Hedging bets with correlated quantum strategies

BY ABEL MOLINA AND JOHN WATROUS*

Institute for Quantum Computing and School of Computer Science,
University of Waterloo, Waterloo, Ontario, Canada

This paper studies the potential advantages of correlated answers in hypothetical tests of a simple interactive type. In these tests, an individual is presented with a question, to which he or she must respond with an answer, leading to an outcome of pass or fail. In quantum information theoretic variants of these tests, we show it is possible for an individual to correlate their answers across multiple tests in a way that produces a striking non-classical behaviour. Specifically, there exist tests for which no strategy can lead to the outcome pass with certainty, but where answers to multiple, independently administered tests can be correlated so that at least one test is passed with certainty. This phenomenon, which gives rise to a perfect form of hedging when considered in a game-theoretic setting, is quantum in nature: it is not possible in classical variants of the tests we consider.

Keywords: quantum information; semidefinite programming; interactive proof systems

1. Introduction

It is well known that quantum information theory allows for correlations among measurement outcomes that are stronger than those possible within any classical theory. Bell (1964) inequality violations provide the archetypal example within this category, where space-like separated measurements of entangled particles yield correlated measurement outcomes that are incompatible with local hidden-variable theories. This paper describes a different scenario in which this phenomenon arises, and provides an example showing a striking difference between quantum and classical theories in this scenario.

We will begin with an operational description of the scenario that we consider in the paper. The following discussion does not assume a particular choice of underlying theory, and will be later specialized to the cases of classical and quantum theory. In simple terms, we imagine that one individual subjects another individual to a test, and for convenience we will refer to the individual administering the test as Alice and to the test-taker as Bob. One may envision that Alice and Bob are devices rather than individuals; we only choose the later
Hedging bets with quantum strategies

1. Alice prepares a question and sends it to Bob.
2. Bob responds by sending an answer to Alice.
3. Based on Bob’s answer, as well as whatever memory she has of her own question, Alice decides whether Bob has passed or failed the test.

In a purely classical setting, one may imagine that Alice’s behaviour is described by a probabilistic process, whereby her questions are selected according to some probability distribution and her final decision might also involve the use of randomness. In the quantum setting, Alice’s questions may take the form of quantum information—possibly entangled with quantum memory of her own—and she may expect quantum information from Bob in return. In both the classical and quantum settings, we make the assumption that Bob has a complete description of the process by which Alice operates, and is generally interested in maximizing his probability of passing the test.

In complexity theory, hypothetical tests along these lines are often studied as a tool to classify computational problems; the corresponding model is known as the interactive proof system model (Babai & Moran 1988; Goldwasser et al. 1989). Interactive proof systems that allow for interactions consisting of multiple rounds are often considered; but in our discussion, we will focus only on those interactive proof systems that consist of a single question followed by a response—or, in other words, those interactions that correspond to the scenario we consider in this paper.

In the context of interactive proof systems, the individual we have called Alice is called the verifier and Bob is called the prover. The verifier’s computational ability is limited (usually to probabilistic or quantum polynomial time) while the prover’s computational ability is unrestricted. For each input string $x$ to a fixed decision problem $L$, the prover and verifier engage in an interaction wherein the prover attempts to convince (or prove to) the verifier that the string $x$ should be accepted as a yes-instance of the problem $L$. To say that such a system is valid for the problem $L$ means two things: one is that it must be possible for a prover to convince the verifier to accept with high probability if the input is truly a yes-instance of the problem, and the second is that the verifier must reject no-instances of the problem with high probability, regardless of the prover’s actions.

The first requirement is called the completeness condition, and is analogous to the condition in formal logic that true statements can be proved. The second condition is called the soundness condition, and is analogous to the condition that false statements cannot be proved.

We will now discuss the specific questions studied in this paper. To do so, for a fixed choice for Alice’s test, we let $p$ denote Bob’s optimal probability of passing this test. Formally speaking, without any assumptions on an underlying mathematical model, $p$ may be defined to be the supremum of all passing probabilities for Bob, taken over all possible choices of his strategy. (In both the classical and quantum models, the supremum will always be achieved, so that it may safely be replaced by the maximum.) By assumption, Alice always makes a definitive decision about whether Bob passes or fails, so he necessarily fails the test with probability at least $1 - p$. 

Proc. R. Soc. A (2012)
Now, consider that Alice instantiates two independent copies of her test in parallel: no correlations exist between the two questions that she presents to Bob, and the processes by which she determines whether Bob passes or fails are completely independent as well. There are a variety of questions that one may ask about this type of situation, including the following.

1. What is the optimal probability with which Bob passes both tests?
2. What is the optimal probability with which Bob passes at least one of the tests?

It is natural to guess that Bob’s optimal probability to pass both tests is $p^2$, while his optimal probability to pass at least one test is $1 - (1 - p)^2$. These are, of course, the optimal probabilities if he treats the two tests independently.

In the classical setting, the probabilities $p^2$ and $1 - (1 - p)^2$ are indeed optimal over all classical strategies, including those that do not respect the independence of the two tests; Bob cannot correlate the tests to his advantage in either case. While these claims can be proved directly with little difficulty, we will see that they fall out naturally as special cases in our analysis of the quantum setting.

In the quantum setting, the natural guess is indeed correct for the first question (as we will later discuss in greater detail): if Bob aims to pass both tests, there is no advantage for him to correlate the two tests. This fact is known to those who have studied quantum interactive proof systems (Kitaev & Watrous 2000), and it is a consequence of a more general result concerning semidefinite programmes (Mittal & Szegedy 2007). For the second question, on the other hand, the natural guess turns out to be wrong. We demonstrate this by giving an example where Bob can correlate the two independent tests in such a way that he passes at least one of the two tests with certainty, despite the fact that $p < 1$. More specifically, our example describes a test where Bob’s optimal passing probability for a single instantiation of the test is $\cos^2(\pi/8) \approx 0.85$, while he never fails both tests if he correlates two independent instantiations in the right way.

