CS 530: High-Performance Computing
Seminar 2: Quantum Computing

Nathan Chapman

Department of Computer Science
Central Washington University

May 25, 2024

Contents

1 History of Quantum Computation & Information

2 Quantum Bits

- The bit and qubit is the most fundamental concept of information
- A classical bit has a state: either 0 or 1
- A quantum bit has a state: $|0\rangle, |1\rangle, \alpha|0\rangle + \beta|1\rangle$ for complex α, β such that $|\alpha|^2 + |\beta|^2 = 1$
- The state of a qubit is a unit vector in a two-dimensional complex vector space. In other words, qubits similar to are unit quarternions.

- $|0\rangle, |1\rangle$ are orthonormal and form computational basis states
- Can't directly measure α, β
- Example: a "quantim coin" with state $|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ and 50-50 probability
- Can write $|\psi\rangle = e^{i\gamma}\left(\cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|0\rangle\right)$
- Because $e^{i\gamma}$ has no observable effect, we can reduced the above to $|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|0\rangle$
- While a qubit can only measure to be 0 or 1, until measurement there is "hidden information" encoded in α and β.

2.1 Multiple Qubits

- For two qubits, there are 2^2 computational basis states where $|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$ where $\alpha \in \mathbb{C}$ such that $\sum |\alpha|^2 = 1$
- Could measure just one qubit, possbly as zero, resulting in the re-normalized post-measurement state $|\psi_0\rangle = \frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}$
- Bell state or EPR state $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$
- Measure one of the bits in the Bell state and the second one must be the same with a 50% chance
- Extend to N qubits for a state with 2^N amplitudes
- ? If $N = 500$, a classical computer could never store 2^500 bits, as that is more than the predicted number of atoms in the universe

3 Quantum Computation

- Classical computers are built with electric circuits consisting of wire and logic gates
- Quantum computers are built with quantum circuits consisting of wires and quantum gates

3.1 Quantum Gates

3.1.1 Single Qubit Gates

- Only non-trivial example is the NOT gate defined by its truth table $0 \to 1$ and $1 \to 0$.
- Physically, there needs to exist some process by which we can "flip" the qubit.
- If $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, then $|\neg\psi\rangle = \beta|0\rangle + \alpha|1\rangle$ (where $\neg$ represents logical negation)
- In a basis representation, $|\psi\rangle = \begin{bmatrix}\alpha \\ \beta\end{bmatrix} \implies |\neg\psi\rangle = \begin{bmatrix}\beta \\ \alpha\end{bmatrix}$
- The mathematical action of the NOT operation can thus be represented by the matrix $X = \begin{bmatrix}0 & 1 \\ 1 & 0\end{bmatrix}$
- Yielding $X\begin{bmatrix}\alpha \\ \beta\end{bmatrix} = \begin{bmatrix}\beta \\ \alpha\end{bmatrix}$
- Quantum gates on a single qubit can be represented by a 2×2 matrix
- Because the result of applying a quantum gate U to a normalized quantum state is itself a normalized quantum state, the matrix representation of the quantum gate said to be *unitary* in the sense that $U^\dagger U = I$, where $U^\dagger$

is the *adjoint* of the operator U or conjugate-transpose of the matrix representation of U, and I is the 2×2 identity matrix.

- It turns out unitarity is the only constraint on quantum gates
- Unlike in classical logic, there are multiple non-trivial single-qubit gates.
- The Z gate effectively just flips the sign on the $|1\rangle$ state by defining $Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
- The *Hadamard* gate H defined as $H \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
- The Hadamard gate can be thought of as the "square root" of the NOT gate, though $H^2 = I \neq X$, because

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \tag{1}$$

$$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{2}$$

each of which transforms its input "halfway" toward the other.

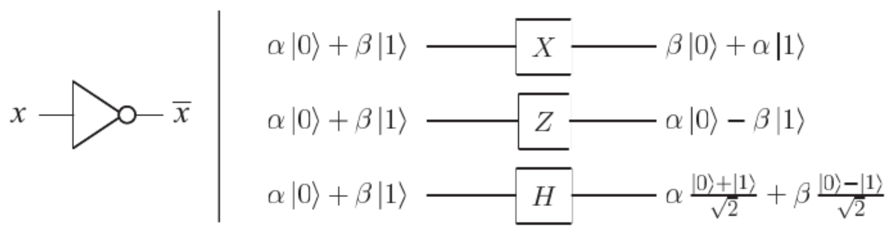

Figure 1: A comparison between logic gates that can act on a single classical or quantum bit.

- It turns out that there are infinitely many unitary single-qubit quantum gates. Each of these gates U can be represented by specifying real-valued $\alpha, \beta, \gamma, \delta$ and

$$U = e^{i\alpha} \begin{bmatrix} e^{-i\beta/2} & 0 \\ 0 & e^{i\beta/2} \end{bmatrix} \begin{bmatrix} \cos(\gamma/2) & -\sin(\gamma/2) \\ \sin(\gamma/2) & \cos(\gamma/2) \end{bmatrix} \begin{bmatrix} e^{-i\delta/2} & 0 \\ 0 & e^{i\delta/2} \end{bmatrix} \tag{3}$$

- This decompisition means that a quantum gate can be thought of as applying a sequence of rotations in different planes

3.1.2 Multi-Qubit Gates

3.2 Quantum Circuits

3.3 Examples

3.3.1 Bell States

3.3.2 Quantum Teleportation

4 Quantum Algorithms

4.1 Examples

4.1.1 The Quantum Fourier Transform

4.1.2 The Quantum Search Algorithm

5 Quantum Information

5.1 Quantum Cryptography

References

[1] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010.