# Toward a General Theory of Quantum Games

Gus Gutoski John Watrous
*Institute for Quantum Computing and School of Computer Science*
*University of Waterloo, Waterloo, Ontario, Canada*

June 22, 2007

**Abstract**

We study properties of *quantum strategies*, which are complete specifications of a given party's actions in any multiple-round interaction involving the exchange of quantum information with one or more other parties. In particular, we focus on a representation of quantum strategies that generalizes the Choi-Jamiołkowski representation of quantum operations. This new representation associates with each strategy a positive semidefinite operator acting only on the tensor product of its input and output spaces. Various facts about such representations are established, and two applications are discussed: the first is a new and conceptually simple proof of Kitaev's lower bound for strong coin-flipping, and the second is a proof of the exact characterization QRG = EXP of the class of problems having quantum refereed games.

## 1 Introduction

The theory of games provides a general structure within which both cooperation and competition among independent entities may be modeled, and provides powerful tools for analyzing these models. Applications of this theory have fundamental importance in many areas of science.

This paper considers games in which the players may exchange and process quantum information. We focus on competitive games, and within this context the types of games we consider are very general. For instance, they allow multiple rounds of interaction among the players involved, and place no restrictions on players' strategies beyond those imposed by the theory of quantum information.

While classical games can be viewed as a special case of quantum games, it is important to stress that there are fundamental differences between general quantum games and classical games. For example, the two most standard representations of classical games, namely the *normal form* and *extensive form* representations, are not directly applicable to general quantum games. This is due to the nature of quantum information, which admits a continuum of pure (meaning extremal) strategies, imposes bounds on players' knowledge due to the uncertainty principle, and precludes the representation of general computational processes as trees. In light of such issues, it is necessary to give special consideration to the incorporation of quantum information into the theory of games.

A general theory of quantum games has the potential to be useful in many situations that arise in quantum cryptography, computational complexity, communication complexity, and distributed computation. This potential is the primary motivation for the work presented in this paper. The following facts are among those proved herein:

- Every multiple round quantum strategy can be faithfully represented by a single positive semidefinite operator acting only on the tensor product of the input and output spaces of the given player. This representation is a generalization of the Choi-Jamiołkowski representation of super-operators. The set of all operators that arise in this way is precisely characterized by the set of positive semidefinite operators that satisfy a simple collection of linear constraints.

- If a multiple round quantum strategy calls for one or more measurements then its representation consists of one operator for each of the possible measurement outcomes. The probability of any given pair of measurement outcomes for two interacting strategies is given by the inner product of their associated operators.

- The maximum probability with which a given strategy can be forced to output a particular result is the *minimum* value of $p$ for which the positive semidefinite operator corresponding to the given measurement result is bounded above (with respect to the Löwner partial order) by the representation of a valid strategy multiplied by $p$.

We give the following applications of these facts:

- A new and conceptually simple proof of Kitaev's bound for strong coin-flipping, which states that every quantum strong coin-flipping protocol allows a bias of at least $1/\sqrt{2} - 1/2$.

- The exact characterization QRG $=$ EXP of the class of problems having quantum refereed games (i.e., quantum interactive proof systems with two competing provers). This establishes that quantum and classical refereed games are equivalent in terms of expressive power: QRG $=$ RG.

**Relation to previous work**

It is appropriate for us to comment on the relationship between the present paper and a fairly large collection of papers written on a topic that has been called *quantum game theory*. Meyer's *PQ Penny Flip* game [27] is a well-known example of a game in the category these papers consider. The work of Eisert, *et al.* [9] is also commonly cited in this area. Some controversy exists over the interpretations drawn in some of these papers—see, for instance, Refs. [5, 10].

A key difference between our work and previous work on quantum game theory is that our focus is on multiple-round interactions. Understanding the actions available to players that have quantum memory is therefore critical to our work, and to our knowledge has not been previously considered in the context of quantum game theory.

A second major difference is that, in most of the previous quantum game theory papers we are aware of, the focus is on rather specific examples of classical games and on identifying differences that arise when so-called quantum variants of these games are considered. As a possible consequence, it may arguably be said that none of the results proved in these papers has had sufficient generality to be applicable to any other studies in quantum information. In contrast, our interest is not on specific examples of games, but rather on the development of a general theory that holds for all games. It remains to be seen to what extent our work will be applied, but the applications that we provide suggest that it may have interesting uses in other areas of quantum information and computation.

A different context in which games arise in quantum information theory is that of *nonlocal games* [8], which include *pseudo-telepathy games* [6] as a special case. These are cooperative games

of incomplete information that model situations that arise in the study of multiple-prover interactive proof systems, and provide a framework for studying Bell Inequalities and the notion of nonlocality that arises in quantum physics. While such games can be described within the general setting we consider, we have not yet found an application of the methods of the present paper to this type of game. Possibly there is some potential for further development of our work to shed light on some of the difficult questions in this area.

## 2 Preliminaries

This section gives a brief overview of various quantum information-theoretic notions that will be needed for the remainder of the paper. We assume the reader has familiarity with quantum information theory, and intend only that this overview will serve to establish our notation and highlight the main concepts that we will need. Readers not familiar with quantum information are referred to the books of Nielsen and Chuang [30] and Kitaev, Shen and Vyalyi [23].

When we speak of the vector space associated with a given quantum system, we are referring to some complex Euclidean space (by which we mean a finite-dimensional inner product space over the complex numbers). Such spaces will be denoted by capital script letters such as $\mathcal{X}$, $\mathcal{Y}$, and $\mathcal{Z}$. We always assume that an orthonormal *standard basis* of any such space has been chosen, and with respect to this basis elements of these spaces are associated with column vectors, and linear mappings from one space to another are associated with matrices in the usual way. We will often be concerned with finite sequences $\mathcal{X}_1, \mathcal{X}_2, \ldots, \mathcal{X}_n$ of complex Euclidean spaces. We then define

$$\mathcal{X}_{i\ldots j} = \mathcal{X}_i \otimes \cdots \otimes \mathcal{X}_j$$

for nonnegative integers $i, j \leq n$, and define $\mathcal{X}_{i\ldots j} = \mathbb{C}$ for $i > j$.

It is convenient to define various sets of linear mappings between given complex Euclidean spaces $\mathcal{X}$ and $\mathcal{Y}$ as follows. Let $\mathrm{L}(\mathcal{X}, \mathcal{Y})$ denote the space of all linear mappings (or *operators*) from $\mathcal{X}$ to $\mathcal{Y}$, and write $\mathrm{L}(\mathcal{X})$ as shorthand for $\mathrm{L}(\mathcal{X}, \mathcal{X})$. We write $\mathrm{Herm}(\mathcal{X})$ to denote the set of Hermitian operators acting on $\mathcal{X}$, $\mathrm{Pos}(\mathcal{X})$ to denote the set of all positive semidefinite operators acting on $\mathcal{X}$, and $\mathrm{D}(\mathcal{X})$ to denote the set of all density operators on $\mathcal{X}$ (meaning positive semidefinite operators having trace equal to 1.) An operator $A \in \mathrm{L}(\mathcal{X}, \mathcal{Y})$ is a *linear isometry* if $A^*A = I_{\mathcal{X}}$. The existence of a linear isometry in $\mathrm{L}(\mathcal{X}, \mathcal{Y})$ of course requires that $\dim(\mathcal{X}) \leq \dim(\mathcal{Y})$, and if $\dim(\mathcal{X}) = \dim(\mathcal{Y})$ then any linear isometry $A \in \mathrm{L}(\mathcal{X}, \mathcal{Y})$ is unitary. We let $\mathrm{U}(\mathcal{X}, \mathcal{Y})$ denote the set of all linear isometries from $\mathcal{X}$ to $\mathcal{Y}$. The operator $I_{\mathcal{X}} \in \mathrm{L}(\mathcal{X})$ denotes the identity operator on $\mathcal{X}$. Transposition of operators is always taken with respect to standard bases.

The Hilbert-Schmidt inner product on $\mathrm{L}(\mathcal{X})$ is defined by

$$\langle A, B \rangle = \mathrm{Tr}(A^*B)$$

for all $A, B \in \mathrm{L}(\mathcal{X})$.

For given operators $A, B \in \mathrm{Herm}(\mathcal{X})$, the notation $A \leq B$ means that $B - A \in \mathrm{Pos}(\mathcal{X})$. This relation is sometimes called the *Löwner partial order* on $\mathrm{Herm}(\mathcal{X})$.

When we refer to *measurements*, we mean POVM-type measurements. Formally, a measurement on a complex Euclidean space $\mathcal{X}$ is described by a collection of positive semidefinite operators

$$\{P_a : a \in \Sigma\} \subset \mathrm{Pos}(\mathcal{X})$$

satisfying the constraint

$$\sum_{a \in \Sigma} P_a = I_{\mathcal{X}}.$$

Here $\Sigma$ is a finite, non-empty set of *measurement outcomes*. If a state represented by the density operator $\rho$ is measured with respect to such a measurement, each outcome $a \in \Sigma$ results with probability $\langle P_a, \rho \rangle = \mathrm{Tr}(P_a \rho)$.

A *super-operator* is a linear mapping of the form

$$\Phi : \mathrm{L}(\mathcal{X}) \to \mathrm{L}(\mathcal{Y}),$$

where $\mathcal{X}$ and $\mathcal{Y}$ are complex Euclidean spaces. A super-operator of this form is said to be *positive* if $\Phi(X) \in \mathrm{Pos}(\mathcal{Y})$ for every choice of $X \in \mathrm{Pos}(\mathcal{X})$, and is *completely positive* if $\Phi \otimes I_{\mathrm{L}(\mathcal{Z})}$ is positive for every choice of a complex Euclidean space $\mathcal{Z}$. The super-operator $\Phi$ is said to be *admissible* if it is completely positive and preserves trace: $\mathrm{Tr}(\Phi(X)) = \mathrm{Tr}(X)$ for all $X \in \mathrm{L}(\mathcal{X})$. Admissible super-operators represent discrete-time changes in quantum systems that can, in an idealized sense, be physically realized.

