Yale University

Quantum Gates

PART B

CPSC 4470/5470

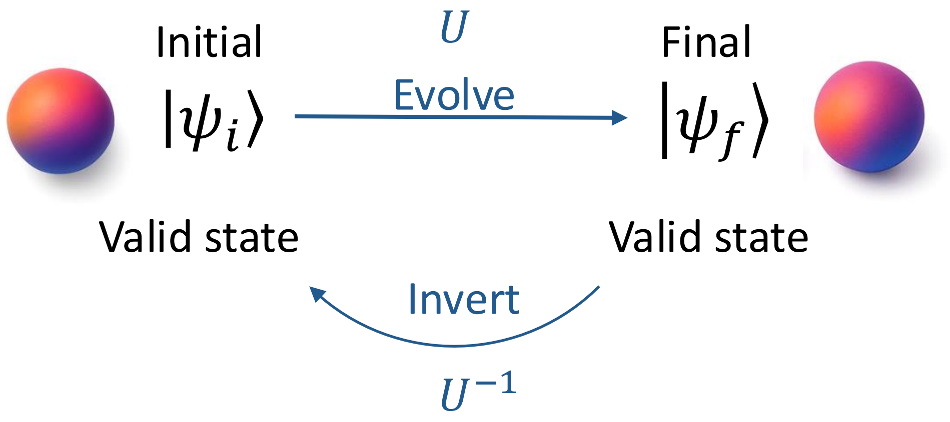
Introduction to Quantum Computing

Instructor: Prof. **Yongshan Ding**

Computer Science, Applied Physics, Yale Quantum Institute

Principle #3 – Transformation

Unitary Transformation: The evolution of a quantum state can be described as a *norm-preserving linear transformation* (a.k.a. unitary matrix).



- **Norm-preserving**:

$$\||\psi_i\rangle\|^2 = \left\||\psi_f\rangle\right\|^2 = 1$$

- **Linear transformation**:

Linear operator: $|\psi_f\rangle = U|\psi_i\rangle$, for some matrix U.

"Preserves inner product."

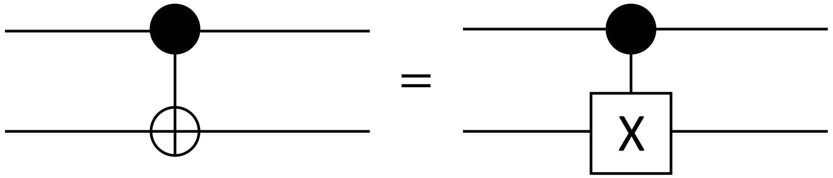
Unitary: $U^\dagger U = I$

- The process is **reversible** and **deterministic**: $U^{-1} = U^\dagger$
- In physics: "Coherent process"

Two-Qubit Gates

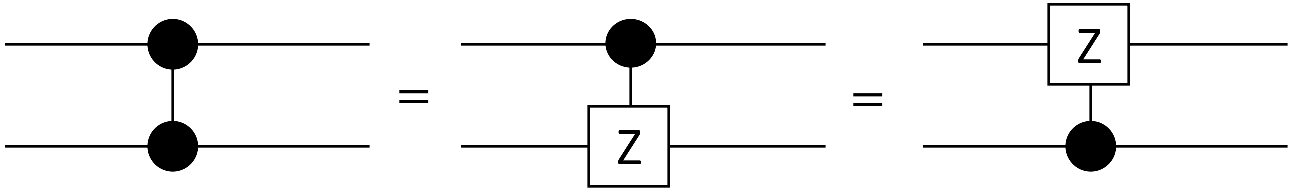
Examples:

CNOT gate:



$$CX = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

CZ gate:

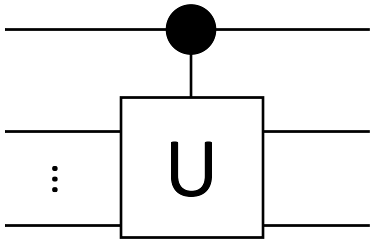


$$CZ = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}.$$

Multi-Qubit Gates

Beyond two-qubit gates? Given any n-qubit unitary matrix U (of size 2^n-by- 2^n)

We can construct: **controlled-U Gate** ("quantum if-else") as a $(n+1)$ qubit gate:



