Lecture 6 - Quantum algorithms 1

Last time we looked at basics of Q.C.

States - $|\psi\rangle \in H_n$, vectors (rays) in Hilbert space

Transformations - $U \in U_n$ unitary matrices

Composition - $\otimes$ tensor product

Measurement - Born rule, projectors $\{P_i\}$

$P_i^2 = P_i^\dagger = P_i$; $Pr(i) = \langle\psi| P_i |\psi\rangle$

Basic unitaries we've seen: H, X, Y, Z, CNOT, CZ

Circuits: ——— wires as qubits

—[U]— boxes as unitaries

This lecture

- universal unitaries/gates and the Bloch sphere
- oracle operations in quantum setting
- the 3 algorithms (DJ, BV, Simon) in quantum setting

A universal set of unitaries

Can any unitary $U \in U_n$ be performed from just unitaries in U_2 (2-qubit unitaries) through products and tensor products?

Yes!

Fact: Any $U \in U_n$ can be expressed as a product of CNOT operations and unitaries from U_1 (this is called unitary synthesis)

What about unitaries from U_1? Does there exist a finite set $U_{US} \subseteq U_1$ s.t $\forall\ U \in U_1$ $\exists$ an N and a sequence $\{s_i\}_{i \leq N}$ $(1 \leq s_i \leq |U_{US}|)$ s.t

(U_{US} → US = universal set)

$$G_{s_1} \cdot G_{s_2} \cdot \cdots G_{s_N} = U$$

for $G_{s_i} \in U_{US}$.

The answer is no, however, there does exist such a set to approximate any $U \in U_1$ (and also any $U \in U_n$) to within fixed precision $\varepsilon > 0$.

(we say that $|U - \tilde{U}| \leq \varepsilon$ if $\forall\, i,j$ it's the case that $|U(i,j) - \tilde{U}(i,j)| \leq \varepsilon$, where $U(i,j)$ is the (i,j) matrix entry of U)

Fact (Solovay-Kitaev theorem): There exists a finite set $U_{VS} \subseteq U_2$, such that any unitary $U \in U_1$ can be approximated to within precision $\varepsilon > 0$ by a sequence of $O(\log^4(1/\varepsilon))$ products (and tensor products) of elements of U_{VS}. (for general $U \in U_n$, sequence is $O(4^n \log^4(1/\varepsilon))$)

What is U_{VS}? $U_{VS} = \{ CNOT, H, T \}$, where

T is a single qubit gate defined as

$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$ called the T gate or the $\pi/4$ gate or the $\pi/8$ gate

(the $\pi/8$ gate name comes from the fact that, up to global phase we can also write $T = \begin{pmatrix} e^{-i\pi/8} & 0 \\ 0 & e^{i\pi/8} \end{pmatrix}$)

Note that $T^4 = Z$

Also T^2 is denoted as $S = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/2} \end{pmatrix}$ and reffered to as the phase gate or $\pi/2$ gate.

From now on we will use the "gate" terminology for unitaries from the universal set.

Note that there can be other universal sets

E.g. $\{CCNOT, H, S\} \subseteq U_3$

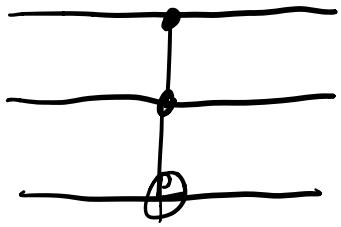
where CCNOT - controlled-controlled NOT (a.k.a Toffoli)

CCNOT acts on 3 qubits

$$CCNOT\,|x\rangle|y\rangle|z\rangle = |x\rangle|y\rangle|z \oplus x\cdot y\rangle$$

Flips 3rd qubit iff. first two are in $|1\rangle$ state

As a circuit



If we only care about unitaries with real entries (which turns out to be sufficient for computation), then

$\{CCNOT, H\}$ is universal.