The Choi-Jamiołkowski representation [20, 7] of super-operators is as follows. Suppose that $\Phi : \mathrm{L}(\mathcal{X}) \to \mathrm{L}(\mathcal{Y})$ be a given super-operator and let $\{|1\rangle, \ldots, |N\rangle\}$ be the standard basis of $\mathcal{X}$. Then the *Choi-Jamiołkowski representation* of $\Phi$ is the operator

$$J(\Phi) = \sum_{1 \leq i,j \leq N} \Phi(|i\rangle \langle j|) \otimes |i\rangle \langle j| \in \mathrm{L}(\mathcal{Y} \otimes \mathcal{X}).$$

It holds that $\Phi$ is completely positive if and only if $J(\Phi)$ is positive semidefinite, and that $\Phi$ is trace-preserving if and only if $\mathrm{Tr}_{\mathcal{Y}}(J(\Phi)) = I_{\mathcal{X}}$.

For two complex Euclidean spaces $\mathcal{X}$ and $\mathcal{Y}$, we define a linear mapping

$$\mathrm{vec} : \mathrm{L}(\mathcal{X}, \mathcal{Y}) \to \mathcal{Y} \otimes \mathcal{X}$$

by extending by linearity the action $|i\rangle \langle j| \mapsto |i\rangle |j\rangle$ on standard basis states. We make extensive use of this mapping in some of our proofs, as it is very convenient in a variety of situations. Let us now state some identities involving the vec mapping, each of which can be verified by a straightforward calculation.

**Proposition 1.** *The following hold:*

1. *For any choice of $A$, $B$, and $X$ for which the product $AXB^{\mathsf{T}}$ makes sense we have*

$$(A \otimes B)\,\mathrm{vec}(X) = \mathrm{vec}(AXB^{\mathsf{T}}).$$

2. *For any choice of $A, B \in \mathrm{L}(\mathcal{X}, \mathcal{Y})$ we have*

$$\mathrm{Tr}_{\mathcal{X}}(\mathrm{vec}(A)\,\mathrm{vec}(B)^*) = AB^*,$$
$$\mathrm{Tr}_{\mathcal{Y}}(\mathrm{vec}(A)\,\mathrm{vec}(B)^*) = (B^*A)^{\mathsf{T}}.$$

3. *For any choice of $A, B \in \mathrm{L}(\mathcal{X})$ we have*

$$\mathrm{vec}(I_{\mathcal{X}})^*(A \otimes B)\,\mathrm{vec}(I_{\mathcal{X}}) = \mathrm{Tr}(AB^{\mathsf{T}}).$$

4. *Let $A \in \mathrm{L}(\mathcal{X}, \mathcal{Y} \otimes \mathcal{Z})$ and suppose $\Phi : \mathrm{L}(\mathcal{X}) \to \mathrm{L}(\mathcal{Y})$ is given by $\Phi(X) = \mathrm{Tr}_{\mathcal{Z}}(AXA^*)$ for all $X \in \mathrm{L}(\mathcal{X})$. Then*

$$J(\Phi) = \mathrm{Tr}_{\mathcal{Z}}(\mathrm{vec}(A)\,\mathrm{vec}(A)^*).$$

For any non-empty set $\mathcal{C} \subseteq \mathrm{Herm}(\mathcal{X})$ of Hermitian operators, the *polar* of $\mathcal{C}$ is defined as

$$\mathcal{C}^{\circ} = \{A \in \mathrm{Herm}(\mathcal{X}) \,:\, \langle B, A\rangle \leq 1 \text{ for all } B \in \mathcal{C}\},$$

and the *support* and *gauge* functions of $\mathcal{C}$ are defined as follows:

$$s(X \mid \mathcal{C}) = \sup\{\langle X, Y\rangle \,:\, Y \in \mathcal{C}\},$$
$$g(X \mid \mathcal{C}) = \inf\{\lambda \geq 0 \,:\, X \in \lambda\mathcal{C}\}.$$

These functions are partial functions in general, but it is typical to view them as total functions from $\mathrm{Herm}(\mathcal{X})$ to $\mathbb{R} \cup \{\infty\}$ in the natural way. For any set $\mathcal{C}$ of positive semidefinite operators, we denote

$$\downarrow\mathcal{C} = \{X \,:\, 0 \leq X \leq Y \text{ for some } Y \in \mathcal{C}\}.$$

**Proposition 2.** *Let $\mathcal{X}$ be a complex Euclidean space and let $\mathcal{C}$ and $\mathcal{D}$ be non-empty subsets of* $\mathrm{Herm}(\mathcal{X})$*. Then the following facts hold:*

1. *If $\mathcal{C} \subseteq \mathcal{D}$ then $\mathcal{D}^{\circ} \subseteq \mathcal{C}^{\circ}$.*
2. *If $-X \in \mathcal{C}$ for each $X \in \mathrm{Pos}(\mathcal{X})$ then $\mathcal{C}^{\circ} \subseteq \mathrm{Pos}(\mathcal{X})$.*
3. *If $\mathcal{C}$ is closed, convex, and contains the origin, then the same is true of $\mathcal{C}^{\circ}$. In this case we have $\mathcal{C}^{\circ\circ} = \mathcal{C}$,*
$$s(\cdot \mid \mathcal{C}) = g(\cdot \mid \mathcal{C}^{\circ}), \quad \text{and} \quad s(\cdot \mid \mathcal{C}^{\circ}) = g(\cdot \mid \mathcal{C}).$$

The first two items in the above proposition are elementary, and a proof of the third may be found in Rockafellar [31].

## 3 Quantum Strategies

In this section we define the notions of a quantum *strategy* and the *Choi-Jamiołkowski representation* of quantum strategy. The remainder of the paper is concerned with the study of these objects and their interactions.

#### Definition of quantum strategies

We begin with our definition for quantum strategies, which we will simply call *strategies* given that the focus of the paper is on the quantum setting.

**Definition 3.** Let $n \geq 1$ and let $\mathcal{X}_1, \ldots, \mathcal{X}_n$ and $\mathcal{Y}_1, \ldots, \mathcal{Y}_n$ be complex Euclidean spaces. An *$n$-turn non-measuring strategy* having input spaces $\mathcal{X}_1, \ldots, \mathcal{X}_n$ and output spaces $\mathcal{Y}_1, \ldots, \mathcal{Y}_n$ consists of:

1. complex Euclidean spaces $\mathcal{Z}_1, \ldots, \mathcal{Z}_n$, which will be called *memory spaces*, and
2. an $n$-tuple of admissible mappings $(\Phi_1, \ldots, \Phi_n)$ having the form
$$\Phi_1 : \mathrm{L}(\mathcal{X}_1) \to \mathrm{L}(\mathcal{Y}_1 \otimes \mathcal{Z}_1)$$
$$\Phi_k : \mathrm{L}(\mathcal{X}_k \otimes \mathcal{Z}_{k-1}) \to \mathrm{L}(\mathcal{Y}_k \otimes \mathcal{Z}_k) \quad (2 \leq k \leq n).$$

An *$n$-turn measuring strategy* consists of items 1 and 2 above, as well as:

3. a measurement $\{P_a \,:\, a \in \Sigma\}$ on the last memory space $\mathcal{Z}_n$.

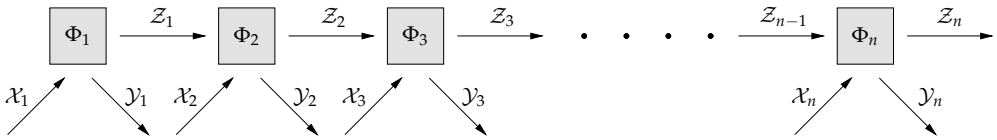


Figure 1: An $n$-turn strategy.

We will use the term *n-turn strategy* to refer to either a measuring or non-measuring $n$-turn strategy.

Figure 1 illustrates an $n$-turn non-measuring strategy.

Although there is no restriction on the dimension of the memory spaces in a quantum strategy, it is established in the proof of Theorem 6 that every measuring strategy is equivalent to one in which $\dim(\mathcal{Z}_k) \leq \dim(\mathcal{X}_{1\ldots k} \otimes \mathcal{Y}_{1\ldots k})$ for each $k = 1, \ldots, n$.

We also note that our definition of strategies allows the possibility that any of the input or output spaces is equal to $\mathbb{C}$, which corresponds to an empty message. One can therefore view simple actions such as the preparation of a quantum state or performing a measurement without producing a quantum output as special cases of strategies.

When we say that an $n$-turn strategy is described by *linear isometries* $A_1, \ldots, A_n$, it is meant that the admissible super-operators $\Phi_1, \ldots, \Phi_n$ defining the strategy are given by $\Phi_k(X) = A_k X A_k^*$ for $1 \leq k \leq n$. Notice that, when it is convenient, there is no loss of generality in restricting ones attention to strategies described by linear isometries in this way. This is because every admissible super-operator can be expressed as a mapping $X \mapsto AXA^*$ for some linear isometry $A$, followed by the partial trace over some "garbage" space that represents a tensor factor of the space to which $A$ maps. By including the necessary "garbage" spaces as tensor factors of the memory spaces, and therefore not tracing them out, there can be no change in the action of the strategy on the input and output spaces. Along similar lines, there is no loss of generality in assuming that a given measuring strategy's measurement is projective.

**Interactions among strategies**

A given $n$-turn strategy expects to interact with something that provides the inputs corresponding to $\mathcal{X}_1, \ldots, \mathcal{X}_n$ and accepts the strategy's outputs corresponding to $\mathcal{Y}_1, \ldots, \mathcal{Y}_n$. Let us define an $n$-turn *co-strategy* to be the sort of object that a strategy interfaces with in the most natural way.