New unitary of size 2^{n+1}-by- 2^{n+1}:

$$\text{C-U} = \begin{bmatrix} I_{2^n} & 0 \\ 0 & U \end{bmatrix}.$$

- I_{2^n}: 2^n-by- 2^n Identity matrix
- 0: all-zero matrix

$$\text{C-U} = \begin{bmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & u_{0,0} & \cdots & u_{0,2^n-1} \\ & & & \vdots & \ddots & \vdots \\ & & & u_{2^n-1,0} & \cdots & u_{2^n-1,2^n-1} \end{bmatrix}$$

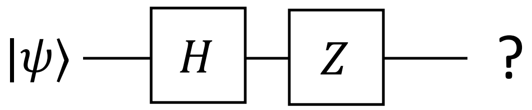
Different from $I \otimes U$:

- C-U $= |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U$
- $I \otimes U = |0\rangle\langle 0| \otimes U + |1\rangle\langle 1| \otimes U$

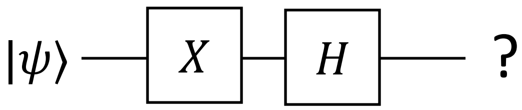
$$I \otimes U = \begin{bmatrix} u_{0,0} & \cdots & u_{0,2^n-1} & & & \\ \vdots & \ddots & \vdots & & & \\ u_{2^n-1,0} & \cdots & u_{2^n-1,2^n-1} & & & \\ & & & u_{0,0} & \cdots & u_{0,2^n-1} \\ & & & \vdots & \ddots & \vdots \\ & & & u_{2^n-1,0} & \cdots & u_{2^n-1,2^n-1} \end{bmatrix}$$

Unitary Transformations

Circuit #1:



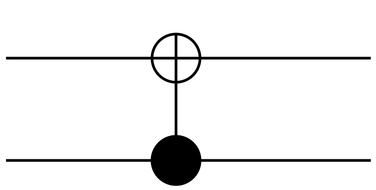
Circuit #2:



They look different, but implement the same unitary:

$$HXH = Z, HZH = X$$

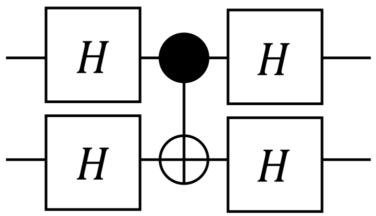
Circuit #3:



?

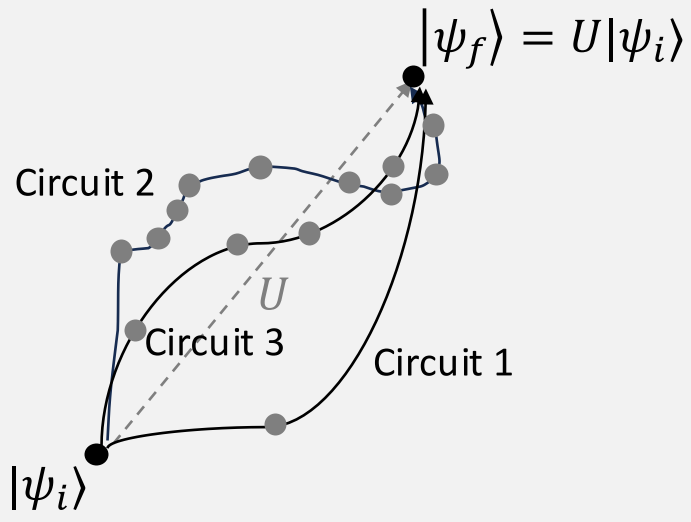
=

Circuit #4:



Flipping who's control and who's target.

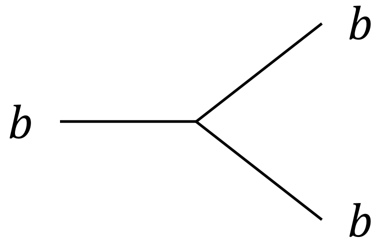
Transforming from $|\psi_i\rangle$ to $|\psi_f\rangle$ in the Hilbert Space



Compiler optimization:
Finding shorter/easier circuits to implement U.

