# Generalizations of Hedging Bets with Correlated Quantum Strategies

Vincent Russo

University of Waterloo : Institute for Quantum Computing

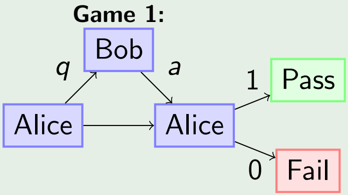
July 16, 2013

## Previous and Current Work

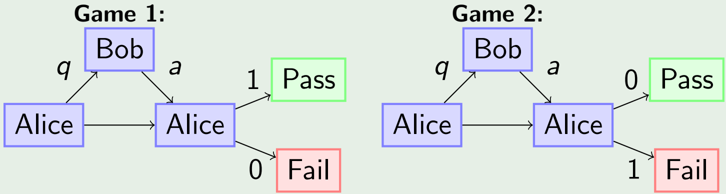
- Based on previous work "Hedging Bets with Correlated Quantum Strategies" - Molina, Watrous arXiv:1104.1140 [1].
- Joint work with Srinivasan Arunachalam, Abel Molina, and John Watrous.

# The Protocol: Basic Setup

## Example




## Example



# Spoiler Alert

**Classical Case**
**Optimal Probability:**

- Passing *both* tests
  - $p^2$
- Passing *at least one* of the tests
  - $1 - (1 - p)^2$

**Quantum Case**
**Optimal Probability:**

- Passing *both* tests
  - $p^2$
- Passing *at least one* of the tests
  - 1 (Spoiler)

# Spoiler Alert

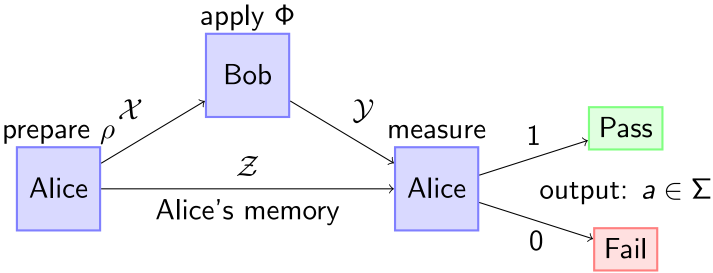
**Classical Case**
**Optimal Probability:**

- Passing *both* tests
  - $p^2$
- Passing *at least one* of the tests
  - $1 - (1 - p)^2$

**Quantum Case**
**Optimal Probability:**

- Passing *both* tests
  - $p^2$
- Passing *at least one* of the tests
  - 1 (Spoiler)

# Formalization of the Testing Protocol (Running One Test)



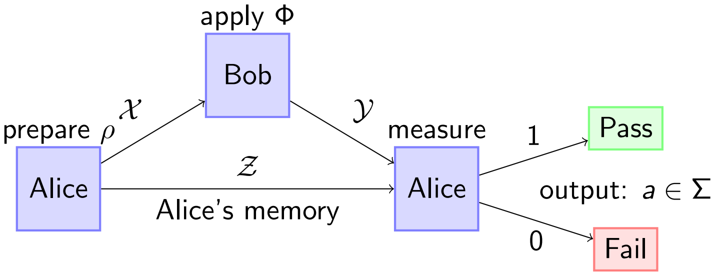

**Alice prepares:** $\rho$

- $u = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
  - $uu^* = \rho \in \mathrm{D}(\mathcal{X} \otimes \mathcal{Y})$

**Alice measures with respect to:** $\{P_0, P_1\}$

- $v = \cos(\theta)|00\rangle + \sin(\theta)|11\rangle$
  - $vv^* = P_1 \in \mathrm{Pos}(\mathcal{Y} \otimes \mathcal{Z}), \quad \mathbb{I} - vv^* = P_0 \in \mathrm{Pos}(\mathcal{Y} \otimes \mathcal{Z})$

