Quantum Computing Notes

Roopa G
rvg9@gatech.edu

April 20, 2025

My notes of Introduction to Classical and Quantum Computing by Thomas G. Wong.

1 Chapter 2. One Quantum Bit

1.1 Superposition

- Qubit and Quantum States
  - A qubit can take two values - 0, 1
  - Braket notation/Dirac notation - $|0\rangle$, $|1\rangle$
  - $|0\rangle$ - north pole of Bloch sphere , $|1\rangle$ - south pole
  - State of a qubit can be combination of $|0\rangle$ and $|1\rangle$. Ex:$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
  - Common States (Fig. 1) -

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

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

$$|i\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i\,|1\rangle) \tag{3}$$

$$|-i\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i\,|1\rangle) \tag{4}$$

  - A qubit can be any point on the Bloch sphere.

- Complex Numbers Review -
  - Cartesian Form: $z = x + iy$
  - Real part $R(z) = x$; Imaginary part $I(z) = y$
  - Polar Form: $z = re^{i\theta}$
  - Cartesian -¿ Polar: $r = \sqrt{x^2 + y^2}$ and $\theta = tan^{-1}(\frac{y}{x})$
  - Polar -¿ Cartesian: $x = rcos\theta$ and $y = rsin\theta$

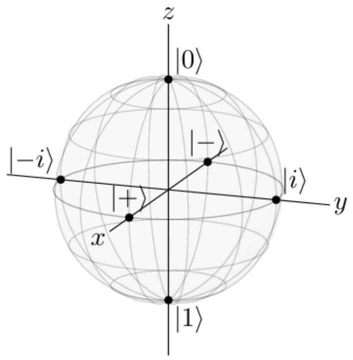


Figure 1: Bloch Sphere Representation of Commonly Used Quantum States

  - Complex Conjugate: $z^* = x - iy = re^{-i\theta}$
  - Norm: $|z| = r = \sqrt{zz^*}$
  - Norm-Square $= |z|^2 = r^2$

1.2 Measurement

- The probability is given by the norm-square of the amplitude.
- If $|\psi\rangle = z_1 |0\rangle + z_2 |1\rangle$, then $P(\langle\psi|0\rangle = |z_1|^2$ and $P(\langle\psi|1\rangle = |z_2|^2$
- Measurement collapses the qubit.
- A quantum state is normalized if its total probability is 1.

1.3 Bloch Sphere Mapping

- Global phases are physically irrelevant
- For example, $e^{i\theta}(\frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle)$
- States that differ by a global phase are actually the same state.
- A relative phase is physically significant.
- For example, $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|i\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$
- Spherical coordinates/Cartesian coordinates -
  - Let $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$
  - $\alpha = cos(\frac{\theta}{2})$ and $\beta = e^{i\phi}sin(\frac{\theta}{2})$ with $0 \leq \theta \leq \pi$ and $0 \leq \phi \leq 2\pi$
  - $x = sin\theta cos\phi$; $y = sin\theta sin\phi$; $z = cos\theta$

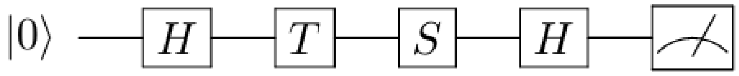


Figure 2: Example Quantum Circuit

1.4 Physical Qubits

- Photons - light polarization
- Trapped Ions
- Cold Atoms - magneto-optical traps
- Nuclear Magnetic Resonance - atom nuclei spin
- Quantum Dots - electron spin
- Defect Qubits - nitrogen vacancy center in diamond
- Superconductors - Josephson junction

1.5 Quantum Gates

- A quantum gate transforms the state of a qubit into other states. Quantum gates are linear maps that keep the total probability equal to 1.
- A quantum gate must be linear. $U(\alpha|0\rangle + \beta|1\rangle) = \alpha U|0\rangle + \beta U|1\rangle$
- Classical reversible logic gates are valid quantum gates.
- Common One-Qubit Quantum Gates -
  - Identity Gate - $I|0\rangle = |0\rangle$ and $I|1\rangle = |1\rangle$
  - Pauli X Gate - $X|0\rangle = |1\rangle$ and $X|1\rangle = |0\rangle$
  - Pauli Y Gate - $Y|0\rangle = i|1\rangle$ and $Y|1\rangle = -i|0\rangle$
  - Pauli Z Gate - $Z|0\rangle = |0\rangle$ and $Z|1\rangle = -|1\rangle$
  - Phase Gate - $S|0\rangle = |0\rangle$ and $S|1\rangle = i|1\rangle$
  - T Gate - $T|0\rangle = |0\rangle$ and $T|1\rangle = e^{i\frac{\pi}{4}}|1\rangle$
  - Hadamard Gate - $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle$ and $H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle$
- One-bit quantum gates are rotations on the Bloch sphere.

1.6 Quantum Circuits

- Quirk - https://algassert.com/quirk

2 Chapter 3. Linear Algebra

2.1 Quantum States

- $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$
- $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$
- Conjugate Transpose: $\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha & \beta \end{pmatrix}$
- $\langle\psi| = \begin{pmatrix} \alpha^* & \beta^* \end{pmatrix}$

2.2 Inner Products

- Let $|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ and $|\phi\rangle = \begin{pmatrix} \gamma \\ \delta \end{pmatrix}$
- $\langle\psi|\phi\rangle = \begin{pmatrix} \alpha^* & \beta^* \end{pmatrix} \begin{pmatrix} \gamma \\ \delta \end{pmatrix} = \alpha^*\gamma + \beta^*\delta = \langle\phi|\psi\rangle$
- $\langle\psi|\psi\rangle = 1$
- Orthogonal States: States with zero inner product. Ex: $\langle 0|1\rangle = 0; \langle +|-\rangle = 0; \langle i| - i\rangle = 0$
- Orthonormal States: Normalized + Orthogonal states. Ex: $|0\rangle \, and \, |1\rangle \, ; |+\rangle \, and \, |-\rangle \, ; |i\rangle \, and \, |-i\rangle$
- For an orthonormal basis $|a\rangle, |b\rangle$ the state of the qubit can be written as $|\psi\rangle = \alpha |a\rangle + \beta |b\rangle$ where $\alpha = \langle a|\psi\rangle$ and $\beta = \langle b|\psi\rangle$
- Example: $\psi = \frac{\sqrt{2}}{2} |0\rangle + \frac{1}{2} |1\rangle$. Measuring this in $|+\rangle, |-\rangle$ basis, amplitude of $|+\rangle$ is $\langle +|\psi\rangle = \frac{\sqrt{3}+1}{2\sqrt{2}}$; and amplitude of $|-\rangle$ is $\langle -|\psi\rangle = \frac{\sqrt{3}-1}{2\sqrt{2}}$

2.3 Quantum Gates

- $U = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \implies U|0\rangle = \begin{pmatrix} a \\ b \end{pmatrix}; U|1\rangle = \begin{pmatrix} c \\ d \end{pmatrix}$
- Let $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ then $U|\psi\rangle = \begin{pmatrix} a\alpha + c\beta \\ b\alpha + d\beta \end{pmatrix}$
- Quantum gates are matrices that keep the total probability equal to 1.
- Common One-Qubit Gates as Matrices -

