1/27

QUANTUM CRYPTOGRAPHY

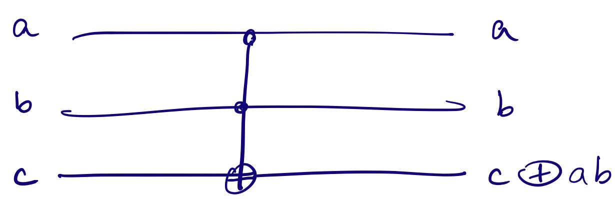
LECTURE - 4

OUTLINE

* More Gates
* Universal reversible computation
* Uncomputing garbage
* Quantum Advantage : Deutsch - Jozsa

Announcement: Amit (or someone) will monitor zoom chat so people attending remotely can ask q's.

Toffoli / CCNOT Gate



When $c = 1$, $c \oplus ab = \text{NAND}(a, b)$.

INPUT	OUTPUT
000	000
001	001
010	010
011	011
100	100
101	101
110	111
111	110

$$T(|\psi\rangle)$$

$$= T\Big(\sum_{x \in \{0,1\}^3} \alpha_x |x\rangle\Big)$$

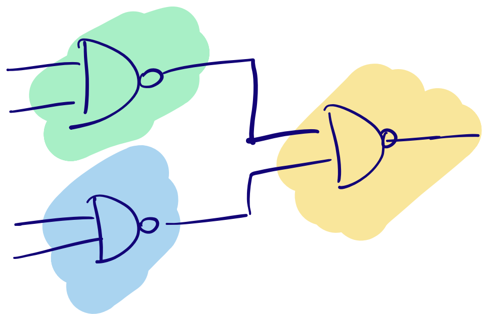
$$= \sum \alpha_x T|x\rangle$$

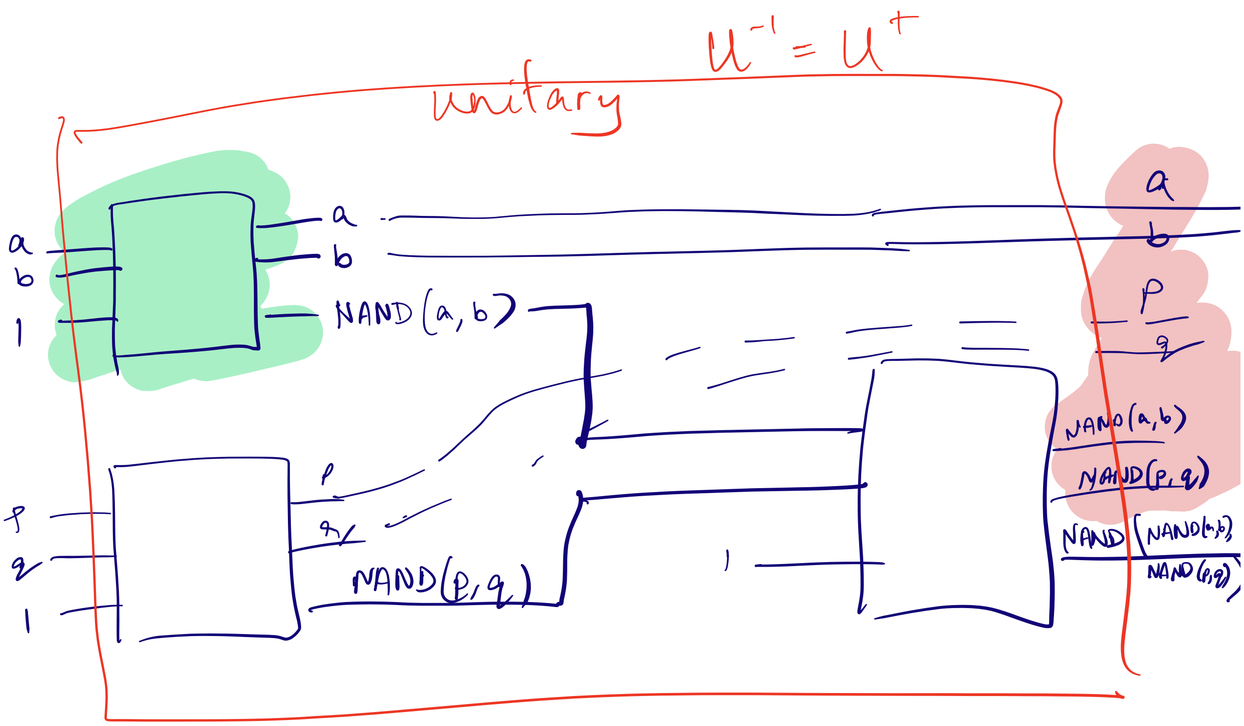
Toffoli gate is universal for reversible classical computations.