# Formalization of the Testing Protocol (Running One Test)



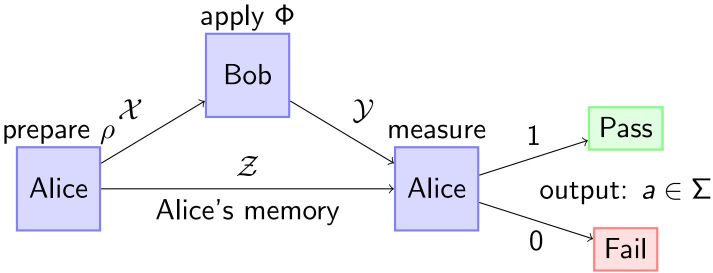

**Alice prepares:** $\rho$

- $u = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
  - $uu^* = \rho \in \mathrm{D}(\mathcal{X} \otimes \mathcal{Y})$

**Alice measures with respect to:** $\{P_0, P_1\}$

- $v = \cos(\theta)\,|00\rangle + \sin(\theta)\,|11\rangle$
  - $vv^* = P_1 \in \mathrm{Pos}(\mathcal{Y} \otimes \mathcal{Z}), \quad \mathbb{I} - vv^* = P_0 \in \mathrm{Pos}(\mathcal{Y} \otimes \mathcal{Z})$

# Formalization of the Testing Protocol (Running One Test)




**Alice prepares:** $\rho$

- $u = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
  - $uu^* = \rho \in \mathrm{D}(\mathcal{X} \otimes \mathcal{Y})$

**Alice measures with respect to:** $\{P_0, P_1\}$

- $v = \cos(\theta)\,|00\rangle + \sin(\theta)\,|11\rangle$
  - $vv^* = P_1 \in \mathrm{Pos}(\mathcal{Y} \otimes \mathcal{Z}), \quad \mathbb{I} - vv^* = P_0 \in \mathrm{Pos}(\mathcal{Y} \otimes \mathcal{Z})$

## Bob's Goal

Bob's goal is to optimize his probability of winning, which may be found by performing the inner product between the final state and a measurement operator $P_a \in \{P_0, P_1\}$.

The state $\sigma = (\Phi \otimes \mathbb{I}_{\mathbf{L}(\mathcal{Z})})(\rho)$ is the resulting state after Bob has applied his channel, $\Phi$, to the initial state $\rho$.

$$p(a) = \langle P_a, \sigma \rangle.$$

# Bob's Goal

Bob's goal is to optimize his probability of winning, which may be found by performing the inner product between the final state and a measurement operator $P_a \in \{P_0, P_1\}$.

The state $\sigma = (\Phi \otimes \mathbb{I}_{\mathbf{L}(\mathcal{Z})})(\rho)$ is the resulting state after Bob has applied his channel, $\Phi$, to the initial state $\rho$.

$$p(a) = \langle P_a, \sigma \rangle.$$

# Maximum and Minimum Measurement Probability

## Definition

Maximum probability for outcome $a$.

$$M(a) = \max_{\Phi \in \mathbf{C}(\mathcal{X},\mathcal{Y})} \langle P_a, (\Phi \otimes \mathbb{I}_{\mathbf{L}(\mathcal{Z})})(\rho) \rangle$$

## Definition

Minimum probability for outcome $a$.

$$m(a) = \min_{\Phi \in \mathbf{C}(\mathcal{X},\mathcal{Y})} \langle P_a, (\Phi \otimes \mathbb{I}_{\mathbf{L}(\mathcal{Z})})(\rho) \rangle$$

Note: max and min are used instead of sup and inf because they are being taken over a linear function on the compact set $\mathbf{C}(\mathcal{X}, \mathcal{Y})$.

# Semidefinite Programs for $M(a)$ and $m(a)$

**SDP for M(a):**

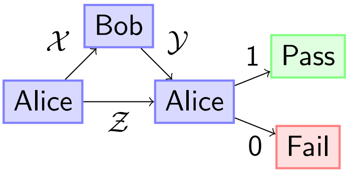
| Primal problem: | | Dual problem: | |
|---|---|---|---|
| maximize: | $\langle Q_a, X \rangle$ | minimize: | $\text{Tr}(Y)$ |
| subject to: | $\text{Tr}_{\mathcal{Y}}(X) = \mathbb{I}_{\mathcal{X}}$, | subject to: | $\mathbb{I}_{\mathcal{Y}} \otimes Y \geq Q_a$, |
| | $X \in \text{Pos}(\mathcal{Y} \otimes \mathcal{X})$. | | $Y \in \text{Herm}(\mathcal{X})$. |