Gate	Action on Computational Basis	Matrix Representation
Identity	$I\|0\rangle = \|0\rangle$ $I\|1\rangle = \|1\rangle$	$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
Pauli X	$X\|0\rangle = \|1\rangle$ $X\|1\rangle = \|0\rangle$	$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
Pauli Y	$Y\|0\rangle = i\|1\rangle$ $Y\|1\rangle = -i\|0\rangle$	$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$
Pauli Z	$Z\|0\rangle = \|0\rangle$ $Z\|1\rangle = -\|1\rangle$	$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
Phase S	$S\|0\rangle = \|0\rangle$ $S\|1\rangle = i\|1\rangle$	$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$
T	$T\|0\rangle = \|0\rangle$ $T\|1\rangle = e^{i\pi/4}\|1\rangle$	$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$
Hadamard H	$H\|0\rangle = \frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$ $H\|1\rangle = \frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$	$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

- Sequential quantum gates can be calculated by multiplying the corresponding gate matrices.
- $|U\psi\rangle = U\,|\psi\rangle$ and $\langle U\psi| = \langle\psi|\,U$
- Unitarity: $UU = I$
- Quantum gates are unitary matrices and unitary matrices are quantum gates.
- Reversibility: Matrix M is reversible if there exists a M^{-1} such that $MM^{-1} = I$.
- A quantum gate U is always reversible and its inverse is U.

2.4 Outer Products

- Let $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ and $|\phi\rangle = \gamma\,|0\rangle + \delta\,|1\rangle$
- Then, $|\psi\rangle\langle\phi| = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \begin{pmatrix} \gamma^* & \delta^* \end{pmatrix} = \begin{pmatrix} \alpha\gamma^* & \alpha\delta^* \\ \beta\delta^* & \beta\delta^* \end{pmatrix}$
- $|\phi\rangle\langle\psi| = |\psi\rangle\langle\phi|$
- Completeness Relation: For any given orthonormal basis $|a\rangle, |b\rangle$, the state of any qubit can be expressed in terms of $|a\rangle$ and $|b\rangle$. $|a\rangle, |b\rangle$ is called a complete orthonormal basis and satisfies $|a\rangle\langle a| + |b\rangle\langle b| = I$.

3 Chapter 4. Multiple Quantum Bits

3.1 Tensor Product

- When we have multiple qubits, we write their states as a tensor product $\otimes$. $|0\rangle \otimes |0\rangle = |0\rangle|0\rangle = |00\rangle$ and $\langle 0| \otimes \langle 0| = \langle 0|\langle 0| = \langle 00|$.

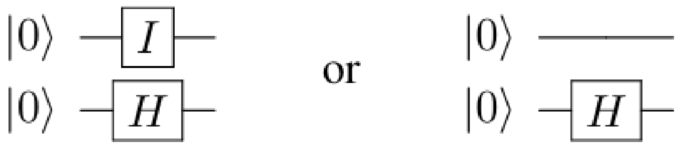


Figure 3: Example Quantum Circuit

- We use little endian notation, ie, $|b_2b_1b_0\rangle = 2^2b_2 + 2^1b_1 + 2^0b_0$.
- Kronecker Product - obtained by multiplying each term of the first matrix/vector by the entire second matrix/vector.

3.2 Entanglement

- Product States: Some quantum states can be factored into the tensor product of individual qubit states. Such states are called product states. Ex. $\frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle) = |+\rangle \otimes |-\rangle$.
- To factor a 2 bit state,
  - Say you have a state $|\psi\rangle = a\,|00\rangle + b\,|01\rangle + c\,|10\rangle + d\,|11\rangle$
  - Start by expressing it as a product of two one bit states, $|\psi\rangle = |\psi_1\rangle\,|\psi_2\rangle$
  - $|\psi_1\rangle = \alpha_1\,|0\rangle + \beta_1\,|1\rangle$ and $|\psi_0\rangle = \alpha_0\,|0\rangle + \beta_0\,|1\rangle$
  - So, $|\psi\rangle = |\psi_1\rangle\,|\psi_2\rangle = \alpha_1\alpha_0\,|00\rangle + \alpha_1\beta_0\,|01\rangle + \beta_1\alpha_0\,|10\rangle + \beta_1\beta_0\,|11\rangle$
  - Now, based on the actual coefficients, a, b, c, d, solve for $\alpha_1, \beta_1, \alpha_0, \beta_0$.
- Entangled States: Quantum states that can't be factored into product states. Ex: $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.
- A general entangled state of n qubits will have $N = 2^n$ amplitudes $c_)$ through c_{N-1}.

3.3 Quantum Gates

- When you have multiple qubits and you want to apply a single qubit gate like to just one qubit, you can express it using products. Ex: $(H \otimes I)$ applies the Hadamard gate to the left qubit in a two bit pair (Fig 3). **Note that the rightmost qubit corresponds to the top row.**
- One qubit gates can't create entangled states, we need gates that operate on multiple qubits for this.
- Two qubit quantum gates -

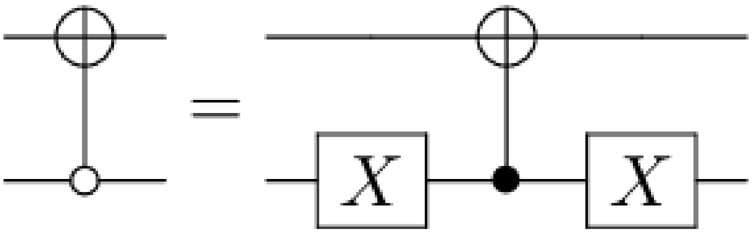
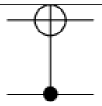
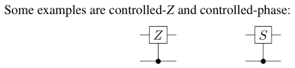
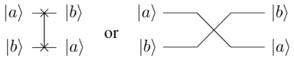
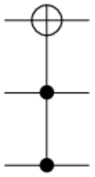


Figure 4: Anti-Controlled NOT using CNOT

Gate	Action on Z Basis	Matrix Representation	Circuit Representation
CNOT	$CNOT\|00\rangle = \|00\rangle$ $CNOT\|01\rangle = \|01\rangle$ $CNOT\|10\rangle = \|11\rangle$ $CNOT\|11\rangle = \|10\rangle$	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$	
CU	$CU\|00\rangle = \|00\rangle$ $CU\|01\rangle = \|01\rangle$ $CU\|10\rangle = \|1\rangle \otimes U\|0\rangle$ $CU\|11\rangle = \|1\rangle \otimes U\|1\rangle$	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & U_{00} & U_{01} \\ 0 & 0 & U_{10} & U_{11} \end{pmatrix}$	 Some examples are controlled-Z and controlled-phase:
SWAP	$SWAP\|00\rangle = \|00\rangle$ $SWAP\|01\rangle = \|10\rangle$ $SWAP\|10\rangle = \|01\rangle$ $SWAP\|11\rangle = \|11\rangle$	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$	 |a⟩ |b⟩ |b⟩ |a⟩ or |a⟩ |b⟩ |b⟩ |a⟩
Toffoli	$Toffoli\|000\rangle = \|000\rangle$ $Toffoli\|001\rangle = \|001\rangle$ $Toffoli\|010\rangle = \|010\rangle$ $Toffoli\|011\rangle = \|011\rangle$ $Toffoli\|100\rangle = \|100\rangle$ $Toffoli\|101\rangle = \|101\rangle$ $Toffoli\|110\rangle = \|111\rangle$ $Toffoli\|111\rangle = \|110\rangle$	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$	

- Some observations -
  - To flip control and target bits in CNOT, $(H \otimes H)CNOT_{10}(H \otimes H) = CNOT_{01}$
  - To make the CNOT 0 controlled instead of 1 controlled (anti-controlled NOT gate) (Fig 4) -
  - SWAP can be implemented using 3 CNOTs as $SWAP = (CNOT)(CNOT_{01})(CNOT)$
- No-Cloning Theorem: Qubits can't be cloned.