FACT.

For any python code that computes an arbitrary function F in time T, there is a classical circuit that implements F with $O(T \log T)$ NAND gates.

There is a reversible circuit implementing F with $O(T \log T)$ Toffoli gates, (and 1 ancillas).

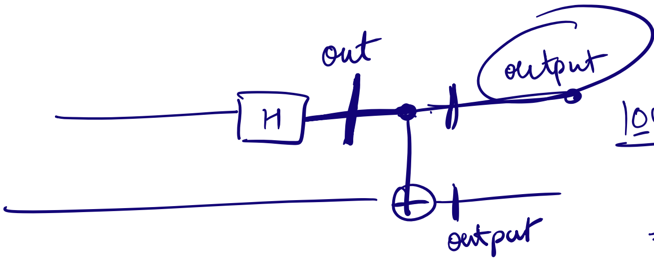




Sanity check. $\exists$ classical ckt computing MULT(p, q) and # gates in this ckt is poly$(|p| + |q|)$.

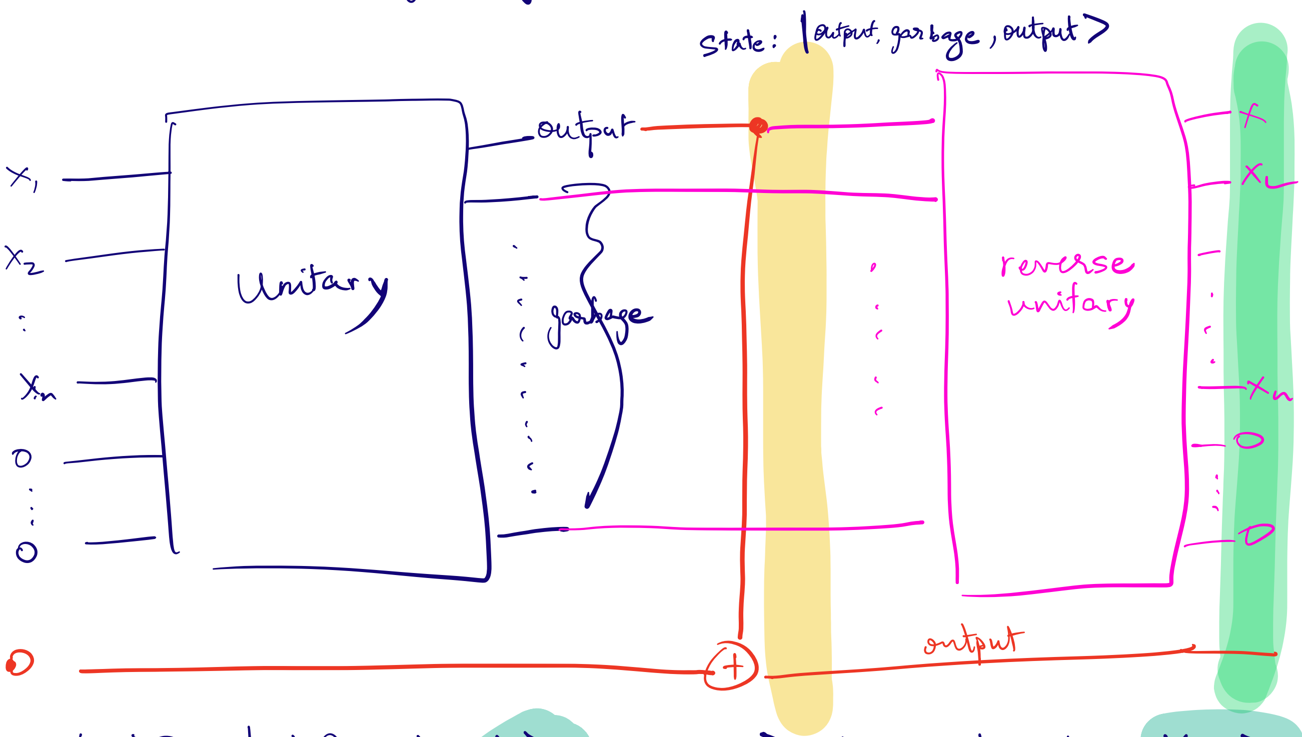
Using Toffoli gates, get a reversible version of MULT.

