CMSC5706 Topics in Theoretical Computer Science

Week 12: Quantum computing

Instructor: Shengyu Zhang
Roadmap

• Intro to math model of quantum mechanics
• Review of quantum algorithms
• The power of quantum computers.
• Quantum games.
Postulate 1: States

• **State space**: Every isolated physical system corresponds to a unit vector in a complex vector space.
  – Unit vector: $\ell_2$-norm is 1.

• Such states are called **pure states**.

• We use a weird "ket" notation $|\cdot\rangle$ to denote such a state.
Ket notation

• Mathematically, $|\cdot\rangle$ is a column vector.
• And $\langle\cdot|$ is a row vector.
• $\langle\psi|\phi\rangle$ is the inner product between the vectors $|\phi\rangle$ and $|\psi\rangle$.
• $\langle\psi|M|\psi\rangle$ is just the quadratic form $\psi^T M \psi$. 
• A quantum bit, or qubit, is a state of the form 
  $\alpha |0\rangle + \beta |1\rangle$
where $\alpha, \beta \in \mathbb{C}$ are called amplitudes, satisfying that 
  $|\alpha|^2 + |\beta|^2 = 1$.
• So a qubit can sit anywhere between 0 and 1 (on the unit circle).
• We say that the state is in superposition of $|0\rangle$ and $|1\rangle$. 

A quantum bit (qubit)
Postulate 2: operation

- **Evolution**: The evolution of a closed quantum system is described by a unitary transformation.

- That is, if a system is in state $|\psi_1\rangle$ at time $t_1$, and in state $|\psi_2\rangle$ at time $t_2$, then there is a unitary transformation $U$ s.t.
  $$|\psi_2\rangle = U|\psi_1\rangle.$$

- **Unitary transformation**: $U^\dagger = U^{-1}$
  - Recall: $U^\dagger = (U^T)^*$, transpose + complex conjugate
  - You can think of it as a rotation operation.
Postulate 3: measurement

• **Measurement:** We can only observe a quantum system by measuring it.

• The outcome of the measurement is random.

• And the system is changed by the measurement.
• If we measure qubit $\alpha|0\rangle + \beta|1\rangle$ in the computational basis $\{|0\rangle, |1\rangle\}$, then outcome “0” occurs with prob. $|\alpha|^2$, and outcome “1” occurs with prob. $|\beta|^2$.

• The system becomes $|0\rangle$ if outcome “0” occurs, and becomes $|1\rangle$ if outcome “1” occurs.
  – The system collapses.
Measurement on general states

• In general, an orthogonal measurement of a $d$-dim state is given by an orthonormal basis $\{ |\psi_1\rangle, ..., |\psi_d\rangle \}$.

• If we measure state $|\phi\rangle$ in basis $\{ |\psi_1\rangle, ..., |\psi_d\rangle \}$, then outcome $i \in \{1, ..., d\}$ occurs with prob. $|\langle \phi | \psi_i \rangle|^2$.

• The system collapses to $|\psi_i\rangle$ if outcome $i$ occurs.
Postulate 4: composition

• Composition: The state of the joint system 
  \((S_1, S_2)\), where \(S_1\) is in state \(|\psi_1\rangle\) and \(S_2\) in \(|\psi_2\rangle\), is \(|\psi_1\rangle \otimes |\psi_2\rangle\).

• \(\otimes\): tensor product of vectors.
  
  - \((a_1, a_2) \otimes (b_1, b_2, b_3) = (a_1 b_1, a_1 b_2, a_1 b_3, a_2 b_1, a_2 b_2, a_2 b_3)\).
  
  - \(\text{dim}(|\psi_1\rangle \otimes |\psi_2\rangle) = \text{dim}(|\psi_1\rangle) \cdot \text{dim}(|\psi_2\rangle)\)
  
  - \(\text{size}(|\psi_1\rangle \otimes |\psi_2\rangle) = \text{size}(|\psi_1\rangle) + \text{size}(|\psi_2\rangle)\)
    
    • size: number of qubits.