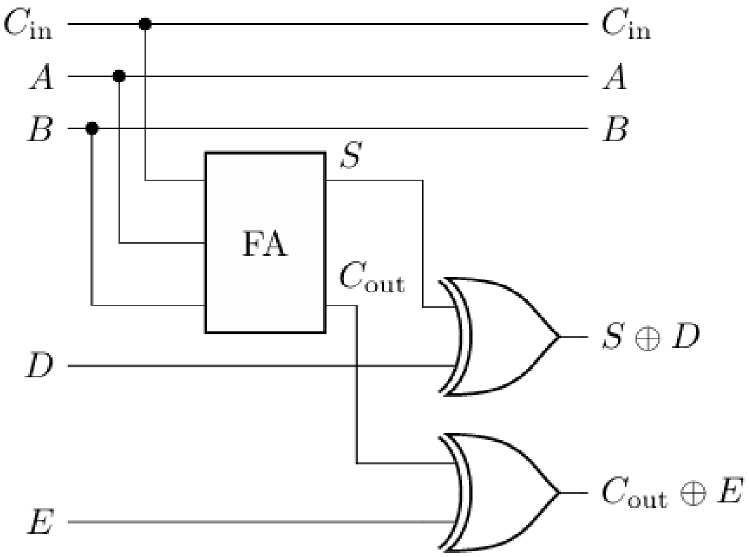


Figure 5: Quantum Adder 1 : Making the classical adder a reversible circuit

3.4 Quantum Adder

- Start with classical adder and turn it into a reversible circuit using XORs on outputs + ancilla bit (Fig 5).
- Start with classical adder (Fig 6), replace each gate with a reversible quantum gate (Fig 7) to get (Fig 8). The ancilla bits can be freed by turning them back into 0. We achieve this by the process of *uncomputation*, where we apply in reverse order the inverses of the gates used to calculate the ancilla.
- Quantum Setup $|a\rangle |b\rangle |c\rangle \rightarrow |a\rangle |s\rangle |c\rangle$.
- Quantum Sum (Fig 9)
- Quantum Carry (Fig 10)
- Quantum Ripple Carry Adder (Fig 11)
- Circuit Complexity (Fig 12)

3.5 Universal Quantum Gates

- Universal Gate Set: A set of quantum gates that allows us to approximate *any* quantum gate to any desired precision.
- Components of a universal gate set -
    1. Superposition
    2. Entanglement
    3. Complex amplitudes

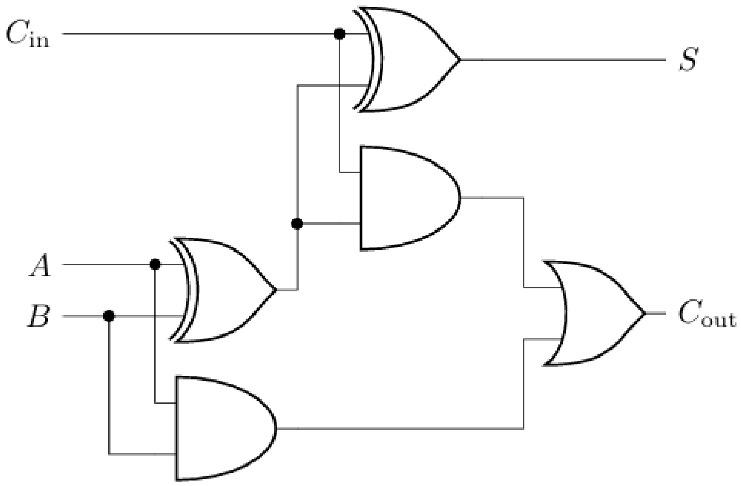
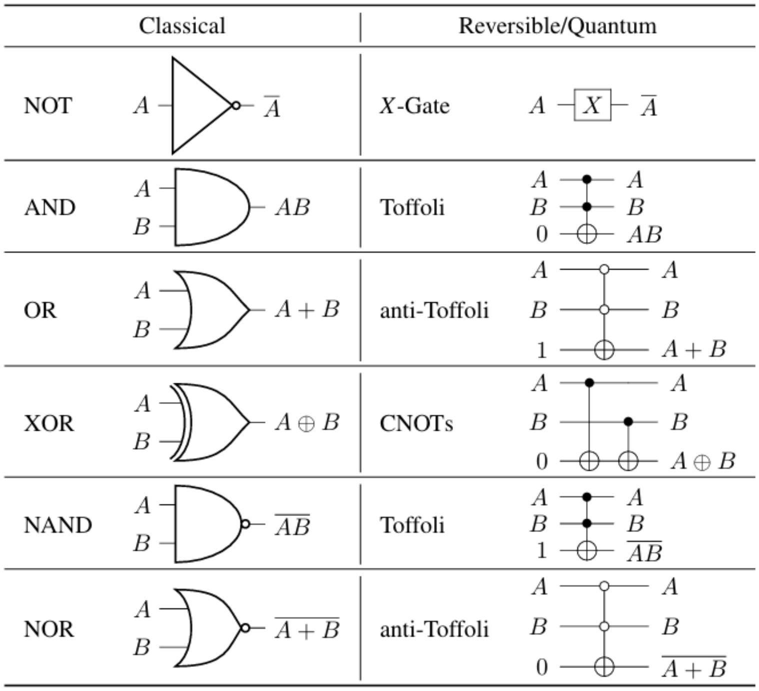


Figure 6: Classical Adder



Classical			Reversible/Quantum		
NOT	A	$\overline{A}$	X-Gate	A $\boxed{X}$	$\overline{A}$
AND	A B	AB	Toffoli	A B 0	A B AB
OR	A B	$A+B$	anti-Toffoli	A B 1	A B $A+B$
XOR	A B	$A \oplus B$	CNOTs	A B 0	A B $A \oplus B$
NAND	A B	$\overline{AB}$	Toffoli	A B 1	A B $\overline{AB}$
NOR	A B	$\overline{A+B}$	anti-Toffoli	A B 0	A B $\overline{A+B}$