We said that unitaries are like rotation matrices, so let's be a bit more explicit for U_1

The Bloch sphere

For $n=1$, $\dim(H_1)=2$, $|\psi\rangle \in H_1$

$$|\psi\rangle = a|0\rangle + b|1\rangle$$

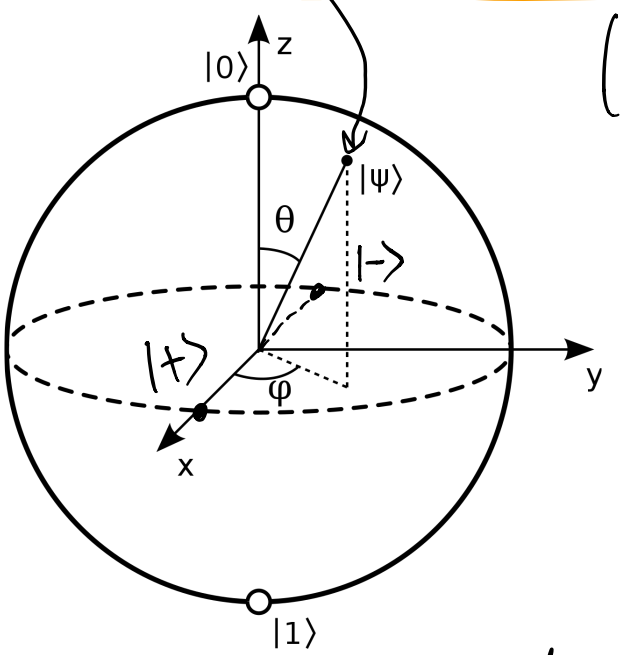
$$|a|^2+|b|^2=1$$

And $|\psi\rangle \sim e^{i\theta}|\psi\rangle$

$\Rightarrow$ $|\psi\rangle$ can be written as

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi}\sin\left(\frac{\theta}{2}\right)|1\rangle$$

$(\theta \in [0,\pi],\ \varphi \in [0,2\pi])$



$\theta = 0 \rightarrow |0\rangle$

$\theta = \pi \rightarrow |1\rangle$

$\theta = \pi/2,\ \varphi = 0 \rightarrow |+\rangle$

$\theta = \pi/2,\ \varphi = \pi \rightarrow |-\rangle$

(wikipedia.org/wiki/Bloch_sphere)

Single qubit unitaries are rotations on the Bloch sphere

X, Y, Z - rotations by π around X, Y, Z axes

General rotation operations

$$R_x(\alpha) = e^{-i\alpha X/2} \qquad X = R_x(\pi)$$

$$R_y(\alpha) = e^{-i\alpha Y/2} \qquad Y = R_y(\pi)$$

$$R_z(\alpha) = e^{-i\alpha Z/2} \qquad Z = R_z(\pi)$$

Z is the easiest to see

$$R_z(\alpha) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix}; \quad R_z(\pi) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = Z$$

Note $T = R_z(\pi/4)$, $S = R_z(\pi/2)$

$H = \frac{1}{\sqrt{2}}(X+Z)$ - rotation by π around the axis in between X and Z $(X+Z)$

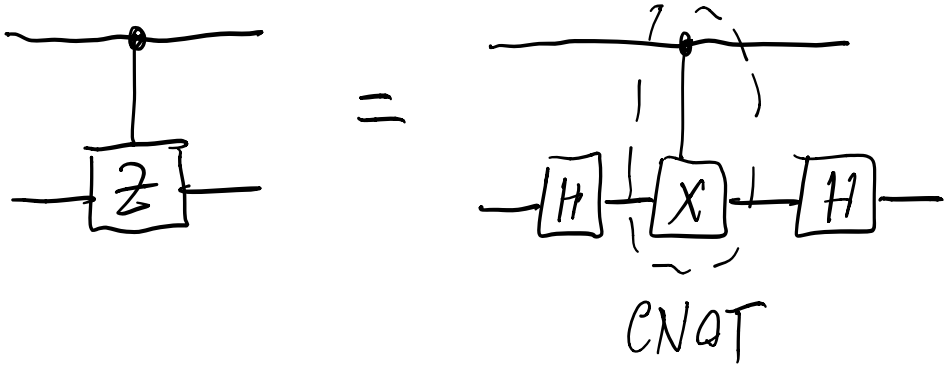
Solovay-Kitaev for 1 qubit unitaries says that any general rotation on the Bloch sphere can be approximated to arbitrary precision using just a $\pi/4$ rotation around Z (T) and a π rotation around $X+Z$ (H)

From now on assume all unitaries we consider can be implemented from $\{H, T, CNOT\}$

