Modeling quantum interactions as games

John Watrous

Institute for Quantum Computing
University of Waterloo

April 25, 2009

Overview

This talk will be about **“quantum games”**, which can model a variety of computational and cryptographic situations involving quantum information.

The main points to be addressed in this talk:

1. An answer to the question: what is a “quantum game”, and what is the motivation for thinking about them?
2. Interesting types of quantum games, and what we know about them.
3. Challenges and future directions.

A key goal in this area:

To understand the full range of options available to individuals or groups in structured, interactive settings.

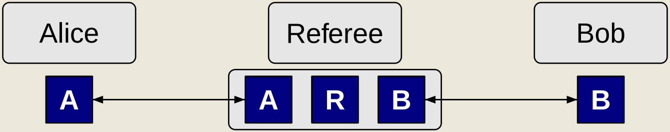
What is a "quantum game"?

For this talk, the term "quantum game" will refer to any **structured interaction** involving **quantum information** in which a collection of **players** have well-defined **goals**.

Examples:

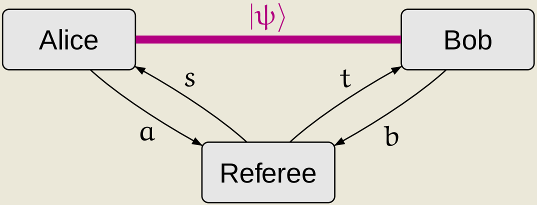
1. **Quantum interactive proof systems**: General setting based on interactive verification of proofs; models certain cryptographic situations.
2. **Nonlocal games**: Cooperative games; related to Bell inequality violations and multi-prover interactive proofs.
3. **Quantum coin-flipping**: interesting quantum task; very little structure in interaction.

Example: one-round zero-sum quantum games



- Two **competing** players: **Alice** and **Bob**. The game is run by a **Referee**.
- Referee prepares a quantum state of three registers $(\mathbf{A}, \mathbf{R}, \mathbf{B})$; and sends **A** to Alice and **B** to Bob.
- Alice performs an operation on **A** and sends it back to the referee. Bob does likewise with **B**.
- Referee measures $(\mathbf{A}, \mathbf{R}, \mathbf{B})$, and the outcome determines whether **Alice wins** (and Bob loses) or **Bob wins** (and Alice loses).

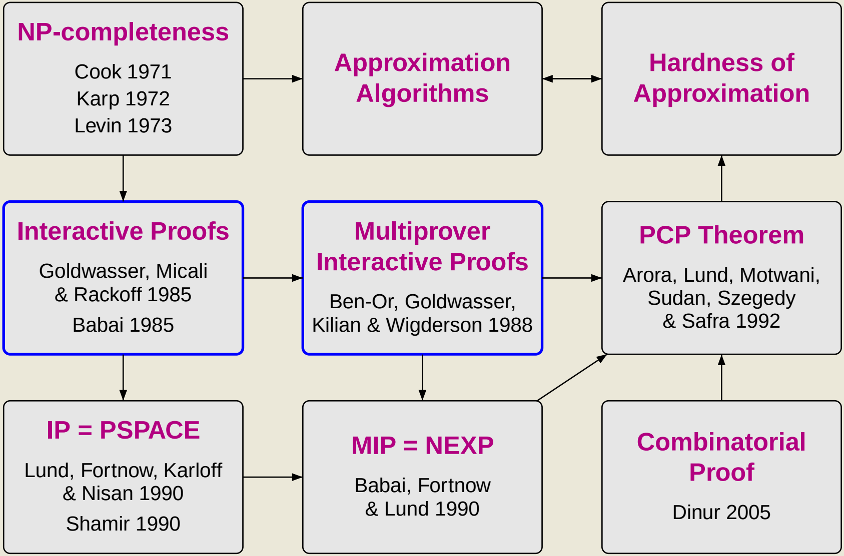
Another example: nonlocal games



- Two **cooperating** players: **Alice** and **Bob**. **No communication once game starts.** (Again the game is run by a **referee**.)
- Referee randomly chooses **classical** questions: s for Alice, t for Bob.
- Alice responds with a, Bob responds with b.
- Referee evaluates a predicate on (s, t, a, b) to determine one of two outcomes: **Alice and Bob win** or **Alice and Bob lose**.

