A brief overview of quantum computing

or,

Can we compute faster in a multiverse?

Tom Carter

May 14, 1999

Brief overview of our topics:

- Hilbert spaces and quantum mechanics.
- Tensor products and entangled quantum states.
- Quantum bits (qubits), the physics of computation, elements of quantum computing.
- Tractability of computation (e.g., factoring and NP/NP-complete problems).
- Theoretical models for quantum computing.
- Suggestions for practical implementations of quantum computers.
- Problems and prospects.

Hilbert space setting for quantum mechanics

- A Hilbert space H is a complete normed vector space over $\mathbb{C}$:

  1. H is a vector space over $\mathbb{C}$

  2. There is an inner product
     $\langle \cdot | \cdot \rangle : H \times H \to \mathbb{C}$
     which is conjugate linear:
     $\langle v|w\rangle = \overline{\langle w|v\rangle}$
     $\langle \alpha v|w\rangle = \alpha\langle v|w\rangle$ for $\alpha \in \mathbb{C}$
     $\langle v+w|z\rangle = \langle v|z\rangle + \langle w|z\rangle$
     $\langle v|v\rangle \geq 0$
     and
     $\langle v|v\rangle = 0$ iff $v = 0$

  3. From the inner product, as usual, we define the norm of a vector:
     $\|v\|^2 = \langle v|v\rangle$

  4. H is complete with respect to the norm.

- We will typically use the bra/ket notation: $|v\rangle$ is a vector in H, and
  $\langle v|$ is the covector which is the conjugate transpose of v.
  This notation also allows us to represent the outer product of a vector and covector as $|v\rangle\langle w|$, which, for example, acts on a vector $|z\rangle$ as $|v\rangle\langle w|z\rangle$. For example, if $\{v_1,v_2\}$ is an orthonormal basis for a two-dimensional Hilbert space, $|v_1\rangle\langle v_2|$ is the transformation that maps $|v_2\rangle$ to $|v_1\rangle$ and $|v_1\rangle$ to $(0,0)^T$ since

$$|v_1\rangle\langle v_2||v_2\rangle = |v_1\rangle\langle v_2|v_2\rangle = |v_1\rangle$$
$$|v_1\rangle\langle v_2||v_1\rangle = |v_1\rangle\langle v_2|v_1\rangle = 0|v_1\rangle = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

  Equivalently, $|v_1\rangle\langle v_2|$ can be written in matrix form where $|v_1\rangle = (1,0)^T$, $\langle v_1| = (1,0)$, $|v_2\rangle = (0,1)^T$, and $\langle v_2| = (0,1)$. Then

$$|v_1\rangle\langle v_2| = \begin{pmatrix} 1 \\ 0 \end{pmatrix}(0,1) = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

- A unitary operator $U : H \to H$ is a linear mapping whose conjugate transpose is its inverse: $U^\dagger = U^{-1}$

- Unitary operators are norm preserving: $\langle v|U^\dagger U|v\rangle = \langle v|v\rangle = \|v\|^2$

- We will think of a quantum state as a (normalized) vector $|v\rangle \in H$, where we think of $\langle v|v\rangle$ as the probability of observing the state. For math folks, we are in effect working in Complex projective space, normalizing to 1 so that the probabilities make sense.

- The dynamical evolution of a quantum system is expressed as a unitary operator acting on the quantum state. Note that probabilities are preserved.

- Eigenvalues of a unitary matrix are of the form $e^{i\omega}$ where ω is a real-valued angle. A unitary operator is in effect a rotation.

- In the Schrödinger equation, U is determined by the *Hamiltonian* or energy operator H via $U = e^{iHt}$.

- A measurement consists of applying an operator O to a quantum state v. To correspond to a classical observable, O must be *Hermitian*, $O^\dagger = O$, so that all its eigenvalues are real. If one of its eigenvalues λ is associated with a single eigenvector u_λ, then we observe the value λ with probability $|\langle v|u_\lambda\rangle|^2$ (i.e., the square of the length of the projection along u_λ).