E.g. $S = T^2$ $\quad X = HT^4H$

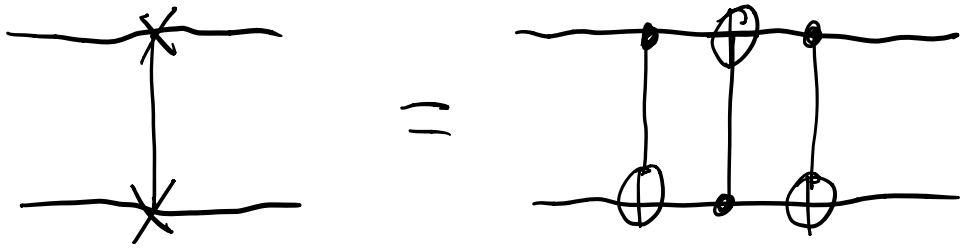
$Z = T^4$ $\quad Y = X \cdot Z$ (up to phase)

$CZ = (I \otimes H)\, CNOT\, (I \otimes H)$



$$SWAP\,|\psi\rangle|\phi\rangle = |\phi\rangle|\psi\rangle$$

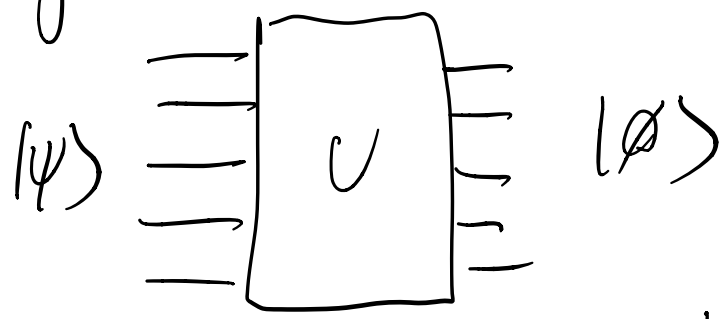
$$SWAP = CNOT_{12}\, CNOT_{21}\, CNOT_{12}$$



Oracle operations

Can any boolean function be implemented as a quantum circuit?

At first glance we might say no. Unitary operations are clearly reversible



$$|\phi\rangle = U|\psi\rangle, \quad |\psi\rangle = U^{\dagger}\cdot|\phi\rangle$$

But a general boolean function need not be reversible

E.g. $f(x) = x \cdot s$, $f : \{0,1\}^n \to \{0,1\}$

Solution: make a unitary that implements f in a reversible manner: $U_f |x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$

($|x\rangle$: n, $|y\rangle$: 1)

Is U_f unitary? Yes, it's just a permutation matrix. Also $U_f^\dagger = U_f$

$$U_f \cdot U_f |x\rangle|y\rangle = U_f |x\rangle|y \oplus f(x)\rangle =$$

$$= |x\rangle|y \oplus \underbrace{f(x) \oplus f(x)}_{0}\rangle = |x\rangle|y\rangle$$

This works even if $y \in \{0,1\}^m$, for some $m > 0$

So for any $f : \{0,1\}^n \to \{0,1\}^m$ there exists a unitary U_f that performs f in a reversible manner.

Assuming the boolean circuit implementing f has $G(n)$ boolean gates, can U_f be implemented with $O(G(n))$ quantum gates?

Yes!

The NAND gate is universal for classical comp. (any boolean function can be implemented with NAND gates)

$$NAND(a,b) = \neg(a \cdot b) = 1 \oplus (a \cdot b)$$

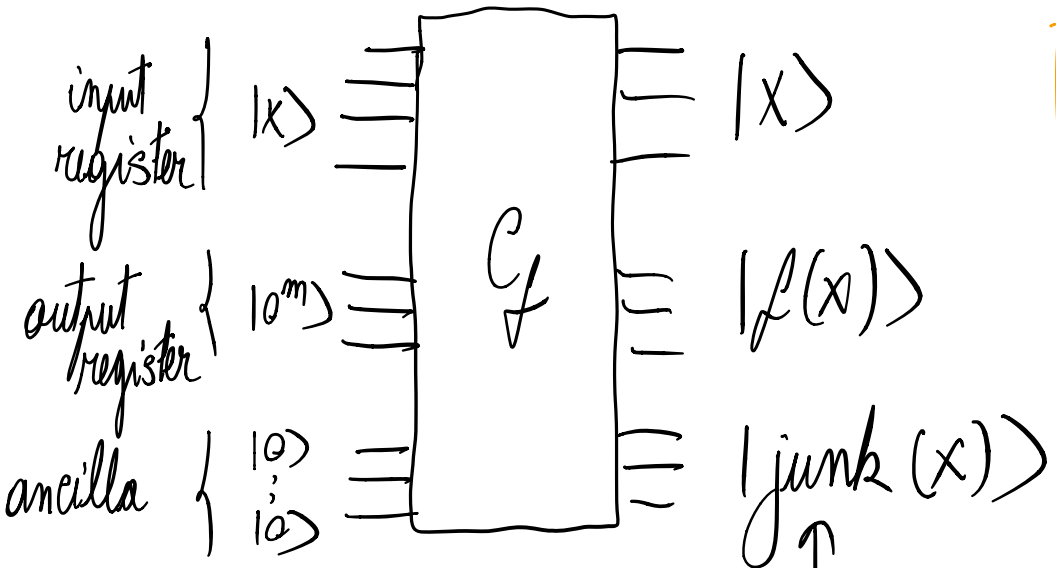
How to do NAND as a q. circuit?

