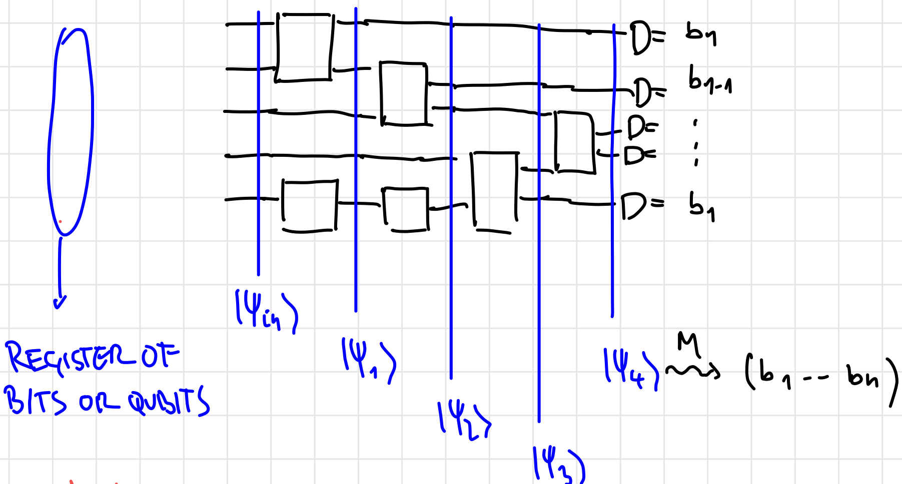
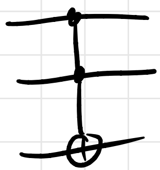
LESSON 2:

CLASSICAL OR QUANTUM CIRCUITS ... EVALUATION

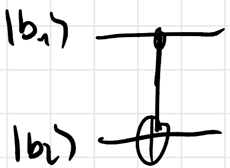


- state
  - ↳ "bitstring"
  - ↳ "probability distribution"
  - ↳ "quantum state" → $|\psi\rangle \in \mathbb{C}^{2^n}$; $|\psi\rangle = \sum_{\vec{b}} \alpha_{\vec{b}} |\vec{b}\rangle$; $\sum |\alpha_{\vec{b}}|^2 = 1$; $|\psi\rangle = \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_N \end{bmatrix}$ $N = 2^n$

Special quantum gate: TOFFOLI

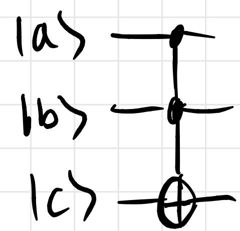


= ctrl-ctrl Not



$|\underbrace{b_1 \oplus b_2}_{\text{"FLIP if } b_1 = 1\text{"}}\rangle$

CNOT [Ctr-Not
ctrl-x]

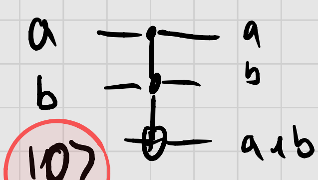


$|c \oplus (a \wedge b)\rangle$

"and", "&"

$\boxed{|c\rangle = |1\rangle}$

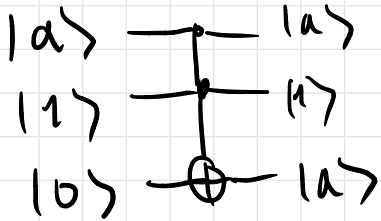
$a, b \to a \wedge b$



"ancilla"

