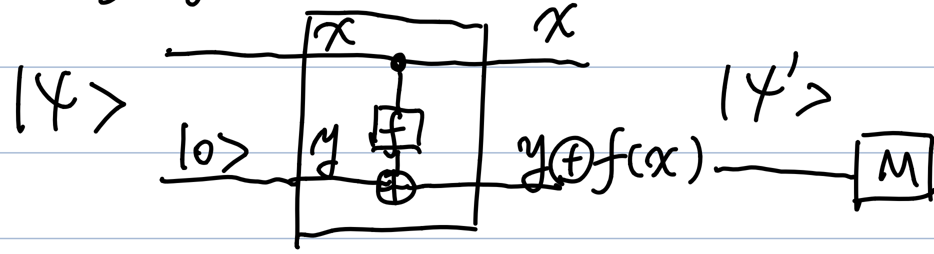
3. Quantum Parallelism

Quantum Parallelism is a useful feature for many quantum algorithms. Quantum parallelism allows quantum computers to evaluate a function $f(x)$ for many different x simultaneously. It sounds perfect! Here we'll first show how quantum parallelism works, and some of its limitations.

Suppose $f(x): \{0,1\} \mapsto \{0,1\}$ is a function taking in one bit and output one bit. We also have the following quantum circuit that takes in two inputs



If we let $y = |0\rangle$, then $y \oplus f(x) = f(x)$.

To evaluate $f(x)$ for $x = 0$ & 1, we can feed in $x = |0\rangle$ and $x = |1\rangle$ respectively to the circuit and measure the results.

We can feed in another state $\frac{|0\rangle + |1\rangle}{\sqrt{2}}$, so the inputs

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle$$

$$= \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$$

the output $|\psi'\rangle$ is

$$|\psi'\rangle = \frac{1}{\sqrt{2}} |0, f(0)\rangle + |1, f(1)\rangle$$

inputs outputs

The output $|\psi'\rangle$ contains the information of both $f(0)$, and $f(1)$.

The idea of using $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ can be easily generalized to multiple bits since

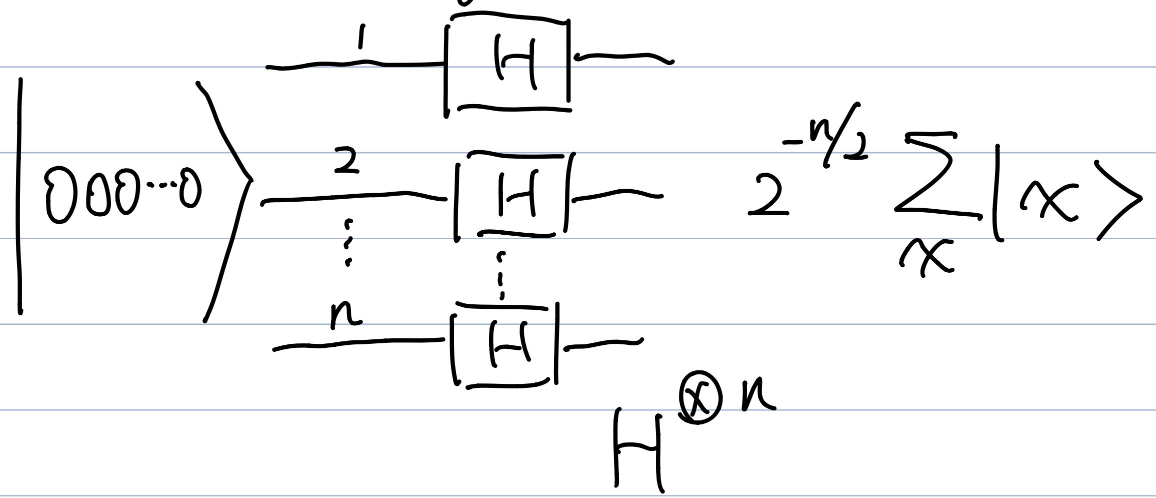
$$\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)=\frac{1}{2}\left(|00\rangle+|01\rangle+|10\rangle+|11\rangle\right)$$

and $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ can also be generated easily using Hadamard gates.