Recall $CCNOT\,|x\rangle|y\rangle|z\rangle = |x\rangle|y\rangle|x \cdot y \oplus z\rangle$

$$CCNOT\,|a\rangle|b\rangle|1\rangle = |a\rangle|b\rangle|a \cdot b \oplus 1\rangle$$

Using $O(G(n))$ CCNOT gates and $O(G(n))$ auxillary qubits (ancilla) we can implement f!

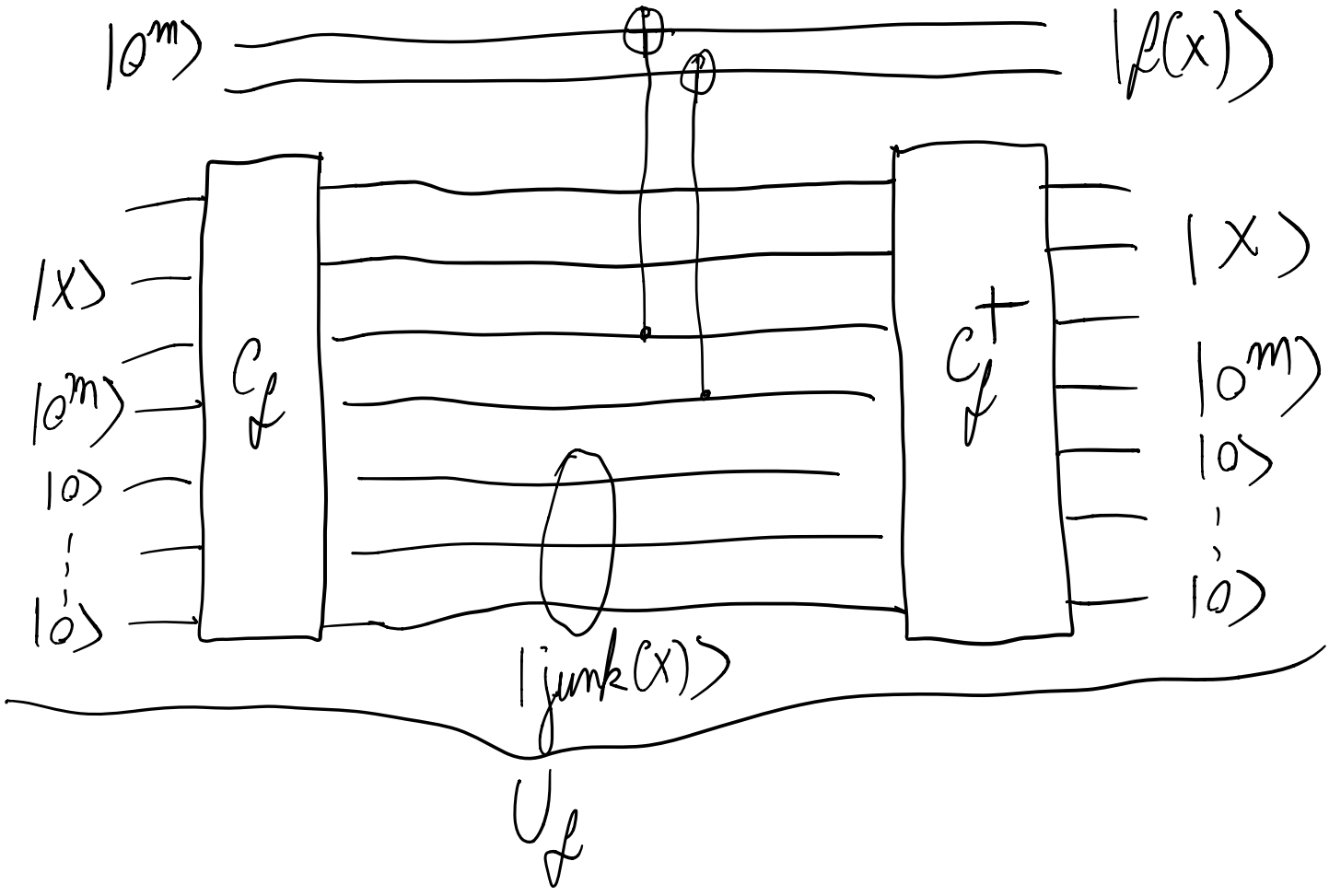
However, this naive implementation will lead to



