Quantum Computing:

The Very Basics

Easterhegg 2025

Tessa Kammermeier, tessa.dog

A qubit of Quantum Mechanics

- a system is described by a set X of pure states

  for today $X = \mathbb{B} = \{0,1\} / \{\text{False}, \text{True}\} / \{\uparrow, \downarrow\}$

- a system can be in a superposition of pure states

  $$\alpha|0\rangle + \beta|1\rangle \quad \text{with} \quad |\alpha|^2 + |\beta|^2 = 1$$

  this is a qubit

- if we measure this state, we measure $|0\rangle$ with a probability of $|\alpha|^2$ and $|1\rangle$ with a probability of $|\beta|^2$

A qubit of Quantum Mechanics

- we can combine two systems into one using $\otimes$

$$(\alpha|0\rangle + \beta|1\rangle) \otimes (\tilde{\alpha}|0\rangle + \tilde{\beta}|1\rangle)$$

$$= \alpha\tilde{\alpha}|0\rangle\otimes|0\rangle + \alpha\tilde{\beta}|0\rangle\otimes|1\rangle + \beta\tilde{\alpha}|1\rangle\otimes|0\rangle + \beta\tilde{\beta}|1\rangle\otimes|1\rangle$$

$$= \alpha\tilde{\alpha}|00\rangle + \alpha\tilde{\beta}|01\rangle + \beta\tilde{\alpha}|10\rangle + \beta\tilde{\beta}|11\rangle$$

this is a system of two qubits

- repeating this, we get systems of n qubits

A qubit of Quantum Mechanics

- superpositions are weird. We can look at

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle.$$

- It's in the state $|00\rangle$ with a 50% probability and in the state $|11\rangle$ with a 50% probability.
- If we measure only the first qubit, we measure $|0\rangle$ and $|1\rangle$ with a 50% probability. same if we only measure the second one.
- But if we measure the first and the result is $|0\rangle$ then the second also has to be in the state $|0\rangle$

Reframing Classical Computation

- to make quantum computation more understandable, we make classical computation less understandable.
- quantum operations are reversible but classical ones aren't. $\&: B^2 = B \times B \to B$ isn't reversible. If $x \& y = 0$, we can't know what x and y are.
- we can fix this by defining

$$\tilde{\&}: B^3 \to B^3, \tilde{\&}(x, y, z) = (x, y, z + (x \& y)).$$

In general, for a $f: B^n \to B^m$, we can define

$$\tilde{f}: B^{n+m} \to B^{n+m}, \tilde{f}(x^{(n)}, y^{(m)}) = (x^{(n)}, y^{(m)} + f(x^{(n)})).$$

Reframing Classical Computation

- let's have a closer look at

$$\tilde{\&} : B^3 \to B^3, \quad \tilde{\&}(x,y,z) = (x, y, z + (x \& y))$$

v	$\tilde{\&}(v)$
000	000
001	001
010	010
011	011
100	100
101	101
110	111
111	110

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

- given a classical computation f, the matrix associated to $\tilde{f}$ only has one 1 in each row/column.

The Quantum Improvement

- quantum operations are not hindered by this limitation

some basic operations on a single qubit are:

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad H = \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix}$$

$$Z|0\rangle = |0\rangle \qquad H|0\rangle = 1/\sqrt{2}|0\rangle + 1/\sqrt{2}|1\rangle$$

$$Z|1\rangle = -|1\rangle \qquad H|1\rangle = 1/\sqrt{2}|0\rangle - 1/\sqrt{2}|1\rangle$$

$\Rightarrow$ quantum computing has parallelisation inherently built in

using an operation like H on an n qubit system, we can in theory explore 2^n paths simultaneously

A Functional Framework of Quantum Computing

- why functional? global variables aren't a natural notion in quantum mechanics (to me!)
  - one cannot use the same quantum variable twice since it's impossible to duplicate quantum data (no cloning property)
  - in general, a quantum operation changes/entangles all input data

A Functional Framework of Quantum Computing

- the set of states of a system with pure states X is described by the $\mathbb{C}$-vector space $\langle X \rangle_{\mathbb{C}}$ freely generated by the set X
  - for the qubit we have $\langle B \rangle_{\mathbb{C}} = \mathbb{C}^2$
- quantum operations are modelled with linear maps

$$H = \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix} : \mathbb{C}^2 \longrightarrow \mathbb{C}^2$$

- this can be done monadically

A Functional Framework of Quantum Computing

- measurement can't be (reasonably) implemented in this monadic setting
- they can be modelled using a structure which generalises monads known as arrows

  (Vizzotto, Altenkirch and Sabry, Structuring quantum effects as arrows)

Why am I interested in this?

- arrows carry a rich categorical structure
  (Atkey, What is a categorical model of arrows?)
- maybe measurements can be nicely implemented using relative monads (active research)
- (topological) quantum computing is deeply related to my main field of research
  (Freedman, Larsen and Wang, A modular functor which is universal for quantum computation)
- maybe someone will give me money to do this

Thank you

for your attention