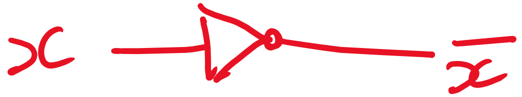
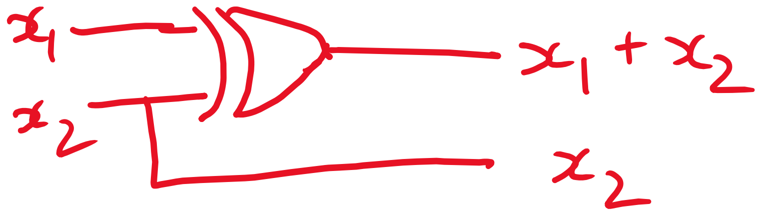
Reversible classical gates $\Longleftrightarrow$ We can know the input by observing the output

i) NOT gate



: This is reversible by definition

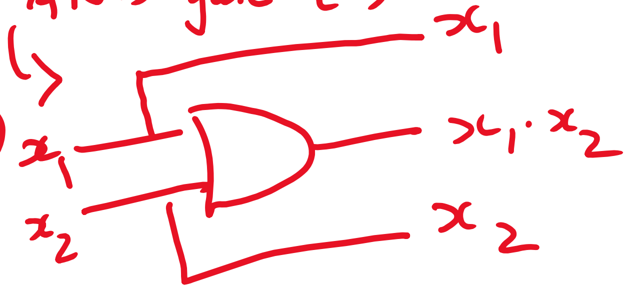
ii) XOR gate $(+)$



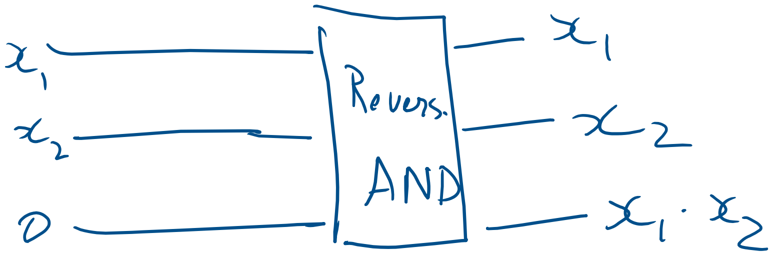
x_1	x_2	x_1+x_2
0	0	0
0	1	1
1	0	1
1	1	0

giving two-output bits ($x_1 + x_2$ & either of x_1 or x_2) will make XOR reversible

iii) AND gate $(\cdot)$



x_1	x_2	$\cdot$
0	0	0
0	1	0
1	0	0
1	1	1



Correspondence between Reversible circuits & Quantum circuits

→ every Quantum gate is represented by a unitary matrix "U"

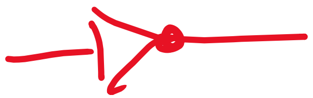
∵ U is unitary ⇒ $U^\dagger U = U U^\dagger = I$

$\dagger \equiv$ transposed conjugate

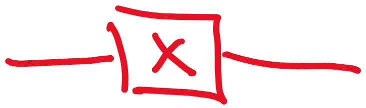
→ Every quantum gate operations are reversible