for superposition states these registers can be entangled

↑ partial results from the computation

Let's get rid of $|junk(x)\rangle$. A neat trick...

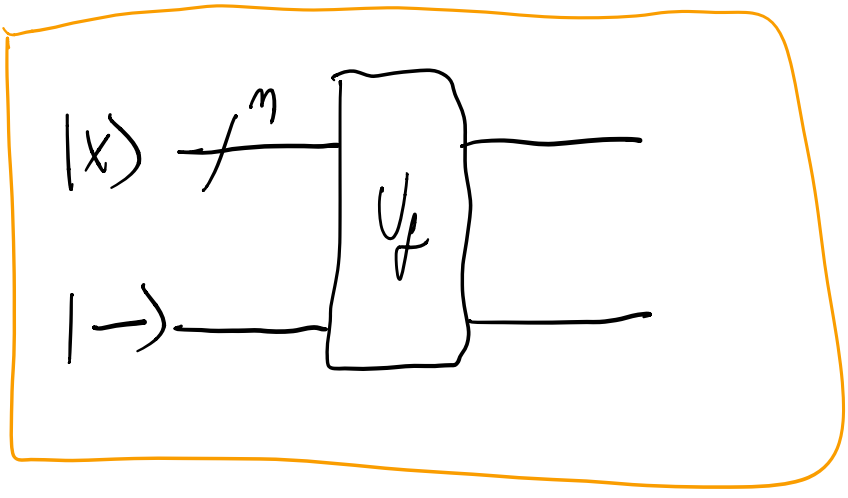


U_f has $O(G(x))$ gates (CCNOT can be performed with a constant number of H, T, CNOT gates)

So the cost of evaluating U_f is, up to constant factors, the same as that of evaluating f.

We will therefore view oracle operations for same f as just the unitary U_f.

Finally, let's consider an alternate oracle that we can construct from U_f when $m=1$ ($f: \{0,1\}^n \to \{0,1\}$)



What is the output of this circuit?

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

So if $f(x) = 0$ we have $|x\rangle \cdot \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

if $f(x) = 1$ we have $|x\rangle \cdot \frac{1}{\sqrt{2}}(|1\rangle - |0\rangle)$

In other words the state is

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

Since bottom qubit is unchanged, we can view this as an n-qubit unitary performing the mapping

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

Note that U_f' is still performing one oracle call to f!

Quantum algorithms

1) Deutsch-Jozsa

$$f: \{0,1\}^n \to \{0,1\} \begin{cases} \text{constant} \\ \text{balanced} \end{cases}$$

We want to approach this using our intuition from interf.

Let's create a state with entries $(-1)^{f(x)}$

$$|\psi_1\rangle = H^{\otimes n}|0\rangle^{\otimes n} = \left(H|0\rangle\right)^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle$$

Apply U_f' to $|\psi_1\rangle$

$$|\psi_2\rangle = U_f'|\psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} U_f'|x\rangle = \frac{1}{\sqrt{2^n}} \sum_x (-1)^{f(x)}|x\rangle$$

Now what? We want an output state whose amplitude

proportional to $\sum_x (-1)^{f(x)}$

Apply Hadamard again!

