Quantum Algorithms, Spring 2022: Lecture 4 Scribe

Debanil Chowdhury, Rishabh Khanna

February 18, 2022

1 Recap of previous lecture

- Postulates of quantum mechanics.
  1. Any isolated physical system is given by its state vector which is a unit vector belonging to a Hilbert Space corresponding to the system's state space.
  2. Evolution of a closed quantum system is given by a unitary transformation.
  3. To ensure that the evolution maintains the state vector to be a unit vector, the operators preserve trace. Trace preserving operators convert a mutually orthonormal set of vectors to another mutually orthonormal set of vectors.
  4. The state space of a composite physical system is the tensor product of the state spaces of the component systems. There are states in this composite physical system that can not be factorized into states of the individual systems, these states are called entangled states.
  5. Quantum measurements are described by a collection of measurement operators acting on the state space of the system.
- Circuit Model of Quantum Computation
  1. Initialization: $|\psi_0\rangle = |0\rangle^{\otimes n}$
  2. Evolution: $|\psi_t\rangle = U_t U_{t-1} \dots U_1 |\psi_0\rangle$
  3. Measurement: Typically we perform measurements in a computational basis.
- A classical computer computes boolean functions with a sequence of logic gates, some of which are universal.
- According to Landauer's principle computation has an energy cost.
- This motivated the study of reversible computing.

2 Reversible Computing

2.1 Fredkin Gate

- Output of remaining two bits depends on control bit.
- Truth table (C is control bit) -

C	A	B	C	A'	B'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	1	0
1	1	0	1	0	1
1	1	1	1	1	1

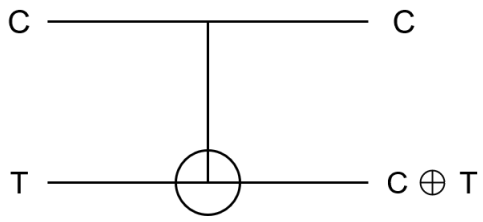
- Fredkin gates are universal

2.2 CNOT Gate

- 2 bit input and 2 bit output (Control bit and Target bit).
- If C is 0 then T is not flipped. If C is 1 then T is flipped.
- Truth table (C is control bit and T is Target bit) -

C	T	C	T'
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

- Representation -

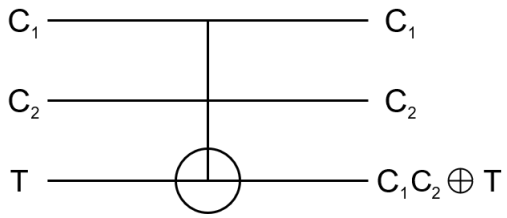


2.3 Toffoli Gate

- 3 bit input and 3 bit output (2 Control bits and a Target bit).
- T is flipped only when both control bits are 1.
- Truth table (C is control bit and T is target bit) -

C_1	C_2	T	C_1	C_2	T'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

- Representation -



2.4 Garbage bit problem

- Reversible gates have a disadvantage - along with desired output we also get useless garbage output.
- In quantum computation, this garbage output can entangle with desired output, hence interfering with computation and producing erroneous result.
- Hence in every computation procedure, we should rectify the issue with a procedure called uncomputation that removes garbage output at the expense of some energy dissipation.

2.5 Uncomputation

- Suppose we have a reversible circuit C_f that computes f. Lets start with 4 registers.

$$(x, 0, 0, y) \longrightarrow (x, f(x), g(x), y)$$

- Apply CNOT gate on registers 2 and 4.

$$(x, f(x), g(x), y) \longrightarrow (x, f(x), g(x), y \oplus f(x))$$

  with this we have copied outcome of second register to fourth register.

- Apply C_f^{-1}. (This is uncomputation).

$$(x, f(x), g(x), y \oplus f(x)) \longrightarrow (x, 0, 0, y \oplus f(x))$$

- This entire process C_f, CNOT, C_f^{-1} is typically known as a reversible circuit for f.

$$(x, y) \longrightarrow (x, y \oplus f(x))$$

- This way, in quantum computing we can uncompute and detangle garbage bits.

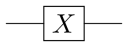
3 Quantum Gates

In the circuit model of quantum computing, quantum gates are unitary operators on quantum states. They have to preserve the norm as they map quantum states to other quantum states.