- In general, if there is more than one eigenvector u_λ associated with the eigenvalue λ, we let P_λ be the projection operator onto the subspace spanned by the eigenvectors, and the probability of observing λ when the system is in state v is $\|vP_\lambda\|^2$.

- Most projection operators do not commute with each other, and are not invertible. Therefore, we can expect that the order in which we do measurements will matter, and that doing a measurement will irreversibly change the state of the quantum system.

Entangled quantum states, tensor products, and qubits

- Tensor products
  We can form tensor products of a wide variety of objects. For example:

  1. The tensor product of an n dimensional vector u and a k dimensional vector v is an nk dimensional vector $u \otimes v$.

  2. If A and B are operators on n and k dimensional vectors, respectively, then $A \otimes B$ is an operator on nk dimensional vectors.

  3. if H_1 and H_2 are Hilbert spaces, then $H_1 \otimes H_2$ is also a Hilbert space. If H_1 and H_2 are finite dimensional with bases $\{u_1, u_2, \ldots u_n\}$ and $\{v_1, v_2, \ldots v_m\}$ respectively, then $H_1 \otimes H_2$ has dimension nm with basis $\{u_i \otimes v_j | 1 \leq i \leq n, 1 \leq j \leq m\}$.

- Tensor products obey a number of nice rules, such as: For matrices A, B, C, D, U, vectors u, v, w, and scalars a, b, c, d the following hold:

$$\begin{aligned}
(A \otimes B)(C \otimes D) &= AC \otimes BD \\
(A \otimes B)(u \otimes v) &= Au \otimes Bv \\
(u + v) \otimes w &= u \otimes w + v \otimes w \\
u \otimes (v + w) &= u \otimes v + u \otimes w \\
au \otimes bv &= ab(u \otimes v)
\end{aligned}$$

Thus for matrices,

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \otimes U = \begin{pmatrix} A \otimes U & B \otimes U \\ C \otimes U & D \otimes U \end{pmatrix},$$

which specializes for scalars to

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \otimes U = \begin{pmatrix} aU & bU \\ cU & dU \end{pmatrix}.$$

- The conjugate transpose distributes over tensor products, i.e.

$$(A \otimes B)^\dagger = A^\dagger \otimes B^\dagger.$$

- The tensor product of several matrices is unitary if and only if each one of the matrices is unitary up to a constant. Let $U = A_1 \otimes \ldots \otimes A_n$. Then U is unitary if $A_i^\dagger A_i = k_i I$ and $\prod_i k_i = 1$.

$$\begin{aligned} U^\dagger U &= (A_1^\dagger \otimes \ldots \otimes A_n^\dagger)(A_1 \otimes \ldots \otimes A_n) \\ &= A_1^\dagger A_1 \otimes \ldots \otimes A_n^\dagger A_n \\ &= k_1 I \otimes \ldots \otimes k_n I \\ &= I \end{aligned}$$

- Note that $\langle u \otimes v | w \otimes z \rangle = \langle u|w \rangle \langle v|z \rangle$. This implies that $\langle 0 \otimes u | 0 \otimes u \rangle = 0$, and therefore $0 \otimes u$ must be the zero vector of the tensor product Hilbert space.

  This in turn implies (reminds us?) that the tensor product space is actually the equivalence classes in a quotient space.

  In particular, if A and B are vector spaces, F is the free abelian group on $A \times B$, and K is the subgroup of F generated by all elements of the following forms (where $a, a_1, a_2 \in A, b, b_1, b_2 \in B, \alpha$ a scalar):

  1. $(a_1 + a_2, b) - (a_1, b) - (a_2, b)$

  2. $(a, b_1 + b_2) - (a, b_1) - (a, b_2)$

  3. $(\alpha a, b) - (a, \alpha b)$

  then $A \otimes B$ is the quotient space F/K.

Qubits

- A quantum bit, or qubit, is a unit vector in a two dimensional complex vector space for which a particular orthonormal basis, denoted by $\{|0\rangle, |1\rangle\}$, has been fixed. It is important to notice that the basis vector $|0\rangle$ is NOT the zero vector of the vector space.