Recall $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ $H(x,y) = \frac{1}{\sqrt{2}} (-1)^{x \cdot y}$

$$H^{\otimes 2}(x_1, x_2, y_1, y_2) = \frac{1}{2} (-1)^{x_1 \cdot y_1} \cdot (-1)^{x_2 \cdot y_2}$$

$$= \frac{1}{2} (-1)^{x_1 \cdot y_1 + x_2 \cdot y_2} = \frac{1}{2} (-1)^{x \cdot y}$$ for

$x = x_1 x_2$, $y = y_1 y_2$

So in general $H^{\otimes n}(x,y) = \frac{1}{\sqrt{2^n}} (-1)^{x \cdot y}$

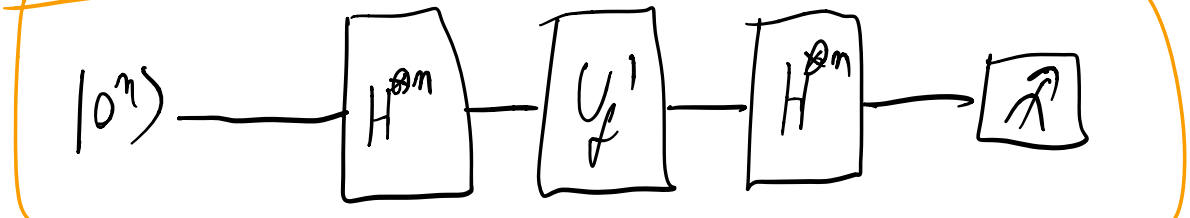
$$H^{\otimes n} |x\rangle = \frac{1}{2^{n/2}} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle$$

$$|\psi_3\rangle = H^{\otimes n} |\psi_2\rangle = \frac{1}{2^n} \sum_{x,y \in \{0,1\}^n} (-1)^{f(x) + x \cdot y} |y\rangle$$

For $|y\rangle = |0\rangle^n$ the amplitude is $\frac{1}{2^n} \sum_x (-1)^{f(x)}$

So if we measure in the computational basis we see $|0\rangle^n$ with prob $\left|\frac{1}{2^n}\sum_x (-1)^{f(x)}\right|^2$

When f is constant this is 1 and when it is balanced it's 0!



2) Bernstein-Vazirani

$f: \{0,1\}^n \to \{0,1\}$ $\quad f(x) = s \cdot x$

find s

As before, we should start by creating

$$|f\rangle = \frac{1}{\sqrt{2^n}} \sum_x (-1)^{f(x)} |x\rangle$$

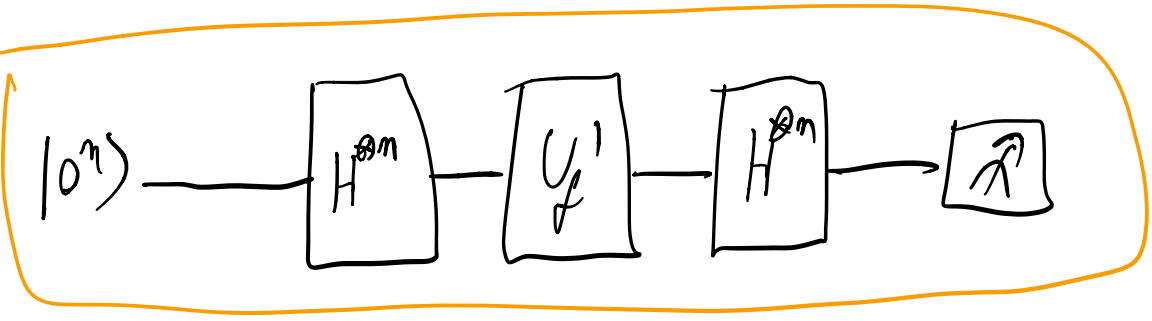
Now what? Hadamard again and measure

$$H^{\otimes n}|f\rangle = \frac{1}{2^n}\sum_{x,y}(-1)^{f(x)+x\cdot y}|y\rangle$$

$$= \frac{1}{2^n}\sum_{x,y}(-1)^{x\cdot s + x\cdot y}|y\rangle$$

So $|s\rangle$ has amplitude 1 and the rest have amplitude 0.

$\Rightarrow$ If we measure we will see s with prob 1!



3) Simon's problem

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

$f(x) = f(x \oplus s)$, $s \in \{0,1\}^n / 0^n$, find s!

This time we can't use U_f', so we're back to U_f.

We still want to apply it in superposition.

