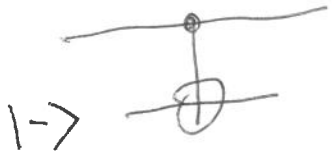
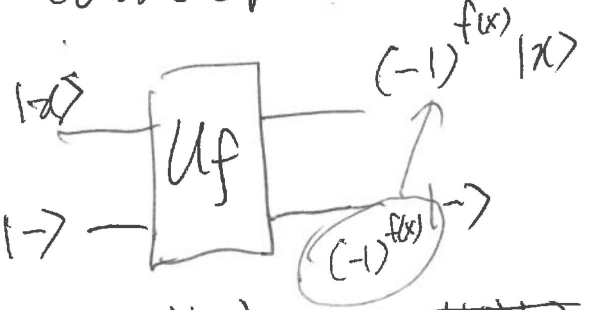
* Phase kickback



Now consider



$U_f(|x\rangle \otimes |-\rangle)$

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

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

$= \frac{1}{\sqrt{2}}\left(|x, f(x)\rangle - |x; \overline{f(x)}\rangle\right)$

$= \frac{1}{\sqrt{2}}|x\rangle \otimes \left(|f(x)\rangle - |\overline{f(x)}\rangle\right)$

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

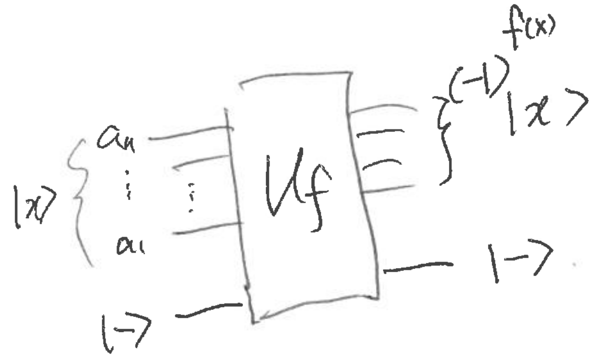
$= (-1)^{f(x)}|x\rangle|-\rangle.$

So $U_f((a|0\rangle + b|1\rangle)|-\rangle) =$ ~~$(a|0\rangle - b|1\rangle)|-\rangle$~~

$= \left(a(-1)^{f(0)}|0\rangle - b(-1)^{f(1)}|1\rangle\right)|-\rangle$

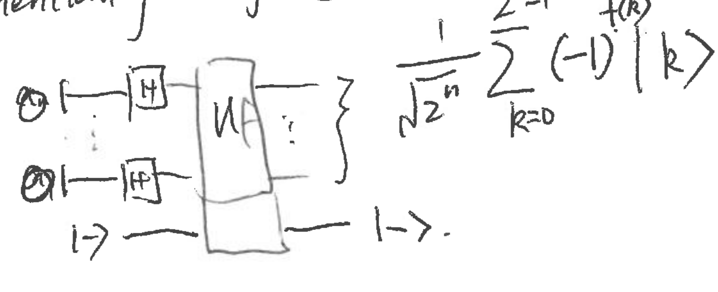
In general,

$|x\rangle = |a_n \cdots a_1\rangle$



* So by using $|-\rangle$ for U_f, we are able to use (-1) to 'mark' the state $|x\rangle$ where $f(x) = 1$.

think of f as a kind of verifier, e.g. x is prime, or x is the solution. We can use H gate to generate the exponentially large (2^n) search space.



* Consider the amplitudes of

Let $N = 2^n$. $\frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} (-1)^{f(k)} |k\rangle$.

$$\underbrace{\left((-1)^{f(k)} \frac{1}{\sqrt{N}}, \cdots, (-1)^{f(k)} \frac{1}{\sqrt{N}} \right)}_{N}.$$

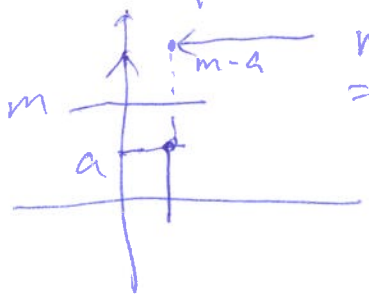
e.g. when $N = 2^3$ only $f(0) = 1$.

$$\underbrace{\left(-\frac{1}{\sqrt{8}}, \frac{1}{\sqrt{8}}, \cdots \frac{1}{\sqrt{8}} \right)}_{8}.$$

if we can somehow amplify $(-\frac{1}{\sqrt{8}})$ and suppress the other, we would be able to find the solution of k, which is

$f(k) = 1$

* So Reflection about mean



We say $\underline{2m-a}$ is a's reflection about m.