**Definition 4.** Let $n \geq 1$ and let $\mathcal{X}_1, \ldots, \mathcal{X}_n$ and $\mathcal{Y}_1, \ldots, \mathcal{Y}_n$ be complex Euclidean spaces. The spaces $\mathcal{X}_1, \ldots, \mathcal{X}_n$ are viewed as the input spaces of some $n$-turn strategy while $\mathcal{Y}_1, \ldots, \mathcal{Y}_n$ are to be viewed as its output spaces. An *n-turn non-measuring co-strategy* to these spaces consists of:

1. complex Euclidean *memory* spaces $\mathcal{W}_0, \ldots, \mathcal{W}_n$,
2. a density operator $\rho_0 \in \mathrm{D}(\mathcal{X}_1 \otimes \mathcal{W}_0)$, and
3. an $n$-tuple of admissible mappings $(\Psi_1, \ldots, \Psi_n)$ having the form

$$\Psi_k : \mathrm{L}(\mathcal{Y}_k \otimes \mathcal{W}_{k-1}) \to \mathrm{L}(\mathcal{X}_{k+1} \otimes \mathcal{W}_k) \quad (1 \leq k \leq n-1)$$
$$\Psi_n : \mathrm{L}(\mathcal{Y}_n \otimes \mathcal{W}_{n-1}) \to \mathrm{L}(\mathcal{W}_n).$$

An *n-turn measuring co-strategy* consists of items 1, 2 and 3 above, as well as:

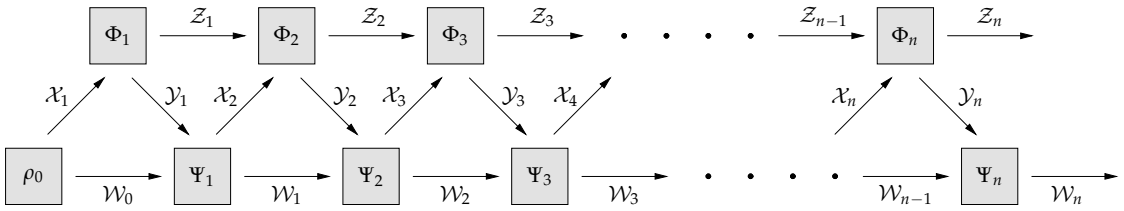


Figure 2: An interaction between an $n$-turn strategy and co-strategy.

4. a measurement $\{Q_b : b \in \Gamma\}$ on the last memory space $\mathcal{W}_n$.

As for strategies, we use the term *n-turn co-strategy* to refer to either a measuring or non-measuring $n$-turn co-strategy.

Figure 2 represents the interaction between an $n$-turn strategy and co-strategy.

We have arbitrarily defined strategies and co-strategies in such a way that the co-strategy sends the first message. This accounts for the inevitable asymmetry in the definitions. While it is possible to view any $n$-turn co-strategy as being an $(n+1)$-turn strategy having input spaces $\mathbb{C}, \mathcal{Y}_1, \ldots, \mathcal{Y}_n$ and output spaces $\mathcal{X}_1, \ldots, \mathcal{X}_n, \mathbb{C}$, it will be convenient for our purposes to view strategies and co-strategies as being distinct types of objects.

Similar to strategies, there will be no loss of generality in assuming that the initial state $\rho_0$ of a co-strategy is pure, that each of the admissible super-operators $\Psi_1, \ldots, \Psi_n$ takes the form $\Psi_j(X) = B_j X B_j^*$ for some linear isometry $B_j$, and, in the case of measuring co-strategies, that the measurement $\{Q_b : b \in \Gamma\}$ is a projective measurement.

An $n$-turn strategy and co-strategy are *compatible* if they agree on the spaces $\mathcal{X}_1, \ldots, \mathcal{X}_n$ and $\mathcal{Y}_1, \ldots, \mathcal{Y}_n$. By the *output* of a compatible strategy and co-strategy, assuming at least one of them is measuring, we mean the result of the measurement or measurements performed after the interaction between the strategies takes place. In particular, if both the strategy and co-strategy make measurements, then each output $(a, b) \in \Sigma \times \Gamma$ results with probability

$$\left\langle P_a \otimes Q_b, (I_{\mathrm{L}(\mathcal{Z}_n)} \otimes \Psi_n) \cdots (\Phi_1 \otimes I_{\mathrm{L}(\mathcal{W}_0)})\rho_0 \right\rangle.$$

**A new way to represent strategies**

The definitions of strategies and co-strategies given above are natural from an operational point of view, in the sense that they clearly describe the actions of the players that they model. In some situations, however, representing a strategy (or co-strategy) in terms of a sequence of admissible super-operators is inconvenient. We now describe a different way to represent strategies that is based on the Choi-Jamiołkowski representation of super-operators.

Let us first extend this representation to $n$-turn non-measuring strategies. To do this, we associate with the strategy described by $(\Phi_1, \ldots, \Phi_n)$ a single admissible super-operator

$$\Xi : \mathrm{L}(\mathcal{X}_{1\ldots n}) \to \mathrm{L}(\mathcal{Y}_{1\ldots n}).$$

This is the super-operator that takes a given input $\xi \in \mathrm{D}(\mathcal{X}_{1\ldots n})$ and feeds the portions of this state corresponding to the input spaces $\mathcal{X}_1, \ldots, \mathcal{X}_n$ into the network pictured in Figure 1, one piece at a time. The memory space $\mathcal{Z}_n$ is then traced out, leaving some element $\Xi(\xi) \in \mathrm{D}(\mathcal{Y}_{1\ldots n})$. Such a map is depicted in Figure 3 for the case $n = 3$. The Choi-Jamiołkowski representation of the strategy

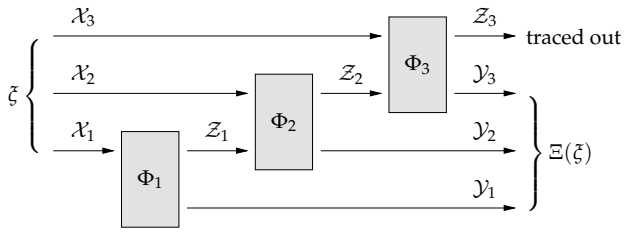


Figure 3: The super-operator $\Xi$ associated with a 3-turn strategy.

described by $(\Phi_1, \ldots, \Phi_n)$ is then simply defined as the Choi-Jamiołkowski representation $J(\Xi)$ of the super-operator $\Xi$ we have just defined.

An alternate expression for the Choi-Jamiołkowski representation of a strategy exists in the case that it is described by linear isometries $(A_1, \ldots, A_n)$. Specifically, its representation is given by $\mathrm{Tr}_{\mathcal{Z}_n}\left(\mathrm{vec}(A)\,\mathrm{vec}(A)^*\right)$ where $A \in \mathrm{L}\left(\mathcal{X}_{1\ldots n}, \mathcal{Y}_{1\ldots n} \otimes \mathcal{Z}_n\right)$ is defined by the product

$$A = \left(I_{\mathcal{Y}_{1\ldots n-1}} \otimes A_n\right)\left(I_{\mathcal{Y}_{1\ldots n-2}} \otimes A_{n-1} \otimes I_{\mathcal{X}_n}\right) \cdots \left(A_1 \otimes I_{\mathcal{X}_{2\ldots n}}\right). \tag{1}$$

Next we consider measuring strategies. Assume that an $n$-turn measuring strategy is given, where the measurement is described by

$$\{P_a \,:\, a \in \Sigma\} \subset \mathrm{Pos}\left(\mathcal{Z}_n\right),$$

for some finite, non-empty set $\Sigma$ of measurement outcomes. In this case we first associate with the strategy a collection of super-operators $\{\Xi_a \,:\, a \in \Sigma\}$, each having the form

$$\Xi_a : \mathrm{L}\left(\mathcal{X}_{1\ldots n}\right) \to \mathrm{L}\left(\mathcal{Y}_{1\ldots n}\right).$$

The definition of each super-operator $\Xi_a$ is precisely as in the non-measuring case, except that the partial trace over $\mathcal{Z}_n$ is replaced by the mapping

$$X \mapsto \mathrm{Tr}_{\mathcal{Z}_n}\left(\left(P_a \otimes I_{\mathcal{Y}_{1\ldots n}}\right)X\right).$$

Notice that

$$\sum_{a\in\Sigma} \Xi_a = \Xi,$$

where $\Xi$ is the mapping defined as in the non-measuring case. Each super-operators $\Xi_a$ is completely positive but generally is not trace-preserving. The Choi-Jamiołkowski representation of the measuring strategy described by $(\Phi_1, \ldots, \Phi_n)$ and $\{P_a \,:\, a \in \Sigma\}$ is defined as $\{J(\Xi_a) \,:\, a \in \Sigma\}$.

In the situation where a measuring strategy is described by linear isometries $A_1, \ldots, A_n$ and a measurement $\{P_a \,:\, a \in \Sigma\}$, its Choi-Jamiołkowski representation is given by $\{Q_a \,:\, a \in \Sigma\}$ for

$$Q_a = \mathrm{Tr}_{\mathcal{Z}_n}\left(\mathrm{vec}(B_a)\,\mathrm{vec}(B_a)^*\right)$$

where

$$B_a = \left(\sqrt{P_a} \otimes I_{\mathcal{Y}_{1\ldots n}}\right) A$$

for $A$ as defined above (1).

It is not difficult to prove that for given input spaces $\mathcal{X}_1, \ldots, \mathcal{X}_n$ and output spaces $\mathcal{Y}_1, \ldots, \mathcal{Y}_n$, a collection $\{Q_a : a \in \Sigma\}$ of operators is the Choi-Jamiołkowski representation of some $n$-turn measuring strategy if and only if $Q = \sum_{a \in \Sigma} Q_a$ is the representation of an $n$-turn non-measuring strategy over the same spaces.

Finally, we define the Choi-Jamiołkowski representation of measuring and non-measuring co-strategies in precisely the same way as for strategies, except that for technical reasons the resulting operators are transposed with respect to the standard basis. (This essentially allows us to eliminate one transposition from almost every subsequent equation in this paper involving representations of co-strategies.) Specifically, a given $n$-turn co-strategy is viewed as an $(n+1)$-turn strategy by including an empty first and last message as discussed previously. This strategy's Choi-Jamiołkowski representation is defined as above. The operators comprising this strategy representation are then transposed with respect to the standard basis to obtain the Choi-Jamiołkowski representation of the co-strategy.

As we work almost exclusively with the Choi-Jamiołkowski representation of strategies and co-strategies hereafter, we will typically use the term *representation* rather than *Choi-Jamiołkowski representation* for brevity.

# 4 Properties of representations

The applications of Choi-Jamiołkowski representations of strategies given in this paper rely upon three key properties of these representations, stated below as Theorems 5, 6, and 9. This section is devoted to establishing these properties.

### Interaction output probabilities

The first property provides a simple formula for the probability of a given output of an interaction between a strategy and a co-strategy.

