Introduction to Quantum Information Processing

Workshop on Quantum Computing, 1 - 5 August 2004, Tehran, IPM

Elham Kashefi
Christ Church College - Univdersity of Oxford
elham.kashefi@chch.ox.ac.uk

1 Introduction

The topic of these lectures lies in the new and rapidly growing field of quantum computing, which explores connections between physics and computing in general. Quantum information processing is a cross-disciplinary field and is of great importance from both a fundamental, as well as technological perspective [27]. From the fundamental perspective we have deepened our understanding of the relationship between physics, information and computation in general, and have also gained a deeper understanding of the fundamental aspects of quantum theory - non-locality and entanglement in particular [31]. From the technological perspective we have manipulated larger and larger quantum systems and obtained powerful practical applications in the domain of communication and cryptography such as the unconditionally secure quantum cryptography (key exchange) and quantum teleportation [7, 14, 5].

Historically, the greater potential of the quantum computer was first realised by Feynman, who noted that quantum systems appear to be exponentially hard to simulate with classical computers [15]. He speculated that, therefore, quantum computers could potentially be much more powerful than their classical counterparts. This intuition has been proven to be correct for some tasks, such as factoring large numbers and searching unstructured databases. Every computer is fundamentally a physical system, and any computation is just a physical process undergone by this system. Quantum physics is the most accurate way of describing physical systems and their behaviour in general. Encoding information into quantum systems and processing it according to the laws of quantum physics results in new features which do not exist in the classical computation.

Large scale quantum computation is still hypothetical. However, Moore's law[1] predicts that technology will reach the level where the quantum effects become important in near future. Parallel to this there is a growing effort to build quantum computers by manipulating larger numbers of quantum systems. Steady progress has now led to ion trap quantum computers with 4 qubits [29], Nuclear Magnetic Resonance (NMR) schemes with 7 qubits [22, 9] and realistic proposals for quantum computing in solid state environments [25]. Simple quantum algorithms such as the Deutsch-Jozsa algorithm [13] or quantum database search algorithms [18] have been experimentally demonstrated in NMR schemes and further progress towards higher numbers of qubits (10) seems likely in the foreseeable future.

Either way, we will enter the quantum realm where every aspect of computing, including storing information, loading and running of programs and reading the output will be

[1] Gordon Moore, one of the founders of the Intel, observed in mid 1960's that the memory capacity of a typical chip doubles roughly every eighteen months while its physical size remains the same.

governed by laws of quantum physics which are completely different from those of classical physics. Therefore there is a great need for theoretical study of quantum computation.

We describe briefly the mathematical foundation of quantum mechanics and discuss the basis of the theory of quantum computation.

2 Quantum Mechanics

Plank, Einstein and Bohr obtained the early great success in the quantum theory in the period from 1900 to 1925. Nevertheless, up to this time there existed no complete mathematical system for quantum theory to capture everything known up to that time in a unified picture. The year 1925 brought the resolution. A procedure initiated by Heisenberg was developed by Born, Heisenberg, Jordan and a little later by Dirac, into a new system of quantum theory. A little later Schrödinger developed the wave mechanics from an entirely different starting point. These two procedures, known as Heisenberg's and Schrödinger's pictures , soon proved to be equivalent.

There are two main mathematical frameworks within which quantum theory can be developed. One takes as its central object a certain algebraic structure (a C^* algebra) on the set of physical observables. States are then defined in relation to this algebra. On the other hand in the well-known Hilbert space approach the primary object is the vector space of states, with observables being defined in relation to this space. A brief review of the Hilbert space framework for quantum mechanics has been described in what follows.

We will use the notation and terminology of the following books: Quantum Theory by Isham [21]; Quantum Computation and Quantum Information by Nielsen and Chuang [27]; and Mathematical Foundation of Quantum Mechanics by von Neumann [32].