There are other settings in which quantum effects that are not possible in the classical world have been discovered to be possible in an interaction between two parties. However, our setting differs from some of the best-known such situations, such as the CHSH game (Clauser et al. 1969), and the Mermin–Peres magic squares game (Mermin 1990; Peres 1990). In our setting, we do not have two parties collaborating to achieve a non-classical outcome. Instead, we have a prover–verifier setting, in which Bob is trying to convince Alice in order to pass a test.

Bob’s ability to correlate two independent tests in the way just described can be seen as a perfect form of hedging, as the following (highly fictitious) scenario illustrates. Bob is offered the opportunity to take part in two potentially lucrative but somewhat risky games of chance, run by Alice. The two games are completely independent and identical in nature: for each, he must put forth $1$ million of his own money to take part, and he has approximately an 85 per cent chance to win if he plays optimally. For each game he wins, Bob receives $3$ million (representing a $2$ million gain over his initial $1$ million investment), while he receives nothing (and loses his $1$ million initial investment) if he loses. For the sake of this example, we are to consider that a $1$ million or greater loss means ruin for Bob.
These are, of course, highly compelling games of chance, and many people would not hesitate to take out a $2 million loan to play both: the expected gain from each one is roughly $1,550,000, and the chance for a loss in both, if they are treated independently, is only about 2.25 per cent. Bob, however, is a highly risk-averse person: while he would enjoy being a millionaire, he cannot accept a 2.25 per cent chance of ruin. Classically speaking, Bob can do nothing to avoid a 2.25 per cent chance of ruin, so he will choose not to play. If the two games are modelled by quantum information as in our example, however, Bob can be guaranteed a $1 million return, and can therefore play without fear: an appropriately chosen quantum strategy allows him to hedge his bets perfectly.

2. Preliminaries

We assume the reader to be familiar with the basics of quantum information theory, and suggest Nielsen & Chuang (2000) to those who are not. The purpose of this section is to summarize some of the notation and basic concepts we make use of, and to highlight a couple of concepts that may be less familiar to some readers.

(a) Basic notation, states, measurements and channels

For any finite-dimensional complex Hilbert space $\mathcal{X}$, we write $L(\mathcal{X})$ to denote the set of linear operators acting on $\mathcal{X}$, we write $\text{Herm}(\mathcal{X})$ to denote the set of Hermitian operators acting on $\mathcal{X}$, we write $\text{Pos}(\mathcal{X})$ to denote the set of positive semidefinite operators acting on $\mathcal{X}$, we write $\text{Pd}(\mathcal{X})$ to denote the set of positive definite operators acting on $\mathcal{X}$, and we write $D(\mathcal{X})$ to denote the set of density operators acting on $\mathcal{X}$. For Hermitian operators $A, B \in \text{Herm}(\mathcal{X})$, the notations $A \geq B$ and $B \leq A$ indicate that $A - B$ is positive semidefinite, and the notations $A > B$ and $B < A$ indicate that $A - B$ is positive definite.

Given operators $A, B \in L(\mathcal{X})$, one defines the inner product between $A$ and $B$ as $\langle A, B \rangle = \text{Tr}(A^* B)$. For Hermitian operators $A, B \in \text{Herm}(\mathcal{X})$, it holds that $\langle A, B \rangle$ is a real number and satisfies $\langle A, B \rangle = \langle B, A \rangle$. For every choice of finite-dimensional complex Hilbert space $\mathcal{X}$ and $\mathcal{Y}$, and for a given linear mapping of the form $F : L(\mathcal{X}) \rightarrow L(\mathcal{Y})$, there is a unique mapping $F^* : L(\mathcal{Y}) \rightarrow L(\mathcal{X})$ (known as the adjoint of $F$) that satisfies $\langle Y, F(X) \rangle = \langle F^*(Y), X \rangle$, for all $X \in L(\mathcal{X})$ and $Y \in L(\mathcal{Y})$.

A register is a hypothetical device that stores quantum information. Associated with a register $\mathcal{X}$ is a finite-dimensional complex Hilbert space $\mathcal{X}$, and each quantum state of $\mathcal{X}$ is described by a density operator $\rho \in D(\mathcal{X})$. Qubits are registers for which $\text{dim}(\mathcal{X}) = 2$. A measurement of $\mathcal{X}$ is described by a set of positive semidefinite operators $\{P_a : a \in \Sigma\} \subset \text{Pos}(\mathcal{X})$, indexed by a finite non-empty set of measurement outcomes $\Sigma$, and satisfying the constraint $\sum_{a \in \Sigma} P_a = 1_{\mathcal{X}}$ (the identity operator on $\mathcal{X}$). If such a measurement is performed on $\mathcal{X}$ while it is in the state $\rho$, each outcome $a \in \Sigma$ results with probability $\langle P_a, \rho \rangle$. A quantum channel is a completely positive and trace-preserving linear mapping of the form $\Phi : L(\mathcal{X}) \rightarrow L(\mathcal{Y})$ that describes a hypothetical physical process that transforms each state $\rho$ of a register $\mathcal{X}$ into the state $\Phi(\rho)$ of another register $\mathcal{Y}$. The set of all channels of this form is denoted $C(\mathcal{X}, \mathcal{Y})$. The identity channel that does nothing to a register $\mathcal{X}$ is denoted $1_{L(\mathcal{X})}$. 

Proc. R. Soc. A (2012)
The Hilbert space corresponding to a pair of registers \((X_1, X_2)\) is the tensor product \(X_1 \otimes X_2\) of the spaces corresponding to \(X_1\) and \(X_2\). Independent states, measurements and channels are represented by elementary tensors in the following straightforward way.