- The orthonormal basis $|0\rangle$ and $|1\rangle$ may correspond to the $|\uparrow\rangle$ and $|\rightarrow\rangle$ polarizations of a photon respectively, or to the polarizations $|\nearrow\rangle$ and $|\nwarrow\rangle$. Or $|0\rangle$ and $|1\rangle$ could correspond to the spin-up and spin-down states ($|\uparrow\rangle$ and $|\downarrow\rangle$) of an electron.

- For the purposes of quantum computing, the basis states $|0\rangle$ and $|1\rangle$ are taken to encode the classical bit values 0 and 1 respectively. Unlike classical bits however, qubits can be in a superposition of $|0\rangle$ and $|1\rangle$ such as $a|0\rangle + b|1\rangle$ where a and b are complex numbers such that $|a|^2 + |b|^2 = 1$. If such a superposition is measured with respect to the basis $\{|0\rangle, |1\rangle\}$, the probability that the measured value is $|0\rangle$ is $|a|^2$ and the probability that the measured value is $|1\rangle$ is $|b|^2$.

- Key properties of quantum bits:

  1. A qubit can be in a superposition state of 0 and 1.

  2. Measurement of a qubit in a superposition state will yield probabilistic results.

  3. Measurement of a qubit changes the state to the one measured.

  4. Qubits cannot be copied exactly. This is known as the 'no cloning' principle. Interestingly, it is nonetheless possible to 'teleport' a quantum state, but in the process, the original quantum state is destroyed . . .

- If we have available more than one (physical) qubit, we may be able to *entangle* them. The tensor product of the Hilbert spaces for the individual qubits is the appropriate model for these entangled systems.

- For example, if we have two qubits with bases $\{|0\rangle_1, |1\rangle_1\}$ and $\{|0\rangle_2, |1\rangle_2\}$ respectively, the tensor product space has the basis

  $$\{|0\rangle_1 \otimes |0\rangle_2, |0\rangle_1 \otimes |1\rangle_2, |1\rangle_1 \otimes |0\rangle_2, |1\rangle_1 \otimes |1\rangle_2\}.$$

  We can (conveniently) denote this basis as

  $$\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}.$$

- More generally, if we have n qubits to which we can apply common measurements, we will be working in the 2^n-dimensional Hilbert space with basis

  $$\{|00\ldots00\rangle, |00\ldots01\rangle, \ldots, |11\ldots10\rangle, |11\ldots11\rangle\}$$

- A typical quantum state for an n-qubit system is

  $$\sum_{i=0}^{2^n-1} a_i|i\rangle$$

  where $a_i \in \mathbb{C}$, and $\{|i\rangle\}$ is the basis, with (in our notation) i written as an n-bit binary number.

- A classical (macroscopic) physical object broken into pieces can be described and measured as separate components. An n-particle quantum system cannot always be described in terms of the states of its component pieces. For instance, the state $|00\rangle + |11\rangle$ cannot be decomposed into separate states of each of the two qubits. In other words, we cannot find a_1, a_2, b_1, b_2 such that

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

  since

  $$(a_1|0\rangle + b_1|1\rangle) \otimes (a_2|0\rangle + b_2|1\rangle) =$$

  $$a_1a_2|00\rangle + a_1b_2|01\rangle + b_1a_2|10\rangle + b_1b_2|11\rangle$$

  and $a_1b_2 = 0$ implies that either $a_1a_2 = 0$ or $b_1b_2 = 0$. States which cannot be decomposed in this way are called entangled states. These are states that don't have classical counterparts, and for which our intuition is likely to fail.

