Task 1: Introduction to Quantum Computing

Summarizing the first 3 weeks of lecture*- CMPT409 - SFU

George Watkins

July 17, 2020

Basic Physical Concepts

Quantum mechanical entities exhibit both particle and wave like behaviour, the wave like one could enable faster than classical computations, by manipulating the amplitudes of the wave model to obtain useful interference patterns. The finding of these patterns is the "Software Problem" in our course.

Interactions in quantum mechanics are probabilistic, and systems of entities are understood by *wave functions*, which only offer a probabilistic description of the state of the system, until measurement. Once an observable quantity of a system is measured (such as velocity, spin, charge...), the wave function is said to have "collapsed" into a single state. However the measurement only yields certain features of the system, thus quantum states cannot be directly converted to classical states because of it (No-Teleportation theorem).To make useful calculations, quantum computers often have run the same circuit many times, so that that the desired properties of the underlying quantum state, which contain the useful result, can be estimated from the measurements.

As well as the nature of quantum computation being probabilistic, there is further uncertainty in the results, caused by noise. Qubits may undesirably interact with each other and the environment, which causes unreliable results. This is the problem of decohrence, considered one of the biggest challenges of the current NISQ (Noisy Intermediate-Scale Quantum) era, the "hardware problem" in our course. [3]

Thermodynamics and Quantum Computing

Information can be seen as a physical concept, closely related to entropy. Similarly to thermodynamic entropy, Shannon formulated a concept of entropy for information [8]. But where the link becomes more evident is in Maxwell's Demon's, whom, if information was not related to energy, would be able to violate the second law of thermodynamics and create a perpetual machine. The connection to information is that the demon needs to know about particles' position and velocity. This connection between information and physical entropy was formalized by Landauer, formulating that to erase one bit of information a certain amount of energy is required [5]. Quantum computations as a sequence of applications of quantum gates is fully reversible since quantum gates are. Therefore

*With Dr. Pearce's permission to make the limit of 5 pages per task, see end of file.

they erase no information, this could allow quantum computers to be significantly more efficient, though there still are theoretical limitations to quantum information processing [4].

Theory of Quantum Computations

Quantum computing is in theory at least as powerful as classical computing as quantum manipulations can replicate the behaviour of a NAND logic gate from which a universal classical computer can be constructed [2]. But the advantage of quantum computing comes from the fact that quantum computations operate on data structures more complex than bits nearly instantaneously.

In complexity theory, one of the most interesting classes of problems, related to quantum computing is BQP, Bounded-error Quantum Polynomial-time decision problems. It is an open question what the relation between BQP and NP is, but many believe no containment in either direction[1]. The hope is to find useful problems in BQP that are not in P. Integer factoring is good a candidate, which can be done using Shor's quantum algorithm. This algorithm happens to be of very much interest because of it's implications in Cryptography.

Mathematical Foundations

In Quantum Computing Dirac notation is often used to represent vectors in $\mathbb{C}^n$:

$$|\phi\rangle = \begin{bmatrix} \phi_1 \\ \phi_2 \\ \vdots \\ \phi_n \end{bmatrix} \qquad \langle\phi| = (|\phi\rangle^T)^* = \begin{bmatrix} \phi_1^* & \phi_2^* & \cdots & \phi_n^* \end{bmatrix}$$

Where the star denotes the complex conjugate. $\langle\phi|\psi\rangle$ represents the inner product given by a matrix multiplication as follows:

$$\langle\phi|\psi\rangle = \begin{bmatrix} \phi_1^* & \phi_2^* & \cdots & \phi_n^* \end{bmatrix} \begin{bmatrix} \psi_1 \\ \psi_2 \\ \vdots \\ \psi_n \end{bmatrix} = \phi_1^*\psi_1 + \phi_2^*\psi_2 + \cdots + \phi_n^*\psi_n$$

and $|\phi\psi\rangle$ or $|\phi\rangle \otimes |\psi\rangle$ the tensor product, which for $\phi \in \mathbb{C}^n$ and $\psi \in \mathbb{C}^m$ is a vector in $\mathbb{C}^{nm}$ most easily defined in terms of its elements:

$$(|\phi\psi\rangle)_{im+j} = \phi_i\psi_j \qquad \text{for } i = 1, \ldots, n \text{ and } j = 1, \ldots, m.$$

One can show that the above defined operation of inner product makes $\mathbb{C}^n$ a inner product space with respect to it. Further we can define a norm over $\mathbb{C}^n$ as $|\,|\psi\rangle\,| = \sqrt{\langle\psi|\psi\rangle}$ (the L^2-norm), and then it can also be shown that the function $d(|x\rangle, |y\rangle) = |\,|x\rangle - |y\rangle\,|$ is a complete metric for $\mathbb{C}^n$. $\mathbb{C}^n$, with the $< \cdot|\cdot >$ inner product and the distance d, satisfies the definition of Hilbert space, which allows us to compute limits and derivatives.