2.1 Hilbert Space Framework

In 1925 Schrödinger proposed one of the first formulations of quantum mechanics. His structure, known as *wave mechanics*, can be generalised within the Hilbert Space framework where the mathematical tool to describe the physical postulates is linear algebra. The standard notation of quantum mechanics for linear algebraic concepts was introduced by Dirac in 1920.

In Dirac's notation, a vector in the state space is represented with $|\psi\rangle$. The sate space of a finite dimensional physical system is $\mathbb{C}^d$ and for infinite dimensional system is a Hilbert space. Postulates 1 below will formalise this fact. The dual of the vector $|\psi\rangle \in \mathcal{H}$ is the function

$$\begin{array}{rcl} \langle\psi| : \mathcal{H} & \rightarrow & \mathbb{C} \\ |\phi\rangle & \mapsto & \langle\psi|\phi\rangle \, , \end{array}$$

where $\langle . | . \rangle$ is the inner product of the two vectors. A linear map (operator, transformation) is always represented by a matrix, A. The following tables gives a summary of the Dirac's notation.

Notation	Description
z^*	Complex conjugate of the complex number z.
$\vert\psi\rangle$	Vector. Also known as a *ket*.
$\langle\psi\vert$	Vector dual to $\vert\psi\rangle$. Also known as a *bra*.
$\langle\phi\vert\psi\rangle$	Inner vector product.
$\vert\phi\rangle \otimes \vert\psi\rangle$	Tensor vector product. For simplicity we omit $\otimes$ and just write $\vert\phi\rangle\vert\psi\rangle$ or $\vert\phi, \psi\rangle$.
A^*	Complex conjugate of the matrix A.
A^T	Transpose of the matrix A.
$A^\dagger$	Hermitian conjugate of the matrix A, $A^\dagger = (A^T)^*$.
$A\vert\psi\rangle$	Application of operator A on vector $\vert\psi\rangle$.
$\langle\phi\vert A\vert\psi\rangle$	The inner product of $\vert\phi\rangle$ and $A\vert\psi\rangle$, $\langle\phi\vert(A\vert\psi\rangle)$.

The four postulates that follow deal with the general mathematical framework within which it has been found possible so far to describe all quantum mechanical systems.

The first postulate sets up the state space in which quantum mechanics takes place.

Postulate 1. The predictions of results of measurements of an isolated system are probabilistic in nature. In situations where the maximum amount of information is available, this probabilistic information is represented mathematically by a vector in a complex Hilbert space $\mathcal{H}$ that forms the state space of the quantum theory. This vector is thought to be the mathematical representative of the physical notion of *state* of the system. In this framework, a physical observable is represented by a Hermitian matrix.

The following postulate is concerned with the evolution of the system.

Postulate 2. In a *closed* system, the evolution of the system is described by a *unitary transformation*. That is, the state $|\psi_1\rangle$ of the system at time t_1 is related to the state $|\psi_2\rangle$ at time t_2 by a unitary operator U which depends only on the time t_1 and t_2,

$$|\psi_2\rangle = U|\psi_1\rangle \, .$$

A refined version of this postulates describes the continuous time evolution of the system as follows.

Postulate 2′. The state vector $|\psi(t)\rangle$ of a closed system changes smoothly in time t according to the time-dependent Schrödinger equation

$$i\hbar \frac{d|\psi(y)\rangle}{dt} = \widehat{H}|\psi(y)\rangle \, .$$

In the above formula, $\hbar$ is the Planck's constant $\hbar \approx 6.63 \times 10^{-34}$ Joule-second divided by $t\pi$ and $\widehat{H}$ is the Hamiltonian operator which is described by a Hermitian matrix.

The next postulate describes the effect of observing (measurement) a quantum system.

Postulate 3. Quantum measurements are described by a collection M_m of *measurements operators*. These are operators acting on the state space of the system being measured. The index m refers to the measurements outcome that may occur in the experiment. If the state of the quantum system is $|\psi\rangle$ immediately before the measurement then the probability that the result m occurs is given by

$$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle \,,$$

and the state of the system after the measurement is

$$\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}} \,.$$

The measurements operators satisfy the *completeness equation*,

$$\sum_m M_m^\dagger M_m = I \,.$$

The last postulate deals with composite quantum system.