• Notation: \(|0\rangle^{\otimes n} = |0\rangle \otimes \cdots \otimes |0\rangle\), \(n\) times.
Quantum mechanics in one slide

Math

Tensor Product

Composition

Projection

Unitary Matrix

Unit Vector

Physical System

Evolution

Measurement

Physics

Classical:

Quantum:

State space for 2 bits: combinations \{00,01,10,11\}

State space for 2 qubits: space \text{span}\{\text{\ket{00}}, \text{\ket{01}}, \text{\ket{10}}, \text{\ket{11}}\}
Density matrix

- If a system is in state $|\psi_1\rangle$ with probability $p_1$, and in state $|\psi_2\rangle$ with probability $p_2$, then the system is in a **mixed state**.
  - The mixed state is represented as a **density matrix**
    \[
    \rho = p_1 |\psi_1\rangle\langle \psi_1 | + p_2 |\psi_2\rangle\langle \psi_2 |. 
    \]
- In general, if a system is in state $|\psi_i\rangle$ with probability $p_i$, then the mixed state is
  \[
  \rho = \sum_i p_i |\psi_i\rangle\langle \psi_i | 
  \]
- For pure state $|\psi\rangle$, $\rho = |\psi\rangle\langle \psi |$. 

Density matrix

- **Fact.** A matrix $\rho$ is a density matrix of some mixed quantum state iff
  - $\rho$ is positive semi-definite (psd)
  - $\text{Tr}(\rho) = 1$.

- **Recall:**
  - A matrix $M$ is psd if all its eigenvalues are nonnegative. Equivalently, if $\langle \nu | M | \nu \rangle \geq 0, \forall \nu$.
  - The trace of a matrix $M$ is $\text{Tr}(M) = \sum_i M_{ii}$. 
Postulates on mixed states

- **Unitary operation** $U: \rho \mapsto U\rho U^\dagger$
  - For pure state $\rho = |\phi\rangle\langle\phi|$, it becomes $U\rho U^\dagger = U|\phi\rangle\langle\phi|U^\dagger = |\phi'\rangle\langle\phi'|$ where $|\phi'\rangle = U|\phi\rangle$.

- **Orthogonal measurement** $\{|\psi_1\rangle, ..., |\psi_d\rangle\}$: outcome $i$ occurs with probability $|\langle\psi|\rho|\psi\rangle|^2$, and the system collapses to $\rho' = |\psi_i\rangle\langle\psi_i|$.
  - For pure state $\rho = |\phi\rangle\langle\phi|$, the probability is $|\langle\phi|\psi_i\rangle|^2$, and the collapsed state is $|\psi_i\rangle$.

- If we measure $\rho \in \mathbb{C}^{d\times d}$ in the computational basis $\{|1\rangle, |2\rangle, ..., |d\rangle\}$, then $\text{Pr}[\text{outcome } i \text{ occurs}] = \rho_{ii}$, the $i$-th diagonal entry of $\rho$. 
• Composition of $\rho_1$ and $\rho_2$ is just $\rho_1 \otimes \rho_2$
  – For pure state $\rho_1 = |\phi_1\rangle\langle\phi_1|$ and $\rho_2 = |\phi_2\rangle\langle\phi_2|$, the joint state is
    $|\phi_1\rangle\langle\phi_1| \otimes |\phi_2\rangle\langle\phi_2|$
    $= (|\phi_1\rangle \otimes |\phi_2\rangle)(\langle\phi_1| \otimes \langle\phi_2|)$