1. If registers \(X_1\) and \(X_2\) are independently prepared in states \(\rho_1\) and \(\rho_2\), then the state of the pair \((X_1, X_2)\) is given by the density operator \(\rho_1 \otimes \rho_2\).
2. If registers \(X_1\) and \(X_2\) are independently measured with respect to the measurements described by the collections \(\{P_{a_1}: a_1 \in \Sigma_1\} \subset \text{Pos}(X_1)\) and \(\{P_{a_2}: a_2 \in \Sigma_2\} \subset \text{Pos}(X_2)\), the resulting measurement on the pair \((X_1, X_2)\) is described by the collection \(\{P_{(a_1,a_2)}: (a_1,a_2) \in \Sigma_1 \times \Sigma_2\}\), where \(P_{(a_1,a_2)} = P_{a_1} \otimes P_{a_2} \in \text{Pos}(X_1 \otimes X_2)\).
3. If registers \(X_1\) and \(X_2\) are independently transformed into registers \(Y_1\) and \(Y_2\) according to the channels \(\Phi_1 \in C(X_1, Y_1)\) and \(\Phi_2 \in C(X_2, Y_2)\), respectively, then the transformation of the pair \((X_1, X_2)\) into the pair \((Y_1, Y_2)\) is described by the channel \(\phi_1 \otimes \phi_2 \in C(X_1 \otimes X_2, Y_1 \otimes Y_2)\).

(b) Linear mappings on operator spaces

Suppose \(\text{dim}(X) = n\) and assume that a standard orthonormal basis \(\{|1\rangle, \ldots, |n\rangle\}\) of \(X\) has been selected. With respect to this basis, one defines the Choi–Jamiolkowski operator \(J(\phi) \in L(Y \otimes X)\) of a linear mapping \(\phi: L(X) \rightarrow L(Y)\) as

\[
J(\phi) = \sum_{1 \leq i,j \leq n} \phi(|i\rangle\langle j|) \otimes |i\rangle\langle j|.
\]

The mapping \(J\) is a linear bijection from the space of mappings of the form \(\phi: L(X) \rightarrow L(Y)\) to the operator space \(L(Y \otimes X)\). It is well known that \(\phi\) is completely positive if and only if \(J(\phi) \in \text{Pos}(Y \otimes X)\), and that \(\phi\) is trace-preserving if and only if \(\text{Tr}_Y(J(\phi)) = 1_X\) (Jamiolkowski 1972; Choi 1975).

While the Choi–Jamiolkowski operator of a linear mapping \(\phi: L(X) \rightarrow L(Y)\) is most commonly considered when \(\phi\) is a channel, the concept is useful in more general settings (as is illustrated in Gutoski & Watrous (2007) and Chiribella et al. (2009), for instance). The following lemma, whose proof makes use of the Choi–Jamiolkowski operator of a particular mapping, gives one technical example that will be useful later in the paper.

**Lemma 2.1.** For every operator \(A \in L(X \otimes Z)\), there exists a mapping \(\Psi_A: L(Z) \rightarrow L(X)\) that possesses the following property: for every mapping \(\phi: L(X) \rightarrow L(Y)\) and every operator \(B \in L(Y \otimes Z)\), the equation

\[
\langle B, (\phi \otimes \mathbb{1}_{L(Z)})(A) \rangle = \langle (\mathbb{1}_{L(Y)} \otimes \Psi_A)(B), J(\phi) \rangle
\]

holds. Moreover, if \(A\) is positive semidefinite, then \(\Psi_A\) is completely positive.

**Proof.** The unique mapping \(\Psi_A: L(Z) \rightarrow L(X)\) for which \(J(\Psi_A) = \tilde{A}\) (the entry-wise complex conjugate of \(A\)) possesses the required property. This fact is easily verified for operators \(A\) taking the form \(A = |i\rangle\langle j| \otimes |k\rangle\langle l|\), in which case \(\Psi_A(Z) = |i\rangle \langle k| Z|l\rangle \langle j|\), and it follows for general operators by the conjugate-linearity/linearity of the inner product. Under the assumption that \(A\) is positive semidefinite, so too is \(\tilde{A}\), from which it follows that \(\Psi_A\) is completely positive. □
Semidefinite programming is a topic that has found several interesting applications within quantum computing and quantum information theory in recent years. It is a valuable analytic tool, as well as a computational one. Here, we provide just a brief summary of semidefinite programming that is focused on the narrow aspects of it that we use. More comprehensive discussions can be found in Vandenberghe & Boyd (1996), Lovász (2003), de Klerk (2002), Boyd & Vandenberghe (2004), for instance.

A semidefinite programme is a triple \((F, A, B)\), where

1. \(F : L(\mathcal{X}) \rightarrow L(\mathcal{Y})\) is a Hermiticity-preserving linear mapping, and
2. \(A \in \text{Herm}(\mathcal{X})\) and \(B \in \text{Herm}(\mathcal{Y})\) are Hermitian operators,

for some choice of finite-dimensional complex Hilbert spaces \(\mathcal{X}\) and \(\mathcal{Y}\). We associate with the triple \((F, A, B)\) two optimization problems, called the *primal* and *dual* problems, as follows:

| primal problem          | dual problem               |
|-------------------------|-----------------------------|
| maximize: \(\langle A, X \rangle\) | minimize: \(\langle B, Y \rangle\) |
| subject to: \(F(X) = B\), \(X \in \text{Pos}(\mathcal{X})\). | subject to: \(F^*(Y) \geq A\), \(Y \in \text{Herm}(\mathcal{Y})\). |

The optimal primal value \(\alpha\) and optimal dual value \(\beta\) of this semidefinite programme are defined as

\[
\alpha = \sup \{ \langle A, X \rangle : X \in \text{Pos}(\mathcal{X}), F(X) = B \}
\]

and

\[
\beta = \inf \{ \langle B, Y \rangle : Y \in \text{Herm}(\mathcal{Y}), F^*(Y) \geq A \}.
\]

(It is to be understood that the supremum over an empty set is \(-\infty\) and the infimum over an empty set is \(\infty\), so \(\alpha\) and \(\beta\) are well-defined values in the set \(\mathbb{R} \cup \{-\infty, \infty\}\). Our interest, however, will only be with semidefinite programmes for which \(\alpha\) and \(\beta\) are finite.)

It always holds that \(\alpha \leq \beta\), which is a fact known as *weak duality*. The condition \(\alpha = \beta\), which is known as *strong duality*, does not hold for every semidefinite programme, but there are simple conditions known under which it does hold. The following theorem provides one such condition (that has both a primal and dual form).

