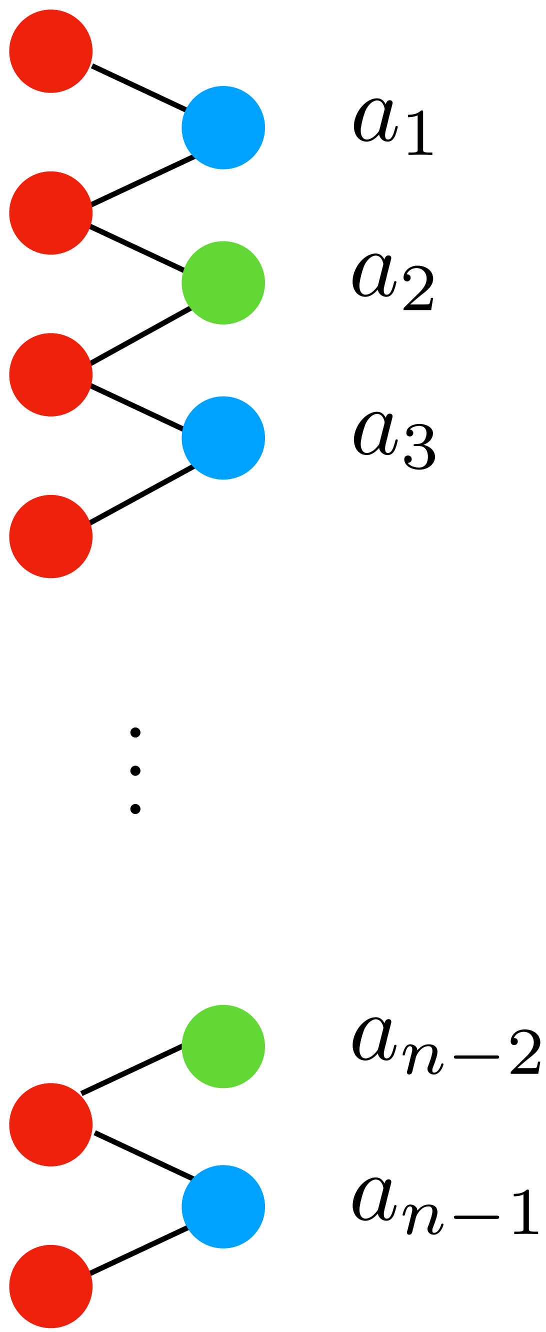
In the quantum case this argument breaks down!



Measure non-red qubits

Constant depth case

In the quantum case this argument breaks down!