We use "$H^{\otimes 2}$" to denote two H gates working parallelly. The result of performing the H transformation on n qubits initially in all $|0\rangle$ state is

$$2^{-n/2}\sum_x |x\rangle \text{ and } x\in\{0,1\}^n$$

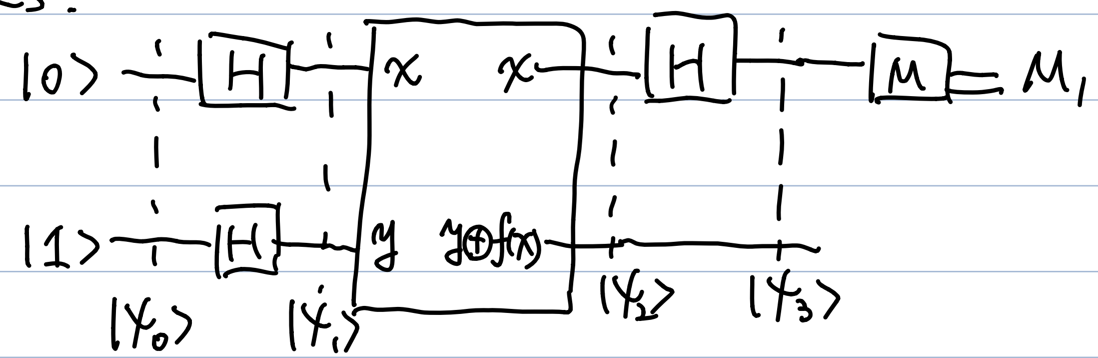
The corresponding circuit is



So far, we express the idea of how to use super-position to do parallel computing, a problem we haven't addressed is how to get the result respectively? Since if we measure the output, we will only have one random result. No worry. we can play some tricks on the input y.

Deutsch's Algorithm

Deutsch's algorithm combines quantum parallelism with quantum interference. Now, let's see how the algorithm works.



For the circuit showing above, inputs are $|0\rangle$ & $|1\rangle$

so $|\psi_0\rangle = |0\rangle|1\rangle$.

After the Hadamard gates,

$$|\psi_1\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}} \cdot \frac{|0\rangle-|1\rangle}{\sqrt{2}} = \frac{1}{2}\left(|00\rangle-|01\rangle+|10\rangle-|11\rangle\right)$$

$$|\psi_2\rangle = \frac{1}{2}\Big(|0\rangle(|0 \oplus f(0)\rangle) - |0\rangle(|1 \oplus f(0)\rangle) + |1\rangle(|0 \oplus f(1)\rangle) - |1\rangle(|1 \oplus f(1)\rangle) \Big)$$

$$= \frac{1}{2}\Big(|0\rangle|f(0)\rangle - |0\rangle|\overline{f(0)}\rangle$$
$$+ |1\rangle|f(1)\rangle - |1\rangle|\overline{f(1)}\rangle \Big)$$

If $f(0) = f(1)$, then $\overline{f}(0) = \overline{f}(1)$

$$|\psi_2\rangle = \frac{1}{2}(|0\rangle + |1\rangle)\big(|f(0)\rangle - |\overline{f(0)}\rangle\big)$$

$f(0) \in \{0, 1\}$.

So, $|f(0)\rangle - |\overline{f(0)}\rangle = \begin{cases} |0\rangle - |1\rangle & \text{if } f(0) = 0 \\ |1\rangle - |0\rangle & \text{if } f(0) = 1 \end{cases}$

So $|\psi_2\rangle = (-1)^{f(0)} \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)$

Then $|\psi_3\rangle = (-1)^{f(0)} \frac{1}{\sqrt{2}} |0\rangle(|0\rangle - |1\rangle)$

If $f(0) = \overline{f(1)}$, then $f(1) = \overline{f}(0)$

$$|\psi_2\rangle = \frac{1}{2}(|0\rangle - |1\rangle)(|f(0)\rangle - |f(\overline{0})\rangle)$$
$$= (-1)^{f(0)} \frac{1}{2}(|0\rangle - |1\rangle)(|0\rangle - |1\rangle)$$

Then $|\psi_3\rangle = (-1)^{f(0)} \frac{1}{\sqrt{2}} |1\rangle(|0\rangle - |1\rangle)$

To sum up

$$|\psi_3\rangle = \frac{(-1)^{f_0}}{\sqrt{2}} |f(0) \oplus f(1)\rangle (|0\rangle - |1\rangle)$$

By measuring the first qubit, $M_1 = 0 \Rightarrow f(0) = f(1)$
$1 \Rightarrow f(0) = 1 - f(1)$

This phenomenon is "quantum interference". By doing 1 operation, we can measure the result from : two function values. This is different from conventional computer.