**Theorem 2.2 (Slater’s theorem for semidefinite programmes).** Let \((\Phi, A, B)\) be a semidefinite programme and let \(\alpha\) and \(\beta\) be its optimal primal and dual values.

1. If \(\beta\) is finite and there exists a positive definite operator \(X \in \text{Pd}(\mathcal{X})\) for which \(\Phi(X) = B\), then \(\alpha = \beta\) and there exists a Hermitian operator \(Y \in \text{Herm}(\mathcal{Y})\) such that \(\Phi^*(Y) \geq A\) and \(\langle B, Y \rangle = \beta\).
2. If \(\alpha\) is finite and there exists a Hermitian operator \(Y \in \text{Herm}(\mathcal{Y})\) for which \(\Phi^*(Y) > A\), then \(\alpha = \beta\) and there exists a positive semidefinite operator \(X \in \text{Pos}(\mathcal{X})\) such that \(\Phi(X) = B\) and \(\langle A, X \rangle = \alpha\).
In words, the first item of this theorem states that if the dual problem is feasible and the primal problem is strictly feasible, then strong duality holds and the optimal dual solution is achievable. The second item is similar, with the roles of the primal and dual problems reversed.

3. Interactive measurements

We now discuss the scenario described in §1 in greater mathematical detail, focusing on the quantum setting. As is to be expected, the classical setting may be seen as a special case of the quantum setting.

Tests of the form described in §1 are modelled by interactive measurements, which are essentially measurements of quantum channels: an interactive measurement consists of a state preparation and a measurement, to be applied to a given quantum channel. More formally speaking, an interactive measurement is specified by three finite-dimensional complex Hilbert spaces $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{Z}$, along with two objects defined over these spaces:

1. A state on the spaces $\mathcal{X}$ and $\mathcal{Z}$, represented by a density operator $\rho \in \mathcal{D}(\mathcal{X} \otimes \mathcal{Z})$.
2. A measurement $\{P_a : a \in \Sigma\} \subset \text{Pos}(\mathcal{Y} \otimes \mathcal{Z})$ on the spaces $\mathcal{Y}$ and $\mathcal{Z}$.

If such an interactive measurement is applied to a given channel $\Phi \in \mathcal{C}(\mathcal{X}, \mathcal{Y})$, the probability associated with each measurement outcome $a \in \Sigma$ is given by

$$p(a) = \langle P_a, (\Phi \otimes \mathbb{I}_{L(\mathcal{Z})})(\rho) \rangle.$$ 

An interactive measurement of a channel $\Phi$ is illustrated in figure 1.

Suppose that an interactive measurement, specified by a state $\rho \in \mathcal{D}(\mathcal{X} \otimes \mathcal{Z})$ and a measurement $\{P_a : a \in \Sigma\} \subset \text{Pos}(\mathcal{Y} \otimes \mathcal{Z})$, has been fixed. For a given measurement outcome $a \in \Sigma$, one may consider both the maximum and minimum probability with which the outcome $a$ appears, over all choices of the quantum channel $\Phi$ upon which the interactive measurement is performed. Let us denote the maximum probability by $M(a)$ and the minimum probability by $m(a)$ for each $a \in \Sigma$, so that

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

and

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

(One notes that the above quantities are the maximization and minimization, respectively, of a linear function on the compact set of quantum channels $\mathcal{C}(\mathcal{X}, \mathcal{Y})$. Thus, the use of the maximum and minimum rather than the supremum and infimum is justified.)

The quantities $M(a)$ and $m(a)$ are expressible as the optimal values of semidefinite programmes, as we now describe. For each $a \in \Sigma$ we let $Q_a \in \text{Pos}(\mathcal{Y} \otimes \mathcal{X})$ be defined as

$$Q_a = (\mathbb{I}_{L(\mathcal{Y})} \otimes \Psi_\rho)(P_a),$$

(3.1)
for $\Psi_\rho$ being the mapping described by lemma 2.1. We then have the following equality for each $a \in \Sigma$ and any choice of a channel $\Phi \in C(\mathcal{X}, \mathcal{Y})$:

$$p(a) = \langle P_a, (\Phi \otimes 1_{L(Z)})(\rho) \rangle = \langle Q_a, J(\Phi) \rangle.$$ 

It therefore holds that

$$M(a) = \max_{\Phi \in C(\mathcal{X}, \mathcal{Y})} \langle Q_a, J(\Phi) \rangle \quad \text{and} \quad m(a) = \min_{\Phi \in C(\mathcal{X}, \mathcal{Y})} \langle Q_a, J(\Phi) \rangle.$$

The operator $J(\Phi)$ ranges over all choices of $X \in \text{Pos}(\mathcal{Y} \otimes \mathcal{X})$ satisfying $\text{Tr}_\mathcal{Y}(X) = 1_\mathcal{X}$ as $\Phi$ ranges over all channels $\Phi \in C(\mathcal{X}, \mathcal{Y})$, and therefore the following semidefinite programme has optimal primal value $M(a)$:

**primal problem**

maximize: $\langle Q_a, X \rangle$

subject to:

$\text{Tr}_\mathcal{Y}(X) = 1_\mathcal{X}$, $X \in \text{Pos}(\mathcal{Y} \otimes \mathcal{X})$.

**dual problem**

minimize: $\text{Tr}(Y)$

subject to:

$1_{\mathcal{Y} \otimes \mathcal{X}} \geq Q_a$, $Y \in \text{Herm}(\mathcal{X})$.

A slight modification yields a semidefinite programme whose optimal primal value is $m(a)$:

**primal problem**

minimize: $\langle Q_a, X \rangle$

subject to:

$\text{Tr}_\mathcal{Y}(X) = 1_\mathcal{X}$, $X \in \text{Pos}(\mathcal{Y} \otimes \mathcal{X})$.

**dual problem**

maximize: $\text{Tr}(Y)$

subject to:

$1_{\mathcal{Y} \otimes \mathcal{X}} \leq Q_a$, $Y \in \text{Herm}(\mathcal{X})$.