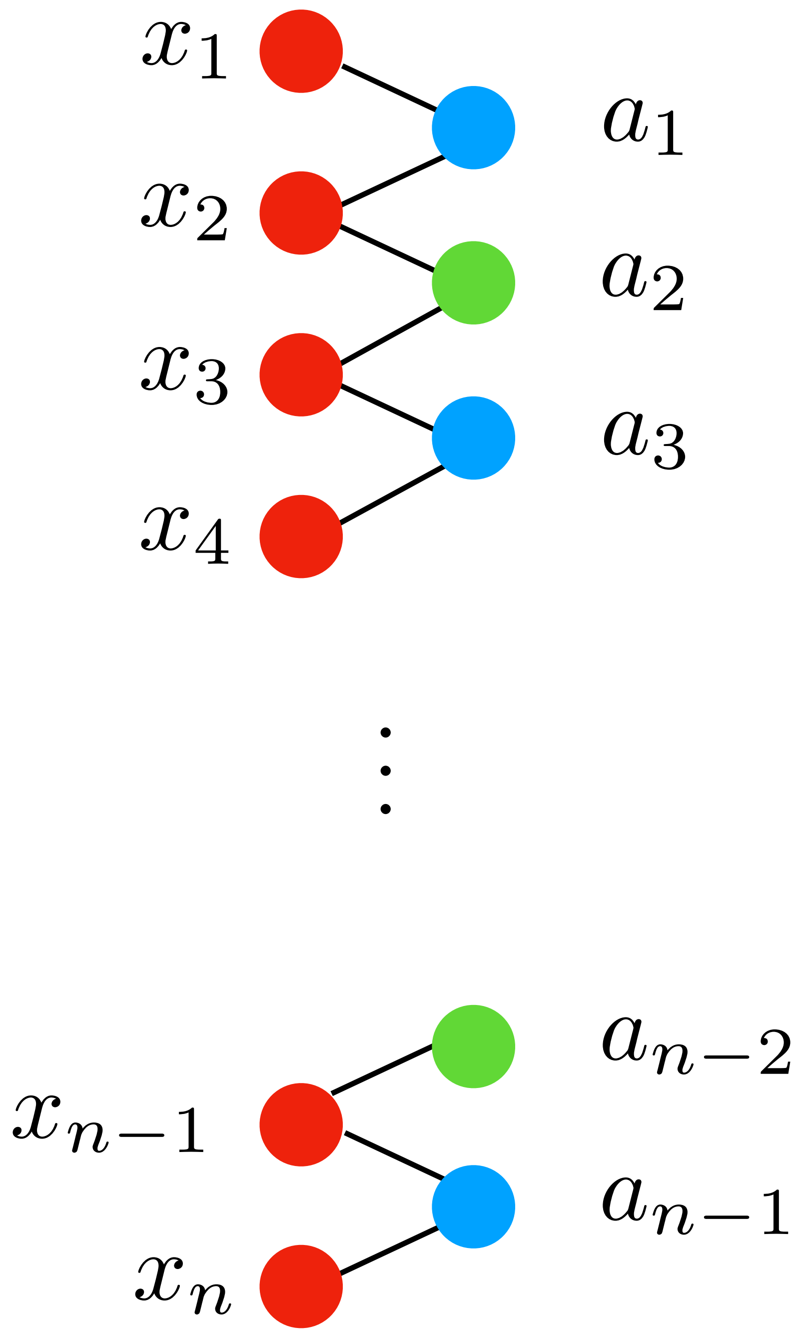
Measure non-red qubits

$$\frac{|z\rangle + |\bar{z}\rangle}{\sqrt{2}}$$

$$z_i \oplus z_{i+1} = a_i$$
$$\bar{z}_i \oplus \bar{z}_{i+1} = a_i$$

Constant depth case

In the quantum case this argument breaks down!



Measure non-red qubits

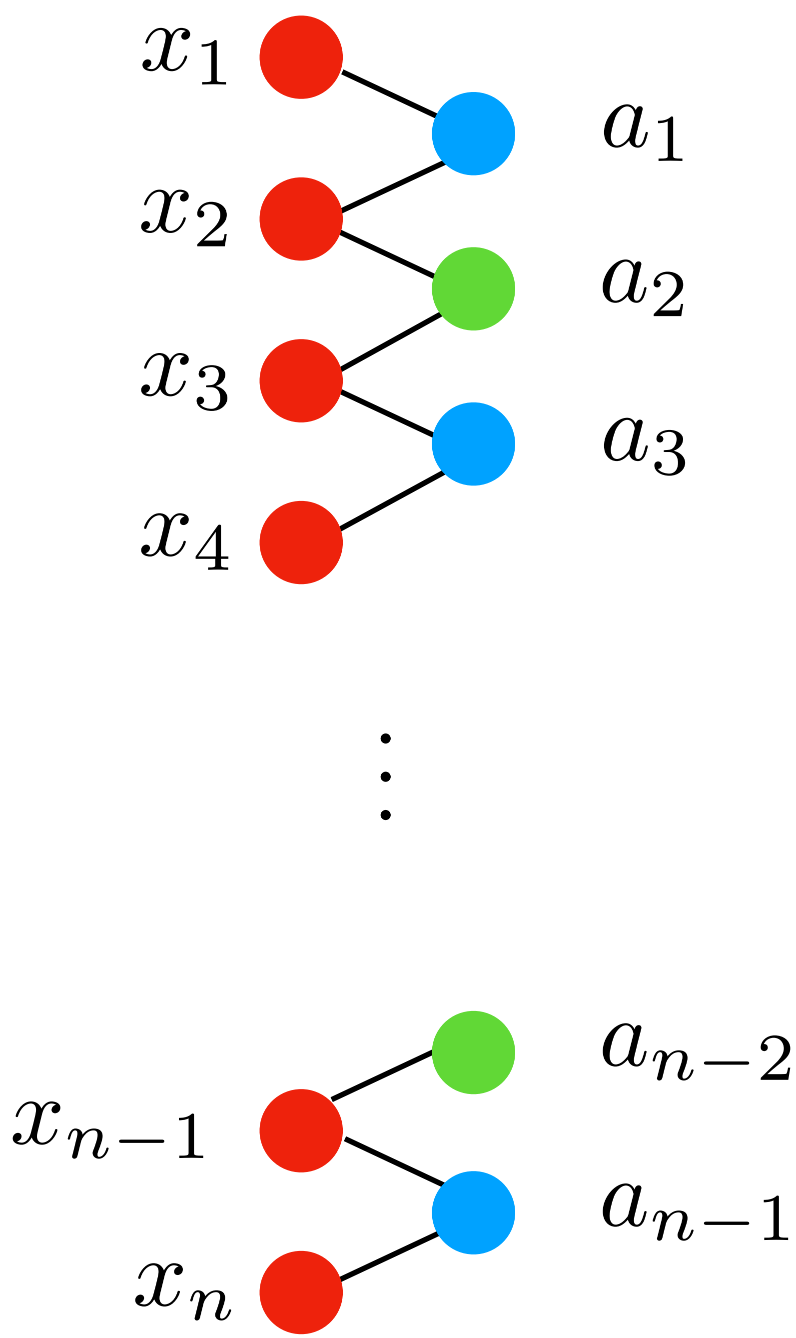
$$\frac{|z\rangle + |\bar{z}\rangle}{\sqrt{2}}$$