Now, let's state a more generalized algorithm

Deutsch-Jozsa Algorithm

Deutsch-Jozsa Algorithm is designed to solve Deutsch problem:

① Alice randomly chooses a number x from $0 \sim 2^{n-1}$ and sends it to Bob.

② Bob sticks to either f_1 or f_2 randomly to x and returns the result. f_1 is a function that always returns a constant: $f_1(x) = C$.

f_2 is a function that for exactly half of the x it returns 1, and for another half returns 0.

Question: How fast can Alice know whether Bob chooses f_1 or f_2 to process the x?

1. Naive method.

Alice tries at most $\frac{2^n}{2}+1 = 2^{n-1}+1$ times to know whether it's f_1 or f_2.

2. Probabilistic method.

Let $S = i$ represents the event that trying i inputs and the results are the same.

The uncertainty $P(\text{"}f_2\text{"})$ is

$$P(\text{"}f_2\text{"} \mid S=1) = \frac{1}{2}$$

$$P(\text{"}f_2\text{"} \mid S=2) = \frac{P(S=2 \mid \text{"}f_2\text{"})\, P(\text{"}f_2\text{"})}{P(S=2)}$$

$$P(S=2 \mid \text{"}f_2\text{"}) = \left(\frac{1}{2}\right)^S \cdot \underset{\substack{\uparrow \\ \text{either 0 or 1}}}{\times\, 2} = 2^{1-S} = \frac{1}{2}$$

$$P(\text{"}f_2\text{"}) = \frac{1}{2}$$

$$\begin{aligned} P(S=2) &= P(S=2 \mid \text{"}f_2\text{"}) \cdot P(\text{"}f_2\text{"}) + P(S=2 \mid \text{"}f_1\text{"}) \cdot P(\text{"}f_1\text{"}) \\ &= 2^{1-S} \cdot \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{2} \\ &= \frac{1}{4}(1 + 2^{-S}) = \frac{5}{16} \end{aligned}$$

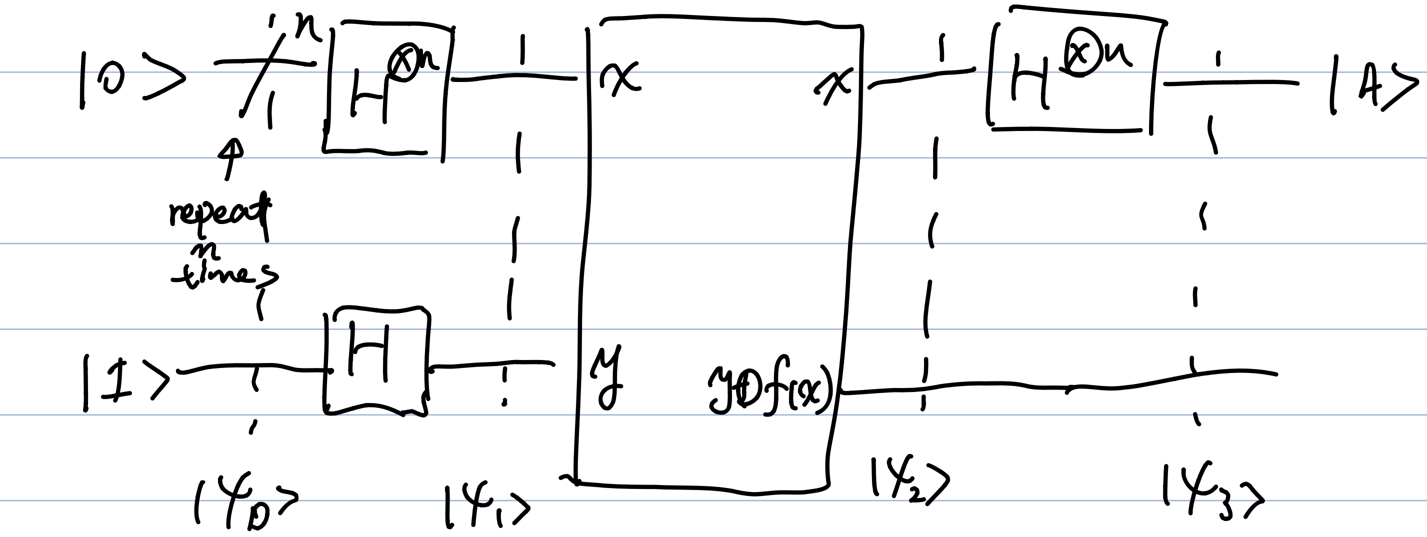
so $P(\text{"}f_2\text{"} \mid S=2) = \dfrac{1/4}{5/16} = \dfrac{4}{5}$