(The most straightforward way to fit this semidefinite programme to the precise formalism described in §2 is to exchange maxima and minima and replace $Q_a$ with $-Q_a$, which yields a semidefinite programme for $-m(a)$. One could alternately extend the definition of semidefinite programmes in a straightforward way to allow for minimizations in the primal problem and maximizations in the dual. The particular choice of these alternatives that one takes has no effect on our analysis.)

It is clear that strict feasibility holds for each of the problems presented: taking $X$ and $Y$ to be appropriately chosen scalar multiples of the identity operator suffices to observe that these properties hold. Strong duality therefore holds for both semidefinite programmes by theorem 2.2, and optimal solutions are achieved for each of the four problem formulations.
Figure 2. Two interactive measurements, specified by pairs \((\rho_1, \{P_{a_1}\})\) and \((\rho_2, \{P_{a_2}\})\), are performed independently. The two interactive measurements are applied to a channel \(\Phi \in C(\mathcal{X}_1 \otimes \mathcal{X}_2, \mathcal{Y}_1 \otimes \mathcal{Y}_2)\), which may not respect the independence of the two interactive measurements, potentially causing a correlation in the two measurement outcomes.

4. Correlations among independent interactive measurements

We now consider the situation in which two interactive measurements, described by pairs \((\rho_1, \{P_{a_1} : a_1 \in \Sigma_1\})\) and \((\rho_2, \{P_{a_2} : a_2 \in \Sigma_2\})\), are performed independently, as suggested in figure 2. While the interactive measurements are themselves performed independently, it is not assumed that the channel \(\Phi \in C(\mathcal{X}_1 \otimes \mathcal{X}_2, \mathcal{Y}_1 \otimes \mathcal{Y}_2)\) respects this independence. Indeed, it is straightforward to devise examples where some choice of the channel \(\Phi\) causes a correlation in the outcomes produced by the two measurements. The main focus of this section is on the nature of the correlations that are possible through the selection of various channels \(\Phi\), especially as these correlations relate to the scenario described in §1.

Consider first the maximum output probability associated with a given pair of measurement outcomes \((a_1, a_2) \in \Sigma_1 \times \Sigma_2\). In the following subsection, we provide a proof that the maximum probability \(M(a_1, a_2)\) with which this pair is output is given by \(M(a_1, a_2) = M_1(a_1) M_2(a_2)\), where \(M_1(a_1)\) and \(M_2(a_2)\) denote the maximum output probabilities of \(a_1\) and \(a_2\) with respect to the individual interactive measurements with which they are associated. Thus, to maximize the probability of outputting \((a_1, a_2)\), there is absolutely no gain in choosing a channel \(\Phi\) that correlates the two interactive measurements: the optimal probability is achieved by some choice \(\Phi = \Phi_1 \otimes \Phi_2\) that respects the independence of the two interactive measurements.

Remarkably, a similar property does not generally hold when the maximum is replaced by the minimum: we provide an example for which \(m_1(a_1) = m_2(a_2) = \sin^2(\pi/8) \approx 0.15\), but \(m(a_1, a_2) = 0\).

(a) Analysis for multiplicativity

To see that \(M(a_1, a_2) = M_1(a_1) M_2(a_2)\), we may consider the semidefinite programme representing the optimal probability \(M(a_1, a_2)\):
we have broken down. In this case, the semidefinite programme whose optimal value is presented is applied to a more general class of semidefinite programmes. The operator $Y$ taking the product rule the operator may not be positive semidefinite in some cases. One may fail to prove that constrains positive semidefinite for optimal dual solutions.

The operator $Y$ is therefore dual feasible, so it is established that $M(a_1, a_2) \leq M(a_1^* a_2^*)$.

We note that this is a particular instance of a semidefinite programme obeying the product rule considered by Mittal & Szegedy (2007), where the argument just presented is applied to a more general class of semidefinite programmes.

When the maximum is replaced by the minimum, however, the above argument breaks down. In this case, the semidefinite programme whose optimal value is $m(a_1, a_2)$ takes the following form:

$$
\begin{align*}
\text{primal problem} & \quad \begin{array}{ll}
\text{maximize:} & (Q_{a_1} \otimes Q_{a_2}, X) \\
\text{subject to:} & \text{Tr}_{\mathcal{Y}_1 \otimes \mathcal{Y}_2}(X) = 1_{\mathcal{X}_1 \otimes \mathcal{X}_2}, \\
& X \in \text{Pos}(\mathcal{Y}_1 \otimes \mathcal{X}_1 \otimes \mathcal{Y}_2 \otimes \mathcal{X}_2).
\end{array}
\end{align*}

\begin{align*}
\text{dual problem} & \quad \begin{array}{ll}
\text{minimize:} & \text{Tr}(Y) \\
\text{subject to:} & \pi(1_{\mathcal{Y}_1} \otimes 1_{\mathcal{Y}_2} \otimes Y) \pi^* \\
& Y \in \text{Herm}(\mathcal{Y}_1 \otimes \mathcal{X}_2). \\
& \geq Q_{a_1} \otimes Q_{a_2},
\end{array}
\end{align*}
\]

The upper-bound $m(a_1, a_2) \leq m_1(a_1) m_2(a_2)$ is easily established by once again taking $X = X_1 \otimes X_2$ for primal optimal points $X_1$ and $X_2$. For the lower-bound $m(a_1, a_2) \geq m_1(a_1) m_2(a_2)$, however, a problem arises: unlike the situation for the maximum, one may not conclude that the operators $1_{\mathcal{Y}_1} \otimes Y_1$ and $1_{\mathcal{Y}_2} \otimes Y_2$ are positive semidefinite for optimal dual solutions $Y_1$ and $Y_2$ (and indeed they may not be positive semidefinite in some cases). One may fail to prove that the operator $Y = Y_1 \otimes Y_2$ is dual-feasible in this case, so that a lower-bound is not established.
(b) An example showing non-classical behaviour

We now present our example of a quantum test that allows for a strong correlation of the sort described in §1. The test is as follows.