Another useful concept it that of a *Hermitian operator*, which is a matrix $\mathbf{M}$ that coincides with its complex transpose $\mathbf{M}^\dagger = (\mathbf{M}^T)^*$. Hermitian operators have real eigenvalues.

Qubits

The most basic computational unit in quantum computing is a *qubit*. While we cannot read directly the state of a qubit (as shown in the No-Teleportation Theorem), we can perform a measurement on them, from which we can read either a "1" or a "0". These are called the basis states of the qubit and are represented as orthogonal vectors:

$$|0\rangle = \begin{bmatrix}1\\0\end{bmatrix} \qquad |1\rangle = \begin{bmatrix}0\\1\end{bmatrix}$$

All quibit states are represented as a normalized vector in $\mathbb{C}^2$. The two complex components of a qubit state are called amplitudes (the name derives from the wave nature). A qubit state $|\psi\rangle$ that is not exactly in the the basis states $|1\rangle$ and $|0\rangle$ is said to be in a superposition of the two basis states. Then $|\psi\rangle$ is linear combination of the reference states:

$$|\psi\rangle = \begin{bmatrix}\alpha\\\beta\end{bmatrix} = \alpha\,|0\rangle + \beta\,|1\rangle$$

When a qubit is measured it probabilistically collapses to one of it's basis values. The proportion of times $|\psi\rangle$ collapses to $|0\rangle$ or $|1\rangle$ is given by Born's rule[6], which applied to our measurement on qubits states, says that the probability of measuring "0" is $|\alpha|^2$ and of measuring "1" is $|\beta|^2$. The normalization requirement on qubit states implies that $|\alpha|^2 + |\beta|^2 = 1$, satisfying the laws of probability.

The states $|0\rangle$ and $|1\rangle$ are pure states, all other possible values of $|\psi\rangle$ are entangled states. The above formulation of born rule is that specific to qubits. It's a special case of the quantum mechanical formulation of the rule in which basis states are the eigenvectors of a Hermitian operator $\mathbf{M}$, and the measured values are the corresponding eigenvalues[10] which are always real. Then the probability of a specific measurement for eigenvalue λ (corresponding to eigenvector $|\lambda\rangle$) is $P(\lambda) = |\,\langle \mathbf{M}|\lambda\rangle\,|^2$. The Hermitian matrix for the observables is that with basis states $|0\rangle$ and $|1\rangle$ as eigenvectors:

$$\mathbf{B} = \begin{bmatrix}1 & 0\\0 & -1\end{bmatrix}$$

And then the probability of measuring "0" from a qubit state $|\psi\rangle$ is $P(0) = |\,\langle 0|\psi\rangle\,|^2 = |\alpha|^2$.

Superposition can be seen as having an amplitude for each possible measurement state. This concept generalizes to multiple qubits.

Qubit registers

Multiple qubits can form a register of a Quantum Computer. An n-bit Quantum Register can have multiple qubits in a superposition of the basis states at the same time, resulting in as many basis states as the 2^n combinations of basis states of n qubits. Each one of the 2^n basis states of a quantum register is associated with a complex amplitude. Thus the state of a qubit register is described by a normalized complex vector, where each entry of this vector corresponds to the amplitude of a basis state. Therefore we express the sate of an n bit qubit register as a normalized vector in $\mathbb{C}^{2^n}$.

Next we arrange the entries in this vector to correspond to binary strings of basis states. We can do so neatly using the tensor product. For example 3 qubit register's qubits were measured as $|0\rangle$, $|1\rangle$ and $|1\rangle$, the tensor product of the 3 states is:

$$|011\rangle = |0\rangle \otimes |1\rangle \otimes |1\rangle = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}^T$$

Following this pattern we have that the j-th binary string (in alphabetical order) of the n qubit measurements corresponds to the column vector with all zeros except the j-th position. Then we can express a superposition of the register's qubits as:

$$|\rho\rangle = \alpha_1 |000\rangle + \alpha_2 |001\rangle + \alpha_3 |010\rangle + \alpha_4 |011\rangle + \alpha_5 |100\rangle + \alpha_6 |101\rangle + \alpha_7 |110\rangle + \alpha_8 |111\rangle$$

$$= \begin{bmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 & \alpha_6 & \alpha_7 & \alpha_8 \end{bmatrix}^T$$

Where $\alpha_1, \ldots, \alpha_8$ are the amplitudes of the corresponding basis state. The probability of actually measuring a certain outcome is given by the modulus squared of the corresponding amplitude. We know that the probabilities add up to one because the vector is normalized. This extension of Born's rule naturally generalizes to more than 3 qubits [9].