$$z_i \oplus z_{i+1} = a_i$$
$$\bar{z}_i \oplus \bar{z}_{i+1} = a_i$$

Measure red qubits

Constant depth case

In the quantum case this argument breaks down!



Measure non-red qubits

$$\frac{|z\rangle + |\bar{z}\rangle}{\sqrt{2}}$$

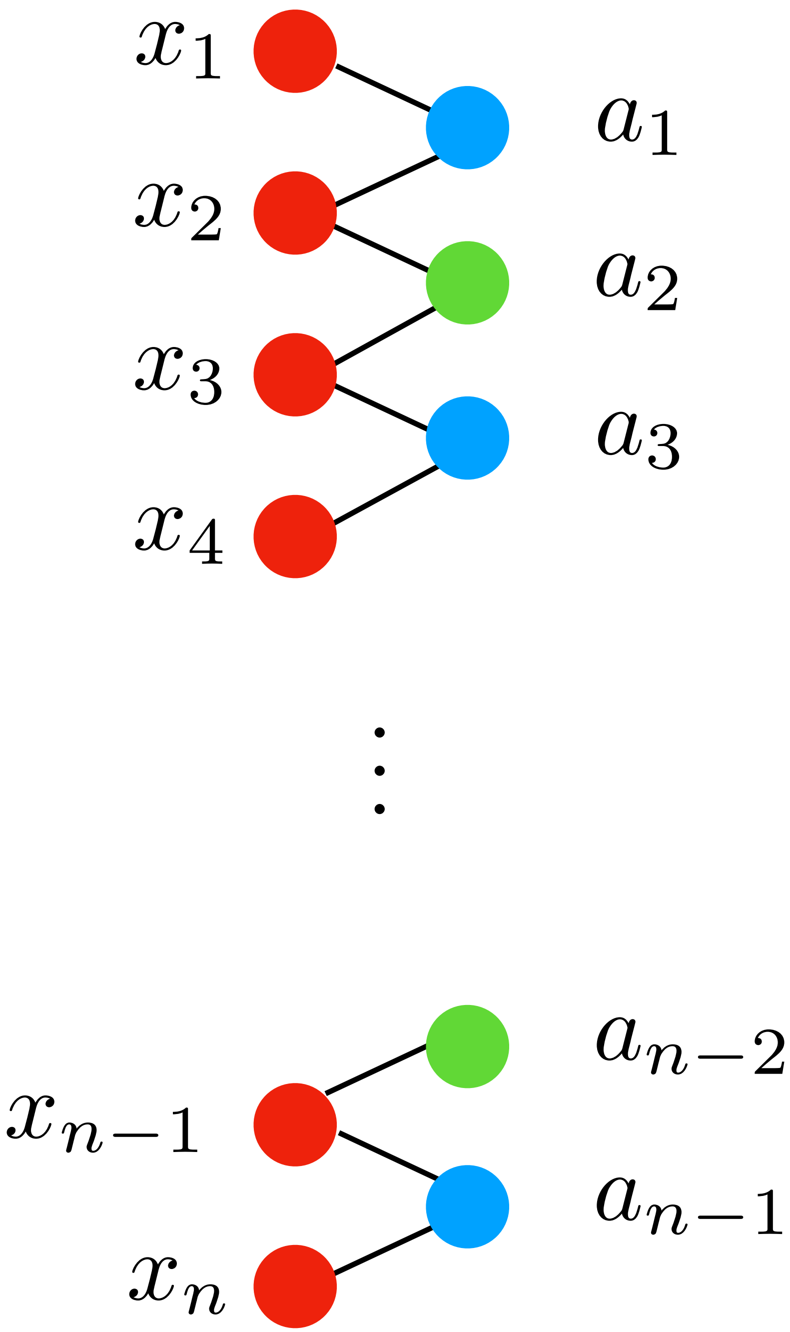
$$z_i \oplus z_{i+1} = a_i$$
$$\bar{z}_i \oplus \bar{z}_{i+1} = a_i$$