1. Alice prepares a pair of qubits \((X, Z)\) in the state
\[
u = \frac{1}{\sqrt{2}} \ket{00} + \frac{1}{\sqrt{2}} \ket{11} \in X \otimes Z,
\]
and sends \(X\) to Bob.

2. Bob applies any quantum channel he likes to \(X\), obtaining a qubit \(Y\) that he sends back to Alice. As a result of his action, the pair \((Y, Z)\) then has some particular state \(\sigma \in \mathcal{D}(Y \otimes Z)\).

3. Alice measures \((Y, Z)\) with respect to the projective measurement \(\{P_0, P_1\}\), where
\[
P_0 = 1 - P_1 \quad \text{and} \quad P_1 = vv^* \quad \text{for} \quad v = \cos \left(\frac{\pi}{8}\right) \ket{00} + \sin \left(\frac{\pi}{8}\right) \ket{11}.
\]
The outcome 1 is to be interpreted that Bob passes the test, while the outcome 0 means that he fails.

Now, if Bob can produce a given state \(\sigma \in \mathcal{D}(Y \otimes Z)\) in step 2, it must hold that
\[
\text{Tr}_Y(\sigma) = \text{Tr}_X(\nu \nu^*) = \frac{1}{2} \mathbb{1}_Z;
\]
no action that Bob performs on his registers can influence the state of Alice’s register. The probability that Alice obtains the outcome 1 is \(\langle P_1, \sigma \rangle = F(vv^*, \sigma)^2\), where \(F(\cdot, \cdot)\) denotes the fidelity function and where the equality holds by virtue of the fact that \(vv^*\) is pure. By the monotonicity of the fidelity function under partial tracing, we have
\[
F(vv^*, \sigma)^2 \leq F(\text{Tr}_Y(vv^*), \text{Tr}_Y(\sigma))^2 = F(Q, R)^2
\]
for
\[
Q = \begin{pmatrix}
\cos^2 \left(\frac{\pi}{8}\right) & 0 \\
0 & \sin^2 \left(\frac{\pi}{8}\right)
\end{pmatrix}
\quad \text{and} \quad
R = \begin{pmatrix}
\frac{1}{2} & 0 \\
0 & \frac{1}{2}
\end{pmatrix}.
\]
By a direct calculation, we determine
\[
F(Q, R)^2 = \|\sqrt{Q} \sqrt{R}\|_1^2 = \frac{1}{2} \left(\cos \left(\frac{\pi}{8}\right) + \sin \left(\frac{\pi}{8}\right)\right)^2 = \cos^2 \left(\frac{\pi}{8}\right).
\]
Alice therefore outputs 1, indicating that Bob passes the test, with probability at most \(\cos^2(\pi/8) \approx 0.85\).

Finally, for two instantiations of the test described above, we consider what happens when Bob applies the phase flip \(\ket{00} \mapsto -\ket{00}, \ket{01} \mapsto \ket{01}, \ket{10} \mapsto \ket{10}\),
Hedging bets with quantum strategies

|11⟩ ↦→ |11⟩ on the two qubits he receives. Alice has prepared the state
\[
\frac{1}{2}|0000⟩ + \frac{1}{2}|0011⟩ + \frac{1}{2}|1100⟩ + \frac{1}{2}|1111⟩ \in X_1 \otimes Z_1 \otimes X_2 \otimes Z_2,
\]
and Bob’s phase flip transforms this state to
\[
-\frac{1}{2}|0000⟩ + \frac{1}{2}|0011⟩ + \frac{1}{2}|1100⟩ + \frac{1}{2}|1111⟩ \in Y_1 \otimes Z_1 \otimes Y_2 \otimes Z_2.
\]
Writing
\[
w = -\sin \left(\frac{\pi}{8}\right) |00⟩ + \cos \left(\frac{\pi}{8}\right) |11⟩
\]
we find that
\[
-\frac{1}{2}|0000⟩ + \frac{1}{2}|0011⟩ + \frac{1}{2}|1100⟩ + \frac{1}{2}|1111⟩ = \frac{1}{\sqrt{2}} v \otimes w + \frac{1}{\sqrt{2}} w \otimes v.
\]
When Alice measures this state with respect to the measurement \(\{P_0, P_1\}\), she obtains exactly one outcome 0 and one outcome 1. Thus, it holds that \(m(0,0) = 0\); Bob passes exactly one of the two tests with certainty.

(c) Analysis for the classical setting

We now observe that the behaviour exhibited in the example just described cannot happen in the classical setting.

Suppose that \(\rho \in D(X \otimes Z)\) and \(\{P_a : a \in \Sigma\} \subset \text{Pos}(Y \otimes Z)\) describe an interactive measurement as before. As is typical in quantum information theory, the classical setting corresponds to the special case in which these operators are all diagonal (with respect to the standard basis). Note that when the density operator \(\rho\) and a given measurement operator \(P_a\) are diagonal, it holds that the operator \(Q_a \in \text{Pos}(Y \otimes X)\) defined by (3.1) is also diagonal.

Now suppose that \(a \in \Sigma\) is a measurement outcome for which \(Q_a\) is diagonal, and consider the semidefinite programme whose optimal primal value describes the minimum probability associated with the outcome \(a\) (i.e. whose optimal value is \(m(a)\)).

\[
\begin{align*}
\text{primal problem} & \quad \text{minimize: } \langle Q_a, X \rangle \\
& \quad \text{subject to: } \text{Tr}_Y(X) = 1_X, \\
& \quad X \in \text{Pos}(Y \otimes X).
\end{align*}
\]

\[
\begin{align*}
\text{dual problem} & \quad \text{maximize: } \text{Tr}(Y) \\
& \quad \text{subject to: } 1_Y \otimes Y \leq Q_a, \\
& \quad Y \in \text{Herm}(X).
\end{align*}
\]

We will observe that there exists a dual optimal solution \(Y\) that is positive semidefinite. It will be helpful for this purpose to let \(A_X \in \mathcal{C}(X, X)\) and \(A_Y \in \mathcal{C}(Y, Y)\) denote the completely dephasing channels corresponding to \(X\) and \(Y\), respectively. More precisely, the mapping \(A_X\) is defined by
\[
A_X(|i⟩⟨j|) = \begin{cases} 
|i⟩⟨j| & \text{if } i = j \\
0 & \text{if } i \neq j
\end{cases}
\]

Proc. R. Soc. A (2012)
for $1 \leq i, j \leq n$, where $\{1, \ldots, n\}$ is the standard basis of $X$, and $A_Y$ is defined similarly with respect to the standard basis of $Y$.

