

QUANTUM COMPUTING FOR DUMMIES

J. VON NATION

1. QUANTUM MECHANICS

We work in the space \mathbb{C}^n of $n \times 1$ column vectors with the inner product $(x, y) = x^\dagger y$. A^\dagger denotes the transpose conjugate of A . We mix math notation and bra(c)ket notation like English and pidgin.

Postulate 1. *An isolated quantum system “is described by” a unit vector in \mathbb{C}^n .*

A unit vector ψ in \mathbb{C}^n is called a *state*. A *qubit* is a unit vector in \mathbb{C}^2 . A linear combination of states is called a *superposition*.

Postulate 2. *The evolution of an isolated system is described by a continuous 1-parameter group of unitary operators.*

That means we have unitary matrices $U(t)$ such that

$$\begin{aligned}U(0) &= I \\U(t_1 + t_2) &= U(t_1)U(t_2) \\ \psi(t) &= U(t)\psi(0)\end{aligned}$$

Example. The Schrödinger equation is

$$i\hbar\psi_t = H\psi$$

where H is the Hamiltonian operator. (In classical physics, the Hamiltonian is the total energy of the system.) Substituting $\psi = U\psi(0)$ yields

$$U_t = -\frac{i}{\hbar}HU.$$

If H is time-independent, the solution is $U = e^{-\frac{i}{\hbar}Ht}$. If H is time dependent you get a path integral in the Lie algebra of the unitary group (see [3], p. 25).

An *observable* corresponds to a Hermitian matrix (see Postulate 3). Recall that any normal matrix ($AA^\dagger = A^\dagger A$) is unitarily diagonalizable, i.e., has an orthonormal basis of eigenvectors. If \mathcal{O} is an observable of a system \mathcal{Q} with eigenvalues λ_a , let $\{e_{ia} : \dots\}$ denote an orthonormal basis of eigenvectors. Then we can write

$$\mathcal{O} = \sum \lambda_a P_a$$

where

$$P_a = e_{1a}e_{1a}^\dagger + \dots + e_{ja}e_{ja}^\dagger$$

is the orthogonal projection onto the eigenspace for λ_a .

Postulate 3. *The result of a measurement is an eigenvalue of an observable. If the system is in the state ψ immediately before the measurement, then*

- (1) *The probability of result a is $p(a) = \psi^\dagger P_a \psi$.*
- (2) *The expected value of the observation is $\psi^\dagger \mathcal{O} \psi = \sum \lambda_a p(a)$.*
- (3) *If the result a is obtained, then the system collapses immediately thereafter to the state*

$$\frac{P_a \psi}{\sqrt{p(a)}}.$$

The Heisenberg Uncertainty Principle. Let $\langle A \rangle$ denote the expected value of an observable A in a quantum system in a state ψ . Let $\Delta A = A - \langle A \rangle$. Let $[A, B] = AB - BA$ be the commutator. Then

$$\langle (\Delta A)^2 \rangle \langle (\Delta B)^2 \rangle \geq \frac{1}{4} |\langle [A, B] \rangle|^2.$$

Following a hint in Strang's *Linear Algebra*, we get this from the Cauchy-Schwarz inequality as follows. Let $P = A - \langle A \rangle$ and $Q = B - \langle B \rangle$, and note that $[P, Q] = [A, B]$. Then

$$\begin{aligned} |\psi^\dagger [P, Q] \psi| &= |\psi^\dagger (PQ - QP) \psi| \\ &\leq |\psi^\dagger PQ \psi| + |\psi^\dagger QP \psi| \\ &= |(P\psi)^\dagger Q\psi| + |(Q\psi)^\dagger P\psi| \\ &\leq 2|P\psi||Q\psi| \end{aligned}$$

which squares to the above inequality.

Postulate 4. *The state space of a composite quantum system is the tensor product of the state spaces of its components.*

That is, if \mathcal{Q} is the combination of quantum systems $\mathcal{Q}_1, \dots, \mathcal{Q}_n$ with underlying spaces $\mathcal{H}_1, \dots, \mathcal{H}_n$, then the state space for \mathcal{Q} is

$$\bigotimes_{j=1}^n \mathcal{H}_j.$$

If each \mathcal{Q}_j is in state ψ_j , and the systems have been united without interacting (*juxtaposed*), then the combined system \mathcal{Q} is in the state

$$\psi_1 \otimes \dots \otimes \psi_n.$$

If the state ψ of the combined system cannot be written in the above form, then we say that \mathcal{Q} is *entangled*.