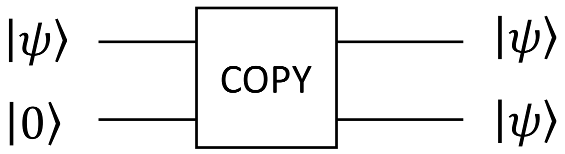
Copying Qubits?

Classical information can be copied:



Classical fanout gate that "duplicates" input $b \in \{0,1\}$

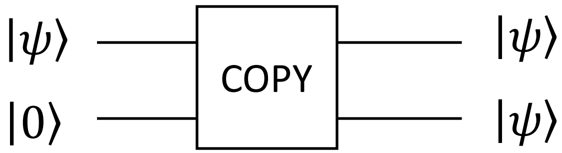
Can we do the same for quantum information?



No-cloning theorem: There's no unitary matrix that can transform arbitrary (unknown) quantum state $|\psi\rangle \otimes |0\rangle$ to $|\psi\rangle \otimes |\psi\rangle$.

Cloning is not possible

No-cloning theorem: There's no unitary matrix that can transform arbitrary (unknown) quantum state $|\psi\rangle \otimes |0\rangle$ to $|\psi\rangle \otimes |\psi\rangle$.



For any α, β: $(\alpha|0\rangle + \beta|1\rangle) \otimes |0\rangle \longrightarrow (\alpha|0\rangle + \beta|1\rangle) \otimes (\alpha|0\rangle + \beta|1\rangle)$

Not linear!

AFSOC, there is a universal cloner U that works for:

$|0\rangle \otimes |0\rangle \xrightarrow{U} |0\rangle \otimes |0\rangle$ and $|+\rangle \otimes |0\rangle \xrightarrow{U} |+\rangle \otimes |+\rangle$

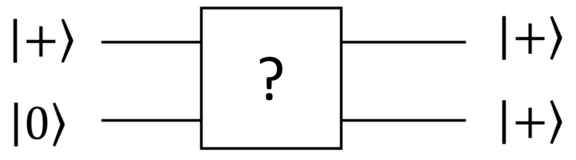
Since U is unitary, it must preserve inner product.

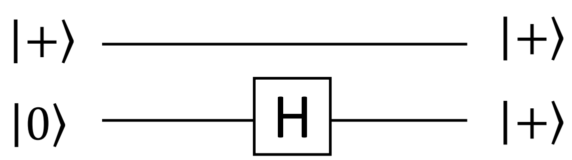
But $(\langle 0| \otimes \langle 0|)(|+\rangle \otimes |0\rangle) \neq (\langle 0| \otimes \langle 0|)(|+\rangle \otimes |+\rangle)$. Contradiction!

Remarks:
- No unitary works universally for all $|\psi\rangle$
- But we can find unitary that works for some $|\psi\rangle$.

Restricted Cloning

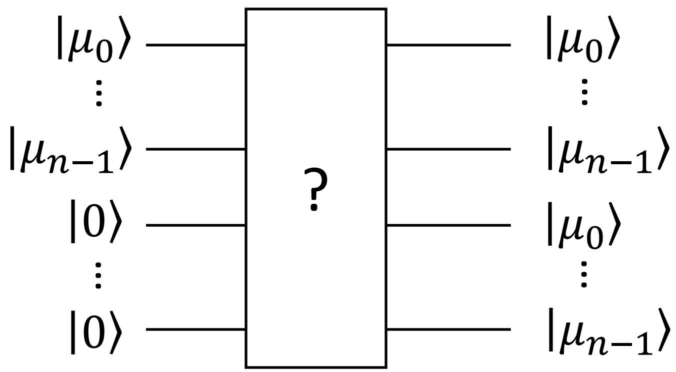
Example #1 (copying $|+\rangle$ state):



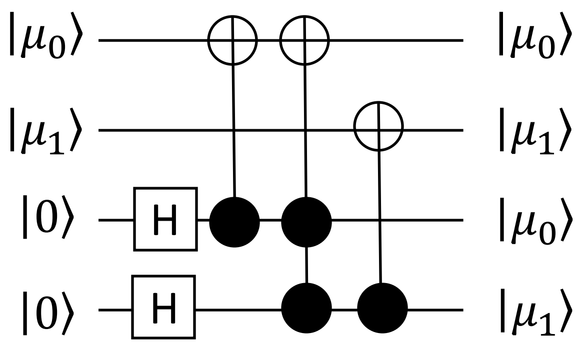


Any state with a known preparation circuit.