Now consider an arbitrary dual optimal solution $Y_0 \in \text{Herm}(X)$. The mapping $A_Y \otimes A_X$ is completely positive, so the relation $1_Y \otimes Y_0 \leq Q_a$ implies that

$$1_Y \otimes A_X(Y_0) = (A_Y \otimes A_X)(1_Y \otimes Y_0) \leq (A_Y \otimes A_X)(Q_a) = Q_a.$$

The diagonal operator $A_X(Y_0)$ is therefore dual feasible. As $A_X$ preserves trace, $A_X(Y_0)$ achieves the same dual objective value as $Y_0$, and is therefore optimal as well. Finally, define

$$Y = \sum_{i=1}^{n} \max\{0, \langle i | A_X(Y_0) | i \rangle\} \langle i | i \rangle.$$

In other words, $Y$ is obtained from $A_X(Y_0)$ by replacing each negative diagonal entry with 0. The inequality $1_Y \otimes Y \leq Q_a$ follows from the inequality $1_Y \otimes A_X(Y_0) \leq Q_a$ together with the observation that each diagonal entry of $Q_a$ is necessarily non-negative (because $Q_a$ is positive semidefinite). As $\text{Tr}(Y) \geq \text{Tr}(A_X(Y_0)) = \text{Tr}(Y_0)$, it follows that $Y$ is also dual optimal. (The reality, of course, is that $Y = A_X(Y_0)$, for otherwise $Y_0$ would not have been dual optimal.) Finally, consider the situation in which two classical interactive measurements, described by pairs $(r_1, \{P_{a_1} : a_1 \in S_1\})$ and $(r_2, \{P_{a_2} : a_2 \in S_2\})$, are performed. One finds that the equality

$$m(a_1, a_2) = m_1(a_1)m_2(a_2)$$

considered before must now hold by an analysis similar to the one for the maximum output probability case: positive semidefinite optimal dual solutions exist for the semidefinite programme described above for each operator $Q_{a_1}$ and $Q_{a_2}$, allowing for the straightforward construction of optimal primal and dual solutions to the semidefinite programme whose optimal value is $m(a_1, a_2)$, thereby implying (4.2).

5. Conclusion

This paper has considered correlated strategies against independently administered hypothetical tests of a simple interactive type. It has been demonstrated that correlations arising in quantum information theoretic variants of these tests can exhibit a non-classical hedging type of behaviour.

One may, of course, consider situations in which more than two independent tests are performed, where a variety of statistics may be of interest. For example, one may consider Bob’s optimal probability to pass some threshold number $t$ of some (possibly large) number $k$ of independently administered tests. Based on our results, we know that a surprising behaviour exists even for the case $t = 1$ and $k = 2$, and it would be interesting to investigate the possible asymptotic behaviours that can arise.

Our work may have relevance in settings considered in cryptography, where certain protocols might very well be abstracted as tests of the sort we have considered. Our results demonstrate that collective quantum attacks to such
protocols may exhibit striking non-classical and counterintuitive properties, reinforcing the practice of giving very careful consideration to attacks of this nature.

Another motive of this work is the problem of error reduction through parallel repetition for quantum interactive proof systems. Indeed, suppose that a particular verifier has been specified (for a fixed decision problem \( L \)) so that the following conditions hold.

1. For each yes-instance \( x \) to \( L \), it is possible for a prover to convince the verifier to accept with probability at least \( \alpha \).
2. For each no-instance \( x \) to \( L \), the verifier always accepts with probability at most \( \beta \), regardless of the prover’s actions.

It may be, for instance, that \( \alpha = 1/2 + \delta \) and \( \beta = 1/2 - \delta \) for some small constant \( \delta > 0 \). A more desirable situation is one in which \( \alpha \) is replaced by \( 1 - \epsilon \) and \( \beta \) is replaced by \( \epsilon \) for a small value of \( \epsilon \). The process of specifying a new verifier based on the original one that meets stronger completeness and soundness conditions, such as the ones just suggested, is called error reduction.

In a purely algorithmic situation, the natural way to reduce error is to gather statistics from multiple independent executions of a given algorithm. For instance, if an algorithm outputs a binary value that is correct (for worst-case inputs) with a probability of at least 2/3 on any single execution of the algorithm, it is straightforward to obtain a new algorithm with a very high probability of correctness: one simply runs the original algorithm independently many times and takes the majority value as the output. A natural adaptation of this idea to interactive proof systems is to define a new verifier that independently runs many instances of the test performed by the original verifier, and accepts if and only if some suitably chosen threshold number of these independent tests would have led the original verifier to acceptance. In the situation under consideration, one is to understand that it is important for the new verifier to run these independent tests in parallel (as opposed to requiring the prover to respond sequentially to the individual tests).

It is not obvious that this works in the context of interactive proof systems for precisely the reason that has been considered in this paper: a hypothetical prover that interacts with many independent executions of an interactive proof system need not respect the independence of these executions. Nevertheless, in the classical setting it has long been known that error reduction through parallel repetition followed by a threshold value computation works perfectly\(^1\) for (single-prover) interactive proof systems. To say that the reduction is perfect means that if \( p \) is the optimal success probability for the original verifier, then the optimal probability to cause at least \( t \) acceptances among \( k \) independent executions of the original verifier is

\[
\sum_{j=t}^{k} \binom{k}{j} p^j (1-p)^{k-j}.
\]  

(5.1)

In other words, a prover gains absolutely no advantage in trying to correlate the independent tests performed by the verifier.

