Some Introductory Notes on Quantum Computing

Markus G. Kuhn
http://www.cl.cam.ac.uk/~mgk25/

Computer Laboratory
University of Cambridge

2000-04-07

Quantum Computing Notation

Quantum Computing is best described in terms of linear algebra, where Dirac's bra-ket notation is usually used:

- The primary objects of quantum computing are vectors and matrices of a **Hilbert space** (vector space with inner product) over the complex numbers.

- Vectors are written as **bras** such as $\langle\Phi|$ and **kets** such as $|\Psi\rangle$.

- $|\Phi\rangle$ corresponds to a normal (vertical) vector

- $\langle\Phi|$ corresponds to transposed (horizontal) and complex-conjugated vectors.

- A matrix (or operator) is written like A
- $A^\dagger := (A^*)^\top$ is the transposed complex conjugate
- Hermitian matrix: $A = A^\dagger$
- Unitarian matrix: $AA^\dagger = \mathrm{Id}$
- Scalar (inner) product: $\langle \Phi | \Psi \rangle$
- Outer product (results in matrix): $|\Phi\rangle\langle\Psi|$
- Normalised Vector: $\langle \Phi | \Phi \rangle = 1$

Some Linear Algebra Revisited

- Projection onto the span of $|\Phi\rangle$ (normalised):

$$|\Phi\rangle\langle\Phi| \qquad \text{(hermitian)}$$

- Spectral decomposition:

$$A = \sum_i \lambda_i \, |\Phi_i\rangle\langle\Phi_i|,$$

where λ_i eigenvalues and Φ_i eigenvectors of hermitian matrix A: $A\,|\Phi_i\rangle = \lambda_i \, |\Phi_i\rangle$.

- Trace:

$$Tr(A) = \sum_i \lambda_i$$

is the sum of the diagonal elements (if hermitian: eigenvalues) of A.

Qubits

A **qubit** is a 2-dimensional, normalized, complex vector in a Hilbert space with base vectors $|0\rangle$ and $|1\rangle$. Each qubit can be represented as

$$|\Phi\rangle = a\,|0\rangle + b\,|1\rangle$$

with complex scalars a and b such that $\langle\Phi|\Phi\rangle = |a|^2 + |b|^2 = 1$.

While a **bit** can either have value 0 or 1, a **qubit** is a linear superposition of both a $|0\rangle$ and $|1\rangle$ value. In addition, a qubit can be **entangled** with other qubits, which is the real reason for the surprising computational power of a quantum computer.

State Vectors

The state space of a quantum computer with n qubits can be represented as the tensor product "$\otimes$" of the respective state spaces of all the individual qubits.

We abbreviate: $|0\rangle \otimes |1\rangle = |01\rangle$, etc. The tensor product of two qubits over the bases $|0\rangle$ and $|1\rangle$ has the four bases $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$.

The (pure) state of a quantum computer with n qubits is a point in a Hilbert space with 2^n orthogonal base vectors, each of which is again a point in a complex 2-dimensional Hilbert space.

Tensor Product

The tensor product follows the distributive law with vector addition, therefore:

$$\bigotimes_{i=1}^{n} (a_i |0\rangle + b_i |1\rangle) =$$
$$a_1 |0\rangle \otimes \left(\bigotimes_{i=2}^{n} a_i |0\rangle + b_i |1\rangle \right) +$$
$$b_1 |1\rangle \otimes \left(\bigotimes_{i=2}^{n} a_i |0\rangle + b_i |1\rangle \right)$$

Example:

$$(a_1 |0\rangle + b_1 |1\rangle) \otimes (a_2 |0\rangle + b_2 |1\rangle) =$$
$$a_1 a_2 |00\rangle + a_1 b_2 |01\rangle + b_1 a_2 |10\rangle + b_1 b_2 |11\rangle$$

Entanglement

Example: Some physical process sends two electrons in opposite directions. Measurements on each single electron have a certain probability of showing an up or down spin. However, measurements on both electrons will always result in opposite spins. The universe allows the two electrons to communicate instantaneously the result of the first measurement. Such an electron pair is called **entangled**.

If the state vector $|\Phi\rangle$ of a system of two qubits can be represented as the tensor product

$$|\Phi\rangle = |\Phi_1\rangle \otimes |\Phi_2\rangle$$

of two qubit states, the two qubits are **not entangled**, that is, measurement of one will not affect the other.