**Theorem 5.** *Let $\{Q_a : a \in \Sigma\}$ be the representation of a strategy and let $\{R_b : b \in \Gamma\}$ be the representation of a compatible co-strategy. For each pair $(a, b) \in \Sigma \times \Gamma$ of measurement outcomes, we have that the output of an interaction between the given strategy and co-strategy is $(a, b)$ with probability $\langle Q_a, R_b \rangle$.*

*Proof.* Let us fix a strategy and co-strategy whose representations are $\{Q_a : a \in \Sigma\}$ and $\{R_a : a \in \Gamma\}$, respectively. Without loss of generality, the strategy is described by linear isometries $A_1, \ldots, A_n$ and a projective measurement $\{\Pi_a : a \in \Sigma\}$, while the co-strategy is described by a pure initial state $u_0$, linear isometries $B_1, \ldots, B_n$ and a projective measurement $\{\Delta_b : b \in \Gamma\}$.

For each output pair $(a, b) \in \Sigma \times \Gamma$, define $v_{a,b} \in \mathcal{Z}_n \otimes \mathcal{W}_n$ as follows:

$$v_{a,b} = (\Pi_a \otimes \Delta_b)(I_{\mathcal{Z}_n} \otimes B_n)(A_n \otimes I_{\mathcal{W}_{n-1}}) \cdots (I_{\mathcal{Z}_1} \otimes B_1)(A_1 \otimes I_{\mathcal{W}_0})u_0.$$

The probability of the outcome $(a, b)$ is $\|v_{a,b}\|^2$ for each pair $(a, b)$.

Now, making use of the vec mapping, we may express $v_{a,b}$ in a different way:

$$v_{a,b} = \left(\operatorname{vec}\left(I_{\mathcal{Y}_{1\ldots n} \otimes \mathcal{X}_{1\ldots n}}\right)^* \otimes I_{\mathcal{Z}_n \otimes \mathcal{W}_n}\right)(x_a \otimes y_b),$$

where

$$\begin{aligned} x_a &= \left(I_{\mathcal{X}_{1\ldots n} \otimes \mathcal{Y}_{1\ldots n} \otimes \mathcal{Z}_n} \otimes \operatorname{vec}(I_{\mathcal{Z}_{1\ldots n-1}})^*\right)(\operatorname{vec}(A_1) \otimes \cdots \otimes \operatorname{vec}(A_{n-1}) \otimes \operatorname{vec}((\Pi_a \otimes I_{\mathcal{Y}_n})A_n)), \\ y_b &= \left(I_{\mathcal{X}_{1\ldots n} \otimes \mathcal{Y}_{1\ldots n} \otimes \mathcal{W}_n} \otimes \operatorname{vec}(I_{\mathcal{W}_{0\ldots n-1}})^*\right)(u_0 \otimes \operatorname{vec}(B_1) \otimes \cdots \otimes \operatorname{vec}(B_{n-1}) \otimes \operatorname{vec}(\Delta_b B_n)). \end{aligned}$$

The probability of outcome $(a, b)$ is therefore

$$\begin{aligned}
\| v_{a,b} \|^2 &= \operatorname{Tr} v_{a,b} v_{a,b}^* \\
&= \operatorname{vec}(I_{\mathcal{Y}_{1\ldots n}} \otimes \mathcal{X}_{1\ldots n})^* \left[ (\operatorname{Tr}_{\mathcal{Z}_n} x_a x_a^*) \otimes (\operatorname{Tr}_{\mathcal{W}_n} y_b y_b^*) \right] \operatorname{vec}(I_{\mathcal{Y}_{1\ldots n} \otimes \mathcal{X}_{1\ldots n}}) \\
&= \operatorname{Tr} \left[ (\operatorname{Tr}_{\mathcal{Z}_n} x_a x_a^*) \, (\operatorname{Tr}_{\mathcal{W}_n} y_b y_b^*)^{\mathsf{T}} \right] \\
&= \langle Q_a, R_b \rangle
\end{aligned}$$

as required. □

**Characterization of strategy representations**

Let us denote by

$$\mathcal{S}_n(\mathcal{X}_{1\ldots n}, \mathcal{Y}_{1\ldots n})$$

the set of all representations of $n$-turn strategies having input spaces $\mathcal{X}_1, \ldots, \mathcal{X}_n$ and output spaces $\mathcal{Y}_1, \ldots, \mathcal{Y}_n$. We may abbreviate this set as $\mathcal{S}_n$ or $\mathcal{S}$ whenever the spaces or number of turns is clear from the context. Similarly, we let

$$\text{co-}\mathcal{S}_n(\mathcal{X}_{1\ldots n}, \mathcal{Y}_{1\ldots n})$$

denote the set of all representations of co-strategies for the same spaces. It will be convenient to define $\mathcal{S}_0(\mathbb{C}, \mathbb{C}) = \text{co-}\mathcal{S}_0(\mathbb{C}, \mathbb{C}) = \{1\}$.

The second property of strategy representations that we prove provides a characterization of $\mathcal{S}_n(\mathcal{X}_{1\ldots n}, \mathcal{Y}_{1\ldots n})$ in terms of linear constraints on $\operatorname{Pos}(\mathcal{Y}_{1\ldots n} \otimes \mathcal{X}_{1\ldots n})$.

**Theorem 6.** *Let $n \geq 1$, let $\mathcal{X}_1, \ldots, \mathcal{X}_n$ and $\mathcal{Y}_1, \ldots, \mathcal{Y}_n$ be complex Euclidean spaces, and let $Q \in \operatorname{Pos}(\mathcal{Y}_{1\ldots n} \otimes \mathcal{X}_{1\ldots n})$. Then*

$$Q \in \mathcal{S}_n(\mathcal{X}_{1\ldots n}, \mathcal{Y}_{1\ldots n})$$

*if and only if*

$$\operatorname{Tr}_{\mathcal{Y}_n}(Q) = R \otimes I_{\mathcal{X}_n}$$

*for $R \in \mathcal{S}_{n-1}(\mathcal{X}_{1\ldots n-1}, \mathcal{Y}_{1\ldots n-1})$.*

*Proof.* Let us first assume that $Q \in \mathcal{S}_n(\mathcal{X}_{1\ldots n}, \mathcal{Y}_{1\ldots n})$, which implies that there exist memory spaces $\mathcal{Z}_1, \ldots, \mathcal{Z}_n$ and admissible super-operators $\Phi_1, \ldots, \Phi_n$ that comprise a strategy whose representation is $Q$. Let $\Xi_n : \mathrm{L}(\mathcal{X}_{1\ldots n}) \to \mathrm{L}(\mathcal{Y}_{1\ldots n})$ be the super-operator associated with this strategy as described in Section 3, and let

$$\Xi_{n-1} : \mathrm{L}(\mathcal{X}_{1\ldots n-1}) \to \mathrm{L}(\mathcal{Y}_{1\ldots n-1})$$

be the super-operator associated with the $(n-1)$-turn strategy obtained by terminating the strategy described by $(\Phi_1, \ldots, \Phi_n)$ after $n-1$ turns. We have

$$\operatorname{Tr}_{\mathcal{Y}_n}(J(\Xi_n)) = J(\operatorname{Tr}_{\mathcal{Y}_n} \circ \Xi_n) = J(\Xi_{n-1} \circ \operatorname{Tr}_{\mathcal{X}_n}) = J(\Xi_{n-1}) \otimes I_{\mathcal{X}_n},$$

and so $\operatorname{Tr}_{\mathcal{Y}_n}(Q) = R \otimes I_{\mathcal{X}_n}$ for

$$R = J(\Xi_{n-1}) \in \mathcal{S}_{n-1}(\mathcal{X}_{1\ldots n-1}, \mathcal{Y}_{1\ldots n-1})$$

as required.

Now assume that $Q \in \operatorname{Pos}(\mathcal{Y}_{1\ldots n} \otimes \mathcal{X}_{1\ldots n})$ satisfies $\operatorname{Tr}_{\mathcal{Y}_n}(Q) = R \otimes I_{\mathcal{X}_n}$ for some choice of $R \in \mathcal{S}_{n-1}(\mathcal{X}_{1\ldots n-1}, \mathcal{Y}_{1\ldots n-1})$. Our goal is to prove that $Q \in \mathcal{S}_n(\mathcal{X}_{1\ldots n}, \mathcal{Y}_{1\ldots n})$. This will be proved by

induction on $n$. In fact, it will be easier to prove a somewhat stronger statement, which is that the assumptions imply that there exists a strategy whose representation is $Q$ that (i) is described by linear isometries $A_1, \ldots, A_n$, and (ii) satisfies $\dim(\mathcal{Z}_n) = \operatorname{rank}(Q)$.

If $n = 1$, there is nothing new to prove: it is well-known that if $Q \in \operatorname{Pos}(\mathcal{Y}_1 \otimes \mathcal{X}_1)$ satisfies $\operatorname{Tr}_{\mathcal{Y}_1}(Q) = I_{\mathcal{X}_1}$, then $Q = J(\Phi_1)$ for some admissible super-operator $\Phi_1 : \operatorname{L}(\mathcal{X}_1) \to \operatorname{L}(\mathcal{Y}_1)$. Any such super-operator can be expressed as

$$\Phi_1(X) = \operatorname{Tr}_{\mathcal{Z}_1} A_1 X A_1^*$$

for $\dim(\mathcal{Z}_1) = \operatorname{rank}(Q)$ and some choice of a linear isometry $A_1 \in \operatorname{L}(\mathcal{X}_1, \mathcal{Y}_1 \otimes \mathcal{Z}_1)$. The 1-turn strategy we require is therefore the strategy described by $A_1$.