**SDP for m(a):**

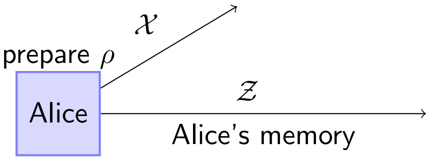
| Primal problem: | | Dual problem: | |
|---|---|---|---|
| minimize: | $\langle Q_a, X \rangle$ | maximize: | $\text{Tr}(Y)$ |
| subject to: | $\text{Tr}_{\mathcal{Y}}(X) = \mathbb{I}_{\mathcal{X}}$, | subject to: | $\mathbb{I}_{\mathcal{Y}} \otimes Y \leq Q_a$, |
| | $X \in \text{Pos}(\mathcal{Y} \otimes \mathcal{X})$. | | $Y \in \text{Herm}(\mathcal{X})$. |

# Running One Test: Example

Running a specific single instance of the test



# Step 1: Alice prepares her state

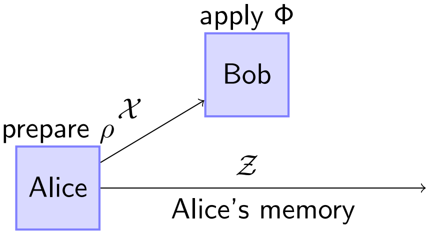



Alice prepares a pair of qubits in the state

$$u = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

and sends one qubit to Bob.

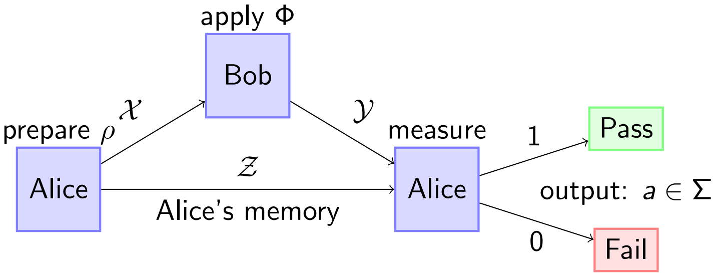
# Step 2: Bob applies his channel:




In this instance, Bob's best strategy is for $\Phi = \mathbb{I}$ since no matter what he does, it will not have an overall effect on the returned state since

$$\mathrm{Tr}_{\mathcal{Y}}(\sigma) = \mathrm{Tr}_{\mathcal{X}}(\rho) = \frac{1}{2}\mathbb{I}_{\mathcal{Z}}.$$

## Step 3: Alice measures




Alice measures with respect to $P_1 = vv^*$ and $P_0 = \mathbb{I} - vv^*$ where

$$v = \cos(\pi/8)\,|00\rangle + \sin(\pi/8)\,|11\rangle$$

# Running One Test: Bob's Probability of Winning

Therefore, Bob's maximum probability of winning is:

$$M(1) = \langle P_1, \sigma \rangle = \cos^2(\pi/8) \approx 0.85.$$

And Bob's minimum probability of losing is:

$$m(0) = \langle P_0, \sigma \rangle = \sin^2(\pi/8) \approx 0.15.$$

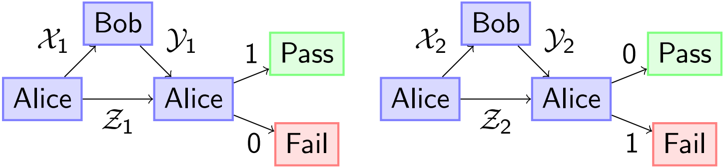
Bob's optimal channel in this case is defined as

$$\Phi = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

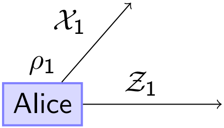
# Running Two Tests: Example

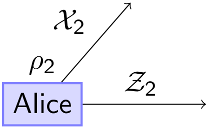
There exists a correlated *quantum* strategy for Bob where he will pass *at least one* of the tests with *certainty*.