Figure 7: Classical Gate - Reversible Quantum Gate

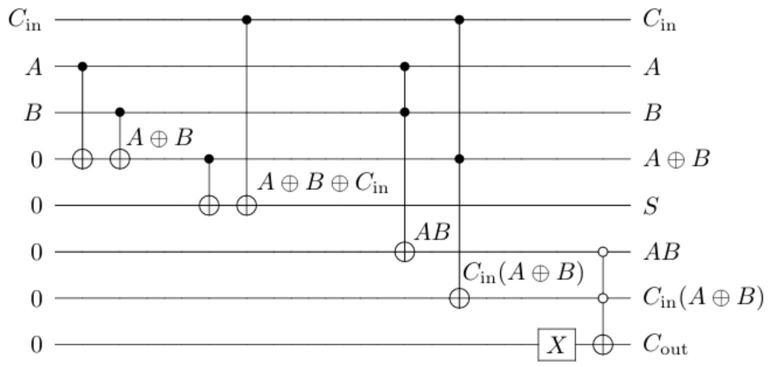


Figure 8: Quantum Adder 2 : Making each gate a reversible gate

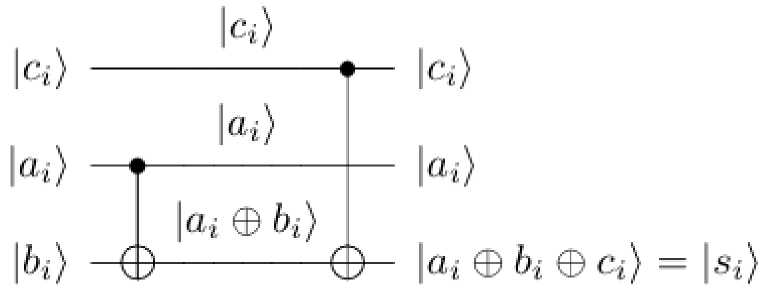


Figure 9: Quantum Sum

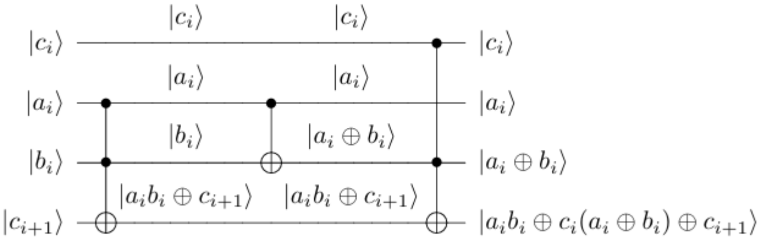


Figure 10: Quantum Carry

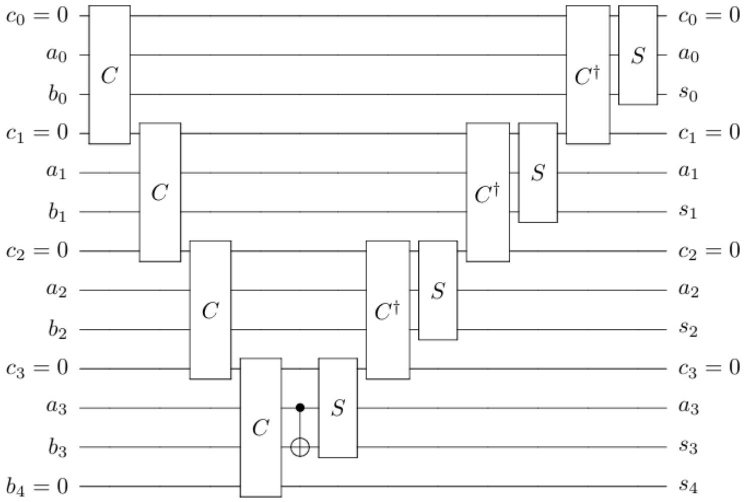
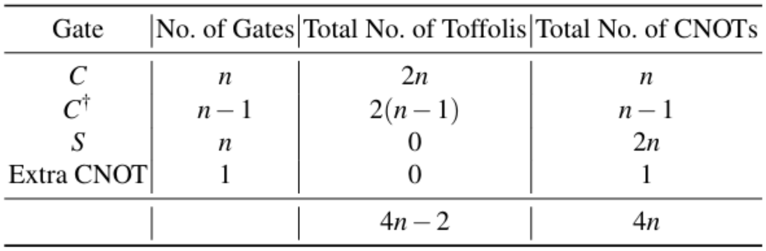


Figure 11: Quantum Ripple Carry Adder



Gate	No. of Gates	Total No. of Toffolis	Total No. of CNOTs
C	n	$2n$	n
$C^\dagger$	$n-1$	$2(n-1)$	$n-1$
S	n	0	$2n$
Extra CNOT	1	0	1
		$4n-2$	$4n$

Figure 12: Enter Caption

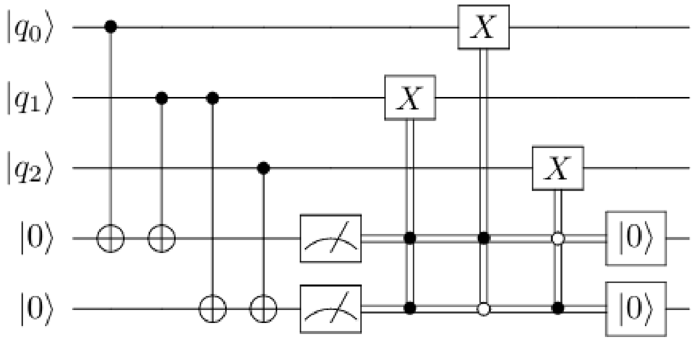


Figure 13: Shor's Bit Flip Code

4. Generate more than the Clifford Group

- A set of gates that satisfy properties 1-3 needn't necessarily be a universal gate set. Ex: $\{CNOT, H, S\}$
- *Gottesman-Knill Theorem:* A quantum circuit containing only $\{CNOT, H, S\}$ gates is efficiently simulated by a classical computer. The set of gates constructed by these gates is called the *Clifford Group*.
- Examples of Universal Gate Sets -
  - {CNOT, all single-qubit gates}
  - {CNOT, H, T}
  - $\{CNOT, R_{\pi/8}, S\}$ where $R_{pi/8} = \begin{pmatrix} cos(\frac{\pi}{8}) & -sin(\frac{\pi}{8}) \\ sin(\frac{\pi}{8}) & cos(\frac{\pi}{8}) \end{pmatrix}$
  - {Toffoli, H, S}
  - H plus almost any two-qubit unitary
  - Toffoli, any single-qubit gate that is basis chaning
  - CH
  - CNOT, any single-qubit gate whose square is basis-changing
- Solovay-Kitaev Theorem: With any universal gate set, we can approximate a quantum gate on n qubits to precision ϵ using $\Theta(2^n log^c(\frac{1}{\epsilon}))$ gates for some constant c.