\(^1\)The situation is very different for multi-prover interactive proof systems, wherein the subject of parallel repetition is complicated (Raz 1998, 2008; Holenstein 2009).
In the quantum setting, however, it was not previously known if parallel repetition followed by a threshold value computation could allow for a perfect error reduction (or indeed any error reduction at all for certain values of $\alpha$ and $\beta$). Our results show that parallel repetition followed by a threshold value computation does not lead to a perfect reduction of error: substituting $k = 2$, $t = 1$ and $p = \cos^2(\pi/8)$ into (5.1) yields an upper bound of approximately 0.98, which is violated by the strategy, we described in the previous section (which achieves the value 1). We note that parallel repetition does work in the case of perfect completeness (i.e. $\alpha = 1$), wherein the threshold value computation is replaced by the logical-AND (Kitaev & Watrous 2000), and that there is a more complicated method for error reduction (based on a logical-AND of majorities), which does allow for error reduction in the general case of the setting under consideration (Jain et al. 2009).

Based on the semidefinite programming formalism we have described, it is possible to prove an upper bound of

$$\sum_{j=t}^{k} \binom{k}{j} p^j$$

on the probability for a quantum prover to cause at least $t$ acceptances among $k$ independent executions as considered above. Unfortunately, this expression does not lead to a reduction of errors for a wide range of choices of $\alpha > \beta$. This bound yields a value larger than 1 in some situations, and when the value is smaller than 1 we do not know how closely it can be approached by a valid quantum strategy.

Abel Molina acknowledges support from QuantumWorks, MITACS, a Mike and Ophelia Lazaridis Graduate Fellowship and a David R. Cheriton Graduate Scholarship. John Watrous acknowledges support from NSERC, CIFAR, QuantumWorks and MITACS.

References

Babai, L. & Moran, S. 1988 Arthur–Merlin games: a randomized proof system, and a hierarchy of complexity classes. *J. Comp. Syst. Sci.* 36, 254–276. (doi:10.1016/0022-0000(88)90028-1)

Bell, J. 1964 On the Einstein–Podolsky–Rosen paradox. *Physics* 1, 195–200.

Boyd, S. & Vandenberghe, L. 2004 *Convex optimization.* Cambridge: Cambridge University Press.

Chiribella, G., D’Ariano, G. & Perinotti, P. 2009 Theoretical framework for quantum networks. *Phys. Rev. A* 80, 022339. (doi:10.1103/PhysRevA.80.022339)

Choi, M.-D. 1975 Completely positive linear maps on complex matrices. *Linear Algebra Appl.* 10, 285–290. (doi:10.1016/0024-3795(75)90075-0)

Clauser, J. F., Horne, M. A., Shimony, A. & Holt, R. A. 1969 Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.* 23, 880–884. (doi:10.1103/PhysRevLett.23.880)

de Klerk, E. 2002 *Aspects of semidefinite programming—interior point algorithms and selected applications*, vol. 65. Applied Optimization. Dordrecht, The Netherlands: Kluwer Academic Publishers.

Goldwasser, S., Micali, S. & Rackoff, C. 1989 The knowledge complexity of interactive proof systems. *SIAM J. Comput.* 18, 186–208. (doi:10.1137/0218012)

Gutoski, G. & Watrous, J. 2007 Toward a general theory of quantum games. In *Proc. 39th Annual ACM Symp. on Theory of Computing*, San Diego, CA, 11–13 June 2007, pp. 565–574. New York, NY: ACM.

Holenstein, T. 2009 Parallel repetition: simplifications and the no-signaling case. *Theory Comput.* 5, 141–172. (doi:10.4086/toc.2009.v005a008)
Hedging bets with quantum strategies

Jain, R., Upadhyay, S. & Watrous, J. 2009 Two-message quantum interactive proofs are in PSPACE. In Proc. 50th Annual IEEE Symp. on Foundations of Computer Science, Atlanta, Georgia, GA, 25–27 October 2009, pp. 534–543. Los Alamitos, CA: IEEE Computer Society. (doi:10.1109/FOCS.2009.30)

Jamiołkowski, A. 1972 Linear transformations which preserve trace and positive semidefiniteness of operators. Reports Math. Phys. 3, 275–278. (doi:10.1016/0034-4877(72)90011-0)

Kitaev, A. & Watrous, J. 2000 Parallelization, amplification, and exponential time simulation of quantum interactive proof system. In Proc. 32nd Annual ACM Symp. on Theory of Computing, Portland, OR, 21–23 May 2000, pp. 608–617. New York, NY: ACM. (doi:10.1145/335305.335387)

Lovász, L. 2003 Semidefinite programs and combinatorial optimization. In Recent Advances in Algorithms and Combinatorics (eds B. A. Reed & C. L. Sales). CMS Books in Mathematics. New York, NY: Springer-Verlag. (doi:10.1007/b98891).

Mermin, N. D. 1990 Simple unified form for no-hidden variables theorems. Phys. Rev. Lett. 65, 3373–3376. (doi:10.1103/PhysRevLett.65.3373)

Mittal, R. & Szegedy, M. 2007 Product rules in semidefinite programming. Fundamentals of computation theory, vol. 4639, pp. 435–445. Lecture Notes in Computer Science. Springer: Springer.

Nielsen, M. A. & Chuang, I. L. 2000 Quantum computation and quantum information. Cambridge: Cambridge University Press.

Peres, A. 1990 Incompatible results of quantum measurements. Phys. Rev. A 151, 107–108. (doi:10.1016/0375-9601(90)90172-K)

Raz, R. 1998 A parallel repetition theorem. SIAM J. Comput. 27, 763–803. (doi:10.1137/S0097539795280895)

Raz, R. 2008 A counterexample to strong parallel repetition. In 49th Annual IEEE Symp. on Foundations of Computer Science, Philadelphia, PA, 25–28 October 2008, pp. 369–373. Los Alamitos, CA: IEEE Computer Society. (doi:10.1109/FOCS.2008.49)

Vandenberghe, L. & Boyd, S. 1996 Semidefinite programming. SIAM Rev. 38, 49–95. (doi:10.1137/1038003)