$(p, q) \longleftrightarrow N$, garbage$(p,q)$



$$\frac{|00\rangle + |11\rangle}{2} \neq \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)$$

"uncompute" garbage



$$|x_1\rangle \otimes \dots |x_n\rangle \otimes |0..0\rangle \otimes |0\rangle \longmapsto |x_1\rangle \otimes \dots |x_n\rangle \otimes |0..0\rangle \otimes |output\rangle$$

$$|x\rangle \otimes |0\rangle \otimes |0....0\rangle \longmapsto |x, output\rangle \otimes |0....0\rangle$$

A quantum circuit C_f implements a classical function $F : \{0,1\}^n \to \{0,1\}^m$ if $\forall x \in \{0,1\}^n$, $\forall y \in \{0,1\}^m$

$$C_f \left(|x\rangle |y\rangle |0^k\rangle \right) \longrightarrow \left(|x\rangle |y \oplus f(x)\rangle |0^k\rangle \right)$$

Sometimes, just say $C_f (|x\rangle |y\rangle) \to |x\rangle |y \oplus f(x)\rangle$

$$C_{mult} \left(|p \overset{\times}{,} q\rangle |y\rangle \right) \to |p \overset{\times}{,} q\rangle |y \oplus pq\rangle$$

Lets think about $f : \{0,1\}^n \to \{0,1\}$.

$$C_f \left(|x\rangle |b\rangle \right) \longrightarrow |x\rangle |b \oplus f(x)\rangle$$

$b = 0$ $\quad |x\rangle |0\rangle \longrightarrow |x\rangle |f(x)\rangle$

$b = 1$ $\quad |x\rangle |1\rangle \longrightarrow |x\rangle |\neg f(x)\rangle$

alternatively $\forall b$, $C_f |x\rangle |b\rangle \longrightarrow |x\rangle |(\neg)^b f(x)\rangle$

What if we compute $C_f \left(|x\rangle |-\rangle \right)$

$|-\rangle \equiv (|0\rangle - |1\rangle)/\sqrt{2}$

What if we compute $C_f(|x\rangle|-\rangle)$

$$|x\rangle|-\rangle \stackrel{C_f}{=} \left(|x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \right)$$

$$= \frac{C_f|x\rangle|0\rangle - C_f|x\rangle|1\rangle}{\sqrt{2}}$$

$$= \frac{|x\rangle|f(x)\rangle - |x\rangle|\neg f(x)\rangle}{\sqrt{2}}$$

$$= |x\rangle \otimes \left(\frac{|f(x)\rangle - |\neg f(x)\rangle}{\sqrt{2}} \right)$$

$f(x)=0$: $\frac{|0\rangle - |1\rangle}{\sqrt{2}} = |-\rangle$

$f(x)=1$: $\frac{|1\rangle - |0\rangle}{\sqrt{2}} = -|-\rangle$

$$= |x\rangle \otimes (-)^{f(x)}|-\rangle$$

$$= (-1)^{f(x)}(|x\rangle \otimes |-\rangle)$$

phase

$U_f(|x\rangle|-\rangle) \longrightarrow (-1)^{f(x)}|x\rangle|-\rangle$

(for boolean output functions).