Postulate 4. The state space of a composite physical system is the tensor product of the state spaces of the component physical systems. Moreover, if we have systems numbered 1 to n, and system i is prepared in the state $|\psi_i\rangle$, then the joint state of the total system is $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$. In other word, the first postulate describes the encoding of the information, the second postulates explains the process of information, the third postulate deals with retrieving the information and finally the last postulates speaks about combining different systems.

Mixed states arise when we do not have complete information about the state of the physical system. This is always the case in experiments, since the system we are trying to prepare in a pure state interacts with an uncontrolled environment. A mixed state is a probabilistic mixture of pure states, denoted by $\{p_i, |\psi_i\rangle\}$ or alternatively with a *density matrix*

$$\rho \equiv \sum_i p_i|\psi_i\rangle\langle\psi_i| \,.$$

A density matrix $\rho \in B(\mathcal{H}_{2^n})$ is a hermitian (i.e. $\rho = \rho^\dagger$) semi positive definite matrix of dimension $2^n \otimes 2^n$ with $\mathrm{Trace}(\rho) = 1$ (where Trace(.) indicates the trace of .). Note that a given pure state $|\psi\rangle$ can also be represented with the density matrix $|\psi\rangle\langle\psi|$.

The most general operation on quantum states are the transformations of density matrices i.e. linear operators on operators (*super-operator*). The physically allowed super-operators are linear completely positive and trace-preserving operators, called *CP maps* for short. A super-operator T is positive if it sends positive semi-definite Hermitian matrices to positive semi-definite Hermitian matrices; it is completely positive if $T \otimes I_d$ is positive, where I_d is the identity operator on d-dimensional Hilbert space.

In what follows we reformulate the postulates of quantum mechanics in terms of density matrices.

Postulate 1. The predictions of results of measurements of an isolated system are probabilistic in nature. This probabilistic information is represented mathematically by a density operator, which is a positive operator ρ with trace one, acting on a complex Hilbert space $\mathcal{H}$ that forms the state space of the quantum theory. If a quantum system is in the state ρ_i with probability p_i, the denisty operator for the system is $\sum_i p_i\rho_i$.

Postulate 2. In a *closed* system, the evolution of the system is described by a *unitary transformation*. That is, the state ρ_1 of the system at time t_1 is related to the state ρ_2 at time t_2 by a unitary operator U which depends only on the time t_1 and t_2,

$$\rho_2 = U\rho_1 U^\dagger \, .$$

Postulate 3. Quantum measurements are described by a collection M_m of *measurements operators*. These are operators acting on the state space of the system being measured. The index m refers to the measurements outcome that may occur in the experiment. If the state of the quantum system is ρ immediately before the measurement then the probability that the result m occurs is given by

$$p(m) = \mathrm{Trace}(M_m^\dagger M_m \rho) \, ,$$

and the state of the system after the measurement is

$$\frac{M_m \rho M_m^\dagger}{\mathrm{Trace}(M_m^\dagger M_m \rho)} \, .$$

The measurements operators satisfy the *completeness equation*,

$$\sum_m M_m^\dagger M_m = I \, .$$

Postulate 4. The state space of a composite physical system is the tensor product of the state spaces of the component physical systems. Moreover, if we have systems numbered 1 to n, and system i is prepared in the state ρ_i, then the joint state of the total system is $\rho_1 \otimes \rho_2 \otimes \cdots \otimes \rho_n$.

3 Quantum Computation

The bounds on encoding and the speed of information processing using quantum systems are different to those based on the laws of classical physics. Since classical laws can be consider as a special case of the more general quantum laws it is clear that a quantum computer will be at least as efficient as the classical computer. In other word a quantum computer can efficiently simulate any classical processing with the same computational costs on a classical computer. The exciting discovery was that quantum computer is in fact provably more efficient than any classical computer [3]. One of the key effects leading to this efficiency is the quantum superposition phenomenon which allows a quantum computer to perform a given tasks simultaneously (in parallel) on multiple data.

