Quantum Computing

An introduction

Mitch Croal

April 29, 2016

You can find these slides online at
`http://z.umn.edu/acm2016quantum`

Overview

Motivation

- You can compute some things much, much faster on quantum computers
  - Shor's algorithm can factor large numbers in polynomial time in size of the number, $O(\log n^3)$
  - Grover's Algorithm can do unstructured search in $O(\sqrt{n})$
  - Quantum simulation is exponentially faster, important for physicists and chemists
  - There's really a big list, can find out more here: `http://www.nature.com/articles/npjqi201523`
- There's much work to be done, but there's been much progress in recent years
- D-Wave is a company that can do quantum computing right now

Units of data

- Binary systems with 2 states
  - The classical bit is an example
- Parallel to quantum information
  - We'll first develop CBits, an analagous linear system
  - From there we'll generalize to the real unit, the QBit

Introducing CBits

- A single CBit
  - The 'state space' is a two-dimensional vector space
  - Spanned by 2 orthonormal vectors, $|0\rangle$ and $|1\rangle$

    $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$
- Systems of multiple CBits
  - We need a way to mathematically combine CBits
  - Can do so with the so-called 'tensor product', denoted by $\otimes$

Tensor Products

The tensor product of column vectors looks like this:

$$\begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \otimes \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} = \begin{pmatrix} a_1 \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} \\ a_2 \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} a_1 b_1 \\ a_1 b_2 \\ a_2 b_1 \\ a_2 b_2 \end{pmatrix}$$

Multiple CBits

- State space of multiple CBits
  - Basis vectors are pairwise tensor products of $|0\rangle$ and $|1\rangle$
  - $|0\rangle \otimes |0\rangle$, $|0\rangle \otimes |1\rangle$ $|1\rangle \otimes |0\rangle$, $|1\rangle \otimes |1\rangle$
  - We now have a 4-dimensional vector space

$$|0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, |0\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix},$$

$$|1\rangle \otimes |0\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, |1\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Multiple CBits Notation

- Often we can leave out the $\otimes$
  $|0\rangle\,|0\rangle \quad |0\rangle\,|1\rangle \quad |1\rangle\,|0\rangle \quad |1\rangle\,|1\rangle$
- For even more readability
  $|00\rangle \quad |01\rangle \quad |10\rangle \quad |11\rangle$
- We can write them in decimal instead, with a subscore to indicate number of CBits
  $|0\rangle_2 \quad |1\rangle_2 \quad |2\rangle_2 \quad |3\rangle_2$
- We can then generalize this to systems of n Cbits, with the following basis vectors
  $|x\rangle_n,\ 0 \leq x < 2^n$

CBits and QBits

- CBits are closely related to the 'real' unit of quantum information, the QBit
  - Usually written as *qubit*
- QBits are realized by actual physical two-state systems
  - Operations on the states of QBits must be reversible
  - With a single exception, 'measurement', which we'll discuss later
  - We'll therefore only consider reversible operations on CBits

Single CBit operations

- Reversibility constrains us a bit
  - Operations like *erase*, $|0\rangle \rightarrow |0\rangle, |1\rangle \rightarrow |0\rangle$, are disallowed
- Therefore only 2 meaningful operations on CBits
  - The identity operator, $\mathbf{1}$
    $\mathbf{1}|0\rangle = |0\rangle, \mathbf{1}|1\rangle = |1\rangle$
  - The swap operator, $\mathbf{X}$
    $\mathbf{X}|0\rangle = |1\rangle, \mathbf{X}|1\rangle = |0\rangle$
- However, 'meaningless' operations can be made useful
  - Introduce the $\mathbf{Z}$ operator
    $\mathbf{Z}|0\rangle = |0\rangle, \mathbf{Z}|1\rangle = -|1\rangle$
- What the heck is $-|1\rangle$?