⋮

$$P(\text{"}f_2\text{"} \mid S=s) = \frac{2^{1-S} \cdot \frac{1}{2}}{\frac{1}{2} \cdot \frac{1}{2} \cdot (1 + 2^{-S})} = \frac{4}{2^S + 1}$$

3. Quantum Algorithm.

Alice will send Bob quantum bits in superposition mode once and get the result.



$$|\psi_0\rangle = |\underbrace{000\cdots\cdots 0}_{n \text{ "0s"}}\rangle \otimes |1\rangle$$

$$= |0\rangle^{\otimes n} |1\rangle$$

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

$$= \frac{1}{\sqrt{2^{n+1}}} \left(\sum_x |x0\rangle - \sum_x |x1\rangle \right)$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2^{n+1}}} \left(\sum_x |x, \underbrace{f(x) \oplus 0}_{f(x)}\rangle - \sum_x |x, \underbrace{f(x) \oplus 1}_{\overline{f(x)}}\rangle \right)$$

$$= \frac{1}{\sqrt{2^{n+1}}} \sum_x |x\rangle \begin{cases} |0\rangle - |1\rangle & \text{if } f(x) = 0 \\ |1\rangle - |0\rangle & \text{if } f(x) = 1 \end{cases}$$

$$= \frac{1}{\sqrt{2^{n+1}}} \sum_x |x\rangle \cdot (-1)^{f(x)} (|0\rangle - |1\rangle)$$

The result of $f(x)$ now sits on the index position.

To interact with f(x). Alice passes the $|x\rangle$ to another Hadamard gate

$$H^{\otimes n}|x_1, x_2, \cdots x_n\rangle = \frac{\sum_{z_1 \cdots z_n \in \{0,1\}} (-1)^{x^T \cdot z} |z\rangle}{\sqrt{2^n}}$$

where $|z\rangle = |z_1, z_2, \cdots, z_n\rangle$

$$|\psi_3\rangle = \frac{1}{\sqrt{2^{n+1}}} \cdot \frac{1}{\sqrt{2^n}} \sum_x \sum_z (-1)^{x^T z + f(x)} |z\rangle(|0\rangle - |1\rangle)$$

$$= \left(\frac{1}{2^n} \sum_x \sum_z (-1)^{x^T z + f(x)} |z\rangle\right) \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

The amplitude for state $|0\rangle^{\otimes n}$ is (when $z = 0$)

$$\frac{1}{2^n} \sum_x (-1)^{x^T \cdot 0 + f(x)} |0\rangle^{\otimes n} \quad --- (*)$$

If $f(x)$ is constant C, then

$$(*) = \frac{1}{2^n} \sum_x (-1)^c |0\rangle^{\otimes n} = (-1)^c |0\rangle^{\otimes n}$$

either -1 or $+1$.

$$\text{so } |\psi_3\rangle = \underbrace{\left((-1)^c |0\rangle^{\otimes n} + \text{other state}\right)}_{(|A\rangle)} \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

Since a quantum state $|A\rangle$ must have amplitato 1, and we already find out a state that has amplitute 1, so "other state" $= \phi$

$\Rightarrow$ if $f(x)$ is constant, $|A\rangle$ must be $|0\rangle^{\otimes n}$.

If $f(x)$ is balanced with half of the chance to be 0 and another half to be +1, then the amplitute for $|z\rangle = |0\rangle^{\otimes n}$ is

$$(*) = \frac{1}{2^n} \sum_x (-1)^{f(x)} \quad |0\rangle^{\otimes n}$$

$$= \frac{1}{2^n}\left(\sum_{x:f(x)=1} (-1)\,|0\rangle^{\otimes n} + \sum_{x:f(x)=0} (-1)^0 \; |0\rangle^{\otimes n} \right)$$

$$= 0$$

So, it's impossible to see $|0\rangle^{\otimes n}$

$\Rightarrow$ if $f(x)$ is balanced, $|A\rangle$ must NOT be $|0\rangle^{\otimes n}$

$\Rightarrow$ if Alice measures $|A\rangle$ and see

$$\begin{cases} |0\rangle^{\otimes n} & \text{using constant function } f_1 \\ \text{o.w.} & f_2. \end{cases}$$