3.6 Quantum Error Correction

- Bit flip $|0\rangle \rightarrow |1\rangle\,; |1\rangle \rightarrow |0\rangle$, Phase flip $|+\rangle \rightarrow |-\rangle\,; |+\rangle \rightarrow |-\rangle$.
- Qubits can also move partially along x-axis or z-axis but not completely. This is called *decoherence*.
- Error Correction: Shor's Bit Flip Code - based on parity. (Fig 13)
- Error Correction: Shor's Phase Flip Code - similar to bit flip, but use H to convert the phase flip into bit flip error. (Fig 14)

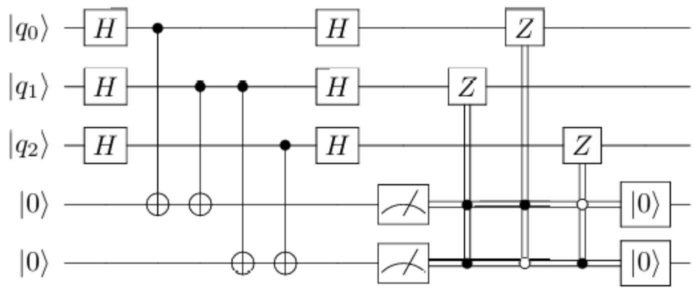


Figure 14: Shor's Phase Flip Code

4 Chapter 6. Entanglement and Quantum Protocols

4.1 Measurement

- If we measure a single qubit in a product state, it doesn't affect the other qubit.
- Maximally Entangles State: If we measure one qubit, we can know with certainity the measurement of the other qubit. Ex: $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.
- Bell States:

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{5}$$

$$|\phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \tag{6}$$

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \tag{7}$$

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \tag{8}$$

- Partially Entangled States: If we measure one qubit, we can know partially the measurement of the other qubit. Ex: $\frac{\sqrt{2}}{2\sqrt{2}}|00\rangle + \frac{\sqrt{2}}{2\sqrt{2}}|01\rangle + \frac{\sqrt{2}}{4}|10\rangle + \frac{1}{4}|11\rangle$

4.2 Bell Inequalities

4.3 Monogamy of Entanglement

- Entanglement is monogamous. Two qubits that are perfectly entangled with each other are not entangled at all with a third party. If two qubits are partially entangled with each other, then there is some possibility for some entanglement with a third qubit.

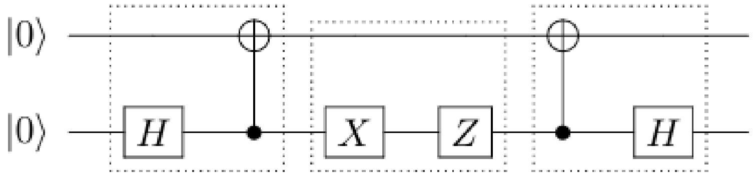


Figure 15: Superdense Coding

4.4 Superdense Coding

- Problem: One needs to send n bits of information using only $n/2$ qubits as opposed to n classical bits.
- Classical Solution: Send n bits.
- Quantum Solution: Alice (sender) and Bob (receiver) share an entangled pair of qubits in the $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ state. Alice applies some gates on her qubit based on what she wants to send and sends it to Bob. Bob measures the entangled pair after applying CNOT, followed by $H \otimes I$. Table 4.4

Alice to send	Alice applies gate	Bob Receives	Bob Measures
$\|00\rangle$	-	$\|\Phi^+\rangle = \frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$	$\|00\rangle$
$\|01\rangle$	X	$\|\Psi^+\rangle = \frac{1}{\sqrt{2}}(\|10\rangle + \|01\rangle)$	$\|01\rangle$
$\|10\rangle$	Z	$\|\Phi^-\rangle = \frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle)$	$\|10\rangle$
$\|11\rangle$	XZ	$\|\Psi^-\rangle = \frac{1}{\sqrt{2}}(\|01\rangle + \|10\rangle)$	$\|11\rangle$

- Circuit: Fig 15

4.5 Quantum Teleportation

- Problem: Send a qubit with unknown state $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$ using only classical bits.
- Classical Solution: If there's only one qubit, there's no way to do this since measuring will collapse the qubit. If there are multiple qubits in state $|\Psi\rangle$, we can use *quantum state tomography* (multiple measurements) to get an idea of what a qubit might be.
- Quantum Solution: Alice (sender) and Bob (receiver) share an entangled pair in the state $|\Phi^+\rangle$. Alice has the target qubit and one part of the entangled pair, she applies a CNOT on her qubits, followed by a H on the target qubit. Finally she measures her qubit and sends the measured value. Bob applies some gates based on the measured value on his part of the entangled pair to retrieve the target qubit. (Table 4.5)

Alice's qubit state	Alice measures	Bob applies gate	Bob's Qubit State
$\alpha\|0\rangle + \beta\|1\rangle$	$\|00\rangle$	-	$\alpha\|0\rangle + \beta\|1\rangle$
$\beta\|0\rangle + \alpha\|1\rangle$	$\|01\rangle$	X	$\alpha\|0\rangle + \beta\|1\rangle$
$\alpha\|0\rangle - \beta\|1\rangle$	$\|10\rangle$	Z	$\alpha\|0\rangle + \beta\|1\rangle$
$-\beta\|0\rangle + \alpha\|1\rangle$	$\|11\rangle$	XZ	$\alpha\|0\rangle + \beta\|1\rangle$

- Circuit: Fig 16

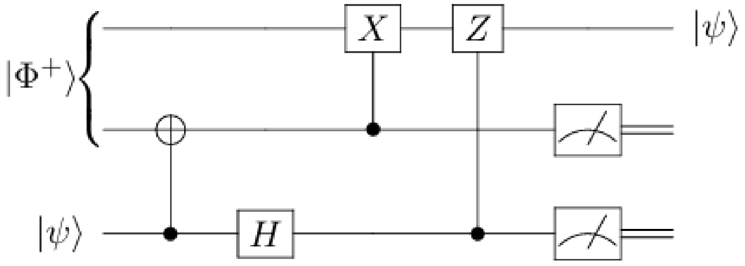


Figure 16: Quantum Teleportation

4.6 Quantum Key Distribution

- Problem: Alice to send data to Bob over the internet, without being intercepted by eavesdropper Eve.
- Classical Solution: Public Key Cryptography
- Quantum Solution: BB84, Quantum Key Distribution
  - Alice begins with some random bits. For each bit, she randomly chooses the z-basis or the x-basis.
  - Bob receives the bits and he randomly measures them in the x-basis or z-basis.
  - Now Alice and Bob share the basis they used for measuring the qubits.
  - If they used the same basis, they know their measurement outcomes should agree, and they've shared a secret bit. If they used a different bases, their measurement outcome might or might not agree, so they discard that bit.
  - If there is an eavesdropper Eve, the probability that Alice and Bob detect Eve is $1 - (\frac{3}{4})^n$ where n is the number of bits in the secret key they share with each other.

5 Chapter 7. Quantum Algorithms

5.1 Circuit and Query Complexity

- Circuit Complexity: The least number of gates required to implement a quantum circuit with respect to some universal set of gates.
- Query Complexity: The number of queries to an oracle required to solve the problem.
- Oracle Separation: Improvement or speedup in the number of oracle queries
- Quantum Oracle: Reversible boolean function
- Phase Oracle: Answer qubit $|y\rangle$ is unchanged, $|x\rangle$ is multiplied by a phase *(phase kickback)*. $|x\rangle|0\rangle \rightarrow^{I\otimes X} |x\rangle|1\rangle^{I\otimes H} \rightarrow |x\rangle|-\rangle$. We can drop the $|y\rangle$ term as it stays the same. So, $|x\rangle \rightarrow_f^U (-1)^{f(x)}|x\rangle$.

