Quantum Hedging in Two-Round Prover-Verifier Interactions

Srinivasan Arunachalam$^{2,3}$, Abel Molina, Vincent Russo$^{1,3}$

$^1$David R. Cheriton School of Computer Science, $^2$Department of Combinatorics & Optimization, and $^3$Institute for Quantum Computing
University of Waterloo, Waterloo, Ontario N2L 3G1, Canada

\[ \text{arXiv:1310.7954} \]

Introduction

The protocol we consider consists of three major steps:

- **Preparation**: Alice prepares a state \( \rho \in \mathcal{D}(Y \otimes Z) \), and sends it to Bob.
- **Action**: Bob applies a quantum channel \( \Phi \) to \( Y \) to obtain \( Y' \), which is sent back to Alice.
- **Measurement**: Alice performs a projective measurement on \( (Y, Z) \) described by \( \{ P_z \} : z \in \{ 0, 1 \} \subseteq \text{Proj}(Y \otimes Z) \).

The following SDP corresponds to running \( n \) repetitions of the protocol, where the optimum value is the maximum probability that Bob wins at least \( k = 1 \) out of the \( n \) repetitions.

### Generalizing the Hedging Model

**Primal problem**

\[
\begin{align*}
\text{maximize:} & \quad \langle Q, \rho \rangle \\
\text{subject to:} & \quad \text{Tr}(\rho) = 1, \quad \rho \in \text{Proj}(Y \otimes Z).
\end{align*}
\]

**Dual problem**

\[
\begin{align*}
\text{minimize:} & \quad \text{Tr}(Y') \\
\text{subject to:} & \quad Y' \in \text{Hermitian}(\mathbb{C}^{2^n}).
\end{align*}
\]

### Winning Angle and Strategy

The winning angles \( (\theta_1, \theta_2) \) and strategies \( (\Phi_1, \Phi_2) \) can be expressed in the following closed forms:

\[
\begin{align*}
\theta_1 &= \tan^{-1} \left( \frac{1}{\sqrt{2^n-1}} - 1 \right), \\
\theta_2 &= \tan^{-1} \left( \frac{1}{\sqrt{2^n-1}} \right).
\end{align*}
\]

Winning Angle and Strategy

Figure 1: A single repetition of the protocol described above.

Motivation: Understand non-locality and entanglement.

Applications: Quantum cryptographic schemes.

### Background

- **Total number of repetitions**: \( n \)
- **Number of repetitions Bob would like to win with certainty**: \( p \)
- **Probability**: \( \rho \in \mathcal{D}(\mathcal{S}) \) of Bob winning where \( \mathcal{S} = \{ 1, \ldots, n \} \)
- **We focus on the case**: \( \rho = \Phi_0 \), \( \Phi = \rho \in \{ 0 \} \cup \sqrt{1 - \gamma^2} \{ 1 \} \).
- **We focus on the case**: \( P = \gamma^2 \), \( \gamma = \text{cas} \{ 0 \} + \text{cas} \{ 1 \} \).

For \( n = 2 \), \( k = 1 \), \( \alpha = \frac{\pi}{4} \), and \( \theta = \frac{\pi}{8} \), a specific strategy [1] exists that outperforms any classical one.

**Hedging in Model with Protocol Errors**

We study a variation of the prover-verifier setting where Bob has the choice not to respond to Alice in the second step of the protocol. If so, the whole interaction is repeated until Bob returns an answer. \( \rho \) is allowed to be an arbitrary finite-dimensional quantum state, and \( P, P_1 \) are arbitrary projective measurement operators.

**Hedging with Protocol Errors**

Figure 2: An \( n \)-repetition competitive game between Alice and Bob. Alice independently prepares questions \( \rho_0 \in \mathcal{D}(Y) \). She sends half of the states to Bob, where he applies a quantum channel \( \Phi \) to Alice’s questions. The protocol works if Bob wins when \( \Phi = \rho_0 \). Finally, Alice measures with respect to \( \{ P_z \} : z \in \{ 0, 1 \} \subseteq \text{Proj}(Y \otimes Z) \).

Winning Angle and Strategy

Figure 3: The X-axis refers to the angle \( \theta \) in Alice’s measurement, and the Y-axis refers to the optimum value of the SDP. Perfect hedging is achieved when the optimum value equals zero. The angles \( \theta_1 \) and \( \theta_2 \) mark the boundaries of that range, and \( \theta_1 \) and \( \theta_2 \) are strategies for those angles that Bob can apply to achieve perfect hedging.

Semidefinite Programming (SDP)

- A generalization of linear programming.
- A powerful tool with many applications in quantum information.
- SDPs are efficiently solvable (polynomial time) for many relevant subclasses.
- Software packages are available to solve SDPs.

Open Problems

- Can a similar closed form be constructed for \( k/n \) as we’ve illustrated for \( 1/n \)?
- Extend the protocol error model to determine if hedging occurs when Bob has to return an answer within a fixed number of iterations.
- Develop a line of work with further generalizations of the model, similar to the one currently ongoing for one round quantum games with two collaborating players.

Software

MATLAB scripts that implement the hedging SDPs using the CVX convex optimization solve.

References


Acknowledgments

This research was supported by Canada’s NSERC and the US ARO.