Quantum Hedging in Two-Round Prover-Verifier Interactions

Srinivasan Arunachalam[2,3], Abel Molina, Vincent Russo[1,3] (arXiv:1310.7954)

[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

Introduction

The protocol we consider consists of three major steps:

- Preparation: Alice prepares a state $\rho \in \mathrm{D}(\mathcal{X} \otimes \mathcal{Z})$, and sends X to Bob.
- Action: Bob applies a quantum channel Φ to X to obtain Y, which is sent back to Alice.
- Measurement: Alice performs a projective measurement on (Y, Z) described by $\{P_a : a \in \{0,1\}\} \subset \mathrm{Pos}(\mathcal{Y} \otimes \mathcal{Z})$.

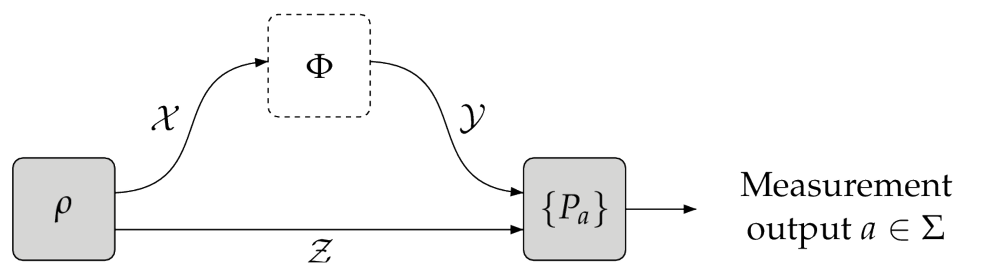

Figure 1: A single repetition of the protocol described above.

Motivation: Understand non-locality and entanglement.
Applications: Quantum cryptographic schemes.

Background

- n – Total number of repetitions.
- k – Number of repetitions Bob would like to win with certainty.
- p – Probability $p \in \mathcal{P}(\Sigma)$ of Bob winning where $\Sigma = \{1, \cdots, n\}$.
- α – We focus on the case $\rho = \psi\psi^*$, $\psi = \alpha\,|00\rangle + \sqrt{1-\alpha^2}\,|11\rangle$.
- θ – We focus on the case $P_1 = \gamma\gamma^*$, $\gamma = \cos(\theta)\,|00\rangle + \sin(\theta)\,|11\rangle$.

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

Classical

- Passing *both* tests : p^2
- Passing *at least one* test : $1-(1-p)^2$

Quantum

- Passing *both* tests : p^2
- Passing *at least one* test : 1

Question: What about perfectly hedging $1/n$?
Question: Applications to more physical settings?

Notation

Choi Representation:

$$J(\Phi) = \sum_{1 \le i,j \le n} \Phi(|i\rangle\langle j|) \otimes |i\rangle\langle j|$$

Alice and Bob's operations in the protocol are represented in our SDPs using the Choi representation:

Alice's Operation:

$$Q_a = \left(\mathbb{1}_{\mathrm{L}(\mathcal{Y})} \otimes \Psi_\rho\right)(P_a) \in \mathrm{Pos}(\mathcal{Y} \otimes \mathcal{X}), J(\Psi_\rho) = \overline{\rho}$$

Bob's Operation:

$$X = J(\Phi) \in \mathrm{Pos}(\mathcal{Y} \otimes \mathcal{X})$$

Generalizing the Hedging Model

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.

Primal problem

$$\begin{array}{ll} \text{minimize:} & \langle Q_0^{\otimes n}, X \rangle \\ \text{subject to:} & \mathrm{Tr}_{\mathcal{Y}^{\otimes n}}(X) = \mathbb{1}_{\mathcal{X}^{\otimes n}}, \\ & X \in \mathrm{Pos}(\mathcal{Y}^{\otimes n} \otimes \mathcal{X}^{\otimes n}). \end{array}$$

Dual problem

$$\begin{array}{ll} \text{maximize:} & \mathrm{Tr}(Y) \\ \text{subject to:} & \mathbb{1}_{\mathcal{Y}^{\otimes n}} \otimes Y \le Q_0^{\otimes n}, \\ & Y \in \mathrm{Herm}(\mathcal{X}^{\otimes n}). \end{array}$$