• Recall tensor product of matrices:

$$
\begin{bmatrix}
  a_{11} & a_{12} \\
  a_{21} & a_{22}
\end{bmatrix} \otimes \begin{bmatrix}
  b_{11} & b_{12} \\
  b_{21} & b_{22}
\end{bmatrix} = 
\begin{bmatrix}
  a_{11}b_{11} & a_{11}b_{12} & a_{12}b_{11} & a_{12}b_{12} \\
  a_{11}b_{21} & a_{11}b_{22} & a_{12}b_{21} & a_{12}b_{22} \\
  a_{21}b_{11} & a_{21}b_{12} & a_{22}b_{11} & a_{22}b_{12} \\
  a_{21}b_{21} & a_{21}b_{22} & a_{22}b_{21} & a_{22}b_{22}
\end{bmatrix}
$$
• For operation, measurement and composition, these formulas for mixed states are all consistent to what we learned for pure states.

• So the formulas for mixed states extend those for pure states.
entanglement

- Consider the following EPR pair state in a 2-qubit system: \( \frac{|00\rangle + |11\rangle}{\sqrt{2}} \)
- It’s in superposition of \( |00\rangle \) and \( |11\rangle \).
- There is no classical counterpart of this.

**Question:** Is it really different than the classical correlation

\[
\begin{align*}
00 & \text{ with prob. } 1/2 \\
11 & \text{ with prob. } 1/2
\end{align*}
\]
CHSH non-local game

• $x \in_R \{0,1\}$, $y \in_R \{0,1\}$

• Goal: A outputs $s$ and B outputs $t$ s.t.
  \[ s \oplus t = x \cdot y \]

• Value = largest $\Pr[s \oplus t = x \cdot y]$.

• Classical value: $3/4 = 0.75$.
  – Even with shared randomness.

• Quantum value: $\frac{1}{2} + \frac{1}{2\sqrt{2}} \approx 0.85$
  – By sharing an EPR pair.
Roadmap

• Intro to math model of quantum mechanics
• Review of quantum algorithms
• The power of quantum computers.
• Quantum games.
Areas in quantum computing

- Quantum algorithms
- Quantum complexity
- Quantum cryptography
- Quantum error correction
- Quantum information theory
- Others: Quantum game theory / control / …
Area 1: Quantum Algorithms

- QFT (Quantum Fourier Transform): exponential speedup; slower than expected.
- Shor: Factoring & Discrete Log
- Factoring: Given an $n$-bit number, factor it (into product of two numbers).
  - Classical (best known): $O \left( 2^{n^{1/3}} \right)$
  - Quantum*1: $O(n^2)$

Area 1: Quantum Algorithms


- QFT (Quantum Fourier Transform): exponential speedup; slower than expected.

- Implication of fast algorithm for Factoring
  - Theoretical: Church-Turing thesis
  - Practical: Breaking RSA-based cryptosystems
Area 1: Quantum Algorithms

QFT (Quantum Fourier Transform): exponential speedup; slower than expected.

- Pell’s Equation: \( x^2 - ny^2 = 1 \).
- Problem: Given \( n \), find solutions \((x, y)\) to the above equation.
- Classical (best known):
  - \( \sim 2^{\sqrt{\log n}} \) (assuming the generalized Riemann hypothesis)
  - \( \sim n^{1/4} \) (no assumptions)
- Quantum\(^1\): \( \text{poly}(\log n) \).

Area 1: Quantum Algorithms


- Shor: Factoring & Discrete Log
- Hallgren: Pell’s Equation
- Kuperberg: HSP-Dihedral

(Quantum Fourier Transform): exponential speedup; slower than expected.

- Hidden Subgroup Problem (HSP): Given a function $f$ on a group $G$, which has a hidden subgroup $H$, s.t. $f$ is
  - constant on each coset $aH$,
  - distinct on different cosets.
Task: find the hidden $H$.
- Factoring, Pell’s Equation both reduce to it.
- Efficient quantum algorithms are known for Abelian groups.
- Main question: HSP for non-Abelian groups?
Area 1: Quantum Algorithms

QFT (Quantum Fourier Transform): exponential speedup; slower than expected.