→ Every reversible classical circuit has a quantum analogue

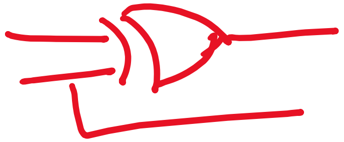
Quantum version of reversible gates



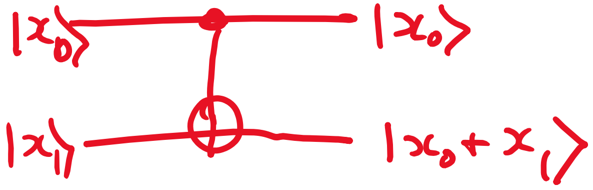
$\equiv$



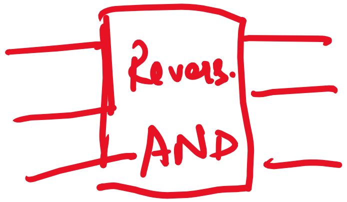
X - gate



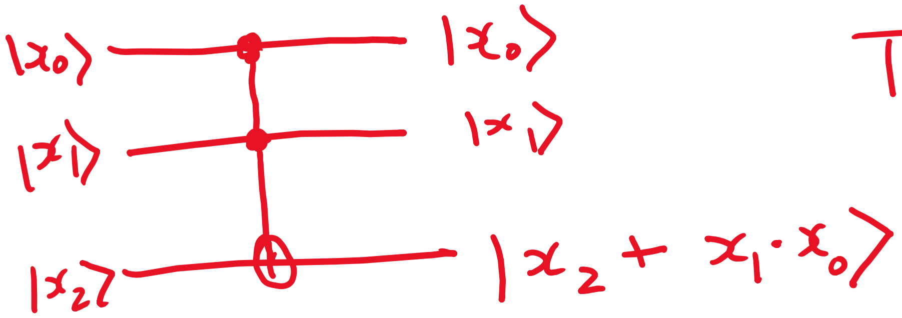
$\equiv$



CNOT - gate



$\equiv$



Toffoli gate

Construction of Bit Oracles (Quantum Oracles)

-> Given a Boolean function $F(x)$

-> construct a Quantum circuit for evaluating that Boolean f^n

i) The ANF (Algebraic normal form of the function is given)

$\{x_i's, +, \cdot\}$

Ex: 1 construct an oracle for $F(x_0, x_1, x_2) = x_0 \cdot x_1 \cdot x_2$

Constructing the circuit for $x_0 \cdot x_1 \cdot x_2 = (x_0 \cdot x_1) \cdot x_2$

NOT – X

XOR – CX

AND – CCX

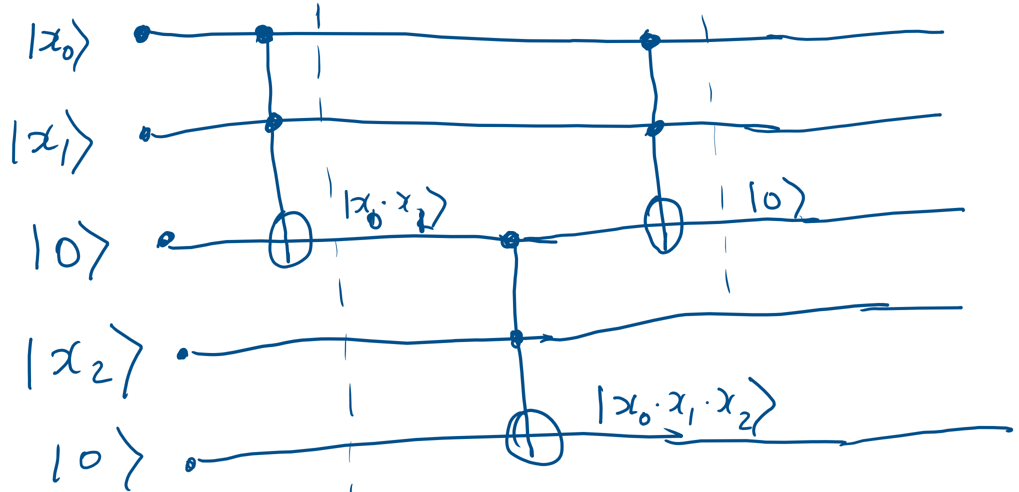
NOT – 1 bit

XOR & AND are two-bit classical gates.

no. of inputs

$$U_F |x\rangle \underset{\text{output}}{|0\rangle} \longrightarrow \underset{3}{|x\rangle} \underset{1}{|F(x)\rangle}$$

$3 + 1 = 4$ qubits



⇒ Bit oracle for $x_0 \cdot x_1 \cdot x_2$

example $|x_0\rangle, |x_1\rangle = |1\rangle$

$$CCX|1\rangle|1\rangle|0\rangle \longrightarrow |1\rangle|1\rangle|1\rangle \xrightarrow{CCX} |1\rangle|1\rangle|0\rangle$$

What about CCCX , CCCCX and so on

→ Physical restriction : only single and two-qubit transformations can be reliably applied

multi-input AND gate

→ every high-degree terms in Boolean functions are in practice we only up to toffoli gates.

$x_0 x_1 x_2 x_3$, $x_0 x_1 x_2$