General Hedging Model

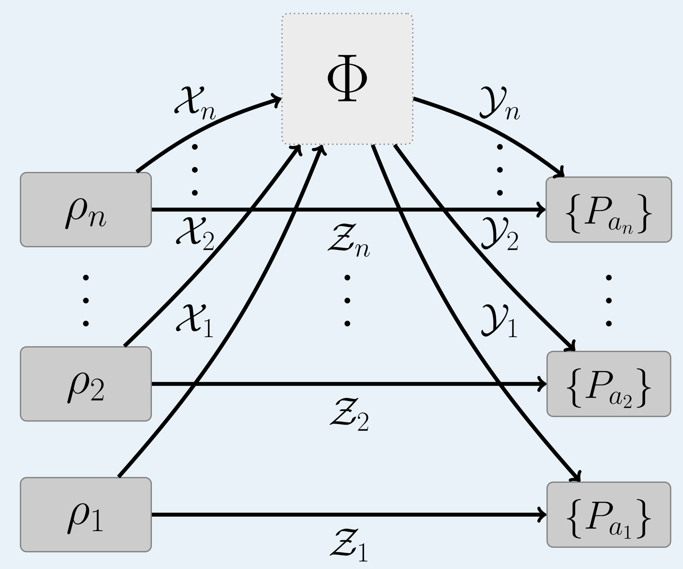

Figure 2: An n-repetition competitive game between Alice and Bob. Alice independently prepares questions $\rho^{\otimes n} \in \mathrm{D}(\mathcal{X}^{\otimes n} \otimes \mathcal{Z}^{\otimes n})$. She sends half of the state to Bob, where he applies a quantum channel Φ to Alice's questions. This yields the state $\Phi(\rho^{\otimes n})$, labeled by $\sigma \in \mathrm{D}(\mathcal{Y}^{\otimes n} \otimes \mathcal{Z}^{\otimes n})$. Finally, Alice measures with respect to $\{P_{a_i} : a_i \in \{0,1\}\} \subset \mathrm{Pos}(\mathcal{Y}^{\otimes n} \otimes \mathcal{Z}^{\otimes n})$ and determines Bob's victory or loss.

Winning Angle and Strategy

The winning angles (θ_1, θ_2) and strategies (Φ_1, Φ_2) can be expressed in the following closed forms:

$$\theta_1 = \tan^{-1}\left(\sqrt{\frac{1}{\alpha^2} - 1}\left(2^{1/n} - 1\right)\right), \Phi_1 = \sum_{\vec{r}} (-1)^{\wedge\vec{r} + \oplus\vec{r}} \,|\vec{r}\rangle\langle\vec{r}|$$

$$\theta_2 = \tan^{-1}\left(\sqrt{\frac{1}{\alpha^2} - 1}\left(\frac{1}{2^{1/n} - 1}\right)\right), \Phi_2 = \sum_{\vec{r}} (-1)^{\vee\vec{r} + \oplus\vec{r}} \,|\vec{r}\rangle\langle\vec{r}|$$