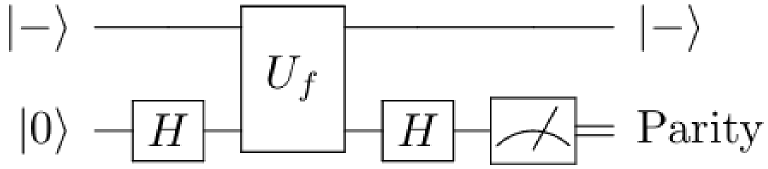


Figure 17: Deutsch's Algorithm Quantum Circuit

5.2 Parity

- Problem: Find parity of two bits $b_0 \oplus b_1$.
- Oracle: $f(0) = b_0$ and $f(1) = b_1$.
- Classical solution: Query oracle twice, the XOR $b_0 \otimes b_1$. Query Complexity: 2
- Quantum solution: Deutsch's Algorithm
- Circuit: Fig 17
- Working through the circuit:
  - $|0\rangle \to^H \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
  - $|-+\rangle \to_f^U \frac{1}{\sqrt{2}}[(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle]$
  - $\implies \frac{1}{\sqrt{2}}[(-1)^{b_0}|0\rangle + (-1)^{b_1}|1\rangle$
  - $\implies (-1)^{b_0}\frac{1}{\sqrt{2}}[|0\rangle + (-1)^{b_1-b_0}|1\rangle]$
  - $\implies \{(-1)^{b_0}|+\rangle, b_0 = b_1; (-1)^{b_0}|-\rangle, b_0 \neq b_1 \to^H = \{(-1)^{b_0}|0\rangle, b_0 = b_1; (-1)^{b_0}|1\rangle, b_0 \neq b_1$
- Quantum Query Complexity: 1

5.3 Constant vs Balanced Functions

- Problem: Given a function $f : 0, 1^n \to 0, 1^n$ that is guaranteed to be constant (outputs all 0s or all 1s) or balanced (outputs equal zeros and ones), find out whether it's constant or balanced.
- Oracle:
- Classical Solution: Query half+1 inputs, query complexity: $2^{n-1} + 1$, $O(2^n)$
- Classical Solution 2: There is a bounded error probabilistic polynomial time algorithm that guess the right answer in $O(1)$ time with error probability $\frac{1}{2^{c-1}}$ where c is the number of different inputs.
- Quantum Solution: Deutsch-Jozsa's algorithm. When we measure the circuit, if we get all zeros the circuit is constant. Else it is balanced.
- Circuit: Fig 18
- Quantum Query Complexity: 1

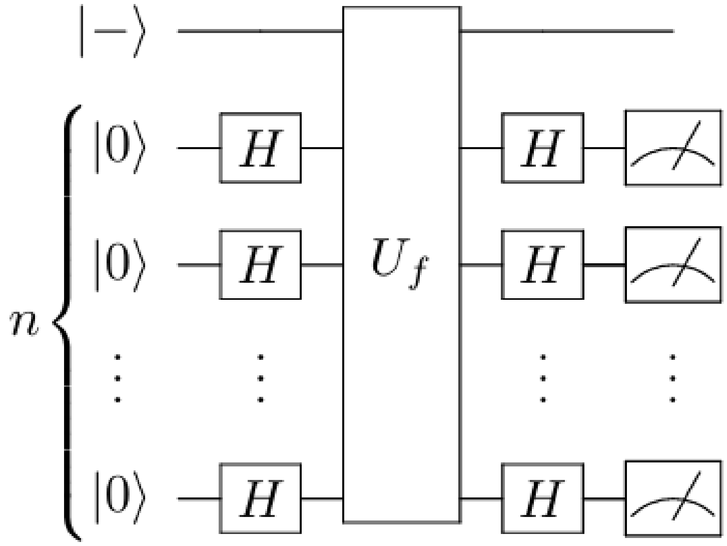


Figure 18: Deutsch-Josza's Algorithm Quantum Circuit

5.4 Secret Dot Product String

- Problem: Given $f : \{0,1\}^n \to \{0,1\}$ and the guarantee that $f(x) = s.x$ where s is some n-bit string $s_{n-1}...s_1s_0$, find s.
- Oracle:
- Classical Solution: Find $f(0...001), f(0...010)...f(1...000)$, Query complexity: n
- Quantum Solution: Bernstein-Vazirani Algorithm
- Circuit: Fig 19
- Working through the cirucit:
    - State of n qubits before measurement is $\sum_{z\epsilon\{0,1\}^n}(\frac{1}{2^n}\sum_{z\epsilon\{0,1\}^n}(-1)^{f(x)+x.z})\,|z\rangle$.
    - Plugging in $f(x) = s.x$, we get $\sum_{z\epsilon\{0,1\}^n}(\frac{1}{2^n}\sum_{z\epsilon\{0,1\}^n}(-1)^{(s+z).x})\,|z\rangle$.
    - Note that $s + z = s \oplus z$.
    - Upon measuring, when $z = s, z + s = 000...0$. Then the amplitude of $|z\rangle$ is $\frac{1}{2^n}\sum_x(-1)^0 = 1$.
- Quantum Query Complexity: 1

5.5 Secret XOR Mask

- Problem: Given $f : 0,1^n \to 0,1^n$ such that $f(x) = f(y)$ iff $x = y \otimes s$ and $y = x \otimes s$ for some secret n-bit string $s = s_{n-1}...s_1s_0 \neq 0...00$, find s.

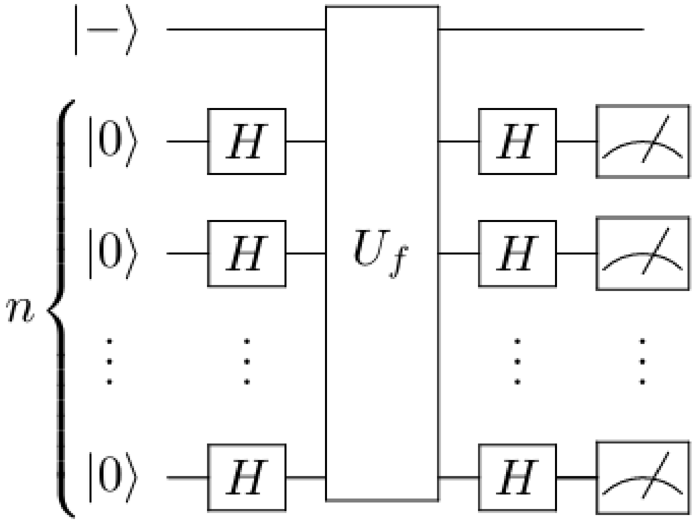


Figure 19: Bernstein Vazirani Algorithm Quantum Circuit

- Oracle:
- Classical Solution: Find a collision (x, y pair such that $f(x) = f(y)$. Then $x \otimes y = s$. Query complexity: $O(2^{n/2})$.
- Quantum Solution: Simon's algorithm $|x\rangle |y\rangle \rightarrow^{U_f} |x\rangle |y \otimes f(x)\rangle$.
- Circuit:
- When we measure the input qubits, we'll get a value $|z\rangle = |z_{n-1}...z_1 z_0\rangle$ such that $s_{n-1}z_{n-1} + ... + s_1 z_1 + s_0 z_0 = 0 \text{ mod } 2$. If we repeat this n times, we'll get n $|z\rangle$'s and we can solve for s.
- Quantum Query Complexity: $O(n)$

5.6 Brute-Force Searching

- Problem: Given $f : \{0,1\}^n \rightarrow \{0,1\}$ which outputs 1 only for one input (w) and 0 for all other inputs, find w.
- Classical Solution: Brute force search, Query complexity $O(N)$ where $N = 2^n$.
- Quantum Solution: Grover's Algorithm
- Circuit: Fig 21
- Intuition:
  - We start with a Hadamard on all qubits, which is an equal super position of all states. So after this Hadamard, the circuit has all 2^n states including our answer state until measure.