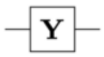
3.1 Single qubit unitary gates

3.1.1 Pauli gates

$X = \sigma_X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{matrix} X|0\rangle = |1\rangle \\ X|1\rangle = |0\rangle \end{matrix}$



$Y = \sigma_X = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \begin{matrix} Y|0\rangle = i|1\rangle \\ Y|1\rangle = -i|0\rangle \end{matrix}$



$Z = \sigma_X = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{matrix} Z|0\rangle = |0\rangle \\ Z|1\rangle = -|1\rangle \end{matrix}$

- $X^2 = Y^2 = Z^2 = 1$

3.1.2 Hadamard gate

$Z = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{matrix} H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{matrix}$

3.1.3 Phase gate

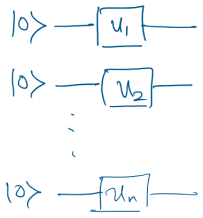
$R_\phi = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix} \begin{matrix} R_\phi|0\rangle = |0\rangle \\ R_\phi|1\rangle = e^{i\phi}|1\rangle \end{matrix}$

$R_{\pi/4} = T\ gate = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$

$R_{\pi/2} = S\ gate = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$

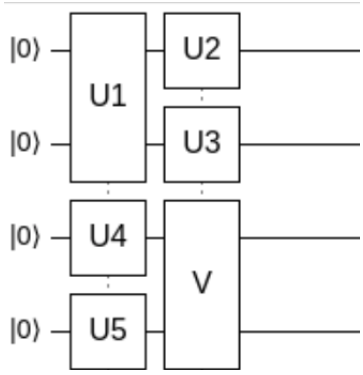
- Pauli matrices give rise to 3 useful unitary matrices when they are exponentialiated (Rotation operations about $\hat{x}$, $\hat{y}$ and $\hat{z}$ axis).
  $R_X(\theta) = e^{-iX\theta} = cos(\theta)1 - isin(\theta)X$
  $R_Y(\theta) = e^{-iY\theta} = cos(\theta)1 - isin(\theta)Y$
  $R_Z(\theta) = e^{-iZ\theta} = cos(\theta)1 - isin(\theta)Z$

- Suppose $\hat{n}$ is a unit vector: (n_x, n_y, n_z). $\hat{\sigma} = (\sigma_X, \sigma_Y, \sigma_Z)$
  $R_{\hat{n}}(\theta) = e^{-i\hat{n}\hat{\sigma}\theta} == cos(\theta)1 - isin(\theta)\hat{n}\hat{\sigma} = cos(\theta)1 - isin(\theta)(n_X\sigma_X + n_y\sigma_Y + n_Z\sigma_Z)$
- $U = e^{i\phi}R_X(\alpha)R_Y(\beta)R_Z(\gamma)$
-
  - Tensor Products:
    If gates are applied to different parts of the register.



    $|\phi\rangle = (U_1 \otimes U_2 ... \otimes U_n)\,|0..0\rangle$
    If $\forall j, U_j = U$
    $|\phi\rangle = U^{\otimes n}\,|0..0\rangle$
  - Ordinary Matrix Products:
    If gates are applied sequentially to the same register.

    $|\phi\rangle = U_n U_{n-1} ... U_1\,|0\rangle$
- Typically a quantum circuit requires both



3.1.4 Hadamard gate

$H\,|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle$
$H\,|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle$
$H\,|x\rangle = \frac{1}{\sqrt{2}}\sum_{Z\in\{0,1\}}(-1)^{xZ}\,|Z\rangle$

What about $H_{\otimes n}\,|0..0\rangle$,

$$H_{\otimes n}\,|0..0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)..\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$
$$= \frac{1}{\sqrt{2^n}}\sum_{j\in\{0,1\}^n}|j\rangle$$

