Universal set of gates = $\{H, S, T, CNOT\}$

INPUT STATE n qubits

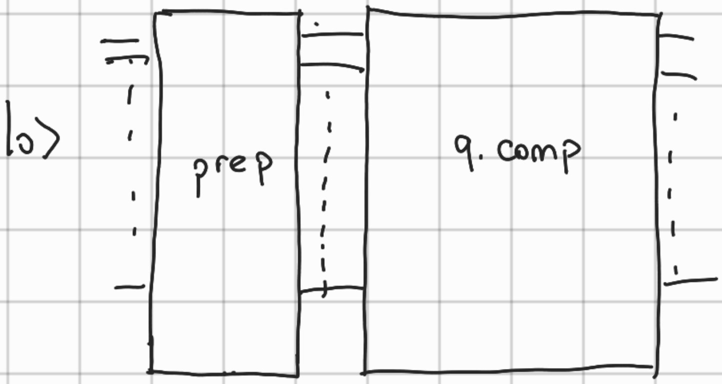
$$|\psi_{in}\rangle = \sum_{j=0}^{2^n-1} \alpha_i |j\rangle$$

Task: start from e.g. $|00\ldots0\rangle$ end with $|\psi_{in}\rangle$

Arbitrary $\hat{U} \Rightarrow$ defining $\forall |j\rangle$ $\hat{U}|j\rangle = |\varphi_j\rangle$

Still exponentially complex (mn)! (1607.05256)

If we restrict to "simple" input $|\psi_{in}\rangle$ then we may start with $|0\ldots0\rangle$ and "prepare" $|\psi_{in}\rangle$ through a q. circuit.

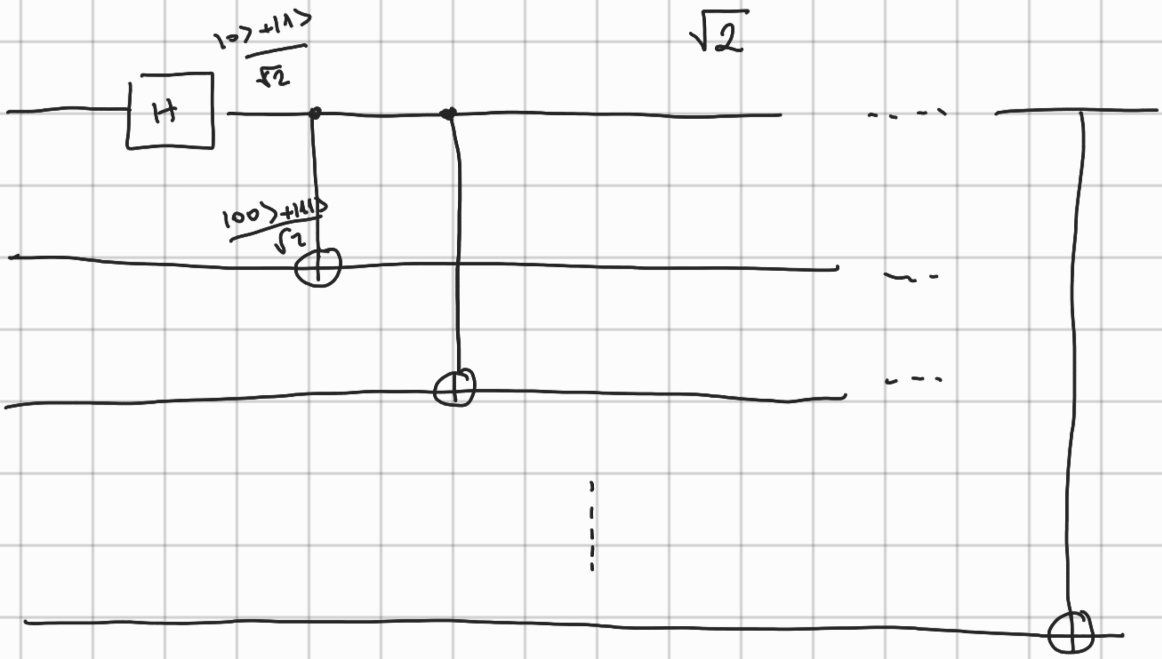


Example: $|\psi_{in}\rangle = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} |j\rangle$

$|\psi_{in}\rangle = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)^{\otimes n}$

It is not entangled.

