Quantum Computing

nambrath@mit.edu

Splash 2019

1 Introduction

Quantum mechanics is the branch of physics that describes how systems behave at their most fundamental level. *Information processing* studies how information can be transferred and transformed. **Quantum information processing** is the theory of communication and computation at the most fundamental physical level. *Quantum computers* store and process information at the level of individual atoms.

> **Why study quantum computing?**
> Quantum mechanics also opens up a world of strange behaviors: electrons, photons, and atoms behave highly counter-intuitively. By exploiting this "quantum weirdness", we could crack cryptographic systems that are currently unbreakable, search databases faster than currently imaginable, and transmit information in unhackable codes.

1.1 Background

Math-free history:

- Planck / ultraviolet catastrophe / blackbody radiation: suggestion that energy is quantized
- Einstein / photoelectric effect: light is quantized! things are photons
- Schrödinger / Heisenberg: formalizing things mathematically and introducing probability
- waves and particles: things aren't just hard balls moving through space, wavefunctions are better
- entanglement $\rightarrow$ quantum weirdness is not a bug, but a feature

How does computing work right now? We manipulate *bits* and do operations via *gates* like NOT/AND/OR.

2 Quantum mechanics

Quantum is counterintuitive! Let's try to get a sense for what's happening. It makes not a lot of sense, but the math works out beautifully and has been experimentally verified! And the math (at first at least) isn't too hard.

2.1 Qubits - anjali

0 is $\begin{pmatrix}1\\0\end{pmatrix}$, 1 is $\begin{pmatrix}0\\1\end{pmatrix}$. We can use ket notation: $|0\rangle, |1\rangle$ General state is $\begin{pmatrix}a\\b\end{pmatrix}$ such that $a^2 + b^2 = 1$.

Why do we normalize? Coefficients are related to probabilities. will get 0 with prob a^2, 1 with b^2.

We can define the row vectors $\langle 0| = \begin{pmatrix} 1 & 0 \end{pmatrix}$, $\langle 1|, \langle \psi|$. Transpose and complex conjugate.

Define inner product, bra-ket and vector notation.

Probabilities as inner products $\langle 0|\psi\rangle = a^2 = P_0$. Projectors and $\langle \psi| P_0 |\psi\rangle$

QM is intrinsically *linear*. State transformations $\rightarrow$ matrix multiplication.

Unitary matrices preserve normalization. In quantum computing, transformations often have to be unitary.

2.2 Spin and observables - emma

spin 1/2 particles (electron, proton): $\pm\hbar/2$, $|\uparrow\rangle, |\downarrow\rangle$ projector onto z-axis is $I_z = \frac{\hbar}{2}(P_\uparrow - P_\downarrow) = \frac{\hbar}{2}\sigma_z$ Pauli matrices! $\sigma^2 = \mathbb{1}$

expectation values

every observable quantity has a corresponding operator $A|a\rangle = a|a\rangle$

eigenvalues / eigenvectors find them for Pauli matrices

2.3 SU(2) - emma

you can rotate these vectors using the pauli matrices: $-i\sigma_x|\uparrow\rangle = -i\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = -i|\downarrow\rangle$ phase doesn't matter!

you can rotate any $|\psi\rangle$ by any θ: decompose a vector into components and rotate each as desired.

rotation by θ around the i-axis is: $e^{-i(\theta/2)\sigma_i} = \cos(\theta/2)\mathbb{1} - i\sin(\theta/2)\sigma_i$

NB: rotating by 2π gives us a phase of -1 so to return to the original state we need to rotate 4π (the dumb hand rotation thing)

2.4 Tensor products - anjali

describe 2+ qubits/systems requires tensor products

2-qubit system is spanned by $|0\rangle \otimes |0\rangle$, $|0\rangle \otimes |1\rangle$, $|1\rangle \otimes |0\rangle$, $|1\rangle \otimes |1\rangle$, can write them as $\mathbb{C}^4$

a general normalized vector can be written as $|\Psi\rangle = \sum_{i,j=0,1} a_{ij}|i\rangle \otimes |j\rangle$

a tensor is a thing with slots sometimes you can't write something as the tensor product of two things $\rightarrow$ then it's **entangled**

operators on tensor products

2.5 no-cloning theorem - emma

Classical information can be copied but not quantum information! implies $|\psi\rangle \otimes |0\rangle \rightarrow U_c|\psi\rangle \otimes |0\rangle = |\psi\rangle \otimes |\psi\rangle$ but it turns out this is highly contradictory because it implies that probabilities have to be either 0 or 1 $\rightarrow$ no-cloning!

this is really important for cryptography: if you're eavesdropping on a channel, you can't copy the message without the recipient knowing about it

2.6 entanglement - anjali

entanglement is a peculiarly quantum-mechanical form of correlation between quantum systems and is at the heart of the speedups that quantum information processing offers

this is quantum weirdness at its best!

the singlet state $|\psi\rangle_{12} = \frac{1}{\sqrt{2}}\Big(|01\rangle - |10\rangle\Big) \rightarrow$ zero angular momentum in total for either particle individually, you know *nothing* about its spin taken together, it's a definite well-defined state, but either one on its own is totally indefinite

spukhafte Fernwirkung

3 Quantum computation!

finally! *reversibility* laws of physics are reversible so the computation necessarily must also be