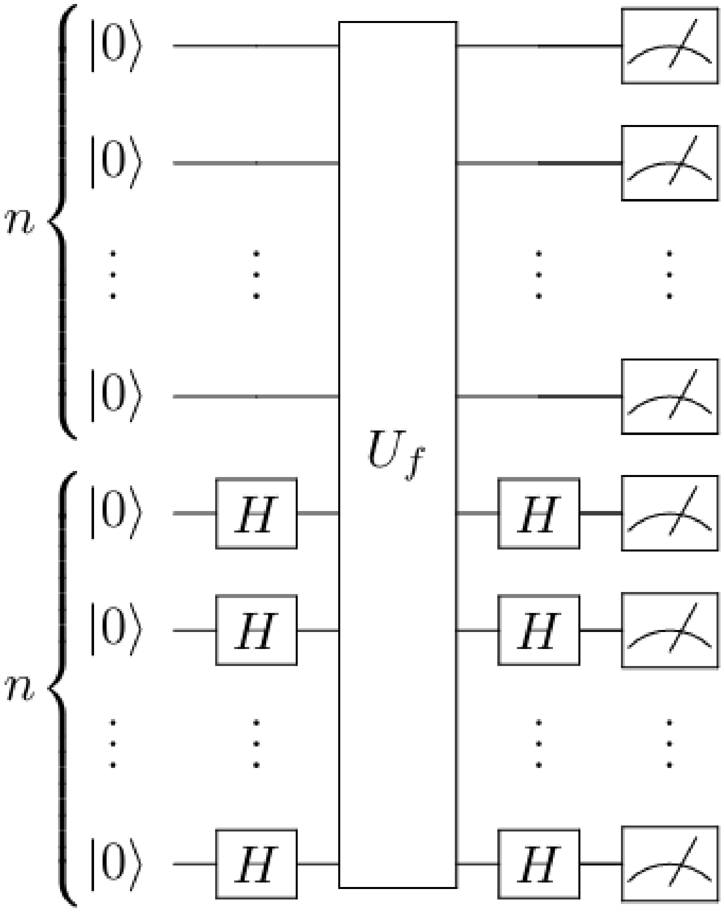


Figure 20: Simon's Algorithm Quantum Circuit

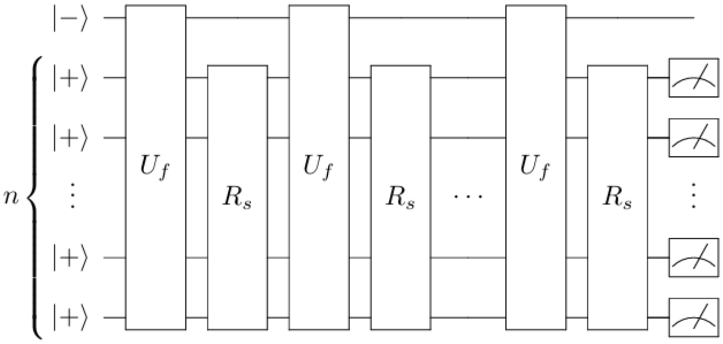


Figure 21: Grover's Algorithm Quantum Circuit

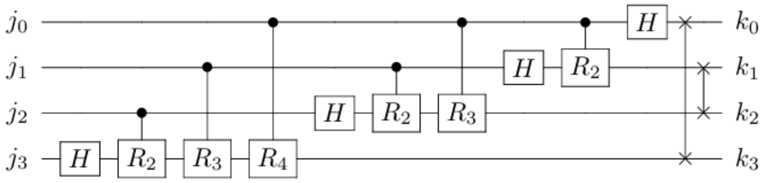


Figure 22: QFT Quantum Circuit

  - How do we increase the amplitude of our answer state so that it has a higher probability of getting measured? To do this, we do a series of phase oracle queries + reflections about s $U_f + R_s$. Each such step increases the amplitude of $|w\rangle$ while reducing the amplitudes of the remaining states.

- Quantum Query Complexity: $O(\sqrt{N})$

5.7 Discrete Fourier Transform

- Problem: We have a wave that has N sample amplitudes $a_0, a_1, ...a_{N-1}$. The discrete fourier transform is the sequence of N points $\phi_0, \phi_1, ...\phi_{N-1}$ such that $\phi_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} a_j e^{2\pi ijk/N}$. Find $\phi_0, ...\phi_{N-1}$.
- Oracle:
- Classical Solution: Fast Fourier Transform. $O(NlogN)$.
- Quantum Solution: QuantumFourier Transform - the discrete Fourier transform can be written as a NxN matrix-vector multiplication, this matrix is unitary and is a valid quantum gate (QFT). QFT transforms the state as -

$$|\psi\rangle = \sum_{j=0}^{N-1} a_j |j\rangle \rightarrow |\phi\rangle = \sum_{k=0}^{N-1} \phi_k |k\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \sum_{j=0}^{N-1} a_j e^{2\pi ijk/N} \tag{9}$$

  This transforms the basis states from $|j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi ijk/N} |k\rangle$

- Circuit: Fig 22
- Working through the cirucit:
- Quantum Query Complexity: $O(log^2 N)$

5.8 Phase/Eigenvalue Estimation

- Problem: Given a matrix A, a vector X is said to be its eigenvector if $AX = \lambda X$ for some λ. And λ is called the eigenvalue. Given a unitary matrix U and one of its eigenvectors $|v\rangle$, find or estimate its eigenvalue. Eigenvalues of a unitary matrix must have the form $e^{i\theta}$ for some real θ. So this is also called the phase estimation problem.
- Oracle:
- Classical Solution: $U|v\rangle = e^{i\theta}|v\rangle$. Expanding this in matrix form, we can use any row to find θ. For example, $U_{11}v_1 + U_{12}v_2 + ... + U_{1N}v_N = e^{i\theta}v_1$. So, $e^{i\theta} = \frac{U_{11}v_1 + U_{12}v_2 + ... + U_{1N}v_N}{v_1}$. Query complexity : $O(N)$.