(**Entanglement** has a major impact on this type of game.)

Historical motivation



Understanding a full range of strategies

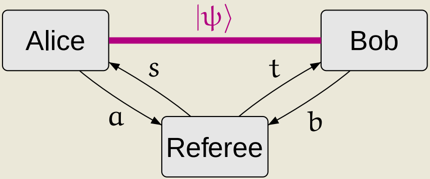
The most **significant** advancements in understanding quantum games, and the most interesting open questions about them, involve understanding the **full range of strategies** available to players.

The full range of strategies available to players is reasonably well-understood, to varying degrees, for these settings:

- Nonlocal games in restricted settings (XOR games and unique games).
- Quantum coin-flipping.
- Single player games and competitive zero-sum games.

Semidefinite programming has turned out to be a very powerful tool in these settings.

Example: XOR games



An **XOR game** is a nonlocal game where $a, b \in \{0, 1\}$, and the referee's final decision depends only on s, t, and $a \oplus b$.

The full range of strategies for Alice and Bob is perfectly represented by a collection of real unit vectors:

$$\{u_s : s \in S\} \cup \{v_t : t \in T\}.$$

On questions (s, t), Alice and Bob answer (a, b) satisfying

$$\langle u_s, v_t \rangle = \Pr[a = b] - \Pr[a \neq b].$$

(TSIRELSON 1987)

Coin-flipping and zero-sum games

There has been great progress in understanding **quantum coin-flipping**:

- KITAEV AND MOCHON (2007): optimal weak quantum coin-flipping.
- CHAILLOUX AND KERENIDIS (2009): optimal strong quantum coin-flipping.

Quantum interactive proofs with single or competing provers, and **zero-sum quantum games** more generally, are also comparatively well-understood:

- KITAEV AND W. (2000): single-prover quantum interactive proofs.
- GUTOSKI AND W. (2007): competing prover quantum interactive proofs and general (multiple-round) zero-sum quantum games.
- JAIN, UPADHYAY, W. (2009): parallel algorithms for simulating certain restricted classes of single-player and zero-sum games.

Challenges

1. General nonlocal games

- Many fundamental questions about nonlocal games remain unanswered, such as:

  How much entanglement is needed for (near) optimal play?

- It has only recently been proved that values of general nonlocal games are computable.
  (Doherty, Liang, Toner and Wehner 2008)
  (Scholz and Werner 2008)

- High-accuracy approximations are NP-hard.
  (Kempe, Kobayashi, Matsumoto, Toner and Vidick, 2008)
  (Ito, Kobayashi and Matsumoto, 2008)

- Parallel repetition is another fascinating problem.

Challenges

2. Multi-prover quantum interactive proofs.

- **Expressive power** is a complete mystery: only trivial bounds are known.
- There is recent progress in understanding other **basic properties** of multi-prover quantum interactive proofs.
  (KEMPE, KOBAYASHI, MATSUMOTO AND VIDICK, 2008)
- Interesting things are known about **variants** of multi-prover quantum interactive proofs, including settings where entanglement among provers is restricted.
  (BEN-OR, HASSIDIM AND PILPEL, 2008)
  (AARONSON, BEIGI, DRUCKER, FEFFERMAN AND SHOR, 2008)

Challenges

3. General games (neither purely cooperative nor competitive).

- Early papers on quantum game theory, including Meyers (1999) and Eisert, Wilkens, and Lewenstein (1999), started a trend:

  Strong constraints (not motivated by physics) are placed on some players' strategies.

- Countless "quantum game theory" papers have followed. Many of them analyze these highly constrained models, and draw conclusions based on superficial connections between quantum and classical variants of games.

  The topic has apparently "split off" from quantum information theory...

- This is a shame, because there is excellent potential for a **good** theory of general quantum games...

Conclusion

The theory of quantum games is an interesting topic worthy of further study.

1. It is central to quantum complexity theory.
2. It has interesting connections to the study of entanglement and nonlocality.
3. It has potential to provide new insights and methods for quantum information and computation.
4. Many fundamental questions about quantum games remain unanswered.

Thank you for your attention.