Measure red qubits

$$p(x_1 | a_1, ..., a_{n-1}) = 1/2$$

Constant depth case

In the quantum case this argument breaks down!



Measure non-red qubits

$$\frac{|z\rangle + |\bar{z}\rangle}{\sqrt{2}}$$

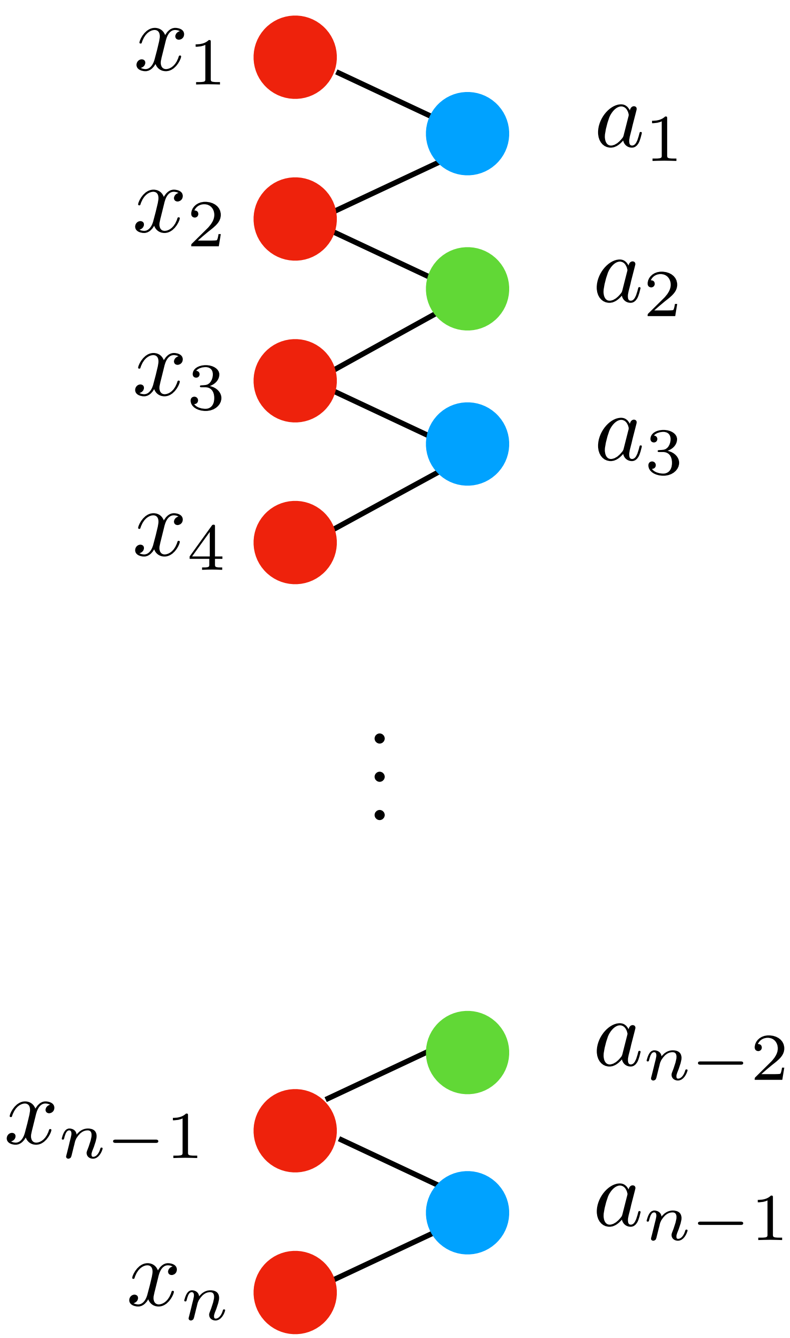
$$z_i \oplus z_{i+1} = a_i$$
$$\bar{z}_i \oplus \bar{z}_{i+1} = a_i$$