More Generally: $|i\rangle = |i_1 i_2 .. i_n\rangle$ and $|j\rangle = |j_1 j_2 .. j_n\rangle$

$$H^{\otimes n} |i\rangle = \frac{1}{\sqrt{2^n}} * \sum_{j \in \{0,1\}^n} (-1)^{i*j} |j\rangle$$
$$i * j = \sum_k i_k j_k$$

$$\begin{aligned} H^{\otimes n} |i\rangle &= H^{\otimes n} |i_1 i_2 .. i_n\rangle \\ &= (H |i_1\rangle)(H |i_2\rangle)..(H |i_n\rangle) \\ &= \frac{1}{\sqrt{2^n}} * (\sum_{j_1 \in \{0,1\}} (-1)^{i_1 j 1} |j_1\rangle) * (\sum_{j_2 \in \{0,1\}} (-1)^{i_2 j 2} |j_2\rangle)..(\sum_{j_n \in \{0,1\}} (-1)^{i_n j n} |j_n\rangle) \\ &= \frac{1}{\sqrt{2^n}} \sum_{j_1, j_2 .. j_n \in \{0,1\}} (-1)^{i_1 j_1 + i_2 j_2 .. + i_n j_n} |j_1 .. j_n\rangle \\ &= \frac{1}{\sqrt{2^n}} \sum_{j \in \{0,1\}^n} (-1)^{i*j} |j\rangle \end{aligned}$$

- $H^2 = 1$,

$$\begin{aligned} H^{\otimes n} * H^{\otimes n} &= 1 \\ &= (H \otimes H \otimes ..H)(H \otimes H \otimes ..H) \\ &= (H^2 \otimes H^2 \otimes ..H^2) \\ &= 1 \end{aligned}$$

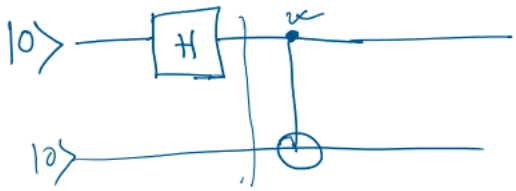
- For any unitary circuit U it is easy to find a circuit for U^{-1}. It's just $U^\dagger$. $U = U_1 U_2 .. U_n$ then $U^{-1} = U^\dagger = U_n^\dagger U_{n-1}^\dagger .. U_1^\dagger$

3.2 2-qubit gates

3.2.1 CNOT gate

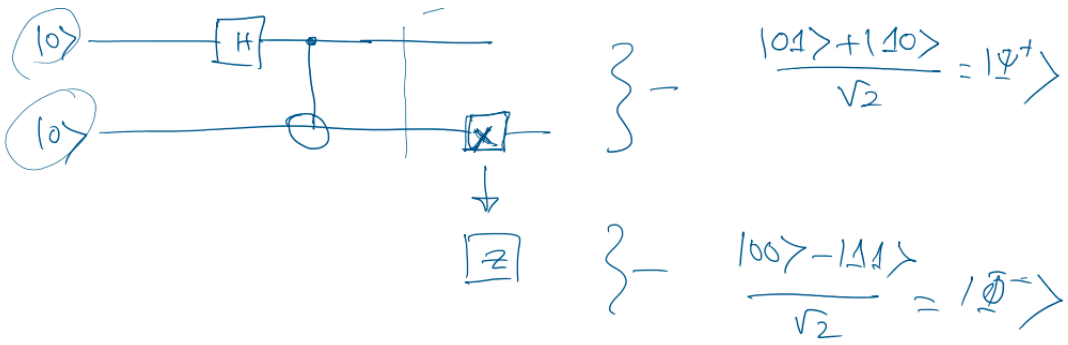
$|00\rangle \longmapsto |00\rangle$
$|01\rangle \longmapsto |01\rangle$
$|10\rangle \longmapsto |11\rangle$
$|11\rangle \longmapsto |10\rangle$

$$\hat{U} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$



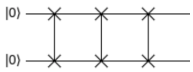
$|00\rangle \longmapsto^{\hat{H} \otimes 1} (\frac{|0\rangle + |1\rangle}{\sqrt{2}}) |0\rangle \longmapsto^{CNOT} \frac{|00\rangle + |11\rangle}{\sqrt{2}} = |\Phi^{dagger}\rangle$

Controlled Operations are entangling



3.2.2 SWAP gate

- $S\,|a,b\rangle = |b,a\rangle$



$|a,b\rangle \longmapsto^{CNOT_{a,2}} |a,a,\oplus b\rangle \longmapsto^{CNOT_{2,1}} |a\oplus(a\oplus),a\oplus b\rangle = |b,a\oplus b\rangle$
$|b,a\oplus b\rangle \longmapsto^{CNOT_{1,2}} |b,(a\oplus b)\oplus b\rangle = |b,a\rangle$