An example of an entangled state is the 2-qubit state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

Aside: density operators. A *density operator* on \mathbb{C}^n is a positive semidefinite Hermetian operator with trace 1. These provide another way to represent the state of a system. If ψ_1, \dots, ψ_m are states and p_1, \dots, p_m satisfy $0 \leq p_i \leq 1$ and $\sum p_i = 1$, then

$$\rho = p_1\psi_1\psi_1^\dagger + \dots + p_m\psi_m\psi_m^\dagger$$

is a density operator. Conversely, each density operator can be so represented. If a density operator ρ can be written in the form $\psi\psi^\dagger$, then it is said to represent a *pure ensemble*. Otherwise, it is said to represent a *mixed ensemble*.

Measurements can be interpreted in terms of density operators as follows, repeatedly using the fact that $\text{trace}(AB) = \text{trace}(BA)$. Let \mathcal{Q} be a system with state represented by the density operator ρ , and let A be an observable.

- (1) The probability of result a is $p(a) = \text{trace } P_a\rho$.
- (2) The expected value of the observation is $\text{trace } \rho A$.
- (3) If the result a is obtained, then the system collapses immediately thereafter to the state with density operator

$$\frac{P_a\rho P_a}{p(a)}.$$

Example. (Section 7.3 of [3]) Suppose at time $t = 0$ we have a 2-qubit in the (unentangled) state

$$\psi_0 = \frac{1}{\sqrt{2}}(|00\rangle - |10\rangle) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ -1 \\ 0 \end{bmatrix}$$

Assume that during the first unit of time the Hamiltonian is

$$H = \frac{\pi\hbar}{2} \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & -1 & 1 \end{bmatrix}$$

We then calculate that

$$U_{t=1} = e^{\frac{-i}{\hbar}H} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

so that

$$\psi_1 = U_1\psi_0 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 0 \\ -1 \end{bmatrix} = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle).$$

So this Hamiltonian H changes an unentangled state to an entangled one in a tick.

Einstein, Podolsky and Rosen (1935) objected to quantum mechanics on the basis that entangled states allowed for the possibility of *non-local* action, i.e., for events separated in

space-time by more than the speed of light to affect each other. Experiments now confirm that this is indeed the case. Get used to it.

The no-cloning theorem. Suppose we have a unitary operator U which, starting with a state ψ and some standard state σ , duplicates ψ , i.e., $U(\psi \otimes \sigma) = (\psi \otimes \psi)$. If this same U works for another state ϕ , so that $U(\phi \otimes \sigma) = (\phi \otimes \phi)$, then taking the inner product we see that $\psi^\dagger \phi = 0$ or 1 . Hence there is no machine which will duplicate an arbitrary pair of states.

Classical irreversible (logical) operators correspond to functions $f : \mathbf{2}^n \rightarrow \mathbf{2}^k$. Classical reversible operators correspond to permutations $\pi \in S_{2^n}$. The irreversible operators can be embedded into the reversible ones (in a larger dimension) using the following scheme: encode $f : \mathbf{2}^{n-1} \rightarrow \mathbf{2}$ by the map $F : \mathbf{2}^n \rightarrow \mathbf{2}^n$ with $F(x_1, \dots, x_n) = (x_1, \dots, x_{n-1}, x_n \oplus f(x_1, \dots, x_{n-1}))$. The latter is a permutation since $F^2 = I$.

Classical reversible operators correspond to permutation matrices, which are unitary. But quantum computing can use an arbitrary unitary matrix.

A catalog of unitary operators.

- (1) Permutation matrices on \mathbf{C}^n .
- (2) On \mathbf{C}^2

$$\mathbf{not} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

- (3) On \mathbf{C}^4 , the controlled-not

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

- (4) More generally, on $\mathbf{C}^2 \otimes V$, the controlled- \mathbf{U}

$$\mathbf{cU} = \begin{bmatrix} \mathbf{I} & 0 \\ 0 & \mathbf{U} \end{bmatrix}$$

- (5) On $\mathbf{V} \otimes W$, the Kronecker product $\mathbf{U}_1 \otimes \mathbf{U}_2$.
- (6) On \mathbf{C}^2 , the Hadamard matrix

$$\mathbf{H} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

- (7) If \mathbf{A} is hermetian, then $e^{i\mathbf{A}}$ is unitary.
- (8) Rotations, generally of the previous form.
- (9) If \mathbf{U} is unitary, then $\sqrt{\mathbf{U}}$ is unitary.

It is also useful to describe nice generating sets for the unitary group.

One can view a classical computer as a device which acts on bit-strings following the instructions in a finite program. The permissible instructions are:

- (1) initialize a bit at 0;
- (2) perform a boolean function on any finite subset of the bits and record it in a bit;

- (3) read bitstrings;
- (4) terminate.

Only these operations are allowed.

A quantum computer is a device which acts similarly on qubit strings. The permissible instructions are

- (1) initialize a qubit at $|0\rangle$;
- (2) perform a unitary operation on any finite subset of the qubits;
- (3) measure qubits in the basis $|0\rangle, |1\rangle$;
- (4) terminate;
- (5) discard a qubit or reset it to $|0\rangle$.