Now assume that $n \geq 2$. By the induction hypothesis, there exist spaces $\mathcal{Z}_1, \ldots, \mathcal{Z}_{n-1}$ and linear isometries $A_1, \ldots, A_{n-1}$ with

$$\begin{aligned} &A_1 \in \operatorname{U}(\mathcal{X}_1, \mathcal{Y}_1 \otimes \mathcal{Z}_1), \\ &A_k \in \operatorname{U}(\mathcal{X}_k \otimes \mathcal{Z}_{k-1}, \mathcal{Y}_k \otimes \mathcal{Z}_k) \quad (2 \leq k \leq n-1), \end{aligned}$$

such that

$$R = \operatorname{Tr}_{\mathcal{Z}_{n-1}} (\operatorname{vec}(A) \operatorname{vec}(A)^*)$$

for $A \in \operatorname{L}(\mathcal{X}_{1\ldots n-1}, \mathcal{Y}_{1\ldots n-1} \otimes \mathcal{Z}_{n-1})$ defined as

$$A = (I_{\mathcal{Y}_{1\ldots n-2}} \otimes A_{n-1}) \cdots (A_1 \otimes I_{\mathcal{X}_{2\ldots n-1}}).$$

As required, we let $\mathcal{Z}_n$ be a complex Euclidean space with dimension equal to the rank of $Q$, and let $B \in \operatorname{L}(\mathcal{X}_{1\ldots n}, \mathcal{Y}_{1\ldots n} \otimes \mathcal{Z}_n)$ be any operator satisfying

$$\operatorname{Tr}_{\mathcal{Z}_n} (\operatorname{vec}(B) \operatorname{vec}(B)^*) = Q.$$

Such a choice of $B$ must exist given that the dimension of $\mathcal{Z}_n$ is large enough to admit a purification of $Q$. Note that

$$\operatorname{Tr}_{\mathcal{Y}_n \otimes \mathcal{Z}_n} (\operatorname{vec}(B) \operatorname{vec}(B)^*) = \operatorname{Tr}_{\mathcal{Y}_n}(Q) = R \otimes I_{\mathcal{X}_n}.$$

Next, let $\mathcal{V}$ be a complex Euclidean space with dimension equal to that of $\mathcal{X}_n$, and let $V \in \operatorname{U}(\mathcal{X}_n, \mathcal{V})$ be an arbitrary unitary operator. We have

$$\operatorname{Tr}_{\mathcal{V}} (\operatorname{vec}(V) \operatorname{vec}(V)^*) = I_{\mathcal{X}_n},$$

and therefore

$$\operatorname{Tr}_{\mathcal{Z}_{n-1} \otimes \mathcal{V}} (\operatorname{vec}(A \otimes V) \operatorname{vec}(A \otimes V)^*) = R \otimes I_{\mathcal{X}_n}.$$

At this point we have identified two purifications of $R \otimes I_{\mathcal{X}_n}$. We will use the isometric equivalence of purifications to define an isometry $A_n$ that will complete the proof. Specifically, because $\mathcal{Z}_{n-1} \otimes \mathcal{V}$ has the minimal dimension required to admit a purification of $R \otimes I_{\mathcal{X}_n}$, it follows that there must exist a linear isometry $U \in \operatorname{U}(\mathcal{Z}_{n-1} \otimes \mathcal{V}, \mathcal{Y}_n \otimes \mathcal{Z}_n)$ such that

$$(I_{\mathcal{Y}_{1\ldots n-1}} \otimes U \otimes I_{\mathcal{X}_{1\ldots n}}) \operatorname{vec}(A \otimes V) = \operatorname{vec}(B).$$

This equation may equivalently be written

$$B = (I_{\mathcal{Y}_{1\ldots n-1}} \otimes U)(A \otimes V).$$

We now define $A_n = U(I_{\mathcal{Z}_{n-1}} \otimes V)$. This is a linear isometry from $\mathcal{X}_n \otimes \mathcal{Z}_{n-1}$ to $\mathcal{Y}_n \otimes \mathcal{Z}_n$ that satisfies

$$B = (I_{\mathcal{Y}_{1\ldots n-1}} \otimes A_n)(A \otimes I_{\mathcal{X}_n}).$$

This implies that the strategy described by $A_1, \ldots, A_n$ has representation

$$\mathrm{Tr}_{\mathcal{Z}_n} \left(\mathrm{vec}(B)\,\mathrm{vec}(B)^*\right) = Q,$$

and therefore completes the proof. □

Theorem 6 is equivalent to the following statement: an operator $Q \in \mathrm{Pos}\left(\mathcal{Y}_{1\ldots n} \otimes \mathcal{X}_{1\ldots n}\right)$ is the representation of some $n$-turn strategy with input spaces $\mathcal{X}_1, \ldots, \mathcal{X}_n$ and output spaces $\mathcal{Y}_1, \ldots, \mathcal{Y}_n$ if and only if there exist operators $Q_1, \ldots, Q_{n-1}$, where $Q_k \in \mathrm{Pos}\left(\mathcal{Y}_{1\ldots k} \otimes \mathcal{X}_{1\ldots k}\right)$, such that the following linear constraints are satisfied:

$$\begin{aligned}
&\mathrm{Tr}_{\mathcal{Y}_{k\ldots n}}(Q) = Q_{k-1} \otimes I_{\mathcal{X}_{k\ldots n}} \quad (2 \leq k \leq n), \\
&\mathrm{Tr}_{\mathcal{Y}_{1\ldots n}}(Q) = I_{\mathcal{X}_{1\ldots n}}.
\end{aligned}$$

Each operator $Q_k$ in of course uniquely determined by the representation $Q$, and represents the strategy obtained by terminating any strategy represented by $Q$ after $k$ turns.

Theorem 6 also gives a characterization of $n$-turn co-strategies, as stated in the following corollary.

**Corollary 7.** *Let $n \geq 1$, let $\mathcal{X}_1, \ldots, \mathcal{X}_n$ and $\mathcal{Y}_1, \ldots, \mathcal{Y}_n$ be complex Euclidean spaces, and let $Q \in \mathrm{Pos}\left(\mathcal{Y}_{1\ldots n} \otimes \mathcal{X}_{1\ldots n}\right)$. Then*

$$Q \in \text{co-}\mathcal{S}_n(\mathcal{X}_{1\ldots n}, \mathcal{Y}_{1\ldots n})$$

*if and only if $Q = R \otimes I_{\mathcal{Y}_n}$ for $R \in \mathrm{Pos}\left(\mathcal{Y}_{1\ldots n-1} \otimes \mathcal{X}_{1\ldots n}\right)$ satisfying*

$$\mathrm{Tr}_{\mathcal{X}_n}(R) \in \text{co-}\mathcal{S}_{n-1}(\mathcal{X}_{1\ldots n-1}, \mathcal{Y}_{1\ldots n-1}).$$

The fact that $\mathcal{S}_n(\mathcal{X}_{1\ldots n}, \mathcal{Y}_{1\ldots n})$ and co-$\mathcal{S}_n(\mathcal{X}_{1\ldots n}, \mathcal{Y}_{1\ldots n})$ are bounded and characterized by the positive semidefinite constraint together with finite collections of linear constraints yields the following corollary.

**Corollary 8.** *Let $n \geq 1$, let $\mathcal{X}_1, \ldots, \mathcal{X}_n$ and $\mathcal{Y}_1, \ldots, \mathcal{Y}_n$ be complex Euclidean spaces. Then the sets $\mathcal{S}_n(\mathcal{X}_{1\ldots n}, \mathcal{Y}_{1\ldots n})$ and* co-$\mathcal{S}_n(\mathcal{X}_{1\ldots n}, \mathcal{Y}_{1\ldots n})$ *are compact and convex.*

Just as $\mathcal{S}_n(\mathcal{X}_{1\ldots n}, \mathcal{Y}_{1\ldots n})$ consists of all representations of non-measuring strategies, the set

$$\downarrow\mathcal{S}_n(\mathcal{X}_{1\ldots n}, \mathcal{Y}_{1\ldots n})$$

consists of all elements of representations of measuring strategies. In other words, for any $n$-turn measuring strategy representation $\{Q_a : a \in \Sigma\}$, it holds that $Q_a \in \downarrow\mathcal{S}_n(\mathcal{X}_{1\ldots n}, \mathcal{Y}_{1\ldots n})$ for each $a \in \Sigma$. Moreover, for each operator $Q$ there exists an $n$-turn measuring strategy $\{Q_a : a \in \Sigma\}$ of which $Q$ is an element if and only if $Q \in \downarrow\mathcal{S}_n(\mathcal{X}_{1\ldots n}, \mathcal{Y}_{1\ldots n})$. The set $\downarrow$co-$\mathcal{S}_n(\mathcal{X}_{1\ldots n}, \mathcal{Y}_{1\ldots n})$ has similar analogous properties.

**Maximum output probabilities**

The final property of strategy representations that we will prove concerns the maximum probability with which some interacting co-strategy can force a given measuring strategy to output a given outcome.

**Theorem 9.** *Let $n \geq 1$, let $\mathcal{X}_1, \ldots, \mathcal{X}_n$ and $\mathcal{Y}_1, \ldots, \mathcal{Y}_n$ be complex Euclidean spaces, and let $\{Q_a : a \in \Sigma\}$ represent an $n$-turn measuring strategy with input spaces $\mathcal{X}_1, \ldots, \mathcal{X}_n$ and output spaces $\mathcal{Y}_1, \ldots, \mathcal{Y}_n$. Then for each $a \in \Sigma$, the maximum probability with which this strategy can be forced to output $a$, maximized over all choices of compatible co-strategies, is given by*

$$\min\{p \in [0,1] \,:\, Q_a \leq pR \;\; \textit{for some } R \in \mathcal{S}_n(\mathcal{X}_{1\ldots n}, \mathcal{Y}_{1\ldots n})\}.$$

*An analogous result holds when $\{Q_a : a \in \Sigma\}$ is a measuring co-strategy.*

The remainder of the present section is devoted to a proof of this theorem.

**Lemma 10.** *Let $\mathcal{V}$ and $\mathcal{W}$ be complex Euclidean spaces and let $\mathcal{D} \subseteq \mathrm{Herm}(\mathcal{V})$ be any closed, convex set that contains the origin. Then for*

$$\mathcal{C} = \{X \in \mathrm{Herm}(\mathcal{V} \otimes \mathcal{W}) \,:\, X \leq Y \otimes I_{\mathcal{W}} \text{ for some } Y \in \mathcal{D}\}$$

*we have*

$$\mathcal{C}^\circ = \{Q \in \mathrm{Pos}(\mathcal{V} \otimes \mathcal{W}) \,:\, \mathrm{Tr}_{\mathcal{W}}(Q) \in \mathcal{D}^\circ\}.$$

*Proof.* The assumption $0 \in \mathcal{D}$ implies that $-R \in \mathcal{C}$ for every $R \in \mathrm{Pos}(\mathcal{V} \otimes \mathcal{W})$, and therefore $\mathcal{C}^\circ \subseteq \mathrm{Pos}(\mathcal{V} \otimes \mathcal{W})$. Consider any choice of $Q \in \mathrm{Pos}(\mathcal{V} \otimes \mathcal{W})$, and note that

$$\langle \mathrm{Tr}_{\mathcal{W}}(Q), Y \rangle = \langle Q, Y \otimes I_{\mathcal{W}} \rangle$$

for every choice of $Y \in \mathrm{Herm}(\mathcal{V})$.