- Two biggest cases:
  - HSP for symmetric group $S_n$: Graph Isomorphism reduces to it.
  - HSP for dihedral group $D_n$: Shortest Lattice Vector reduces to it.

- HSP($D_n$):
  - Classical (best known): $2^{\log |G|}$
  - Quantum*1: $2^{O(\sqrt{\log |G|})} \cdot 2^{O(\sqrt{\log |G|})}$

Area 1: Quantum Algorithms

QFT (Quantum Fourier Transform): exponential speedup; slower than expected.

QS (Quantum Search): polynomial speedup; most solved.

- Shor: Factoring & Discrete Log
- Hallgren: Pell’s Equation
- Kuperberg: HSP-Dihedral

*Given $n$ bits $x_1, \ldots, x_n$, find an $i$ with $x_i = 1$.
- Classical: $\Theta(n)$
- Quantum*1: $\Theta(\sqrt{n})$

Area 1: Quantum Algorithms

- QFT: Quantum Fourier Transform - exponential speedup; slower than expected.
- QS: Quantum Search - polynomial speedup; most solved.
- Shor: Factoring & Discrete Log
- Hallgren: Pell’s Equation
- Kuperberg: HSP-Dihedral
- Grover: Search
- Many combinatorial/graph problems
- QW: Quantum Walk - poly and exp speedup; rapidly developed.

*1: D. Aharonov, A. Ambainis, J. Kempe, U. Vazirani. STOC'01
• Classical random walk on graphs: starting from some vertex, repeatedly go to a random neighbor
  – Many algorithmic applications

• Quantum walk on graphs: even definition is non-trivial.
  – For instance: classical random walk converges to a stationary distribution, but quantum walk doesn’t since unitary is reversible.

(Quantum Walk): poly and exp speedup; rapidly developed.

*1: D. Aharonov, A. Ambainis, J. Kempe, U. Vazirani. STOC'01
Area 1: Quantum Algorithms


- Element Distinctness: Given $n$ integers, decide whether they are all distinct.
- Classical: $\Theta(n)$
- Quantum: $\Theta(n^{2/3})$

*1: A. Ambainis, FOCS’04

(Quantum Walk): poly and exp speedup; rapidly developed.
Area 1: Quantum Algorithms


QW: Quantum Walk; poly and exp speedup; rapidly developed.

AAKV: A. Ambainis, A. Childs, B. Reichardt, R. Spalek, S. Zhang. FOCS’07

- Classical: $\Theta(n)$
- Quantum: $\sim \Theta(\sqrt{n})$
- apply QW on the formula graph with weight carefully designed for inductions to work.

Grover’s search: OR function

general formula by \{AND-OR-NOT\}

AAKV: Def
Ambainis: Ele. Dist.
ACRSZ*1: Formula Evaluation

*1: A. Ambainis, A. Childs, B. Reichardt, R. Spalek, S. Zhang. FOCS’07
Roadmap

• Intro to math model of quantum mechanics
• Review of quantum algorithms
• The power of quantum computers.
• Quantum games.
Power of quantum computing

- **Question**: How powerful is quantum computer?
- **P**: problems solvable in polynomial time
  - One characterization of efficient computation
- **BPP**: problems solvable in probabilistic polynomial time w/ a small error tolerated
  - Another characterization of efficient computation
- **BQP**: problems solvable in polynomial time by a quantum computer w/ a small error tolerated
  - Yet another characterization of efficient computation, if you believe large-scale quantum mechanics.
Classical upper bound of BQP

• Central in complexity theory: comparison of different modes of computation
• How to compare classical and quantum efficient computation?
• Quantum is more powerful: \( \text{BPP} \subseteq \text{BQP} \)
• An upper bound (of quantum by classical)
• [Thm*1] \( \text{BQP} \subseteq \text{PSPACE} \)
  – PSPACE: problems solvable in polynomial space.
  – Believed to be much larger than NP.