Bell States

The **Bell States** are the four states of **maximum entanglement** for a pair of qubits (ignoring variants that differ merely by a complex factor):

$$\begin{aligned} |00\rangle &+ |11\rangle \\ |00\rangle &- |11\rangle \\ |01\rangle &+ |10\rangle \\ |01\rangle &- |10\rangle \end{aligned}$$

Note that none of these can be represented as a tensor product of the form

$$(a_1 |0\rangle + b_1 |1\rangle) \otimes (a_2 |0\rangle + b_2 |1\rangle) =$$
$$a_1 a_2 |00\rangle + a_1 b_2 |01\rangle + b_1 a_2 |10\rangle + b_1 b_2 |11\rangle$$

Density Matrix

If we know that a state vector $|\Psi\rangle$ is in the (pure) state $|\Psi_i\rangle$ with probability p_i, then **all** our knowledge about $|\Psi\rangle$ can be represented in the **density matrix**

$$\rho = \sum_i p_i \, |\Psi_i\rangle\langle\Psi_i|$$

Measurement

The process of extracting information from a set of qubits is called **measurement**. A measurement is represented by a hermitian matrix

$$A = \sum_i \lambda_i \, |\Phi_i\rangle\langle\Phi_i|.$$

The result of the measurement will be one of the eigenvalues λ_i of A, and the state of the measured system will after the measurement be exactly in the state $|\Phi_i\rangle$ described by the corresponding eigenvector. This happens with probability $|\langle\Phi_i|\Psi\rangle|^2$ if $|\Psi\rangle$ is the original state of the system.

Measurement changes the state of the system and cannot provide a snapshot of the entire state.

If a state is characterized by the density matrix $\rho = \sum_i p_i \, |\Psi_i\rangle\langle\Psi_i|$, then the probability for getting the measurement result $|\Phi_i\rangle$ is

$$p(\Phi_i) = Tr(\, |\Phi_i\rangle\langle\Phi_i| \, \rho \,).$$

Quantum Gates

The operations of a quantum computer consist of multiplications of the state vector with a series of unitarian matrices (quantum gates must be reversible), followed by a measurement.

Some examples for quantum gates:

- C-NOT (controlled not):

$$\begin{aligned} |00\rangle &\rightarrow |00\rangle \\ |01\rangle &\rightarrow |01\rangle \\ |10\rangle &\rightarrow |11\rangle \\ |11\rangle &\rightarrow |10\rangle \end{aligned}$$

- Hadamard gates

- phase shifts

Functions of a full Quantum Computer

1. well characterized qubits

2. initialize state (e.g. to $|000\ldots0\rangle$)

3. decoherence rate sufficiently low (avoid interaction of qubits with environment, which would have the same effect as a too early measurement)

4. universal gate operations (typically sequenced by a classical computer)

5. single-qubit measurements

Proposed Implementations

- nuclear magnetic resonance
- neutral atoms or ions trapped in standing waves
- cavity QED
- electrons on liquid helium
- superconductors
- solid-state spin spectroscopy
- quantum dots

The experimental physics involved is very demanding. No operational full quantum computers expected in the next decade(s).

Error Correction

Digital circuits are stable and noise-free because of the voltage non-linearity of each gate. Quantum operations are fully linear and therefore will quickly accumulate noise.

Elegant solution: Use quantum gates to calculate redundant error-correction information (so-called **ancillary**) that is entangled with the actual signal. Measure the ancillary. This will not collapse the actual qubits, but will project their states back onto the orthogonal base vectors, without destroying the entangled state.

Algorithms and Applications

- Deutsch: distinguish constant vs. balanced vectors
- Grover: universal search in $O(\sqrt{n})$ time
- Shor: integer factorization in polynomial time

Potential main practical application seems to be cryptanalysis, where Grover's algorithm allows brute-force searches in $O(\sqrt{2^k}) = O(2^{k/2})$ time as opposed to $O(2^k)$ on a conventional computer with k unknown bits (corresponding to a search space size $n = 2^k$). Polynomial algorithms for puzzles such as not only factorization could endanger computational security of asymmetric cryptography. Symmetric cryptography might only require doubled keylength.

Literature

Probably the best introduction into quantum computing currently available are the lecture notes by John Preskill at Caltech:

`http://theory.caltech.edu/people/preskill/ph229/#lecture`

The Centre for Quantum Computation at the University of Oxford has a good web site with many references and links:

`http://www.qubit.org/`