**Game 1:** **Game 2:**



# Step 1: Alice prepares her state

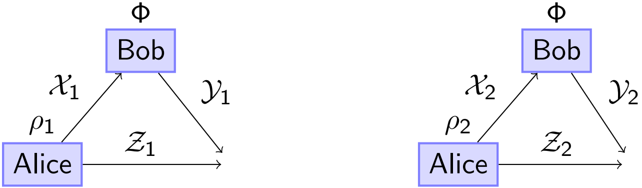



The state over both games in terms of $u$ is defined as

$$u \otimes u = \frac{1}{2}(|0000\rangle + |0011\rangle + |1100\rangle + |1111\rangle)$$

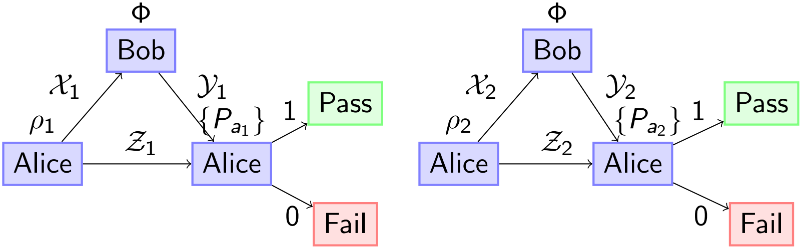
# Step 2: Bob applies his channel




It can be shown (by running the SDP) that

$$\frac{1}{2}(-|0000\rangle + |0011\rangle + |1100\rangle + |1111\rangle)$$

# Step 3: Alice measures




Selecting $w = -\sin(\pi/8)|00\rangle + \cos(\pi/8)|11\rangle$ orthogonal to $v$, we can write Bob's returned state as

$$-\frac{1}{2}|0000\rangle + \frac{1}{2}|0011\rangle + \frac{1}{2}|1100\rangle + \frac{1}{2}|1111\rangle = \frac{1}{\sqrt{2}} v \otimes w + \frac{1}{\sqrt{2}} w \otimes v$$

# Step 3: Alice measures

In other words, the final state is written in terms of a superposition of either *passing the first test and failing the second* or *failing the first test and passing the second*.

$$\underbrace{\frac{1}{\sqrt{2}} v \otimes w}_{\text{Bob wins the first, and loses the second}} + \underbrace{\frac{1}{\sqrt{2}} w \otimes v}_{\text{Bob loses the first, and wins the second}}$$

## Generalizing This Behavior: Natural Question

- We saw a specific instance of improvement in Bob's probability when a quantum strategy is adopted for winning 1 out of 2 repetitions of the test.
  - **Question:** Can this behavior be generalized for winning $1/n$? In other words, can we find an angle $\theta$ and a strategy $\Phi$ for Bob, such that he can always win $1/n$ with certainty?

# Generalizing the Angle for Winning $1/n$:

Recall that $\{P_0, P_1\}$ are defined in terms of $v = \cos(\theta)\,|00\rangle + \sin(\theta)\,|11\rangle$.

$$(\cos(\theta) + \sin(\theta))^{\otimes n} = 0 \Leftrightarrow (\cos(\theta) - \sin(\theta))^n = -2\sin(\theta)^n \Leftrightarrow$$
$$\cos(\theta) - \sin(\theta) = -(2)^{1/n}\sin(\theta) \Leftrightarrow \tan(x) = \frac{1}{1 - 2^{1/n}}$$

The angles at which perfect hedging is achieved falls within the range:

$$\theta \in \left[\tan^{-1}\left(2^{1/n} - 1\right), \tan^{-1}\left(\frac{1}{2^{1/n} - 1}\right)\right] \tag{1}$$

# Generalizing the Strategy for Winning $1/n$

Bob's strategy for the end points of (1) can be characterized by:

$$\Phi_1 = \sum_{i=0}^{n} (-1)^{AND(i)+PARITY(i)} |i\rangle\langle i|, \quad \Phi_2 = \sum_{i=0}^{n} (-1)^{OR(i)+PARITY(i)} |i\rangle\langle i| \tag{2}$$

In fact, Bob's optimal strategy at any point is always unitary.