$a, b \longmapsto \neg(a \wedge b)$

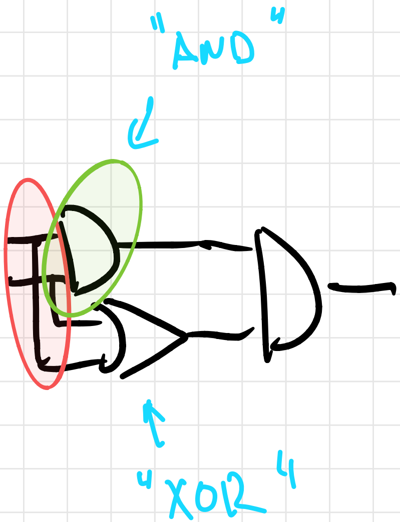
$\boxed{\text{NAND}}$

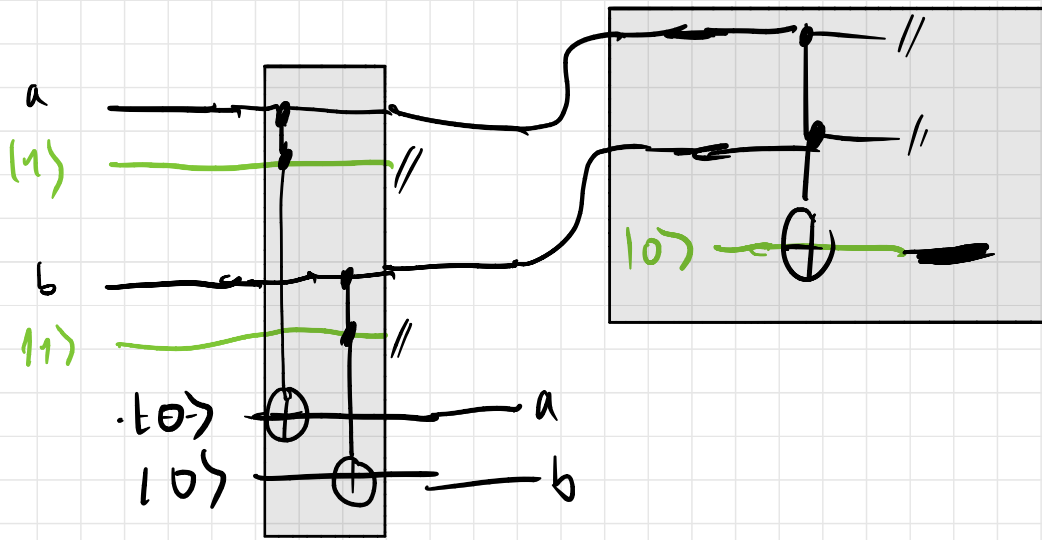


$c = 0, \; b = 1$

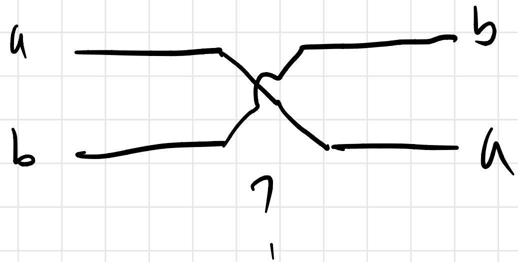
"FANOUT"

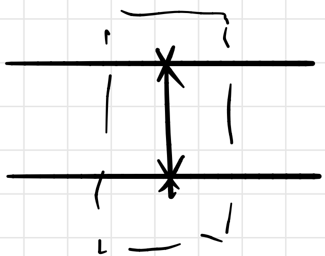
TOFFOLI + ANCILLA (QU)BITS = ALL CLASSICAL GATES





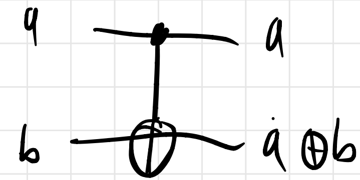
SWAPPING ⁉



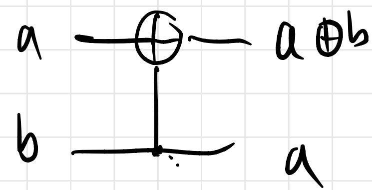


$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

HW:



$= \mathrm{CNOT}(12)$



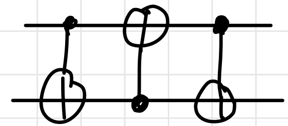
$= \mathrm{CNOT}(21)$

SWAP

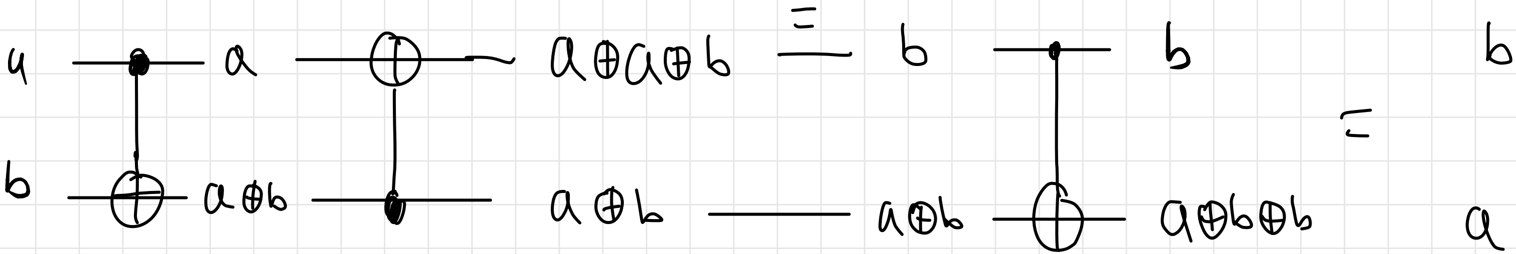
USING $\mathrm{CNOT}(12)$

AND $\mathrm{CNOT}(21)$

"CLASSICAL COMPUTATION"



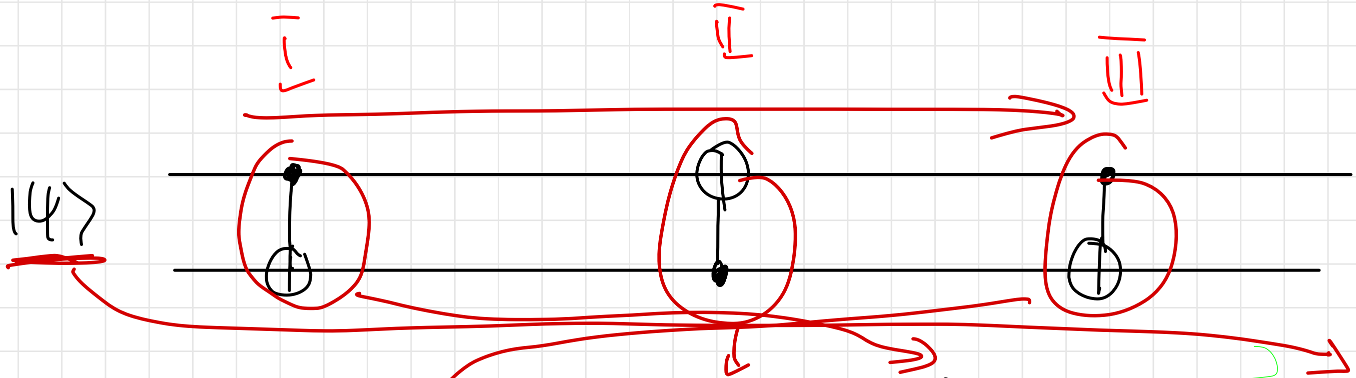
= SWAP



bits specify basis states ...

action on bits FULLY SPECIFIES UNITARY IN THIS CASE

"QUANTUM COMPUTATION"



$$\underbrace{\begin{pmatrix} \mathbb{1} & 0 \\ 0 & X \end{pmatrix}}_{\mathrm{III}} \cdot \underbrace{\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}}_{\mathrm{II}} \cdot \underbrace{\begin{pmatrix} \mathbb{1} & 0 \\ 0 & X \end{pmatrix}}_{\mathrm{I}} \underbrace{\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix}}_{|\psi\rangle}$$

= <u>MULTIPLYING LARGE MATRICES.</u>

TOFFOLI + ANCILLA = ALL CLASSICAL COMPUTATIONS..

→ CLASSICAL REVERSIBLE GATES! = PERMUTATION (0-1) MATRICES

$\boxed{\text{Any } n\text{-bit computation with } m \text{ gates can be realized via an } n+m \text{ qubit computation with } \leq n+2m \text{ gates}}$

$$CC \subseteq QC$$

FUN PUZZLE:

TOFFOLI IS IN ALMOST EVERY SENSE A "CLASSICAL" GATE.
BUT IT IS "3-LOCAL", ACTS ON 3 (QU) BITS.
CAN YOU BREAK IT INTO

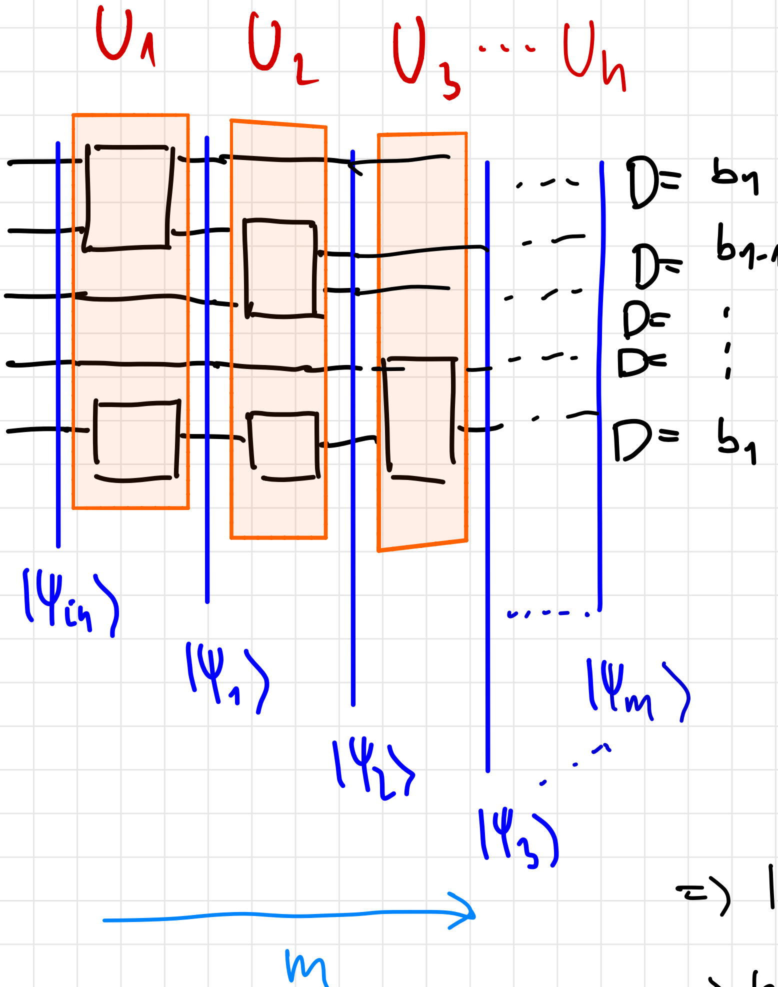
a) SEQUENE OF 2bit "CLASSICAL" REVERSIBLE GATES (CNOT, X, $\mathbb{1}$)

b) SEQUENE OF 2bit QUANTUM REVERSIBLE GATES (CNOT, X, $\mathbb{1}$ + $\pi/8$ + H)

QUESTION

$$QC \overset{?}{\subseteq} CC$$

"GIVEN A Q. CIRCUIT (and an input state), CAN I SIMULATE THE OUTPUT USING A CLASSICAL COMPUTER"



$$|\psi_1\rangle = U_1 |\psi_{in}\rangle$$

$$|\psi_2\rangle = U_2 |\psi_1\rangle = U_2 U_1 |\psi_{in}\rangle$$

$$\vdots$$

$$|\psi_n\rangle = U_n U_{n-1} \cdots U_1 |\psi_{in}\rangle$$

$$|\psi_k\rangle \in \mathbb{C}^{2^n} = \begin{bmatrix} \alpha_{0\ldots0} \\ \vdots \\ \alpha_{11\ldots1} \end{bmatrix}$$

$$U_k \in \mathbb{C}^{2^n \times 2^n}$$

EACH $|\psi_k\rangle \to U|\psi_{k+1}\rangle$

M-V- multiplication

$\Rightarrow$ $|\psi_n\rangle$ using $O(m \times 2^{2n})$ multiplications

$\Rightarrow$ $b_1 .. b_n$ by sampling $[\bar{O}(n \times 2^n)$ at most$]$

QUANTUM COMPUTING CAN BE SIMULATED ON A CLASSICAL COMPUTER WITH EXPONENTIAL SLOW-DOWN

$\Rightarrow$ QC cannot compute *more* than CC

But it may be faster

- QC = $m \in poly(n)$ gates; $O(poly(n))$
- CC = $poly(n) \times O(2^{2n}) \rightarrow$ exponential cost / time