- Particles are entangled if a measurement of one affects a measurement of the other. For example, the state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ is entangled since the probability of measuring the first bit as $|0\rangle$ is 1/2 if the second bit has not been measured. However, if the second bit has been measured, the probability that the first bit is measured as $|0\rangle$ is either 1 or 0, depending on whether the second bit was measured as $|0\rangle$ or $|1\rangle$, respectively. On the other hand, the state $\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle)$ is not entangled. Since $\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle) = |0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, any measurement of the first bit will yield $|0\rangle$ regardless of measurements of the second bit. Similarly, the second bit has a fifty-fifty chance of being measured as $|0\rangle$ regardless of measurements of the first bit. Note that entanglement in terms of particle measurement dependence is equivalent to the definition of entangled states as states that cannot be written as a tensor product of individual states.

Quantum Computing

- This exponential growth in number of states, together with the ability to subject the entire space to transformations (either unitary dynamical evolution of the system, or a measurement projection into an eigenvector subspace), provides the foundation for quantum computing.

- An interesting (apparent) dilemma is the energetic costs/irreversability of classical computing. Since unitary transformations are invertible, quantum computations (except measurements) will all be reversible. The classical boolean operations such as $b_1 \wedge b_2$, $b_1 \vee b_2$, and $b_1 \not\leftarrow b_2$ are irreversible, and therefore cannot directly be used as basic operations for quantum computers.

- The logical nand-gate ($b_1 \barwedge b_2$) is sufficient to generate all the traditional boolean functions (e.g., $\sim b \equiv b \barwedge b$). We will look for simple quantum gates that are similarly generic for quantum operations.

Simple quantum gates

- These are some examples of useful single-qubit quantum state transformations. Because of linearity, the transformations are fully specified by their effect on the basis vectors. The associated matrix is also shown.

$$
\begin{array}{lrcll}
I: & |0\rangle & \rightarrow & |0\rangle & \left(\begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array}\right) \\
 & |1\rangle & \rightarrow & |1\rangle & \\
X: & |0\rangle & \rightarrow & |1\rangle & \left(\begin{array}{cc} 0 & 1 \\ 1 & 0 \end{array}\right) \\
 & |1\rangle & \rightarrow & |0\rangle & \\
Y: & |0\rangle & \rightarrow & |1\rangle & \left(\begin{array}{cc} 0 & -1 \\ 1 & 0 \end{array}\right) \\
 & |1\rangle & \rightarrow & -|0\rangle & \\
Z: & |0\rangle & \rightarrow & |0\rangle & \left(\begin{array}{cc} 1 & 0 \\ 0 & -1 \end{array}\right) \\
 & |1\rangle & \rightarrow & -|1\rangle &
\end{array}
$$

  I is the identity transformation, X is negation, Z is a phase shift operation, and $Y = ZX$ is a combination of both. All these gates are unitary. For example

$$YY^* = \left(\begin{array}{cc} 0 & -1 \\ 1 & 0 \end{array}\right)\left(\begin{array}{cc} 0 & 1 \\ -1 & 0 \end{array}\right) = I.$$

- Probably the most important gate is the controlled-not gate, C_{not}, which operates on two qubits as follows: it changes the second bit if the first bit is 1 and leaves the bit unchanged otherwise.

$$C_{not}: \begin{array}{lcl} |00\rangle & \rightarrow & |00\rangle \\ |01\rangle & \rightarrow & |01\rangle \\ |10\rangle & \rightarrow & |11\rangle \\ |11\rangle & \rightarrow & |10\rangle \end{array} \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

  The transformation C_{not} is unitary since $C_{not}^* = C_{not}$ and $C_{not}C_{not} = I$. The C_{not} gate cannot be decomposed into a tensor product of two single-bit transformations.

Tractability of computation

- Creativity and Art

  1. Knowing when to pattern

  2. Symbol attachment and creation; patterns/symbols as revealers and concealers

  3. Levels of patterning

- Multiple patterns and selection
  $(x-1)(x-2)(x-3)-6$
  $x^3-6x^2+11x-12$
  $(x-4)(x^2-2x+3)$

- Adaptive pattern recognition

- Are the patterns really there?