$\Rightarrow$ create $\sum_x |x\rangle|0^n\rangle$ and apply U_f

$$\Rightarrow \boxed{|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle|f(x)\rangle}$$

Measure second register and get $|y\rangle$ s.t $y = f(x_1) = f(x_2)$ for some x_1, x_2 with $x_1 \oplus x_2 = s$

If we apply $\boxed{I \otimes |y\rangle\langle y|}$ on $|\psi\rangle$ we have

$$\frac{1}{\sqrt{2^n}} \sum_x \left[(I \otimes |y\rangle\langle y|) \cdot |x\rangle \otimes |f(x)\rangle \right]$$

$$\langle y|f(x)\rangle = \begin{cases} 1, & y = f(x) \\ 0 & \text{otw} \end{cases}$$

$\Rightarrow$ we are left with $\boxed{\frac{1}{\sqrt{2}} \left(|x_1\rangle + |x_2\rangle\right) \otimes |y\rangle}$

Best we know $x_1 \oplus x_2 = s$

Let's apply $H^{\otimes n}$ to the x register

$$\frac{1}{\sqrt{2}}\left(H^{\otimes n}|x_1\rangle + H^{\otimes n}|x_2\rangle\right) =$$

$$= \frac{1}{\sqrt{2^{n+1}}}\left(\sum_z (-1)^{x_1 \cdot z}|z\rangle + \sum_z (-1)^{x_2 \cdot z}|z\rangle\right)$$

$$= \frac{1}{\sqrt{2^{n+1}}} \sum_z \left((-1)^{x_1 \cdot z} + (-1)^{x_2 \cdot z}\right)|z\rangle =$$

$$= \frac{1}{\sqrt{2^{n+1}}} \sum_x (-1)^{x_1 \cdot z}\left(1 + (-1)^{z \cdot s}\right)|z\rangle$$

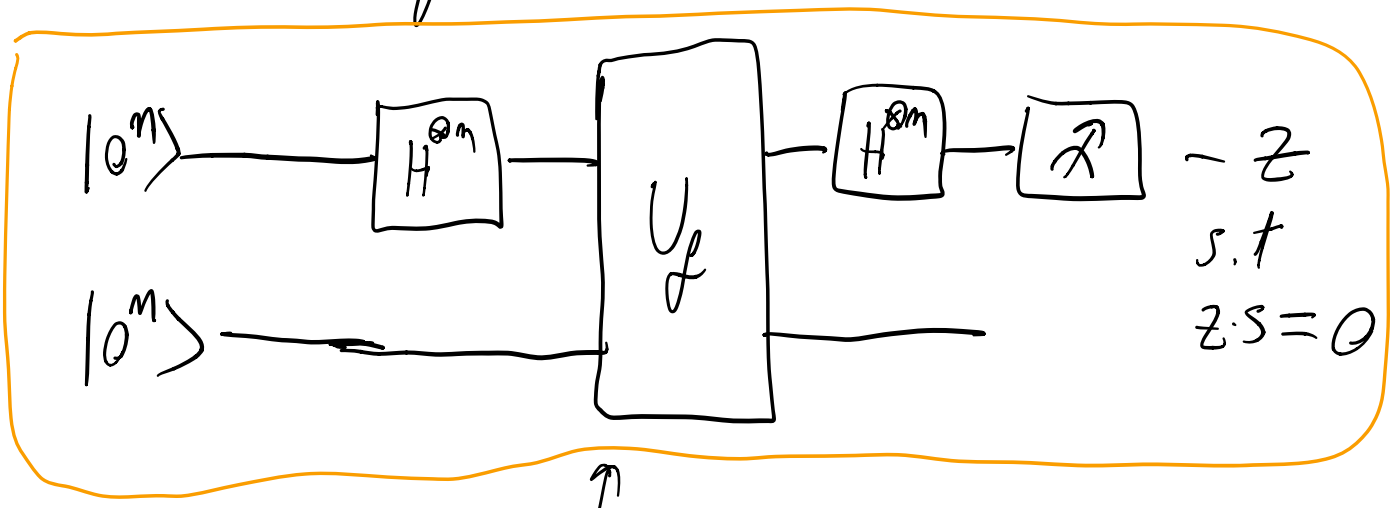
If $z \cdot s = 1 \Rightarrow$ 0 amplitude

If $z \cdot s = 0 \Rightarrow$ non-zero amplitude

$\Rightarrow$ if we measure in comp. basis we'll get a z s.t. $z \cdot s = 0$

Repeat $O(n)$ times and solve with Gaussian elimination to find s.

One iteration of the circuit looks like this



this is what inter/2 was doing