There are few distinct algorithms which show that a quantum computer can be more efficient than its classical counterpart. These include factoring of numbers [28], database search [18], solution to the Pell's equation [19, 24], computing orders for solvable groups [33] to name a few [11]. There are also a number of quantum communication protocols that can be viewed as elementary quantum computations, such as the cryptographic key exchange [7], quantum teleportation [5] and dense coding [4]. The clearest advantage of using quantum systems is seen in factorisation which is an NP problem on the classical computer [28], whereas on the quantum computer it can be performed in polynomial time [16]. Factorisation is also potentially of great importance for the field of cryptography. It is known that this algorithm is a special case of a general problem, the hidden sub-group problem (HSP) [23]. HSP has been studied recently and for the Abelian case the general solution is known [26]. The other key example for the quantum speed-up is Grover's database search [18], which can achieve a quadratic speed-up over its classical counter-part. Grover's search idea has been generalised to the amplitude amplification method which can be applied to speed up a number of other algorithms [17]. Search itself lies at the root of many other important difficult computational tasks so that this algorithm has a wide applicability. All these indicate that there is an enormous potential in using quantum systems to encode and process information which is much more powerful than the present classical computers.

3.1 Quantum Circuit Model

Here we discuss the quantum circuit model for quantum computation [12, 34]. In analogy with a classical bit, a two-state quantum system is called a *qubit* or a *quantum bit.* Mathematically, a qubit takes a value in the vector space $\mathbb{C}^2$. We single out two orthogonal basis vectors, $|0\rangle$ and $|1\rangle$, to denote the computational basis. A quantum circuit is built out of logical quantum wires carrying qubits, and quantum gates acting on these qubits.

Definition 1 *A quantum gate, U, of order k is a unitary linear map on k qubits. Its action on a state $|\psi\rangle$ is denoted as $U|\psi\rangle$.*

The matrix representations of some known quantum operations are:

$$\begin{aligned}
\text{Hadamard} \quad H &= \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \\
\text{Pauli-X} \quad X &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \\
\text{Pauli-Y} \quad Y &= \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \\
\text{Pauli-Z} \quad Z &= \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \\
\text{Phase} \quad P &= \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}, \\
\text{Rotation-}\pi/8 \quad T &= \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}, \\
\text{controlled-Not} \quad CNOT &= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \\
\text{swap} \quad S &= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.
\end{aligned}$$

A set of quantum gates is said to be *universal for quantum computation* if any unitary operation can be approximated to arbitrary accuracy by a quantum circuit involving only those gates. in the literature, there exists many examples of universal set of gates [27]:

- The Hadamard, Phase, CNOT and $\pi/8$ Rotation gates,
- The Hadamard, Phase, CNOT and Toffoli gates,
- Single qubit and CNOT gates.

In quantum circuit model, measurements can always be moved to the end of the circuit and this process is performed in the computational basis of one or more of the qubits of the circuit.

All the different settings of *exact*, *zero-error* and *two-sided bounded error* can be also considered for the computation of a function with a quantum circuit model.

In the remaining part of this subsection we present the quantum circuits model in the most general setting, with mixed state, which was introduced by Aharonov et al. in [1]. They also showed that this model is polynomially equivalent in computational power to the standard unitary quantum circuit model, introduced by Deutsch [12].

We start by definition of the building blocks of a network i.e. gates.