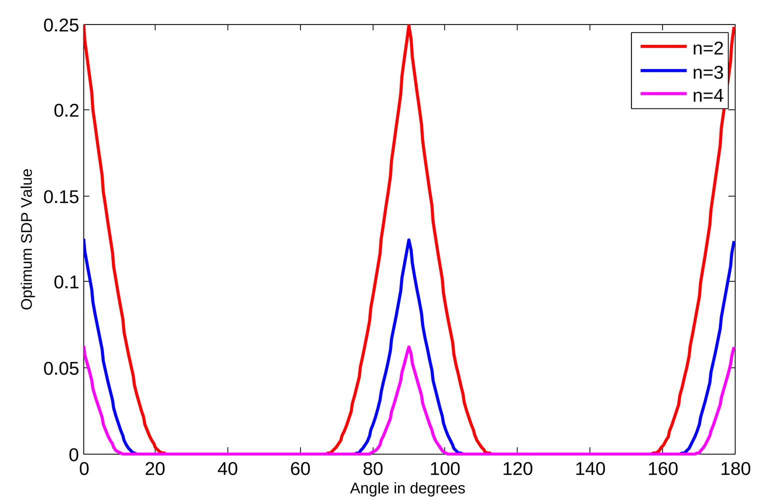

Figure 3: The X-axis refers to the angle θ in Alice's measurement, and the Y-axis refers to the optimum value of the SDP. Perfect hedging is achieved when the optimum value equals zero. The angles θ_1 and θ_2 mark the boundaries of that range, and Φ_1 and Φ_2 are strategies for those angles that Bob can apply to achieve perfect hedging.

Hedging in Model with Protocol Errors

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

Primal problem

$$\begin{array}{ll} \text{maximize:} & \langle Q_1, X \rangle \\ \text{subject to:} & \mathrm{Tr}_{\mathcal{Y}}(X) \le \mathbb{1}_{\mathcal{X}}, \\ & X \in \mathrm{Pos}(\mathcal{Y} \otimes \mathcal{X}). \end{array}$$

Reduces to

Simplified Primal problem

$$\begin{array}{ll} \text{maximize:} & \dfrac{x^* \sqrt{(\sum_i Q_i)^+}\, Q_1 \sqrt{(\sum_i Q_i)^+}\, x}{x^* x} \\ \text{subject to:} & x \in \mathcal{Y} \otimes \mathcal{X}, x \perp \ker(\sum_i Q_i). \end{array}$$

Hedging with Protocol Errors

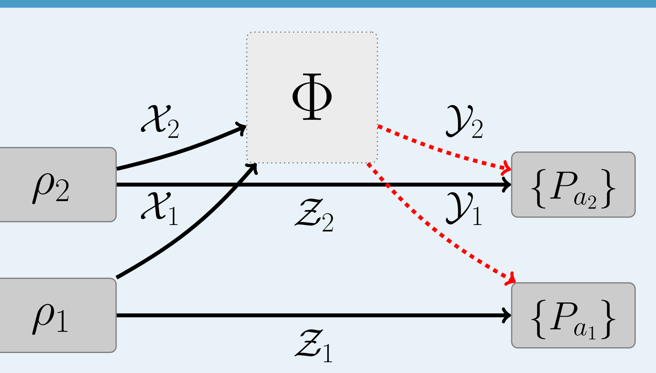

Figure 4: The red dashed lines indicate Bob's ability to not respond.

Absence of Hedging

The value of the above SDP can be seen to correspond to the value of:

$$\left\| \left(\left(\sum_i Q_i\right)^+\right)^{1/2} Q_1 \left(\left(\sum_i Q_i\right)^+\right)^{1/2} \right\|_\infty$$

Using this formula and considering the case with n repetitions, perfect hedging is shown to *not* to be possible in our protocol error model for any choice of k and n.

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.
- Duality theory:

Primal problem

$$\begin{array}{ll} \text{maximize:} & \langle A, X \rangle \\ \text{subject to:} & \Phi(X) = B, \\ & X \in \mathrm{Pos}(\mathcal{X}). \end{array}$$

Dual problem

$$\begin{array}{ll} \text{minimize:} & \langle B, Y \rangle \\ \text{subject to:} & \Phi^*(Y) \ge A, \\ & Y \in \mathrm{Herm}(\mathcal{Y}). \end{array}$$

Optimum value: α β

Weak Duality Theorem: For every SDP, $\alpha \le \beta$.

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 solver:

- https://bitbucket.org/vprusso/quantum-hedging

References

[1] A. Molina and J. Watrous, Proceedings of the Royal Society A: Mathematical, Physical and Engineering Science **468**, (2012).

[2] G. Gutoski and J. Watrous, Proceedings of the thirty-ninth annual ACM symposium on Theory of computing, (2007).

[3] S. Arunachalam, A. Molina, and V. Russo, arXiv:1310.7954, (2013)

[4] S. Bandyopadhyay, R. Jain, J. Oppenheim, C. Perry, arXiv:1306.4683, (2013).

Acknowledgments

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