Example #2 (copying Fourier states):



E.g., for $n = 2$



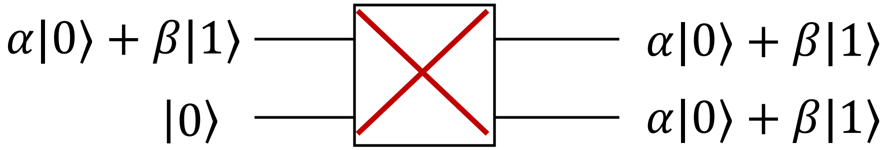
Works for any $x \in \{0,1\}^2$

Any *subset* of states with the same known preparation circuit.

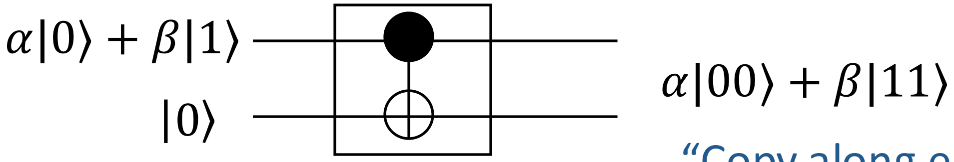
$|\mu_k\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i x/2^{n-k}}|1\rangle\right)$, for some $x \in \{0,1\}^n$

Quantum Fanout Gate

Separate copies not possible:

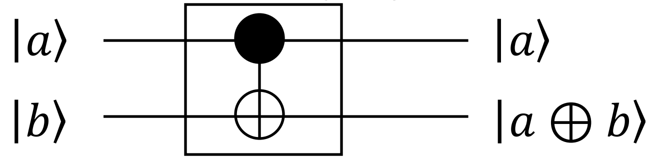


Entangled copies are possible:

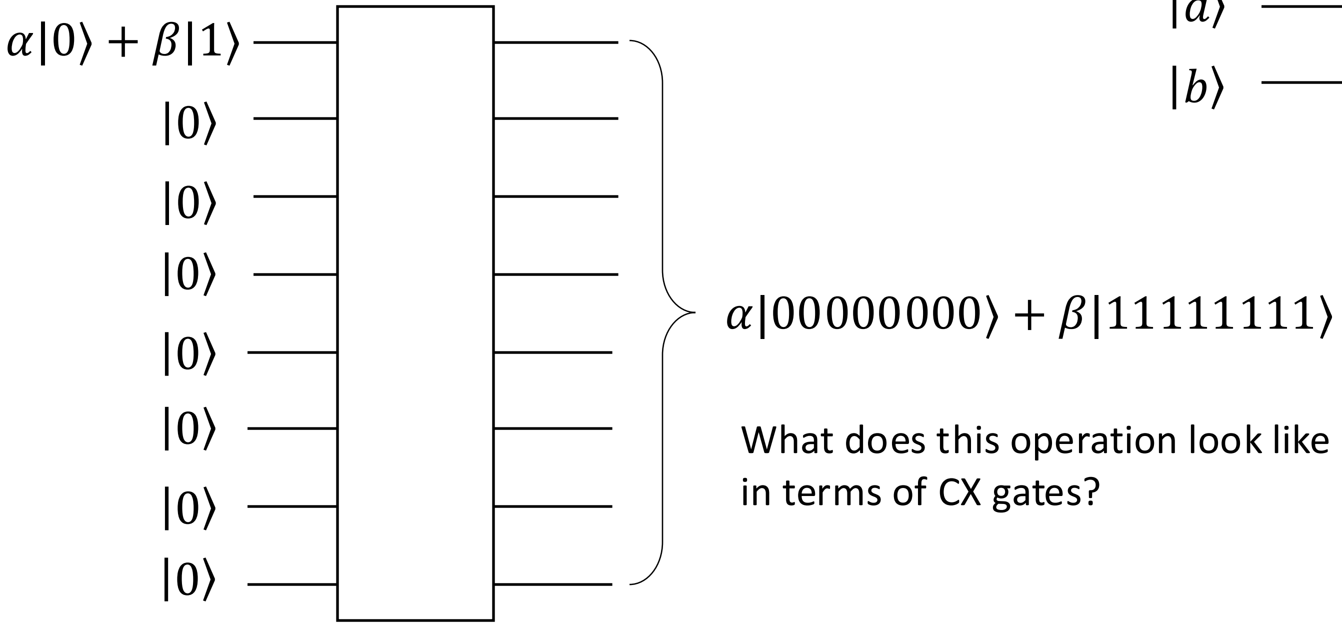


"Copy along each basis"