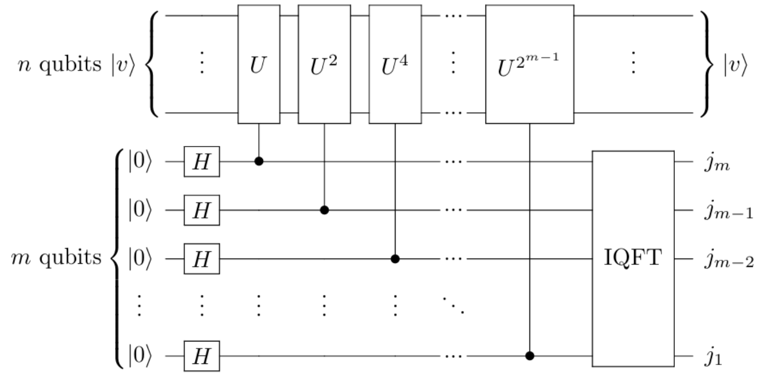


Figure 23: Phase Estimation Quantum Circuit

- Quantum Solution: We use the phase estimation circuit describe below, which uses IQFT. To estimate the eigenvalue to m bits precision, we need m Hadamard gates, m controlled-U^p operations and an IQFT on m qubits that takes $O(m^2)$ gates. When we have multiple eigenstates, we can prepare the eigenstate register as a superposition of these two, and generate the eigenvalue register as a superposition of the two eigenvalues.
- Circuit: Fig 23
- Working through the circuit:
  - We start with two m and n qubit quantum registers $|0...000\rangle |v\rangle$.
  - $|v\rangle$ has the eigen state.$|0...000\rangle$ will have the eigenvalue.
  - After the Hadamard, these become $|+... + ++\rangle |v\rangle$.
  -
- Quantum Query Complexity: $O(m^2)$ where m is the number of bits of precision we want for θ

5.9 Period of Modular Exponentiation

- Problem: *Modular exponentiation* - taking the power of a number modulo some other number. Example - $2^0 mod 7 = 1 mod 7, 2^1 mod 7 = 2 mod 7$ etc. The period or order r of the modular exponential is the length of the repeating sequence. So for $2^n mod 7$, the order is 3 (1,2,4,1,2,4...). Another way to describe the period is, it is the smallest positive exponent r for which $a^r mod N = 1$.
- Classical Solution: Repeated squaring method. $kO(n^3)$
- Quantum Solution:
  - Consider a quantum gate U which performs modular multiplication $U|y\rangle = |ay mod N\rangle$. By repeatedly applying U to $|1\rangle$ we get $U^r|1\rangle = |a^r mod N\rangle = |a^0 mod N\rangle$. Now consider a superposition of $|a^0 mod N\rangle, |a^1 mod N\rangle, ... |a^{r-1} mod N\rangle$ with respective coefficients $e^{-2\pi i s(0)/r}, e^{-2\pi i s(1)/r} ... e^{-2\pi i s(r-1)/r}$ where s is an integer taking the values 0,1,...r-1. We get equation 10

$$|v_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi i s k/r} |a^k mod N\rangle \tag{10}$$

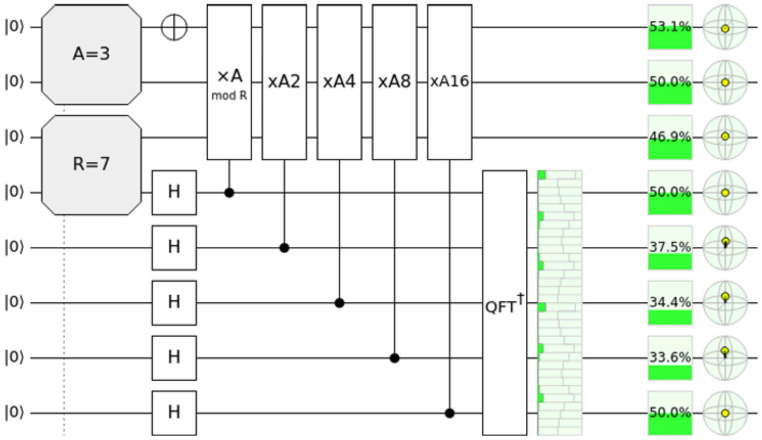


Figure 24: Period Of Modular Exponentiation Circuit

  - $|v_s\rangle$ is an eigenvector of U with eigenvalue $e^{2\pi is/r}$. We can use the phase-estimation algorithm to figure out the corresponding eigen value $e^{2\pi is/r}$. So we have s/r for some s.
  - Three open questions remain - constructing controlled-U gates for phase-estimation, constructing the eigen vector $|v_s\rangle$ for phase estimation and taking the result of phase estimation - finding r from s/r.
  - Constructing controlled-U gates for phase-estimation: If we choose to approximate the eigenvalue to $m = O(n)$ bits, writing the control qubit as $|z\rangle$ and the target bit as $|y\rangle$, the operation of CU^{2^j} is equation 11

$$CU^{2^j} |z\rangle |y\rangle = |z\rangle |a^{z2^j} ymodN\rangle \tag{11}$$

  - Constructing the eigen vector $|v_s\rangle$: Instead of preparing a single eigenvector, prepare the superposition $\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |v_s\rangle$.
  - Finding r from s/r, use convergents of the irrational number (p337-339, not going in detail).

- Circuit: Fig 24
- Quantum Query Complexity: $O(n^3)$

5.10 Factoring

- Problem: Say we have $N = pq$ where p and q are prime, find p and q.
- Classical Solution: Number field sieve. $O(e^{n^{1/3}})$
- Quantum Solution: Shor's algorithm
  - Pick any number $1 < a < N$. Find $gcd(a, N)$. If $gcd(a, N)! = 1$, stop. Else, let $p = gcd(a, N)$. Then $q = N/p$.
  - Find period r of $a^x modN$ using period finding algorithm. If r is odd, go back to Step 1 and find a different a. If $a^{r/2} modN = N - 1$, find a different a from Step 1.
  - $p = gcd(a^{r/2} - 1, N)$ and $q = gcd(a^{r/2} + 1, N)$.
- Quantum Query Complexity: $O(n^3)$

5.11 Summary

Problem	Classical	Quantum	Quantum	Notes
	Queries	Algorithm	Queries	
n-bit Parity	n	Deutsch	$n/2$	No speedup
Constant vs Balanced	Exact: $2^{n-1} + 1$ Bounded: $O(1)$	Deutsch-Jozsa	1	BPP = $\frac{1}{2^{c-1}}$
Dot Product String	n	Bernstein-Vazirani	1	Polynomial speedup
Rec. Dot Product String	$\Omega(n^{\log_2 n})$	Rec. Bernstein-Vazirani	n	Superpolynomial speedup
XOR Mask	$O(2^{n/2})$	Simon	$O(n)$	$P(anyZ) = \frac{1}{2^{n-1}}$; $s.z = 0 modz$
Brute Force Search	$O(2^n)$	Grover's	$O(\sqrt{N})$	$N = 2^n$; $P(\|q\rangle) = sin^2((r + \frac{1}{2})\theta)$
FT	$O(NlogN)$	QFT	$O(log^2 N)$	$H + CR$ gates - $\frac{n(n+1)}{2}$; SWAP gates - $\frac{n}{2}$
Phase Estimation	O(N)		$O(m^2)$	H gates - m; CU gates - m; m - precision
POME	$kO(n^3)$		$O(n^3)$	
Factoring	$e^{n^{1/3}}$		$O(n^3)$	
Superdense Coding	n bits		$n/2$ qubits	
Quantum Teleportation	many bits		2 classical bits	
Quantum Key Distribution				P(A,B detect E) = $1 - (\frac{3}{4})^n$