3.1 Hadamard and CNOT and toffoli gates - emma

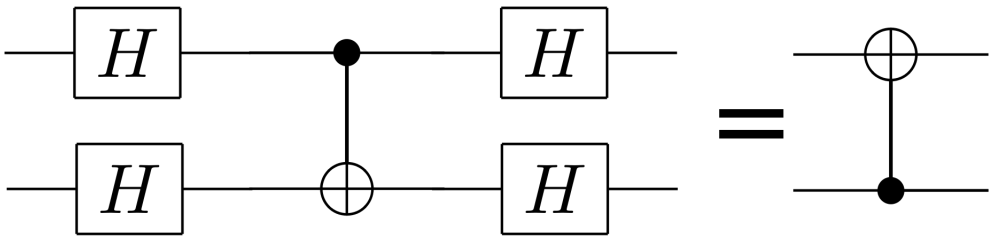


Figure 1: CNOT gate

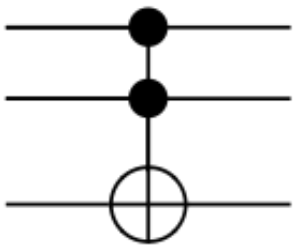


Figure 2: Toffoli gate circuit diagram

3.2 quantum parallelism - anjali

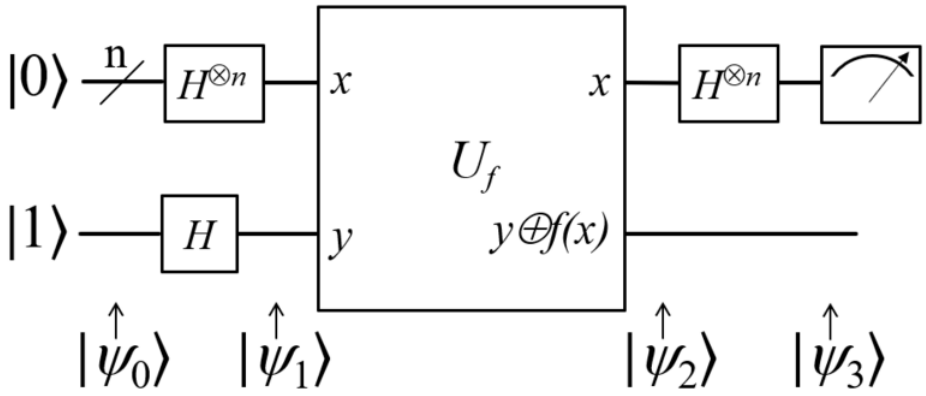
you can perform computations on superpositions! but you don't get all the answers as an output – you'd get a randomly selected output

3.3 Deutch-Jozsa - anjali

it is a *deterministic* algorithm - always produces an answer, and the answer is always right

is exponentially faster than any possible deterministic classical algorithm

eventually inspired Shor's algorithm which kicked off the quantum computing revolution



we are given a black box quantum computer known as an oracle that implements some function $f : \{0,1\}^n \to \{0,1\}$, takes n-digit binary values as input and produces either a 0 or a 1 as output for each such value

is the function constant or balanced??
classically you need to query the function a bunch a bunch of times and then you can find out
to prove that f is constant, just over half the set of inputs ($2^{n-1}+1$) must be evaluated and their outputs found to be identical
in DJ you just have to query it once

Specifically we were given a boolean function whose input is 1 bit, $f : \{0,1\} \to \{0,1\}$ and asked if it is constant.

start with $|0\rangle^n \otimes |1\rangle$ then Hadamard all of the registers:

$$\frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} |x\rangle \left(|0\rangle - |1\rangle\right)$$

the oracle does $|x\rangle|y\rangle$ to $|x\rangle|y \oplus f(x)\rangle$ ($\oplus$ is addition modulo 2)

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

applying more hadamards:

$$\frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f(x)} \left[\sum_{y=0}^{2^n-1} (-1)^{x \cdot y}|y\rangle\right] = \frac{1}{2^n} \sum_{y=0}^{2^n-1} \left[\sum_{x=0}^{2^n-1} (-1)^{f(x)}(-1)^{x \cdot y}\right] |y\rangle$$

$x \cdot y = x_0 y_0 \oplus x_1 y_1 \oplus \cdots \oplus x_{n-1} y_{n-1}$

the probability of measuring $|0\rangle^n$:

$$\left|\frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f(x)}\right|^2$$

1 if constant, 0 if balanced

4 how do you build a quantum computer

there are lots of ways to build a quantum computer, some of them more promising than others. the name of the game is to create a two-state quantum system that you can control well and that lasts long enough to compute on

it's really hard but people have lots of ideas about how to do it

4.1 superconducting circuits

this is the most popular architecture currently – if you've seen the cool headlines about quantum computing breakthroughs by Google or IBM, this is how they're made. these qubits are really fast but really short-lived, and have to be operated at 15 millikelvin!

basically, when you cool a piece aluminum below 4 K, the electrons all act like one big wave (for very complicated reasons). We can take advantage of this to make a circuit with energy levels that are both quantized and easy to tell apart (that is, you can easily tell if you're on the lowest energy level, or the second-lowest, and so on) because they're different distances apart.

the lowest and second-lowest energy levels are the "zero" and "one," and there's plenty of quantum weirdness to compute with

4.2 diamond color centers

with current nanotechnologies, we can introduce single-atom defects into a diamond crystal lattice. these defects have spin levels with different energies, so spin down could be "zero" and spin up could be "one"

these are longer-lived than superconducting circuits, but until recently were slow and gave off really weak signals because the photons used to detect the state of the standard silicon-vacancy color centers would get mixed up in the diamond crystal lattice

now people are trying other kinds of defects that might have better energy profiles