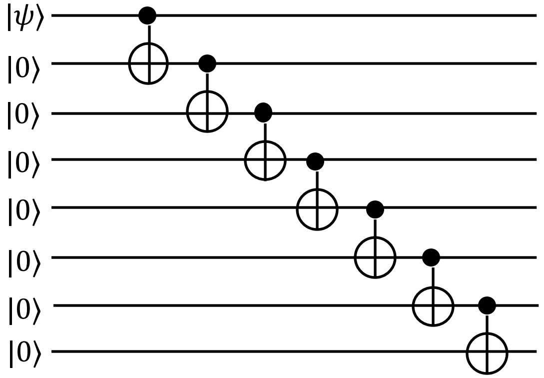
Along each basis ($a, b \in \{0,1\}$):



More (entangled) copies are also possible:



What does this operation look like in terms of CX gates?

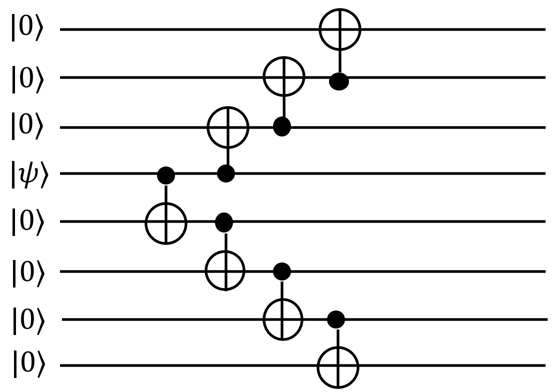


Can we do better (in "circuit depth")?

Quantum Fanout Gate

Quantum fanout: Not only possible, but efficient in circuit depth.

