Notes about Quantum Computing

Leo Liberti

Centre for Process Systems Engineering
Imperial College of Science, Technology and Medicine

(l.liberti@ic.ac.uk)

9 May 2000

Abstract

This is a short account of what I consider to be the most important introductory points to be made about quantum computation.

1 Introduction

Having thought about how nice it would be to have a quantum algorithm for nonlinear optimization, and not nowing much about quantum computing, here's a first attempt to throw some light in the darkness. Most of the material comes from [Ste97, NC00, BDMT98], with some help from [FLS66, AF68, MM56, KF75].

2 Notation

The most commonly used notation in quantum mechanics (and in particular in quantum computing) is the "bra" and "ket" notation, where a column vector $\underline{v}$ in a vector space V is indicated by $|v\rangle$ and a row vector $\underline{u}$ by $\langle u|$. The scalar product between two vectors $\langle u|$ and $|v\rangle$ is indicated by $\langle u|v\rangle$.

3 Qubits

The elementary unit of quantum information is the *qubit*. A *quantum system* has n qubits if it can be mathematically described in a Hilbert space of 2^n dimensions. Such a space has 2^n mutually orthogonal vectors (also called *state vectors*), so it is ideal to describe the somewhat physically abstract notion of "superposition of states". A vector in a quantum system having n qubits is indicated by $|i_1 i_2 \ldots i_n\rangle$ where $i_j \in \{0,1\}$ for all $j \leq n$. A basis for a quantum system having 3 qubits is given by

$$\{|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle\}.$$

4 Gates

Simple unitary operations on qubits are called *quantum logic gates*. For example, if a qubit evolves as $|0\rangle \to |0\rangle$, $1 \to e^{i\omega t}|1\rangle$ then after time t we say that the gate

$$P(\vartheta) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\vartheta} \end{pmatrix}$$

has been applied to the qubit, where $\vartheta = \omega t$. This can also be written

$$P(\vartheta) = |0\rangle\langle 0| + e^{i\vartheta}|1\rangle\langle 1|$$

Logic gates are unitary operators H in the Hilbert space representing the quantum system. A unitary operator is such that $\mathcal{H} = (\mathcal{H}^*)^{-1}$.

Operators in quantum mechanics are always Hermitian ($\mathcal{H} = \mathcal{H}^*$) because the probability that the system is in *some* state must be constant. This "certainty condition" is expressed as

$$\int \psi^*(\mathcal{H}\psi)dx = k.$$

This implies $\langle\psi^*|\mathcal{H}|\psi\rangle = 0$ which in turn means $\langle\psi|\mathcal{H}^*|\psi^*\rangle = 0$, that is, $\mathcal{H}$ is represented by a matrix $H = (h_{ij})$ such that $h_{ij} = h^*_{ji}$.

4.1 1-qubit Gates

Logic gates which transform 1-qubit state vectors are called 1-qubit gates. The identity operator acting on a qubit is given by $I = |0\rangle\langle 0| + |1\rangle\langle 1|$. The NOT gate is given by $X = |0\rangle\langle 1| + |1\rangle\langle 0|$.

How do they work? Since state vectors are mutually orthogonal, we have

$$\langle 0|0\rangle = 1, \langle 0|1\rangle = 0, \langle 1|0\rangle = 0, \langle 1|1\rangle = 1,$$

hence

$$\begin{aligned} I|0\rangle &= |0\rangle\langle 0|0\rangle + |1\rangle\langle 1|0\rangle = |0\rangle \\ I|1\rangle &= |0\rangle\langle 0|1\rangle + |1\rangle\langle 1|1\rangle = |1\rangle \\ X|0\rangle &= |0\rangle\langle 1|0\rangle + |1\rangle\langle 0|0\rangle = |1\rangle \\ X|1\rangle &= |0\rangle\langle 1|1\rangle + |1\rangle\langle 0|1\rangle = |0\rangle \end{aligned}$$

Other interesting 1-qubit gates are

$$\begin{aligned} Z &= P(\pi) \\ Y &= XZ \\ H &= \frac{1}{\sqrt{2}}\left[(|0\rangle + |1\rangle)\langle 0| + (|\langle\rangle 0) - |\langle\rangle 1)\rangle\langle 1|\right]. \end{aligned}$$

Notice that the set $\{I, X, Y, Z\}$ forms a group under operator multiplication, and that the last operator H is called the *Hadamard* operator.

4.2 2-qubit Gates

If U and V are 1-qubit operators, the operator $U \otimes V$ is 2-qubit operator (it acts on state vectors of length 2). For example, the XOR gate is given by

$$|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$$

5 No Cloning Theorem

5.1 Theorem
An unknown quantum state cannot be cloned

Proof. To generate a copy of a quantum state $|\alpha\rangle$, we must cause a pair of quantum systems to undergo the evolution $U(|\alpha\rangle|0\rangle) = |\alpha\rangle|\alpha\rangle$ where U is a unitary cloning operator. If this is to work for any state, then U must not depend on α, and therefore $U(|\beta\rangle|0\rangle) = |\beta\rangle|\beta\rangle$ for $|\beta\rangle \neq |\alpha\rangle$. However, if we consider the state $|\gamma\rangle = (|\alpha\rangle + |\beta\rangle)/\sqrt{2}$, we have

$$U(|\gamma\rangle|0\rangle) = \frac{|\alpha\rangle|\alpha\rangle + |\beta\rangle|\beta\rangle}{\sqrt{2}} \neq |\gamma\rangle|\gamma\rangle.$$

so the cloning operation fails, in general. Cloning may work on some particular states (e.g. on $|\alpha\rangle$ and $|\beta\rangle$ above) but it fails on some superposition of states. □