If it is the case that $Q \in \mathcal{C}^\circ$ then we have $\langle Q, Y \otimes I_{\mathcal{W}} \rangle \leq 1$ for all $Y \in \mathcal{D}$, and therefore $\mathrm{Tr}_{\mathcal{W}}(Q) \in \mathcal{D}^\circ$. On the other hand, if $\mathrm{Tr}_{\mathcal{W}}(Q) \in \mathcal{D}^\circ$ then $\langle Q, Y \otimes I_{\mathcal{W}} \rangle \leq 1$ for all $Y \in \mathcal{D}$. It follows from the fact that $Q$ is positive semidefinite that $\langle Q, X \rangle \leq 1$ for all $X \leq Y \otimes I_{\mathcal{W}}$, and therefore $Q \in \mathcal{C}^\circ$. □

**Lemma 11.** *Let $\mathcal{V}$ be a complex Euclidean space, let $\mathcal{A}, \mathcal{B} \subset \mathrm{Pos}(\mathcal{V})$ be non-empty closed and convex sets, and suppose*

$$(\downarrow \mathcal{A})^\circ = \{X \in \mathrm{Herm}(\mathcal{V}) \,:\, X \leq Q \;\; \textit{for some } Q \in \mathcal{B}\}.$$

*Then*

$$(\downarrow \mathcal{B})^\circ = \{Y \in \mathrm{Herm}(\mathcal{V}) \,:\, Y \leq R \;\; \textit{for some } R \in \mathcal{A}\}.$$

*Proof.* Let

$$\mathcal{C} = \{Y \in \mathrm{Herm}(\mathcal{V}) \,:\, Y \leq R \text{ for some } R \in \mathcal{A}\}.$$

As $-P \in \mathcal{C}$ for every $P \in \mathrm{Pos}(\mathcal{V})$, it follows that $\mathcal{C}^\circ \subseteq \mathrm{Pos}(\mathcal{V})$. Clearly $\downarrow \mathcal{A} \subseteq \mathcal{C}$, and therefore $\mathcal{C}^\circ \subseteq (\downarrow \mathcal{A})^\circ$. Thus,

$$\mathcal{C}^\circ \subseteq (\downarrow \mathcal{A})^\circ \cap \mathrm{Pos}(\mathcal{V}) = \downarrow \mathcal{B}.$$

On the other hand, we have that every $Q \in \downarrow \mathcal{B}$ is contained in $(\downarrow \mathcal{A})^\circ$, implying that $\langle Q, R \rangle \leq 1$ for all $R \in \mathcal{A}$. As $Q \geq 0$, this implies that $\langle Q, X \rangle \leq 1$ for $X \leq R$. Consequently, $Q \in \mathcal{C}^\circ$. Thus $\downarrow \mathcal{B} = \mathcal{C}^\circ$, and so $(\downarrow \mathcal{B})^\circ = \mathcal{C}$ as required. □

**Lemma 12.** *Let $n \geq 1$ and let $\mathcal{X}_1, \ldots, \mathcal{X}_n$ and $\mathcal{Y}_1, \ldots, \mathcal{Y}_n$ be complex Euclidean spaces. Then for all $X \in \mathrm{Herm}\,(\mathcal{Y}_{1\ldots n} \otimes \mathcal{X}_{1\ldots n})$ we have*

1. *$X \in (\downarrow \mathcal{S}_n(\mathcal{X}_{1\ldots n}, \mathcal{Y}_{1\ldots n}))^\circ$ if and only if $X \leq Q$ for some choice of $Q \in \text{co-}\mathcal{S}_n(\mathcal{X}_{1\ldots n}, \mathcal{Y}_{1\ldots n})$.*
2. *$X \in (\downarrow \text{co-}\mathcal{S}_n(\mathcal{X}_{1\ldots n}, \mathcal{Y}_{1\ldots n}))^\circ$ if and only if $X \leq Q$ for some choice of $Q \in \mathcal{S}_n(\mathcal{X}_{1\ldots n}, \mathcal{Y}_{1\ldots n})$.*

*Proof.* The proof is by induction on $n$. As $\downarrow \mathcal{S}_0 = \downarrow \text{co-}\mathcal{S}_0 = [0, 1]$ and $(\downarrow \mathcal{S}_0)^\circ = (\downarrow \text{co-}\mathcal{S}_0)^\circ = (-\infty, 1]$, the lemma holds for the case $n = 0$.

Now suppose that $n \geq 1$. The two items in the statement of the lemma are equivalent by Lemma 11, so it will suffice to prove the first.

Define $\mathcal{E} \subset \mathrm{Herm}\,(\mathcal{Y}_{1\ldots n-1} \otimes \mathcal{X}_{1\ldots n})$ as

$$\mathcal{E} = \{Y \,:\, Y \leq P \otimes I_{\mathcal{X}_n} \text{ for some } P \in \downarrow \mathcal{S}_{n-1}\}.$$

By Lemma 10 we have

$$\mathcal{E}^\circ = \{Q \in \mathrm{Pos}\,(\mathcal{Y}_{1\ldots n-1} \otimes \mathcal{X}_{1\ldots n}) \,:\, \mathrm{Tr}_{\mathcal{X}_n}(Q) \in (\downarrow \mathcal{S}_{n-1})^\circ\}.$$

Also define $\mathcal{F} \subset \mathrm{Herm}\,(\mathcal{Y}_{1\ldots n} \otimes \mathcal{X}_{1\ldots n})$ as

$$\mathcal{F} = \{Z \,:\, Z \leq Q \otimes I_{\mathcal{Y}_n} \text{ for some } Q \in \mathcal{E}^\circ\}.$$

Again applying Lemma 10, we obtain

$$\mathcal{F}^\circ = \{R \in \mathrm{Pos}\,(\mathcal{Y}_{1\ldots n} \otimes \mathcal{X}_{1\ldots n}) \,:\, \mathrm{Tr}_{\mathcal{Y}_n}(R) \in \mathcal{E}\}.$$

Now, by Theorem 6 we have $\mathcal{F}^\circ = \downarrow \mathcal{S}_n(\mathcal{X}_{1\ldots n}, \mathcal{Y}_{1\ldots n})$, and so $\mathcal{F} = (\downarrow \mathcal{S}_n(\mathcal{X}_{1\ldots n}, \mathcal{Y}_{1\ldots n}))^\circ$. By the induction hypothesis we have

$$\mathcal{E}^\circ = \{Q \in \mathrm{Pos}\,(\mathcal{Y}_{1\ldots n-1} \otimes \mathcal{X}_{1\ldots n}) \,:\, \mathrm{Tr}_{\mathcal{X}_n}(Q) \in \downarrow \text{co-}\mathcal{S}_{n-1}\},$$

and therefore

$$\mathcal{F} = \{Z \,:\, Z \leq Q \otimes I_{\mathcal{Y}_n} \text{ for } \mathrm{Tr}_{\mathcal{X}_n}(Q) \in \downarrow \text{co-}\mathcal{S}_{n-1}\}.$$

By Corollary 7 we have that

$$\mathcal{F} = \{Z \,:\, Z \leq R \text{ for some } R \in \downarrow \text{co-}\mathcal{S}_n\},$$

which completes the proof. □

*Proof of Theorem 9.* Let $p_a \in [0, 1]$ denote the maximum probability with which $\{Q_a \,:\, a \in \Sigma\}$ can be forced to output $a$ in an interaction with some compatible co-strategy. It follows from Theorem 5 that $p_a = s(Q_a \mid \text{co-}\mathcal{S})$. Using Lemma 12, along with the fact that $Q_a$ is positive semidefinite, we have

$$s(Q_a \mid \text{co-}\mathcal{S}) = s(Q_a \mid \downarrow \text{co-}\mathcal{S}) = g(Q_a \mid (\downarrow \text{co-}\mathcal{S})^\circ) = g(Q_a \mid \downarrow \mathcal{S}),$$

which completes the proof. □

# 5 Applications

**Kitaev's bound for strong coin-flipping**

Quantum coin-flipping protocols aim to solve the following problem: two parties, Alice and Bob, at separate locations, want to flip a coin but do not trust one another. A quantum coin-flipping protocol with bias $\varepsilon$ is an interaction between two (honest) strategies $A$ and $B$, both having output sets $\{0, 1, \text{abort}\}$, that satisfies two properties:

1. The interaction between the honest parties $A$ and $B$ produces the same outcome $b \in \{0, 1\}$ for both players, with probability $1/2$ for each outcome. (Neither player outputs "abort" when both are honest.)

2. If one of the parties does not follow the protocol but the other does, neither of the outcomes $b \in \{0, 1\}$ is output by the honest player with probability greater than $1/2 + \varepsilon$.

Protocols that satisfy these conditions are generally referred to as *strong* coin-flipping protocols, because they require that a cheater cannot bias an honest player's outcome toward either result 0 or 1. (In contrast, *weak* protocols assume that Alice desires outcome 0 and Bob desires outcome 1, and only require that cheaters cannot bias the outcome toward their desired outcome.)

Kitaev [22] proved that no strong quantum coin-flipping protocol can have bias smaller than $1/\sqrt{2} - 1/2$, meaning that one cheating party can always force a given outcome on an honest party with probability at least $1/\sqrt{2}$. Kitaev did not publish this proof, but it appears in Refs. [2, 32]. Here we give a different proof based on the results of the previous section.