Some history

- Physics
- Philosophy (theory of knowledge)
- Mathematics
  1. Matrix manipulation
  2. Topology
  3. Algebra
  4. Lie groups
  5. Manifolds and relativity theory
  6. Algebraic topology

We have the map $b_n : \Sigma^2 U(n) \to SU(n+1)$ given by

$$b_n(g, r, s) = [i(g), v_n(r, s)]$$

where $i(g)$ is the inclusion, $[g, h] = ghg^{-1}h^{-1}$ and

$v_n(r, s) =$

$$\begin{bmatrix}
\alpha & 0 & 0 & \cdots & 0 & \beta(-\overline{\alpha})^0 \\
\beta(-\overline{\alpha})^0\overline{\beta} & \alpha & 0 & \cdots & 0 & \beta(-\overline{\alpha})^1 \\
\beta(-\overline{\alpha})^1\overline{\beta} & \beta(-\overline{\alpha})^0\overline{\beta} & \alpha & \cdots & 0 & \beta(-\overline{\alpha})^2 \\
\vdots & \vdots & \vdots & & \vdots & \vdots \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
\vdots & \vdots & \vdots & & \vdots & \vdots \\
\beta(-\overline{\alpha})^{n-1}\overline{\beta} & \beta(-\overline{\alpha})^{n-2}\overline{\beta} & \cdots & \cdots & \alpha & \beta(-\overline{\alpha})^n \\
-(-\overline{\alpha})^n\overline{\beta} & -(-\overline{\alpha})^{n-1}\overline{\beta} & \cdots & \cdots & -(-\overline{\alpha})^0\overline{\beta} & -(-\overline{\alpha})^n
\end{bmatrix}$$

where

$$\alpha = \alpha(r, s) = \cos(\pi r) + i \sin(\pi r) \cos(\pi s)$$

$$\beta = \beta(r, s) = i \sin(\pi r) \sin(\pi s)$$

```
We have the map
$ b_n: \Sigma^2U(n) \rightarrow SU(n+1) $ \newline
given by
\[ b_n(g, r, s) = \left[ i(g), v_n(r, s) \right] \]
where $i(g)$ is the inclusion,
$\left[g, h\right] = ghg^{-1}h^{-1}$ \newline
and

$ v_n(r,s) = $

\[
\left[ \begin{array}{cccccc}
\alpha & 0 & 0 & \cdots & 0 & \beta (-\overline{\alpha})^0 \\
\beta (-\overline{\alpha})^0\overline{\beta} &
   \alpha  &  0  & \cdots & 0 &
   \beta (-\overline{\alpha})^1 \\
\beta (-\overline{\alpha})^1\overline{\beta} &
   \beta (-\overline{\alpha})^0\overline{\beta} &
   \alpha & \cdots & 0 & \beta (-\overline{\alpha})^2 \\
\vdots & \vdots & \vdots &  & \vdots & \vdots \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
\vdots & \vdots & \vdots &  & \vdots & \vdots \\
\beta (-\overline{\alpha})^{n-1}\overline{\beta} &
   \beta (-\overline{\alpha})^{n-2}\overline{\beta} &
   \cdots &  \cdots & \alpha &
   \beta (-\overline{\alpha})^n \\
-(-\overline{\alpha})^n\overline{\beta} &
   -(-\overline{\alpha})^{n-1}\overline{\beta} &
   \cdots &  \cdots & -(-\overline{\alpha})^0
   \overline{\beta} & -(-\overline{\alpha})^n \\
\end{array} \right]
\]
where
\[ \alpha = \alpha(r,s) =
\cos(\pi r) + i \sin(\pi r)\cos(\pi s) \]
\[ \beta = \beta(r,s) = i \sin(\pi r)\sin(\pi s) \]
```

What's wrong in computing today

- Not enough resolution on displays
- Not enough processing power and memory
- Not enough parallelism
- Software tools are "flat" and sequential rather than hierarchical

The intelligent mathematical assistant

- Adaptive symbolic input and output
- Strong basic skills (all of arithmetic through college calculus and elementary discrete structures)
- First order logic capabilities
- Adaptive "patterning" and "symboling"
- Elementary hypothesis generation and testing