Reflection about mean allows us to amplify ~~@~~ amplitude.

e.g. for $[-\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}]$

~~we can apply $\lambda a.\ 2m-a$~~

the mean $\mu = (-\frac{1}{2}+\frac{1}{2}+\frac{1}{2}+\frac{1}{2})/4 = \frac{1}{4}$.

we apply $\lambda a.\ 2\mu - a$ to the list, we get $[1, 0, 0, 0]$. So we amplify the ~~prop~~ probability ~~@~~ from $-\frac{1}{2}$ to 1.

while ~~@~~ suppressing the other amplitudes. (amplitude)

* How to do 'reflection about mean' in a quantum setting?

First some basics: $|0\rangle, |1\rangle : \mathbb{C} \to \text{Qubit}$.

$$|0\rangle(1) = |0\rangle$$
$$|1\rangle(1) = |1\rangle$$

So $|0\rangle, |1\rangle$ state can be viewed as a linear function $\mathbb{C} \to \text{Qubit}$.

we define 'dual state'

$$\langle 0|, \langle 1| : \text{Qubit} \to \mathbb{C}.$$

s.t. $\langle 0|(|0\rangle) = \langle 0|0\rangle = 1$

$\langle 0|(|1\rangle) = \langle 0|1\rangle = 0$.

$\langle 1|0\rangle = 0$

$\langle 1|1\rangle = 1$.

So $\langle 0|, \langle 1|$ are also linear functions.

we introduce a 'dagger functor' $(-)^\dagger$

s.t. $|0\rangle^\dagger = \langle 0|$ $|1\rangle^\dagger = \langle 1|$

and when U is unitary, $U^\dagger = U^{-1}$.

and $(G \circ F)^\dagger = F^\dagger \circ G^\dagger$.

* Projector.

$P : Q \to Q$ is a projector if P is linear and $P \cdot P = P$.

e.g. $|0\rangle\langle 0|$: Qubit → Qubit.

i.e. $|0\rangle$ ~~function~~

first apply $\langle 0|$ function, then apply $|0\rangle$ function.

so. $|0\rangle\langle 0|0\rangle = |0\rangle$

$|0\rangle\langle 0|1\rangle = 0$

$|0\rangle\langle 0|$ is a projector because

$|0\rangle\langle 0| \circ |0\rangle\langle 0|$

$= |0\rangle\langle 0|0\rangle\langle 0| = |0\rangle\langle 0|$.

similarly $|1\rangle\langle 1|$ is also a projector.

Note that a projector is not necessarily a unitary.

* the reason we talk about projector is that we can make a projector to calculate the mean of amplitude.

Claim: $|+\rangle\langle+|$ calculates the mean of a state $a|0\rangle + b|1\rangle$.

Pf: $|+\rangle\langle+|(a|0\rangle + b|1\rangle)$

$= \frac{1}{2}(|0\rangle+|1\rangle)\cdot(\langle 0|+\langle 1|)(a|0\rangle+b|1\rangle)$

$= \frac{1}{2}(|0\rangle+|1\rangle)(a+b)$

$= \frac{a+b}{2}|0\rangle + \frac{a+b}{2}|1\rangle.$

In general, $|\psi\rangle = \underbrace{|+\rangle\otimes|+\rangle\cdots\otimes|+\rangle}_{n}$.

$|\psi\rangle\langle\psi|$ calculates the mean of a n-qubit state.

* Question. $|\psi\rangle\langle\psi|$ is still not a unitary operation, so how to make a unitary out of it?

* Answer: if P is a projector,

$2P - I$ is unitary.

because $(2P-I)^{-1} = 2P - I$.

i.e. $(2P-I)\cdot(2P-I) = 4P - 2P - 2P + I$

$= I$.

So the unitary that can perform "reflection about mean" is

$2|\psi\rangle\langle\psi| - I$.

* How to build a circuit for it?

e.g. $2|+\rangle\langle+| - I$

$= 2(H|0\rangle)(\langle 0|H) - H \cdot H$

$= H(2|0\rangle\langle 0| - I)H$.

$2|0\rangle\langle 0| - I$: Z-gate!

in the case when $n = 1$.

$(2|0\rangle\langle 0| - I)|0\rangle = 2|0\rangle - |0\rangle = |0\rangle$

$(2|0\rangle\langle 0| - I)|1\rangle = -|1\rangle$.