Multiple CBit operations

- It's useful to have compact notation for operators that act on many qubits
  - Begin by labelling each qubit $0, 1, 2, \ldots$
  - Thus if x has the binary expansion $x = 8x_3 + 4x_2 + 2x_1 + x_0$

$$\begin{aligned} |x\rangle_4 = |x_3x_2x_1x_0\rangle &= |x_3\rangle\,|x_2\rangle\,|x_1\rangle\,|x_0\rangle \\ &= |x_3\rangle \otimes |x_2\rangle \otimes |x_1\rangle \otimes |x_0\rangle \end{aligned}$$

- An operation that acts only on Cbit $\#2$ is $\mathbf{X}_2 = \mathbf{1} \otimes \mathbf{X} \otimes \mathbf{1} \otimes \mathbf{1}$
- It follows from the definition of our tensor product that $\mathbf{X}[\ |x_3\rangle \otimes |x_2\rangle \otimes |x_1\rangle \otimes |x_0\rangle\ ] = |x_3\rangle \otimes [\ \mathbf{X}\,|x_2\rangle\ ] \otimes |x_1\rangle \otimes |x_0\rangle$

Multiple CBit operations

- Less trivial operations are available when working with multiple CBits
  - The swap operator, $\mathbf{S}$
    $\mathbf{S}\left|xy\right\rangle = \left|yx\right\rangle$
  - The controlled 'not', $\mathbf{C}$
    $\mathbf{C}\left|0x\right\rangle = \left|0\right\rangle\left|x\right\rangle, \mathbf{C}\left|1\right\rangle\left|x\right\rangle = \left|1\right\rangle\left|\neg x\right\rangle$
- We can build up these operations using 'meaningless' operators, like $\mathbf{Z}$
- First consider the operator $\mathbf{A} = \frac{1}{2}(\mathbf{1} + \mathbf{Z}_1\mathbf{Z}_0)$
  - $\mathbf{A}$ acts as the identity on the 2 states $\left|00\right\rangle$ and $\left|11\right\rangle$
  - $\mathbf{A}$ gives 0 (clasically meaningless) for $\left|01\right\rangle$ and $\left|10\right\rangle$

Multiple CBit operations

- The *Hadamard* operator, $\mathbf{H}$, is particularly well known
  $\mathbf{H} = \frac{1}{\sqrt{2}}(\mathbf{X} + \mathbf{Z}) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
- $\mathbf{H}$, like $\mathbf{Z}$, can be used to build up useful multi-CBit operations

QBits

- QBits, the units of quantum information, are much like CBits
  - General form of the CBit is $a\,|0\rangle + b\,|1\rangle$
  - General form of the QBit is $\alpha\,|0\rangle + \beta\,|1\rangle$, where α and β are complex numbers
- Quantum states are also subject to the *normalization* condition
  - $|\alpha|^2 + |\beta|^2 = 1$
- This is because QBits correspond to actual 'observables'
  - The probability of observing state $|x\rangle_n$ corresponds to its 'probability amplitude'
  - Coin demonstration, $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
- Generalizing to n QBits, the general form is this:
  $|\psi\rangle = \sum_{0 \le x < 2^n} a_x\,|x\rangle$

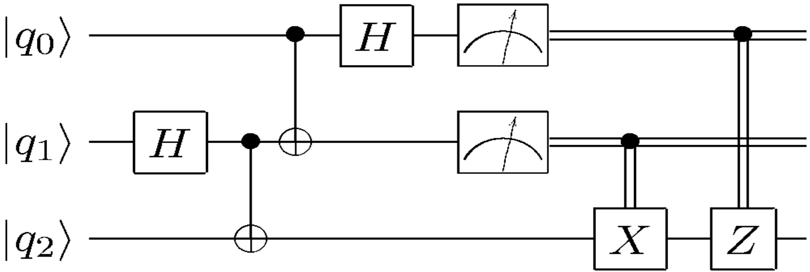
Quantum Wierdness

- Quantum computing deals heavily with *hidden information*
  - We're often given a state $|\psi\rangle$, but we don't know the coefficients, which can be arbitrarily precise
  - A set of n QBits has 2^n amplitudes corresponding to each combination of $|0\rangle$ and $|1\rangle$
  - Operators like **Z** and **H** can be chained to operate on all this data at once!
- Pretty cool, right? There's a catch
- Measurement collapses quantum states
  - Remember the coin?
  - We didn't know before, but after we knew, it didn't change

Quantum Algorithms

- Doing real work with quantum circuits are notoriously tricky
  - How do you even get any useful information when it's all random?
  - At a high level, it's all about reinforcing the amplitudes you want, diminishing the rest, and then measuring
- I think a real example of how this all comes together would be helpful

Anatomy of a Quantum Circuit



- Inputs on the left, each line corresponds to a single QBit
- The boxes are operators (or gates)
  - **H** is the Hadamard Gate, **X** and **Z** are the Pauli X and Y
- The meters do measurement, and collapse the measured QBit
- The black dots and lines indicate control QBits