Definition 2 *A quantum gate, g, of order (k, l) is a trace preserving, completely positive, linear map from density matrices on k qubits to density matrices on l qubits. Its action on a density matrix ρ is denoted as $g \circ \rho$.*

The definition of a quantum network in the general setting of working with mixed states and CP maps is:

Definition 3 *Let $\mathcal{G}$ be a family of quantum gates. A quantum circuit that uses gates from $\mathcal{G}$ is a directed acyclic graph. Each node v in graph is labeled by a gate $g_v \in \mathcal{G}$ of order (k_v, l_v). The in-degree and out-degree of v are equal k_v and l_v, respectively. An arbitrary subset of the inputs are labeled blank. An arbitrary subset of the outputs are labeled result.*

The final definition describes the function computed by a quantum network:

Definition 4 *Let Q be a quantum circuit, with n inputs and r result outputs. The probabilistic function computed by Q, $f_Q : \{0,1\}^n \to [0,1]^{\{0,1\}^r}$ is defined as follows: For input i, the probability for getting the output j is*

$$f_{i,j} = \langle j | (Q \circ |i\rangle\langle i|)|_A | j \rangle \,,$$

where A is the set of the result outputs.

4 Quantum Query Model

One important way of comparing the efficiencies of quantum and classical algorithms is by analysing *query complexity*, which measures the number of invocations of an *oracle* — which may be a standard circuit (or a Turing machine) implementing a useful sub-routine, a physical device, or a purely theoretical construct — needed to complete a task.

We consider an oracle to be a given quantum circuit which efficiently implements a boolean function $f : \{0,1\}^n \to \{0,1\}$. Equivalently, an oracle (black-box) contains an N-tuple ($N = 2^n$) of Boolean variables $X = (x_0, x_1, \cdots, x_{N-1})$. The box is equipped to output x_i on input i. The goal is to determine some property of X accessing the x_i only through the black box. Such a black-box access is called a *query* and assumes to have a unit cost of evaluation. A property of X is any Boolean function that depends on X. Assume $N = 2^n$, a property can be represented with a function of the following type:

$$F : \{0,1\}^N \to \{0,1\} \,.$$

As mentioned before we can consider different settings for computing F on $\{0,1\}^N$ in the query model. The minimum number of queries required by a quantum circuit to compute

F in the exact, zero-error, and bounded-error settings, is denoted by $Q_E(F), Q_0(F)$ and $Q_2(F)$, respectively.

A number of general results show the limitations and advantages of quantum computers using the query complexity models [13, 6, 3, 2, 30, 8, 10]. It is clear that upper bounds in the query model implies upper bounds for computational complexity, i.e. for the circuit description model in which the function X is succinctly described as a $(\log N)^{\mathcal{O}(1)}$-sized circuit computing x_i from i. On the other hand, lower bounds in the black-box model do not imply lower bounds in the circuit model, though they can provide useful guidance, indicating what certain algorithmic approaches are capable of accomplishing. In [2], some general lower bounds for query complexity of computing an arbitrary Boolean function F are given.

References

[1] D. Aharonov, A. Kitaev, and N. Nisan. Quantum circuits with mixed states. In *Proceedings STOCK'98 – Symposium on Theory of Computing*, Dallas, TX USA, 1998. ACM.

[2] R. Beals, H. Buhram, R. Cleve, M. Mosca, and R. Wolf. Quantum lower bounds by polynomials. In *Proceedings of FOCS'98 – Symposium on Foundations of Computer Science*, 1998.

[3] C. Bennett, E. Bernstein, G. Brassard, and U. Vazirani. Strengths and weaknesses of quantum computing. *SIAM Journal on Computing*, 26:1510, 1997.

[4] C. H. Bennett and S. J. Wiesner. Communication via one- and two-particle operators on einstein-podolsky-rosen states. *Phys. Rev. Lett.*, 69, 1992.

[5] C.H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W.K. Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett.*, 70, 1993.

[6] A. Berthiaume and G. Brassard. The quantum challenge to structural complexity theory. In *Proceedings of the 7th Annual IEEE conference on Structure in Complexity Theory*, Boston, 1992.

[7] G. Brassard and C.H. Bennett. Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers Systems and Signal Processing*, Bangalore India, 1984.

[8] H. Buhrman and W. van Dam. Quantum bounded query complexity. In *Proceedings of COCC'99 – Annual IEEE Conference on Computational Complexity*, page 149, Atlanta,USA, 1999. IEEE Press.