# Connections to Other Areas of Research

- Error reduction and the class QIP(2):
  - Protocol was originally considered to study error reduction in QIP(2). The specific example for winning 1 out of 2 repetitions of the test illustrates that perfect parallel repetition cannot be used as a valid method of error reduction.
- Quantum State Discrimination
  - The hedging protocol an be viewed in the general sense as a framework for state discrimination.
- Misc:
  - Rank-1 One-Player Games
  - Cryptography

# Connections to Other Areas of Research

- Error reduction and the class QIP(2):
  - Protocol was originally considered to study error reduction in QIP(2). The specific example for winning 1 out of 2 repetitions of the test illustrates that perfect parallel repetition cannot be used as a valid method of error reduction.
- Quantum State Discrimination
  - The hedging protocol an be viewed in the general sense as a framework for state discrimination.
- Misc:
  - Rank-1 One-Player Games
  - Cryptography

## Connections to Other Areas of Research

- Error reduction and the class QIP(2):
    - Protocol was originally considered to study error reduction in QIP(2). The specific example for winning 1 out of 2 repetitions of the test illustrates that perfect parallel repetition cannot be used as a valid method of error reduction.
- Quantum State Discrimination
    - The hedging protocol an be viewed in the general sense as a framework for state discrimination.
- Misc:
    - Rank-1 One-Player Games
    - Cryptography

# Thank You!

Thanks!

Questions? / Comments?

# References I


- A. Molina and J. Watrous, "Hedging bets with correlated quantum strategies," *Arxiv preprint arXiv:1104.1140*, 2011.
- J. Watrous, "Theory of quantum information: Lecture notes," 2011.
- B. Rosgen, "Computational distinguishability of quantum channels," *Arxiv preprint arXiv:0909.3930*, 2009.
- G. Gutoski, "Quantum strategies and local operations," *Arxiv preprint arXiv:1003.0038*, 2010.
- C. Marriott and J. Watrous, "Quantum arthur–merlin games," *Computational Complexity*, vol. 14, no. 2, pp. 122–152, 2005.

# References II

- L. Vandenberghe and S. Boyd, “Semidefinite programming,” *SIAM review*, pp. 49–95, 1996.
- S. Boyd and L. Vandenberghe, *Convex optimization*. Cambridge Univ Pr, 2004.
- R. Horn and C. Johnson, *Matrix analysis*. Cambridge Univ Pr, 1990.
- R. Bhatia, *Matrix analysis*, vol. 169. Springer Verlag, 1997.
- L. Debnath and P. Mikusiński, *Hilbert spaces with applications*. Academic press, 2005.

# References III

P. Kaye, R. Laflamme, and M. Mosca, *An introduction to quantum computing*.
Oxford University Press, USA, 2007.

M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*.
Caimbridge University Press, 2000.

G. Gutoski and J. Watrous, "Toward a general theory of quantum games," in *Proceedings of the thirty-ninth annual ACM symposium on Theory of computing*, pp. 565–574, ACM, 2007.

# References IV


- A. Kitaev and J. Watrous, "Parallelization, amplification, and exponential time simulation of quantum interactive proof systems," in *Proceedings of the thirty-second annual ACM symposium on Theory of computing*, pp. 608–617, ACM, 2000.
- R. Raz, "A parallel repetition theorem," in *Proceedings of the twenty-seventh annual ACM symposium on Theory of computing*, pp. 447–456, ACM, 1995.
- T. Holenstein, "Parallel repetition: simplifications and the no-signaling case," in *Proceedings of the thirty-ninth annual ACM symposium on Theory of computing*, pp. 411–419, ACM, 2007.

# References V


- R. Raz, "A counterexample to strong parallel repetition," in *Foundations of Computer Science, 2008. FOCS'08. IEEE 49th Annual IEEE Symposium on*, pp. 369–373, IEEE, 2008.
- R. Mittal and M. Szegedy, "Product rules in semidefinite programming," in *Fundamentals of computation theory*, pp. 435–445, Springer, 2007.