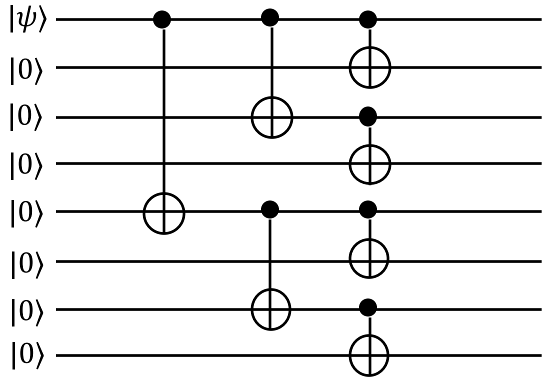
Circuit Depth: $O(n)$



Linear-depth,
1D nearest-neighbor

=

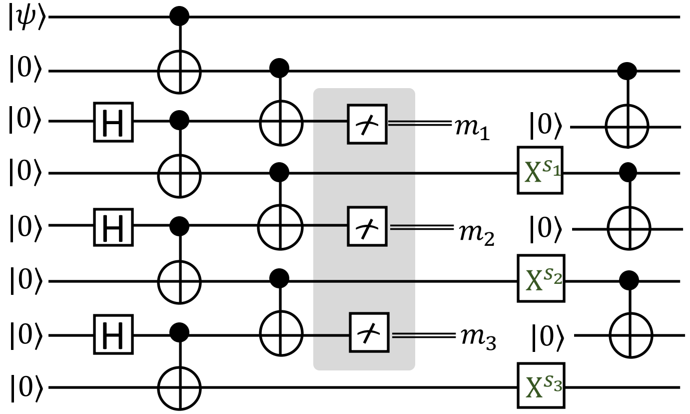
Circuit Depth: $O(\log n)$



Logarithmic-depth,
non-nearest-neighbor

=

Circuit Depth: $O(1)$

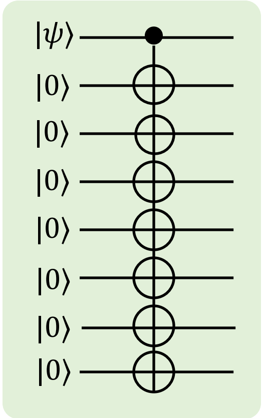


$s_1 = m_1$
$s_2 = m_1 \oplus m_2$
$s_3 = m_1 \oplus m_2 \oplus m_3$

Prefix parity

Constant **quantum** depth
Logarithmic **classical** depth
1D nearest-neighbor

=



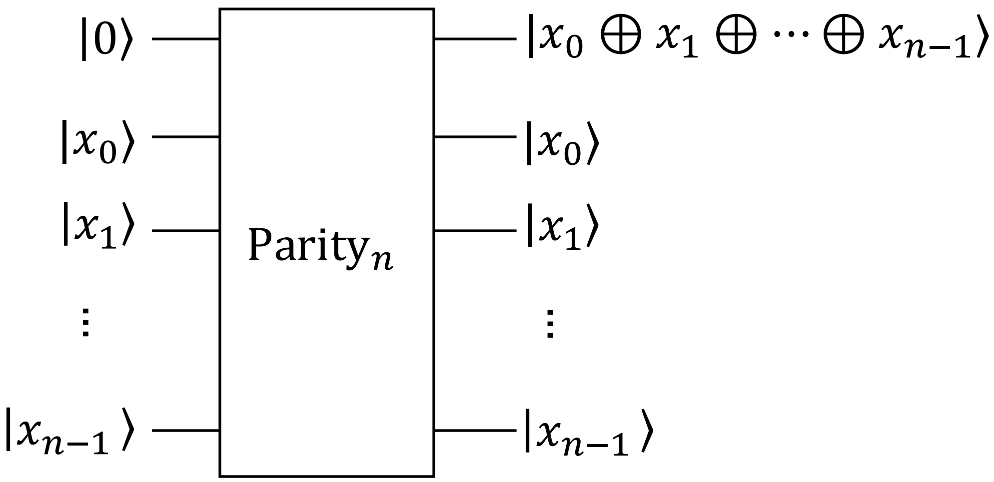
More about this in **Lecture 7** (Teleportation).

Computing Parity Function

Quantum fanout is powerful.

Example: n-bit parity function.

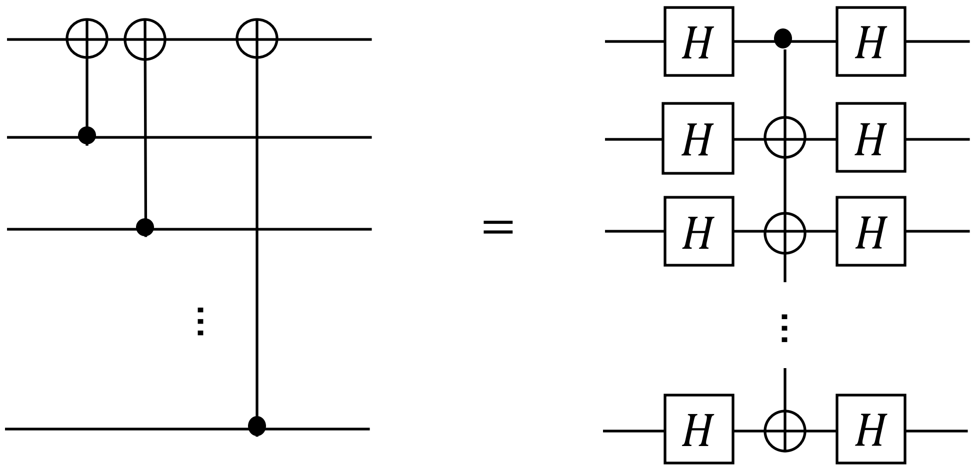
$$\text{Parity}_n(x) = x_0 \oplus x_1 \oplus \cdots \oplus x_{n-1}$$



Remark: These examples are "surprising" because none of these have efficient (constant-depth) classical circuit (with access to 1-bit and 2-bit gates and fanout).

<u>Derive on board</u>:

- How to implement Parity in *linear* depth with CX?
- How to implement Parity in *constant* depth with Fanout?



Quantum constant-depth circuit (with 1-q, 2-q, Fanout gates) can compute a large set of Boolean functions.

More examples:

- Majority function [Høyer, Špalek, 05]
- And function [Takahashi, Tani, 16]