Suppose $\{A_0, A_1, A_{\text{abort}}\}$ is the representation of honest-Alice's strategy and $\{B_0, B_1, B_{\text{abort}}\}$ is the representation of honest-Bob's co-strategy in some coin-flipping protocol. These strategies may involve any fixed number of rounds of interaction. The first condition above implies

$$\frac{1}{2} = \langle A_0, B_0 \rangle = \langle A_1, B_1 \rangle .$$

Now, fix $b \in \{0, 1\}$, and let $p$ be the maximum probability that a cheating Bob can force honest-Alice to output $b$. Obviously we have $p \geq 1/2$. Theorem 9 implies that there must exist a strategy $Q$ for Alice such that $A_b \leq p\, Q$. If a cheating Alice plays this strategy $Q$, then honest-Bob outputs $b$ with probability

$$\langle Q, B_b \rangle \geq \frac{1}{p} \langle A_b, B_b \rangle = \frac{1}{2p}.$$

Given that

$$\max \left\{ p, \frac{1}{2p} \right\} \geq \frac{1}{\sqrt{2}}$$

for all $p > 0$, we have that either honest-Alice or honest-Bob can be convinced to output $b$ with probability at least $1/\sqrt{2}$.

This proof makes clear the limitations of strong coin-flipping protocols: the inability of Bob to force Alice to output $b$ directly implies that Alice can herself bias the outcome toward $b$. Weak coin-flipping does not directly face this same limitation. Currently the best bound known on the bias of weak quantum coin-flipping protocols, due to Ambainis [1], is that $\Omega(\log\log(1/\varepsilon))$ rounds of communication are necessary to achieve a bias of $\varepsilon$. The best weak quantum coin-flipping protocol currently known, which is due to Mochon [28], achieves bias approximately 0.192 (which surpasses the barrier $1/\sqrt{2} - 1/2 \approx 0.207$ on strong quantum coin-flipping).

**Zero-sum quantum games**

Next, we define quantum refereed games. It will be noted that von Neumann's Min-Max Theorem for zero-sum quantum refereed games follows from the facts we have proved about representations of strategies together with well-known generalizations of the classical Min-Max Theorem. Although it is completely expected that the Min-Max Theorem should hold for quantum games, it has not been previously noted in the general case with which we are concerned. (Lee and Johnson [26] proved this fact in the one-round case.) This discussion will also be helpful for the application to interactive proof systems with competing provers that follows.

Let us first define specifically what is meant by a zero-sum quantum refereed game. Such a game is played between two players, Alice and Bob, and is arbitrated by a referee. The referee's output after interacting with Alice and Bob for some fixed number of rounds determines their pay-offs.

**Definition 13.** An *n-turn referee* is an $n$-turn measuring co-strategy $\{R_a : a \in \Sigma\}$ whose input spaces $\mathcal{X}_1, \ldots, \mathcal{X}_n$ and output spaces $\mathcal{Y}_1, \ldots, \mathcal{Y}_n$ take the form

$$\mathcal{X}_k = \mathcal{A}_k \otimes \mathcal{B}_k \qquad \text{and} \qquad \mathcal{Y}_k = \mathcal{C}_k \otimes \mathcal{D}_k$$

for complex Euclidean spaces $\mathcal{A}_k$, $\mathcal{B}_k$, $\mathcal{C}_k$ and $\mathcal{D}_k$, for $1 \leq k \leq n$. An *n-turn quantum refereed game* consists of an $n$-turn referee along with functions

$$V_A, V_B : \Sigma \to \mathbb{R}$$

defined on the referee's set of measurement outcomes, representing Alice's payoff and Bob's pay-off for each output $a \in \Sigma$. Such a game is a *zero-sum* quantum refereed game if $V_A(a) + V_B(a) = 0$ for all $a \in \Sigma$.

The referee's actions in a quantum refereed game are completely determined by its representation $\{R_a : a \in \Sigma\}$. During each turn, the referee simultaneously sends a message to Alice and a message Bob, and a response is expected from each player. The spaces $\mathcal{A}_k$ and $\mathcal{B}_k$ correspond to the messages sent by the referee during turn number $k$, while $\mathcal{C}_k$ and $\mathcal{D}_k$ correspond to their responses. After $n$ turns, the referee produces an output $a \in \Sigma$.

A refereed quantum game does not in itself place any restrictions on the strategies available to Alice and Bob. For example, Alice and Bob might utilize a strategy that allows quantum communication, they might share entanglement but be forbidden from communicating, or might even be forbidden to share entanglement. Specific characteristics of a given game, such as its Nash equilibria, obviously depend on such restrictions in general.

The focus of the remainder of the paper is on the comparatively simple setting of zero-sum quantum refereed games. In this case, we assume that Alice and Bob do not communicate or share entanglement before the interaction takes place. More precisely, we assume that Alice and Bob play independent strategies represented by $A \in \mathcal{S}_n(\mathcal{A}_{1\ldots n}, \mathcal{C}_{1\ldots n})$ and $B \in \mathcal{S}_n(\mathcal{B}_{1\ldots n}, \mathcal{D}_{1\ldots n})$, respectively. The combined actions of Alice and Bob are therefore together described by the operator $A \otimes B \in \mathcal{S}_n(\mathcal{X}_{1\ldots n}, \mathcal{Y}_{1\ldots n})$.

It is a completely natural assumption that Alice and Bob play independent strategies in a zero-sum quantum refereed game, given that it cannot simultaneously be to both players' advantage to communicate directly with one another or to initially share an entangled state. This should not be confused with the possibility that entanglement among the players and referee might exist at various points in the game, or that the referee might choose to pass information from one player to the other. These possibilities are not disallowed when Alice and Bob's joint strategy is represented by $A \otimes B$.

Now, assume that a zero-sum quantum refereed game is given, and that Alice and Bob play independent strategies $A$ and $B$ as just discussed. Let us write

$$V(a) = V_A(a) = -V_B(a),$$

and define

$$R = \sum_{a \in \Sigma} V(a) R_a.$$

Alice's expected pay-off is then given by

$$\sum_{a \in \Sigma} V(a) \left\langle A \otimes B, R_a \right\rangle = \left\langle A \otimes B, R \right\rangle,$$

while Bob's expected pay-off is $-\left\langle A \otimes B, R \right\rangle$.

Now, $\left\langle A \otimes B, R \right\rangle$ is a real-valued bilinear function in $A$ and $B$. Because the operators $A$ and $B$ are drawn from compact, convex sets $\mathcal{S}_n(\mathcal{A}_{1\ldots n}, \mathcal{C}_{1\ldots n})$ and $\mathcal{S}_n(\mathcal{B}_{1\ldots n}, \mathcal{D}_{1\ldots n})$ respectively, we have that

$$\max_{A \in \mathcal{S}_n(\mathcal{A}_{1\ldots n}, \mathcal{C}_{1\ldots n})} \min_{B \in \mathcal{S}_n(\mathcal{B}_{1\ldots n}, \mathcal{D}_{1\ldots n})} \left\langle A \otimes B, R \right\rangle = \min_{B \in \mathcal{S}_n(\mathcal{B}_{1\ldots n}, \mathcal{D}_{1\ldots n})} \max_{A \in \mathcal{S}_n(\mathcal{A}_{1\ldots n}, \mathcal{C}_{1\ldots n})} \left\langle A \otimes B, R \right\rangle.$$

This is the Min-Max Theorem for zero-sum quantum games.

Note that the above expression does not immediately follow from von Neumann's original Min-Max Theorem, but follows from an early generalization due to J. Ville [33] and several subsequent generalizations such as the well-known Min-Max Theorem of Ky Fan [11]. The real number represented by the two sides of this equation is called the *value* of the given game.

**Quantum interactive proofs with competing provers**

Classical interactive proof systems with competing provers have been studied by several authors, including Feige, Shamir, and Tennenholts [14], Feige and Shamir [13], Feigenbaum, Koller, and Shor [15], and Feige and Kilian [12]. A quantum variant of this model is defined by allowing the verifier to exchange quantum information with the provers [19, 18]. In both cases these interactive proof systems are generalizations of single prover interactive proof systems [3, 4, 16, 24, 34].

Interactive proof systems with two competing provers are naturally modeled by zero-sum refereed games. To highlight this connection we will refer to the verifier as the referee and the two provers as Alice and Bob. The referee is assumed to be computationally bounded while Alice and Bob are computationally unrestricted. Alice, Bob, and the referee receive a common input string $x \in \{0,1\}^*$, and an interaction follows. After the interaction takes place, the referee decides that either Alice wins or Bob wins.

A language or promise problem $L = (L_{\text{yes}}, L_{\text{no}})$ is said to have a classical refereed game if there exists a referee, described by a polynomial-time randomized computation, such that: (i) for every input $x \in L_{\text{yes}}$, there is a strategy for Alice that wins with probability at least $3/4$ against every strategy of Bob, and (ii) for every input $x \in L_{\text{no}}$, there is a strategy for Bob that wins with probability at least $3/4$ against every strategy of Alice.

The class of promise problems having classical refereed games is denoted RG. It is known that RG is equal to EXP. The work of Koller and Megiddo [25] implies RG $\subseteq$ EXP, while Feige and Kilian [12] proved the reverse containment.

Let us note that zero-sum classical refereed games, and therefore the class RG, are unaffected by the assumption that Alice and Bob may play quantum strategies, assuming the referee remains

classical. This assumes of course that the classical referee is modeled properly within the setting of quantum information, which requires that any quantum information that it touches immediately loses coherence. Equivalently, the referee effectively measures all messages sent to it by Alice and Bob with respect to the standard basis before any further processing takes place. As there also cannot be a mutual advantage to Alice and Bob to correlate their strategies using shared entanglement, there is no advantage to Alice or Bob to play a quantum strategy against a classical referee. This is not the case in the cooperative setting, because there Alice and Bob might use a shared entangled state to their advantage [8].

Quantum interactive proof systems with competing provers are defined in a similar way to the classical case, except that the referee's actions are described by polynomial-time generated quantum circuits and the referee may exchange quantum information with Alice and Bob. The complexity class of all promise problems having quantum refereed games is denoted QRG. The containment EXP $\subseteq$ QRG follows from EXP $\subseteq$ RG. It was previously known that QRG $\subseteq$ NEXP $\cap$ co-NEXP [18], and we will improve this to QRG $\subseteq$ EXP. This establishes the characterization QRG $=$ EXP, and implies that quantum and classical refereed games are equivalent with respect to their expressive power.