Measure red qubits

$$p(x_1|a_1, ..., a_{n-1}) = 1/2$$
$$p(x_1|a_1, ..., a_{n-1}, {\color{red}x_n}) \in \{0, 1\}$$

Constant depth case

In the quantum case this argument breaks down!



Measure non-red qubits

$$\frac{|z\rangle + |\bar{z}\rangle}{\sqrt{2}}$$

$$z_i \oplus z_{i+1} = a_i$$
$$\bar{z}_i \oplus \bar{z}_{i+1} = a_i$$

Measure red qubits

$$S(x_1|a_1, ..., a_{n-1}) = 1$$
$$S(x_1|a_1, ..., a_{n-1}, \textcolor{red}{x_n}) = 0$$

Constant depth case

But why is the quantum case hard?

Constant depth case

But why is the quantum case hard?

$$\frac{|z\rangle + |\bar{z}\rangle}{\sqrt{2}}$$

Constant depth case

But why is the quantum case hard?

$$\frac{|z\rangle + |\bar{z}\rangle}{\sqrt{2}}$$

Perform Z rotations on qubits i and j $\quad R_Z(\theta)_i \quad R_Z(\phi)_j$

Constant depth case

But why is the quantum case hard?

$$\frac{|z\rangle + |\bar{z}\rangle}{\sqrt{2}}$$

Perform Z rotations on qubits i and j $\quad R_Z(\theta)_i \quad R_Z(\phi)_j$

$$\frac{1}{\sqrt{2}}(|z\rangle + e^{\theta+\phi}|\bar{z}\rangle)$$

Up to a global phase

Constant depth case

Leverage this fact to encode

$$f(b, x) = Ax + b \cdot u + e \ (mod \ q)$$

$$g(b, x) = Ax + b \cdot (As + e') + e \ (mod \ q)$$

in phases of noisy GHZ states

Constant depth case

Leverage this fact to encode

$$f(b, x) = Ax + b \cdot u + e \ (mod \ q)$$
$$g(b, x) = Ax + b \cdot (As + e') + e \ (mod \ q)$$

in phases of noisy GHZ states

$$\frac{1}{\sqrt{2}}\left(|z\rangle + e^{\frac{2\pi i}{q}(\langle a_i, x\rangle + b \cdot u_i + e_i)}|\bar{z}\rangle\right)$$

Constant depth case

Leverage this fact to encode

$$f(b, x) = Ax + b \cdot u + e \ (mod\ q)$$
$$g(b, x) = Ax + b \cdot (As + e') + e \ (mod\ q)$$

in phases of noisy GHZ states

$$\frac{1}{\sqrt{2}}\left(|z\rangle + e^{\frac{2\pi i}{q}(\langle a_i, x\rangle + b \cdot u_i + e_i)}|\bar{z}\rangle\right)$$

$$\frac{1}{\sqrt{2}}\left(|z\rangle + e^{\frac{2\pi i}{q}(\langle a_i, x\rangle + b \cdot (As + e')_i + e_i)}|\bar{z}\rangle\right)$$

Constant depth case

Leverage this fact to encode

$$f(b,x) = Ax + b\cdot u + e\ (mod\ q)$$
$$g(b,x) = Ax + b\cdot (As + e') + e\ (mod\ q)$$

in phases of noisy GHZ states

$$\sum_x |x\rangle|\widetilde{f(x)}\rangle$$

$$\sum_x |x\rangle|\widetilde{g(x)}\rangle$$

Conclusion

Classical and quantum entropy estimation are hard for log-depth circuits!

For constant depth, classical is easy, quantum is hard

Quantum requires arbitrary rotation gates.
Possible with fixed gate set?

Connections to cryptography

Potential connections to quantum gravity (AdS/CFT)

Conclusion

Classical and quantum entropy estimation are hard for log-depth circuits!