It's worth noting that the measurement outcome of one of the qubits of a quantum register can affect the probability of the measurement outcomes of another qubit. For example, if in a certain state of a 2 qubit register, $|11\rangle$ has an amplitude of greater magnitude than $|10\rangle$, measuring "1" from the first qubit implies a higher chance of measuring "1" than "0" in the second one. This is a manifestation of *quantum entanglement*. Quantum states such as the Bell state, $\frac{1}{\sqrt{2}}(|11\rangle + |00\rangle)$, where the measurement of one qubit determines uniquely what the measurement of the other is going to be, are said to be *fully entangled*.

This effect travels faster than the speed of light: if two qubits are put in an entangled state, moved far away from each other, and measured at times less apart than the time it would take for light to travel between them, their measurements still exhibits entangled behaviour. Unfortunately this kind interaction doesn't allow for faster than light transfer of information because the value measured from the first bit is probabilistic to the same extent the second is.

When the state of an n-qubit register is unaffected by the surroundings it's said to be in a *pure state* and it can be described by the 2^n-dimensional ket that represents what is called a *coherent superposition* of it's basis states (applies to $n = 1$ as well). When there is some interaction with something unobservable, the system is said to be in a *mixed state*, and a more complex representation, such as a density matrix is required for the state of the system[11].

Postulates of Quantum Computing

Quantum mechanics has fundamental principles [7]. Given the above definitions of qubit and qubit registers, here is a possible set of intuitive postulates for Quantum Computing derived from the Quantum Mechanical ones[1], as a summary:

[1]Based on slide 189 of PPT2. Relation to [7]: Superposition is given axiom 1, Unitary Evolution by 2 and 3, Measurement by 4 and 5, while Entanglement is a consequence of the fact that equations in axiom 3 describe a whole isolated system.

- *Superposition*: The definition of qubit is a complex linear combination of the orthogonal states $|0\rangle$ and $|1\rangle$ in $\mathbb{Q}^2$.
- *Unitary Evolution*: Qubits can be processed by reversible operations in the form of quantum gates (an abstraction of the Hamiltonian).
- *Measurement*: Measurement yields either "1" or "0", with probabilities defined by Born's rule, and the quantum state is collapsed to the corresponding basis value.
- *Entanglement*: Entangled qubits, when measured, affect each other's measurement outcome probabilities. Thus qubits register states are represented by a superposition of all combinations of the basis states of the individual qubits of the register.

References

[1] S. Aaronson. Bqp and the polynomial hierarchy. In *Proceedings of the forty-second ACM symposium on Theory of computing*, pages 141–150, 2010.

[2] D. Deutsch. Quantum theory, the church–turing principle and the universal quantum computer. *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, 400(1818):97–117, 1985.

[3] W. Greiner. *Quantum mechanics: an introduction*. Springer Science & Business Media, 2011.

[4] S. Lloyd. Ultimate physical limits to computation. *Nature*, 406(6799):1047–1054, 2000.

[5] E. Lutz and S. Ciliberto. From maxwells demon to landauers eraser. *Phys. Today*, 68(9):30, 2015.

[6] A. Neumaier. Born's rule and measurement. *arXiv preprint arXiv:1912.09906*, 2019.

[7] L. Nottale and M.-N. Célérier. Derivation of the postulates of quantum mechanics from the first principles of scale relativity. *Journal of Physics A-mathematical and Theoretical - J PHYS A-MATH THEOR*, 401, 11 2007.

[8] C. E. Shannon. A mathematical theory of communication. *Bell system technical journal*, 27(3):379–423, 1948.

[9] E. Strubell. An introduction to quantum algorithms. *COS498 Chawathe Spring*, 13:19, 2011.

[10] L. Susskind and A. Friedman. *Quantum mechanics: the theoretical minimum*. Basic Books, 2014.

[11] K. The University of Tennessee. The density matrix. https://web.archive.org/web/20120115220044/http://electron6.phys.utk.edu/qm1/modules/m6/statistical.htm, Archived: 2012.