[9] I.L. Chuang, N. Gershenfeld, and M. Kubinec. Experimental implementation of fast quantum searching. *Phys. Rev. Lett.*, 80:3408, 1998.

[10] R. Cleve. An introduction to quantum computational complexity. In C. Macchiavello, G.M. Palma, and A. Zeilinger, editors, *Collected Papers on Quantum Computation and Quantum Information Theory.* World Scientific, 1999.

[11] R. Cleve, A. Ekert, L. Henderson, C. Macchiavello, and M. Mosca. On quantum algorithms. *Complexity*, 4, 1998.

[12] D. Deutsch. Quantum computational networks. In *Proc. Roy. Soc. Lond A*, volume 425, page 467, 1989.

[13] D. Deutsch and R. Jozsa. Rapid solution of problems by quantum computation. In *Proc. Roy. Soc. Lond A*, volume 439, page 553, 1992.

[14] A. Ekert. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.*, 67, 1991.

[15] R.P. Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21(6/7):467, 1982.

[16] M. Garey and D. Johnson. *Computers and intractability: a guide to the theory of NP-completeness*. Freeman, San Francisco, 1979.

[17] G.Brassardand, P.Höyer, M. Mosca, and A. Tapp. Quantum amplitude amplification and estimation. *AMS Contemporary Mathematics Series Millennium*, Quantum Computation & Information, 2000.

[18] L.K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of STOC'96 – Symposium on the Theory of Computing*, page 212, Philadelphia, Pennsylvania, 1996. ACM.

[19] S. Hallgren. Polynomial-time quantum algorithms for pell's equation and the principal ideal problem. In *Proceedings of the Annual Symposium on Theoretical Aspect of Computer Sciences*, Lecture Note in Computer Sceinece, 2002.

[20] C.A. Hooker, editor. *The Logico-Algebraic Approach to Quantum Mechanics*, volume I – Historical Evolution. Reidel, Dordrecht – Bosten, 1975.

[21] C.J. Isham. *Lectures on Quantum Theory – Mathematical and Structural Foundations.* Imperial College Press, London, 1995.

[22] J.A. Jones, M. Mosca, and R.H. Hansen. Implementation of a quantum search algorithm on a quantum computer. *Nature*, 393:344, 1998.

[23] R. Jozsa. Quantum factoring, discrete logarithms and the hidden subgroup problem. *Special issue of IEEE Computing in Science and Engineering*, 3, 2001.

[24] R. Jozsa. Notes on hallgren's efficient quantum algorithm for solving pell's equation. *quant-ph/0302134*, 2003.

[25] B.E. Kane. A silicon-based nuclear spin quantum computer. *Nature*, 393:133, 1998.

[26] M. Mosca and A. Ekert. The hidden subgroup problem and eigenvalue estimation on a quantum computer. In *Proceedings of the 1st NASA International Conference on Quantum Computing and Quantum Communication*, 1999.

[27] M.A. Nielsen and I.L. Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press, Cambridge, 2000.

[28] P.W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings of FOCS'94 – Symposium on Foundations of Computer Science*, page 124, Santa Fe, New Mexico, 1994. IEEE Press.

[29] Q.A. Turchette. *Phys. Rev. Lett.*, 81, 1998.

[30] W. van Dam. In *Proceedings of FOCS'98 – Symposium on Foundations of Computer Science*, page 362, 1998.

[31] V. Vedral. The role of relative entropy in quantum information theory. *Rev. Mod. Phys.*, 2002.

[32] J. von Neumann. *Mathematical Foundations of Quantum Mechanics*. Princeton University Press, Princeton, 1955.

[33] J. Watrous. Quantum algorithms for solvable groups. In *Proceedings of STOC'01 – Symposium on Theory of Computing*, page 60, 2001.

[34] A. C. C. Yao. Quantum circuit complexity. In *Proceedings of FOCS'93 – Symposium on Foundations of Computer Science*. IEEE Press, 1993.