*1: Bernstein, Vazirani. STOC’93, SIAM J. on Computing, 1997
Where does BQP sit in?

- BQP contains BPP and P.
- But it probably doesn’t contain all NP.
- Yet it’s possible to be outside PH.
- It’s position may be weird.
Roadmap

• Intro to math model of quantum mechanics
• Review of quantum algorithms
• The power of quantum computers.
• Quantum games.
Meyer’s game: classical

- Actions $A_i, B_i$: to flip or not to flip
- A Nash equilibrium: $A_i, B_i$ flip with half prob.
  - Then each wins with half prob.
Meyer’s game: quantum

- Bob remains classical: $B_1$ is either $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ (Swap $|0\rangle$ and $|1\rangle$) or identity (doing nothing).
- Alice is quantum: $A_i$ can be any 1-qubit operation.
- Alice’s Goal: $|0\rangle$. Bob’s Goal: $|1\rangle$.
- Now Alice can win for sure by applying a Hadamard gate. $A_1: |0\rangle \rightarrow |+\rangle$. $A_2: |+\rangle \rightarrow |0\rangle$. 
Meyer’s game: fairness issue

Despite the quantum advantage, there is a clear fairness issue.
- Alice has two actions.
- And the actions are in a fixed order of $A_1 \rightarrow B_1 \rightarrow A_2$.

**Question:** Can quantum advantage still exist in a more fair setting?

For fairness: each player makes just one action, simultaneously.
- This is nothing but strategic games!
Quantization*¹ of strategic game: Penny Matching

|φ⟩ = ½|+⟩|0⟩ + ½|−⟩|1⟩

|φ⟩ is an equilibrium if both players are classical,
  – Each wins with half prob.

If Alice turns to quantum: A = H turns |φ⟩ into ½|0⟩|0⟩ + ½|1⟩|1⟩. Then she wins for sure!

- Message: quantum player has a huge advantage when playing against a classical player.

*¹ Zu, Wang, Chang, Wei, Zhang, Duan, NJP, 2012.
• State is symmetric, so it doesn’t matter who takes which qubit.
• We can also let the classical player Bob to choose the target goal.
  – If Bob wants $a = b$, then Alice applies $XH$. 

Quantization of strategic game: Penny Matching

$$|\varphi\rangle = \frac{|+\rangle|0\rangle + |\rangle 1\rangle}{\sqrt{2}}$$

$$= \frac{|0\rangle|+\rangle + |1\rangle|\rangle}{\sqrt{2}}$$
Quantum advantage in strategic games

\[ |\varphi\rangle = \frac{|+\rangle|0\rangle + |-\rangle|1\rangle}{\sqrt{2}} \]

Entangled. Necessary?

No! \( \rho = \frac{1}{4} \left( |+\rangle(+)| \otimes |0\rangle\langle 0| + |0\rangle\langle 0| \otimes |+\rangle(+)| \right) \)

No entanglement. But has discord.

- \( \rho \) is an equilibrium if both players are classical, each winning with prob. = \( \frac{1}{2} \)
- If Alice uses quantum, \( A = H \) increases her winning prob. to \( \frac{3}{4} \).
- \textbf{Question*2: Is discord necessary?}
  - Yes, if each player’s part (of the shared state) is a qubit,
  - No, if each player’s part (of the shared state) has dimension 3 or more.

Games between quantum players

• After these examples, Bob realizes that he should use quantum computers as well.

• **Question**: Any advantage when both players are quantum?

• Previous correspondence results imply a negative answer for complete information games.