6 The Heisenberg Uncertainty Principle

Suppose A, B are two Hermitian operators and $|\psi\rangle$ is a quantum state. Suppose $\langle\psi|AB|\psi\rangle = x + iy$ where $x, y \in \mathbb{R}$ (hence $\langle\psi|BA|\psi\rangle = x - iy$). The *commutator* of A, B is $[A, B] = AB - BA$ and the *anti-commutator* of A, B is $\{A, B\} = AB + BA$. Note that $\langle\psi|[A, B]|\psi\rangle = 2iy$ and $\langle\psi|\{A, B\}|\psi\rangle = 2x$. This implies

$$|\langle\psi|[A, B]|\psi\rangle|^2 + |\langle\psi|\{A, B\}|\psi\rangle|^2 = 4|\langle\psi|AB|\psi\rangle|^2.$$

By Cauchy-Schwarz inequality,

$$|\langle\psi|AB|\psi\rangle|^2 \leq \langle\psi|A^2|\psi\rangle\langle\psi|B^2|\psi\rangle,$$

which implies

$$\langle\psi|[A, B]|\psi\rangle^2 \leq 4\langle\psi|A^2|\psi\rangle\langle\psi|B^2|\psi\rangle.$$

Suppose C, D are observables (Hermitian operators on the state space of the system being observed). C, D have spectral decomposition $\sum_c cP_c, \sum_d dP_d$; the probability of getting result c on measuring state ψ is $p(c) = \langle\psi|P_c|\psi\rangle$ and similarly for D; the averages of C, D are $\langle C\rangle = \sum_c cp(c)$ and similarly for D. Standard deviations for C, D are therefore $S(C) = \langle C^2\rangle - \langle C\rangle^2$ and similarly for D.

Now, substituting $A = C - \langle C\rangle$ and $B = D - \langle D\rangle$ into the last equation, we obtain Heisenberg's uncertainty principle

$$S(C)S(D) \geq \frac{1}{2}|\langle\psi|[C, D]|\psi\rangle|.$$

7 Shor's "Polynomial" Algorithm to Factor Prime Numbers

First the classical part: let N be the number to factor, and let a be a random number such that $1 \leq a \leq N$. Let $f(x) = a^x \mod N$. Notice $f(x)$ is periodic and it can be shown that for all a the period r of f is even; furthermore, $(a^{\frac{r}{2}} + 1)$ and $(a^{\frac{r}{2}} - 1)$ have a common factor with N (which can be easily found with Euclid's algorithm). So the problem reduces to finding the period r of a periodic function f. Classically, this problem is exponentially difficult.

Now for the magic: consider a quantum system of t qubits, where t is the smallest number of binary digits needed to represent N (i.e. $\mathrm{ceil}(\log_2(N))$), and consider $2N + 1$ such systems $x_0, \ldots, x_{2N}$ and to each of these associate systems $y_0, \ldots, y_{2N}$ initialized at $|0\rangle$. Initialize the whole system to the state

$$\sum_{x=0}^{2N} |x\rangle|0\rangle.$$

We now build a unary operator U such that $U|x\rangle = |f(x) >$ (periodic functions like the modular integral f above have such an associated unary operator).

$$\sum_{x=0}^{2N} |x\rangle|f(x)\rangle.$$

Notice that in one "step" we have calculated $f(x)$ for all x. This is a piece of quantum magic! At this point we measure the Y subsystem to get the value u. The quantum measurement causes the associated probabilities of the quantum state superposition to be

$$\sum_{x:f(x)=u} |x\rangle|u\rangle.$$

Since f is periodic, this means $x = d + jr$ for $1 \leq j \leq M$ where d is the phase, r is the period and M is about $\frac{2N}{r}$. For example, if $X = (0,1,2,3,4,5,6,7,8)$ and $Y = (1,2,4,3,1,2,4,3,1)$, then observing Y will fix a measurement u, say $u = 3$ and X "becomes" $(-,-,-,3,-,-,-,7,-)$ whilst Y "becomes" $(-,-,-,3,-,-,-,3,-)$. These system change in the sense that the probabilities associated with the states that become "$-$" go to zero after the measurement. In the example, $x = d+jr$ where $d = 3, j = 1,2$ and $r = 4$. This is the other crucial magic quantum-mechanical step.

In order to obtain r from the equation $x = d+jr$ the algorithm applies some discrete Fourier transforms to this equation. In certain cases there is a risk of getting the wrong answer, but the algorithm allows one to spot the wrong answers and restart the process if needed.

The unary operator U depends on f and it can be difficult to build. For $f(x) = a^x \mod N$ it is easy ($^2 \mod N$ repeatedly).

8 Conclusion

These notes have been compiled rather hurriedly so they may be at points hugely inaccurate. They represent my interpretation of this field after a couple of months of study.

References

[AF68] M. Alonso and E.J. Finn. *Fundamental University Physics vol. III.* Addison-Wesley, Singapore, 1968.

[BDMT98] G.P. Berman, G.D. Doolen, R. Mainieri, and V.I. Tsifrinovich. *Introduction to Quantum Computers.* World Scientific, London, 1998.

[FLS66] R.P. Feynman, R.B. Leighton, and M. Sands. *The Feynman Lectures of Physics vol. III.* Addison-Wesley, London, 1966.

[KF75] A.N. Kolmogorov and S.V. Fomin. *Introductory Real Analysis.* Dover, New York, 1975.

[MM56] H. Margenau and G.M. Murphy. *The Mathematics of Physics and Chemistry.* Van Nostrand, Princeton, NJ, second edition, 1956.

[NC00] M.A. Nielsen and I.L. Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press, Cambridge, 2000.

[Ste97] A. Steane. Quantum computing. *Preprint*, Los Alamos National Lab web repository(9707??):1–65, July 1997.