Example $|\psi_{in}\rangle = \frac{|000\ldots 0\rangle + |11\ldots 1\rangle}{\sqrt{2}}$



Readout

Output state of a QC is $|\psi_{out}\rangle$ "measure in the comp. basis" e.g. measure Z on one qubit.

$$|\Psi_{out}\rangle \xrightarrow{\text{meas } Z} |0\rangle \quad \text{(outcome } +1)$$

$$\xrightarrow{\text{meas. } Z} |1\rangle \quad \text{(outcome } -1)$$

n qubits

Measure Z on the 1^{st} qubit

$$|\Psi_{out}\rangle \longrightarrow |0\rangle \otimes |\tilde{\varphi}\rangle$$

or

$$|1\rangle \otimes |\tilde{\varphi}\rangle$$

Measure Z on the 2^{nd} qubit

$$|\Psi_{out}\rangle = \sum_{j=0}^{2^n-1} \alpha_j |j\rangle$$

A QC can measure (proj) $|j\rangle$ with prob. $|\alpha_j|^2$

What if measure $\hat{O}$ observable ?

$$\hat{O} = \sum_{j=0}^{2^n-1} o_j |\varphi_j\rangle\langle\varphi_j|$$

? Degenerate eigenvectors

$o_j \in \mathbb{R}$ eigenvalues

$|\varphi_j\rangle$ eigenvectors

$$\hat{O}\,|\varphi_j\rangle = o_j\,|\varphi_j\rangle$$

Take the Unitary $\hat{U}$ that diagonalize $\hat{O}$

$$\hat{U}\hat{O}\hat{U}^{+} = \sum_{j=0}^{2^n-1} o_j\,|j\rangle\langle j|$$

$$|j\rangle = \hat{U}|\varphi_j\rangle \qquad \forall j = 0, \ldots\ldots, 2^n-1$$

Measuring $\hat{U}\hat{O}\hat{U}^{-1}$ is same as measuring $\hat{O}$ but on the computational basis.

$$|\Psi_{out}\rangle = \sum_{j=0}^{2^n-1} \beta_j\,|\varphi_j\rangle$$

Apply U^{+} to $|\Psi_{out}\rangle$

$$U^{+}|\Psi_{out}\rangle = \sum \beta_j\, U^{+}|j\rangle$$

Then Apply U

$$\underbrace{UU^{+}}_{\mathbb{I}}|\Psi_{out}\rangle = \sum \beta_j\,\underbrace{UU^{+}}_{\mathbb{I}}|j\rangle$$

$$|\Psi_{out}\rangle = \sum \beta_j\,|j\rangle$$

obtain $|j\rangle$ with prob. $|\beta_j|^2$

Measuring $\hat{O} = \sum_j o_j |\varphi_j\rangle\langle\varphi_j|$

$$= \sum_j o_j \, U|j\rangle\langle j| U^\dagger$$

is equivalent to meas. on the comp. basis

after applying $|\tilde{\Psi}_{out}\rangle = \hat{U}|\Psi_{out}\rangle$

Bitwise Measurement (on the computational basis)

Example 2-qubits

$$|\Psi_{out}\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

Measuring 1st qubit:

$$\hat{M}_0 = |0\rangle\langle 0| \otimes \mathbb{I}$$

$$\hat{M}_1 = |1\rangle\langle 1| \otimes \mathbb{I}$$

$$|\tilde{\Psi}_{out}\rangle = \frac{\hat{M}_0 |\Psi_{out}\rangle}{\|\cdot\|}$$

$$|\tilde{\Psi}_{out}\rangle = \frac{\hat{M}_0 |\Psi_{out}\rangle}{\| \hat{M}_0 |\Psi_{out}\rangle \|} = \frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}$$

$$P_1(0) = \langle \Psi_{out} | \hat{M}_0 | \Psi_{out}\rangle = |\alpha_{00}|^2 + |\alpha_{01}|^2$$

Measure qubit 2 on $|\tilde{\Psi}_{out}\rangle$ suppose I get $|1\rangle$

$$|\tilde{\tilde{\Psi}}_{out}\rangle = |01\rangle$$

$$P(01) = \frac{|\alpha_{01}|^2}{|\alpha_{00}|^2 + |\alpha_{01}|^2}$$

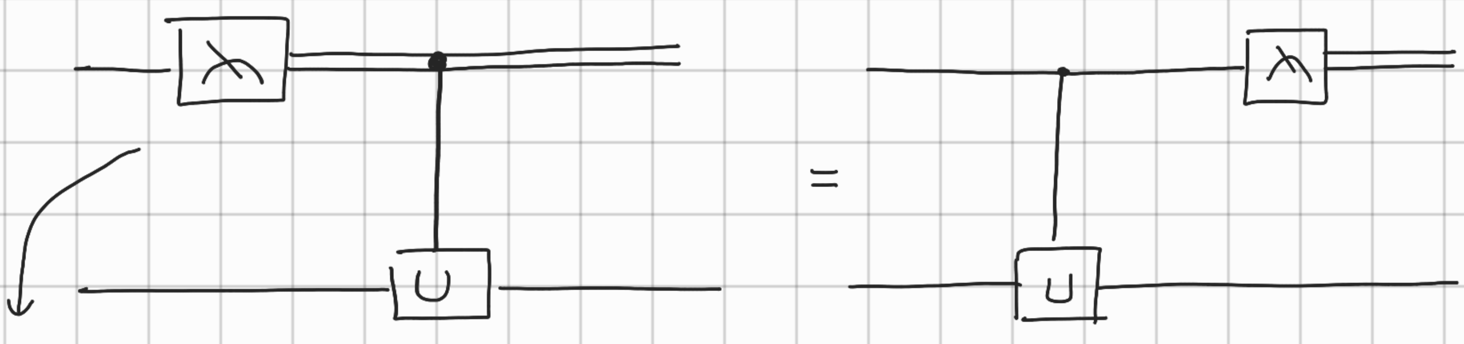
Overall prob. of meas. $|01\rangle$ on $|\Psi_{out}\rangle$?