• But quantum advantage exists for Bayesian games!
Quantum Bayesian games

- Each player $i$ has a private input/type $x_i$.
  - $x_i$ is known to Player $i$ only.
  - The joint input is drawn from some distribution $P$.
- Each player $i$ can potentially apply some operation $\phi_i$.
- A measurement in the computational basis gives output $|y_i\rangle$ for Player $i$, who receives utility $u_i(x_1, x_2, y_1, y_2)$. 
Quantum Bayesian games

- Classical state $|\varphi\rangle = (r_1, r_2) \leftarrow$ distribution $Q$.
- Classical strategy $\Phi_i = c_i(x_i, r_i)$.
- Classical payoff
  $$E[u_i] = E_{x \leftarrow P, r \leftarrow Q}[u_i(x, c_1(x_1, r_1), c_2(x_2, r_2))]$$
- $(Q, c_1, c_2)$ is equilibrium if no player can gain a higher payoff by changing her strategy unilaterally.
Quantum Bayesian games

- Quantum strategy $\Phi_1 = \{E_{x_1}^{y_1}: E_{x_1}^{y_1} \succeq 0, \sum_{y_1} E_{x_1}^{y_1} = I\}$, $\Phi_2 = \{F_{x_2}^{y_2}: F_{x_2}^{y_2} \succeq 0, \sum_{y_2} F_{x_2}^{y_2} = I\}$.
- Quantum payoff
  $E[u_i] = E_x[p] \langle \varphi | E_{x_1}^{y_1} \otimes F_{x_2}^{y_2} \varphi \rangle \cdot u_i(x, y)$
- $(|\varphi\rangle, \Phi_1, \Phi_2)$ is equilibrium if no player can gain a higher payoff by changing her strategy unilaterally.

potential action classical outcome utility

$(x_1, x_2) \leftarrow P$

$|\varphi\rangle$

$|y_1\rangle \quad u_1(x_1, x_2, y_1, y_2)$

$|y_2\rangle \quad u_2(x_1, x_2, y_1, y_2)$
Quantum Bayesian games

A game\(^*1\) combining Battle of the Sexes and CHSH.

The players need to coordinate like in CHSH, except when \(x_1 = x_2 = 1\), in which case they need to anti-coordinate.

In Table I, they have conflicting interest.

\(^*1\) Pappa, Kumar, Lawson, Santha, Zhang, Diamanti, Kerenidis, \textit{PRL}, 2015.
Quantum Bayesian games

- \( P \) is uniform.
- Classical: \( u_1 + u_2 \leq 9/8 \).
  And \( \exists \) a fair equilibrium with \( u_1 = u_2 = 9/16 = 0.5625 \).
- Quantum: \( \exists \) a fair equilibrium with 
  \( u_1 = u_2 = (3/4) \cos^2(\pi/8) \approx 0.64 \).

<table>
<thead>
<tr>
<th>( y_A = 0 )</th>
<th>( y_B = 0 )</th>
<th>( y_B = 1 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( y_A = 0 )</td>
<td>(1,1/2)</td>
<td>(0,0)</td>
</tr>
<tr>
<td>( y_A = 1 )</td>
<td>(0,0)</td>
<td>(1/2,1)</td>
</tr>
</tbody>
</table>

Table I: \( x_A \land x_B = 0 \)

\[
\begin{array}{c|c|c}
 y_A & y_B = 0 & y_B = 1 \\
--- & --- & --- \\
 y_A = 0 & (0,0) & (3/4,3/4) \\
 y_A = 1 & (3/4,3/4) & (0,0) \\
\end{array}
\]

Table II: \( x_A \land x_B = 1 \)

Viewed as non-locality

• Traditional quantum non-local games exhibit quantum advantages when the two players have the common goal.
  – CHSH, GHZ, Magic Square Game, Hidden Matching Game, Brunner-Linden game.

• Now the two players have conflicting interests.

• Quantum advantages still exist.

• **Message**: If both players play quantum strategies in an equilibrium, they can also have advantage over both being classical.
Summary

• Quantum algorithms: offer huge speedup for certain computational problems.
• Quantum entanglement:
  – A distinctive feature of quantum mechanics.
  – Proof that our world is quantum mechanical.
• Quantum games: quantum players can have big advantages.