For constant depth, classical is easy, quantum is hard

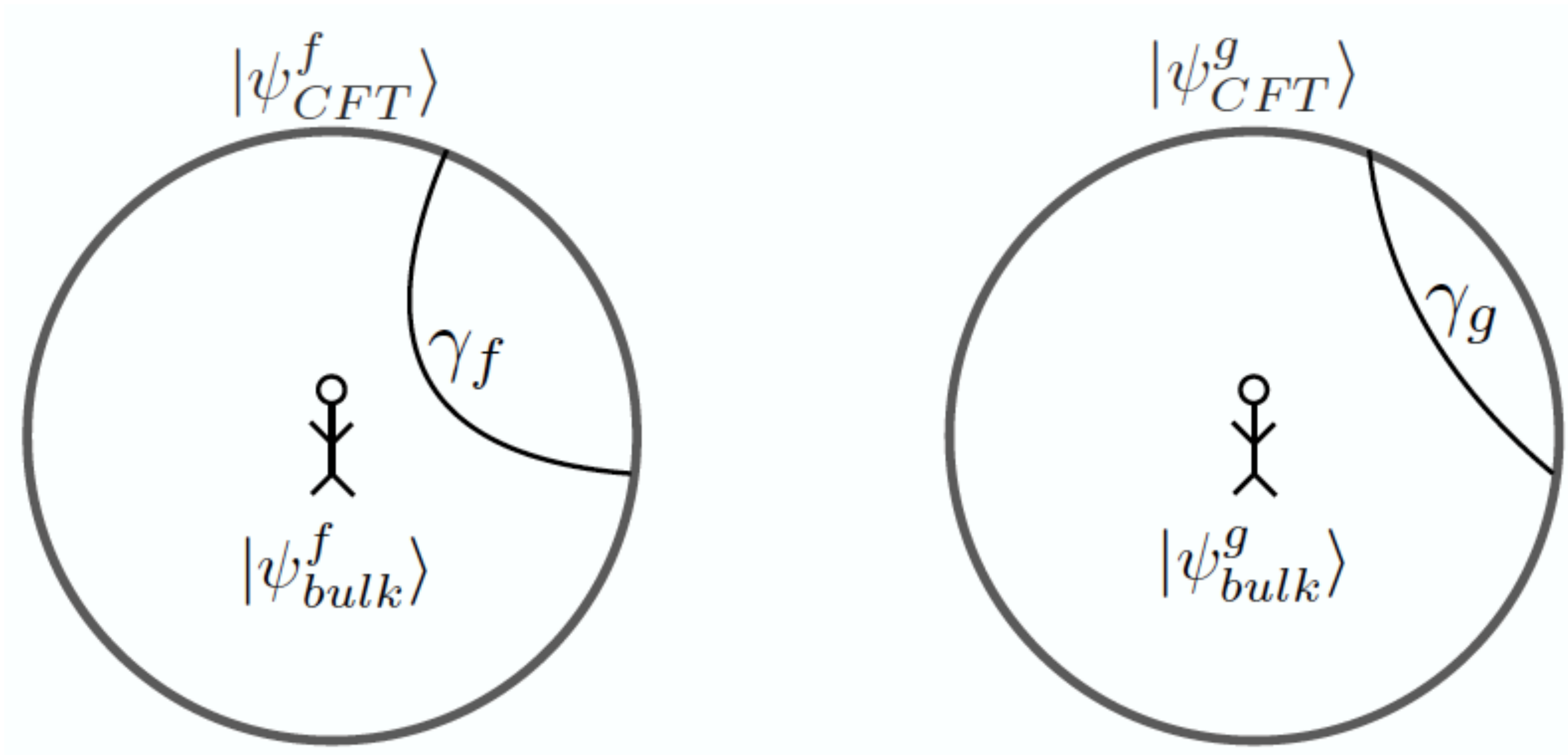
Quantum requires arbitrary rotation gates.
Possible with fixed gate set?

Connections to cryptography

Potential connections to quantum gravity (AdS/CFT)

Thanks!

AdS/CFT


$|\psi^f_{CFT}\rangle$
γ_f
$|\psi^f_{bulk}\rangle$
$|\psi^g_{CFT}\rangle$
γ_g
$|\psi^g_{bulk}\rangle$