"Phase kickback trick".

$$\sum_{x\in\{0,1\}^n} \frac{|x\rangle \otimes |-\rangle}{2^{n/2}} \longrightarrow \sum_{x\in\{0,1\}^n} \frac{(-1)^{f(x)}|x\rangle|-\rangle}{2^{n/2}}$$

$$= \frac{|000\ldots0\rangle + |00\ldots1\rangle + \ldots\ldots 2^n \text{ terms}}{2^{n/2}}$$

EXAMPLE: $n = 1$.

$f : \{0,1\} \longrightarrow \{0,1\}$

I tell you f is either

- Constant $\quad f(0) = f(1)$

or

- balanced $\quad f(0) \neq f(1)$.

Can you find out which is the case?

Classical.

Alice | Oracle (f)

query $x \in \{0,1\}^n$ $\longrightarrow$

$f(x)$ $\longleftarrow$

"oracle" access to f.

Quantum

Alice | Oracle

$\sum \alpha_x \underline{|x\rangle} |y\rangle$ $\longrightarrow$

$\longleftarrow$ $\sum \alpha_x |x\rangle |y \oplus f(x)\rangle$

$n=1$.

Classically, need 2 queries.

$n=1$

Quantumly, need just 1 query.

$|+\rangle$

Query is $\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right) \otimes |-\rangle$.

Answer is $\left(\frac{(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle}{\sqrt{2}}\right) \otimes |-\rangle$

f is balanced: $f(0) \neq f(1)$ $\quad \pm\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) \otimes |-\rangle$

f is constant: $f(0)=f(1)$ $\quad \pm\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right) \otimes |-\rangle$

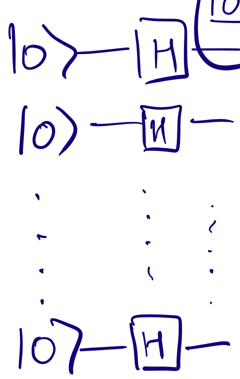
Alice's answer is $|\psi\rangle \otimes |-\rangle$

She computes $H(|\psi\rangle) \otimes |-\rangle$ then measures in the computational basis.

Answer will be 0 when f is constant $\left(H\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right) \to |0\rangle\right)$
and 1 when f is balanced. $\left(H\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) \to |1\rangle\right)$

General: n arbitrary. $\quad f:\{0,1\}^n \to \{0,1\}$.

Input query: $\sum_{x\in\{0,1\}^n} \frac{|x\rangle}{2^{n/2}} \otimes |-\rangle$.



$\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)^{\otimes n} = \sum_{x\in\{0,1\}^n} \frac{|x\rangle}{2^{n/2}}$ ← How to generate uniform superposition over n-bit strings

Again, output $\frac{\sum (-1)^{f(x)} |x\rangle}{2^{n/2}} = |\psi\rangle$

When f is constant this is $\pm \left(\frac{\sum |x\rangle}{2^{n/2}}\right)$

Apply $\pm H^{\otimes n}\left(\frac{\sum |x\rangle}{2^{n/2}}\right) \longrightarrow \pm |0\rangle^{\otimes n}$

Measure in computational basis to get 0^n.

When f is balanced, the $H^{\otimes n}(|\psi\rangle)$ then measuring c.b. will give you something non-0^n.

Claim. For balanced f,

$$H^{\otimes n}\left(\sum_x \frac{(-1)^{f(x)}|x\rangle}{2^{n/2}}\right) \neq 0^n.$$

[Think about how one would prove this, we will discuss next lecture.]