$$\left(\underset{|\Psi_{out}\rangle}{p(01)} = |\alpha_{01}|^2 \right)$$

$$\underset{1,|\Psi_{out}\rangle}{p(0)} \cdot \underset{|\tilde{\Psi}_{out}\rangle}{p(01)} = \left(|\alpha_{00}|^2 + |\alpha_{01}|^2 \right) \times \frac{|\alpha_{01}|^2}{|\alpha_{00}|^2 + |\alpha_{01}|^2}$$

$$= |\alpha_{01}|^2 \quad //$$

Principle of deferred measurement



Measuring in the middle
not in the end

Any measurement on the comp. basis can be

deferred to the end of the circuit

Principle of implicit measurement

Not measuring some qubits at the end of the comp., is equivalent to measuring them and not knowing the result.

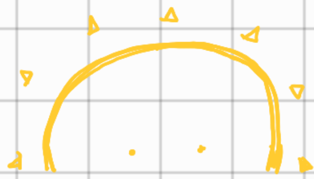
Deutsch's Algorithm → 1985

Task given an (unknown) function

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

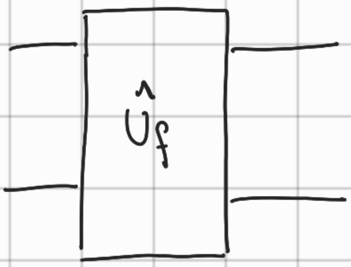
Decide if f is degenerate

$\Rightarrow$ if $f(0) = f(1)$?

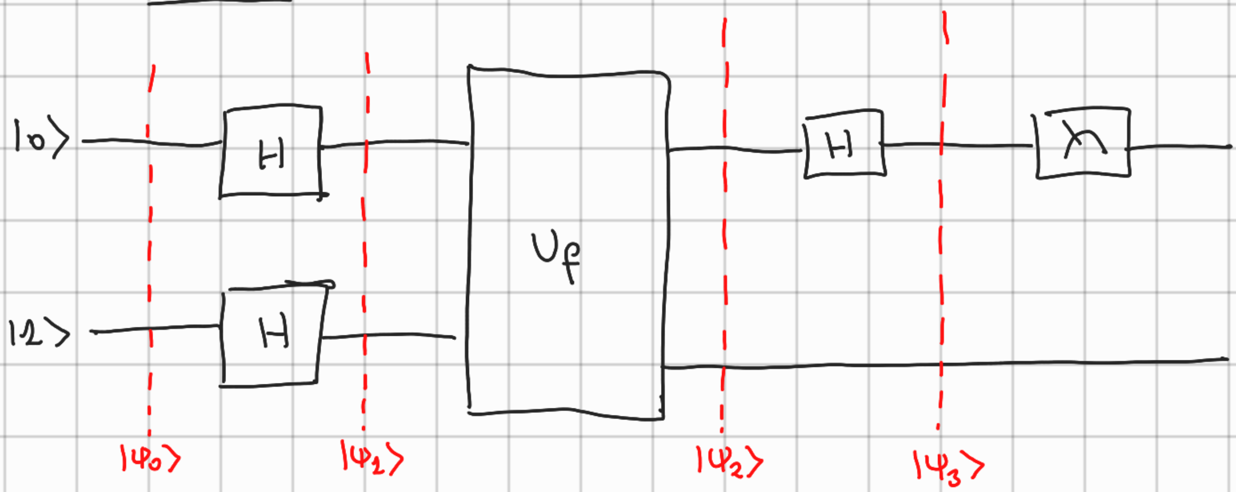


"Oracle"

$$\hat{U}_f : |x\rangle|y\rangle \longrightarrow |x\rangle\,|y \oplus f(x)\rangle$$



flips qubit 2 if f(qubit) = 1



$$|\psi_0\rangle = |01\rangle$$

$$|\psi_1\rangle = \frac{1}{2}\underbrace{(|0\rangle + |1\rangle)}_{\nearrow 1^{st}\text{ qubit}} \otimes \underbrace{(|0\rangle - |1\rangle)}_{\nearrow 2^{nd}\text{ qubit}}$$

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

$$|\psi_3\rangle = \frac{1}{2\sqrt{2}}\left(\left[(-1)^{f(0)} + (-1)^{f(1)} \right] |0\rangle + \left[(-1)^{f(0)} - (-1)^{f(1)} \right] |1\rangle \right) \left(|0\rangle - |1\rangle \right)$$

if $f(0) = f(1) \longrightarrow$ output 1^{st} qubit $= 0$

$f(0) \neq f(1) \longrightarrow$ output 1^{st} qubit $= 1$