It is important that the system evolves only by these transformations. This is much more a practical factor for quantum computers than for classical ones. It suffices to use only one- and two-qubit operators.

A Quantum Algorithm. You are given a “black box” operator which operates on 3 qubits by permuting the basis according to the scheme $\text{BB} |abc\rangle = |ab(x \cdot a \oplus y \cdot b \oplus c)\rangle$ where $x, y \in \{0, 1\}$. (Here $u \cdot v$ denotes multiplication and uv is concatenation.) The object is to find x and y using BB only once.

Step 0: Initialize $\psi_0 = |000\rangle$.

Step 1: $\psi_1 = (\mathbf{H} \otimes \mathbf{H} \otimes \mathbf{H} \text{ not})\psi_0$.

Step 2: $\psi_2 = \text{BB} \psi_1$.

Step 3: $\psi_3 = (\mathbf{H} \otimes \mathbf{H} \otimes \mathbf{I})\psi_2$.

Step 4. We currently have $\psi_3 = \frac{1}{\sqrt{2}}(|xy0\rangle - |xy1\rangle)$. Measure the first two projections to determine x and y .

The proof uses the binary representation of numbers. Note that

$$\psi_1 = \frac{1}{2^{\frac{3}{2}}} \sum_{s=0}^3 (|s0\rangle - |s1\rangle).$$

Now $\text{BB}(|ab0\rangle - |ab1\rangle) = (-1)^{xy*ab}(|ab0\rangle - |ab1\rangle)$, where $u * v$ denotes the *bitwise* inner product of the binary numerals u and v . Hence

$$\psi_2 = \frac{1}{2^{\frac{3}{2}}} \sum_{s=0}^3 (-1)^{xy*s} (|s0\rangle - |s1\rangle).$$

Note that

$$H^{\otimes n} = \frac{1}{2^{\frac{n}{2}}} \sum_{u=0}^{2^n-1} \sum_{v=0}^{2^n-1} (-1)^{u*v} |u\rangle \langle v|.$$

So

$$\psi_3 = \frac{1}{2^{\frac{5}{2}}} \sum_{s=0}^3 \sum_{u=0}^3 (-1)^{(xy \oplus u)*s} (|u0\rangle - |u1\rangle).$$

Now when $u = xy$ we get 8 nonzero terms, totalling $\frac{1}{\sqrt{2}}(|xy0\rangle - |xy1\rangle)$, which is a vector of length 1. So the coefficients of $|u0\rangle$ and $|u1\rangle$ for $u \neq xy$ must all cancel.

The Deutsch-Josza Algorithm. You have a function $f : \mathbf{2}^n \rightarrow \mathbf{2}$ which is either constant or balanced (zero exactly half the time), but you don't know which. Let U_f be the unitary operator which operates on $n + 1$ qubits by permuting the basis according to the scheme $U_f|\mathbf{x}y\rangle = |\mathbf{x}(y \oplus f(\mathbf{x}))\rangle$. The object is to find out which case you are in using U_f only once.

Step 0: Initialize $\psi_0 = |0 \dots 0\rangle$.

Step 1: $\psi_1 = (\mathbf{H}^{\otimes n} \otimes \mathbf{H} \text{ not})\psi_0$.

Step 2: $\psi_2 = U_f\psi_1$.

Step 3: $\psi_3 = (\mathbf{H}^{\otimes n} \otimes \mathbf{I})\psi_2$.

Step 4. We currently have

$$\psi_4 = \frac{1}{2^{n+\frac{1}{2}}} \sum_{x=0}^{2^n-1} \sum_{u=0}^{2^n-1} (-1)^{f(x) \oplus x*u} |u\rangle (|0\rangle - |1\rangle).$$

Measure the first n qubits, and consider the part with $u = 0$. If f is constant, then the probability of $|0 \dots 0\rangle$ is 1, while if f is balanced, the probability of $|0 \dots 0\rangle$ is 0. So if the result of the measurement is $|0 \dots 0\rangle$ then f is constant, and if the result is anything else, f is balanced.

These two algorithms are almost identical, except that different unitary operators are used in Step 2 to solve different problems. While the problems are somewhat artificial, the algorithms illustrate clearly how the qubit setting allows one to obtain parallelism.

REFERENCES

- [1] S. Gudder, *Quantum computation*, Amer. Math. Monthly, **110** (2003), 181–201.
- [2] E. Knill, R. Laflamme et al., *Introduction to Quantum Information Processing*, Los Alamos Science **27** (2002), 2–37.
- [3] S. Lomonaco, Jr. (ed.), *Quantum Computation*, Proceedings of Symposia in Applied Mathematics **58**, Amer. Math. Soc., Providence, 2002.