In the refereed game associated with a competing prover quantum interactive proof system, the referee declares either Alice or Bob to be the winner. Specifically, the referee outputs one of two possible values $\{a, b\}$, with $a$ meaning that Alice wins and $b$ meaning that Bob wins. By setting $V(a) = 1$ and $V(b) = 0$, we obtain a quantum refereed game whose value is the maximum probability with which Alice can win. We will show that this optimal winning probability for Alice can be efficiently approximated: it is the value of a semidefinite programming problem whose size is polynomial in the total dimension of the input and output spaces of the referee. It follows from the polynomial-time solvability of semidefinite programming problems [21, 17, 29] that QRG $\subseteq$ EXP.

We will use similar notation to the previous subsection: for a fixed input $x$, the referee is represented by operators $\{R_a, R_b\}$, and assuming $n$ is the number of turns for this referee we let the input and output spaces to Alice be denoted by $\mathcal{A}_1, \mathcal{C}_1, \ldots, \mathcal{A}_n, \mathcal{C}_n$ while $\mathcal{B}_1, \mathcal{D}_1, \ldots, \mathcal{B}_n, \mathcal{D}_n$ denote the input and output spaces to Bob. The assumption that the referee is described by polynomial-time generated quantum circuits implies that the entries in the matrix representations of $R_a$ and $R_b$ with respect to the standard basis can be approximated to very high precision in exponential time.

Now, given any strategy $A \in \mathcal{S}_n(\mathcal{A}_{1\ldots n}, \mathcal{C}_{1\ldots n})$ for Alice, let us define

$$\Omega_a(A) = \mathrm{Tr}_{\mathcal{C}_{1\ldots n} \otimes \mathcal{A}_{1\ldots n}} \left( (A \otimes I_{\mathcal{D}_{1\ldots n} \otimes \mathcal{B}_{1\ldots n}}) R_a \right),$$
$$\Omega_b(A) = \mathrm{Tr}_{\mathcal{C}_{1\ldots n} \otimes \mathcal{A}_{1\ldots n}} \left( (A \otimes I_{\mathcal{D}_{1\ldots n} \otimes \mathcal{B}_{1\ldots n}}) R_b \right).$$

The functions $\Omega_a$ and $\Omega_b$ are linear and extend to uniquely defined super-operators. Under the assumption that Alice plays the strategy represented by $A \in \mathcal{S}_n(\mathcal{A}_{1\ldots n}, \mathcal{C}_{1\ldots n})$ and Bob plays the strategy represented by $B \in \mathcal{S}_n(\mathcal{B}_{1\ldots n}, \mathcal{D}_{1\ldots n})$, we have that the referee outputs $a$ with probability $\langle A \otimes B, R_a \rangle = \langle B, \Omega_a(A) \rangle$ and outputs $b$ with probability $\langle A \otimes B, R_b \rangle = \langle B, \Omega_b(A) \rangle$. One may think of $\{\Omega_a(A), \Omega_b(A)\}$ as being the co-strategy that results from "hard-wiring" Alice's strategy represented by $A$ into the referee.

Now, Alice's goal is to minimize the maximum probability with which Bob can win. For a given strategy $A$ for Alice, the maximum probability with which Bob can win is

$$\max \left\{ \langle B, \Omega_b(A) \rangle \,:\, B \in \mathcal{S}_n(\mathcal{B}_{1\ldots n}, \mathcal{D}_{1\ldots n}) \right\}$$

which, by Theorem 9, is given by

$$\min\left\{p \geq 0 : \Omega_b(A) \leq p\, Q,\ Q \in \text{co-}\mathcal{S}_n(\mathcal{B}_{1\ldots n}, \mathcal{D}_{1\ldots n})\right\}.$$

The following optimization problem therefore determines the maximum probability $p$ for Bob to win, minimized over all strategies for Alice:

$$\begin{array}{ll} \text{Minimize:} & p \\ \text{Subject to:} & \Omega_b(A) \leq p\, Q, \\ & A \in \mathcal{S}_n(\mathcal{A}_{1\ldots n}, \mathcal{C}_{1\ldots n}), \\ & Q \in \text{co-}\mathcal{S}_n(\mathcal{B}_{1\ldots n}, \mathcal{D}_{1\ldots n}). \end{array}$$

This optimization problem can be expressed in terms of linear and semidefinite constraints as follows:

$$\begin{array}{lll} \text{Minimize:} & \text{Tr}(P_1) & \\ \text{Subject to:} & \Omega_b(A_n) \leq Q_n, & \\ & \text{Tr}_{\mathcal{C}_k}(A_k) = A_{k-1} \otimes I_{\mathcal{A}_k} & (2 \leq k \leq n), \\ & \text{Tr}_{\mathcal{C}_1}(A_1) = I_{\mathcal{A}_1}, & \\ & Q_k = P_k \otimes I_{\mathcal{D}_k} & (1 \leq k \leq n), \\ & \text{Tr}_{\mathcal{B}_k}(P_k) = Q_{k-1} & (2 \leq k \leq n), \\ & A_k \in \text{Pos}\left(\mathcal{C}_{1\ldots k} \otimes \mathcal{A}_{1\ldots k}\right) & (1 \leq k \leq n), \\ & Q_k \in \text{Pos}\left(\mathcal{D}_{1\ldots k} \otimes \mathcal{B}_{1\ldots k}\right) & (1 \leq k \leq n), \\ & P_k \in \text{Pos}\left(\mathcal{D}_{1\ldots k-1} \otimes \mathcal{B}_{1\ldots k}\right) & (1 \leq k \leq n). \end{array}$$


### Acknowledgements

This research was supported by Canada's NSERC and the Canadian Institute for Advanced Research (CIAR).


## References


[1] AMBAINIS, A. A new protocol and lower bounds for quantum coin flipping. In *Proceedings of the Thirty-Third Annual ACM Symposium on Theory of Computing* (2001), pp. 134–142.

[2] AMBAINIS, A., BUHRMAN, H., DODIS, Y., AND RÖHRIG, H. Multiparty quantum coin flipping. In *Proceedings of the 19th Annual IEEE Conference on Computational Complexity* (2004), pp. 250–259.

[3] BABAI, L. Trading group theory for randomness. In *Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing* (1985), pp. 421–429.

[4] BABAI, L., AND MORAN, S. Arthur-Merlin games: a randomized proof system, and a hierarchy of complexity classes. *Journal of Computer and System Sciences 36*, 2 (1988), 254–276.

[5] BENJAMIN, S., AND HAYDEN, P. Comment on "Quantum games and quantum strategies". *Physical Review Letters 87*, 6 (2001), article 069801.

[6] BRASSARD, G., BROADBENT, A., AND TAPP, A. Quantum pseudo-telepathy. *Foundations of Physics 35*, 11 (2005), 1877–1907.

[7] CHOI, M.-D. Completely positive linear maps on complex matrices. *Linear Algebra and Its Applications 10*, 3 (1975), 285–290.

[8] CLEVE, R., HØYER, P., TONER, B., AND WATROUS, J. Consequences and limits of nonlocal strategies. In *Proceedings of the 19th Annual IEEE Conference on Computational Complexity* (2004), pp. 236–249.

[9] EISERT, J., WILKENS, M., AND LEWENSTEIN, M. Quantum games and quantum strategies. *Physical Review Letters 83*, 15 (1999), 3077–3080.

[10] ENK, S. V., AND PIKE, R. Classical rules in quantum games. *Physical Review A 66* (2002), article 024306.

[11] FAN, K. Minimax theorems. *Proceedings of the National Academy of Sciences 39* (1953), 42–47.

[12] FEIGE, U., AND KILIAN, J. Making games short. In *Proceedings of the Twenty-Ninth annual ACM Symposium on Theory of Computing* (1997), pp. 506–516.

[13] FEIGE, U., AND SHAMIR, A. Multi-oracle interactive protocols with constant space verifiers. *Journal of Computer and System Sciences 44* (1992), 259–271.

[14] FEIGE, U., SHAMIR, A., AND TENNENHOLTZ, M. The noisy oracle problem. In *Advances in Cryptology – Proceedings of Crypto'88* (1990), vol. 403 of *Lecture Notes in Computer Science*, Springer–Verlag, pp. 284–296.

[15] FEIGENBAUM, J., KOLLER, D., AND SHOR, P. A game-theoretic classification of interactive complexity classes. In *Proceedings of the 10th Conference on Structure in Complexity Theory* (1995), pp. 227–237.

[16] GOLDWASSER, S., MICALI, S., AND RACKOFF, C. The knowledge complexity of interactive proof systems. *SIAM Journal on Computing 18*, 1 (1989), 186–208.

[17] GRÖTSCHEL, M., LOVÁSZ, L., AND SCHRIJVER, A. *Geometric Algorithms and Combinatorial Optimization*. Springer–Verlag, 1988.

[18] GUTOSKI, G. Upper bounds for quantum interactive proofs with competing provers. In *Proceedings of the 20th Annual IEEE Conference on Computational Complexity* (2005), pp. 334–343.

[19] GUTOSKI, G., AND WATROUS, J. Quantum interactive proofs with competing provers. In *Proceedings of the 22nd Symposium on Theoretical Aspects of Computer Science* (2005), vol. 3404 of *Lecture Notes in Computer Science*, Springer, pp. 605–616.

[20] JAMIOŁKOWSKI, A. Linear transformations which preserve trace and positive semidefiniteness of operators. *Reports on Mathematical Physics 3*, 4 (1972), 275–278.

[21] KHACHIYAN, L. A polynomial time algorithm in linear programming. *Soviet Mathematics Doklady 20* (1979), 191–194.

[22] KITAEV, A. Quantum coin-flipping. Presentation at the 6th Workshop on *Quantum Information Processing* (QIP 2003), 2002.

[23] KITAEV, A., SHEN, A., AND VYALYI, M. *Classical and Quantum Computation*, vol. 47 of *Graduate Studies in Mathematics*. American Mathematical Society, 2002.

[24] KITAEV, A., AND WATROUS, J. Parallelization, amplification, and exponential time simulation of quantum interactive proof system. In *Proceedings of the 32nd ACM Symposium on Theory of Computing* (2000), pp. 608–617.

[25] KOLLER, D., AND MEGIDDO, N. The complexity of two-person zero-sum games in extensive form. *Games and Economic Behavior 4* (1992), 528–552.

[26] LEE, C.-F., AND JOHNSON, N. Efficiency and formalism of quantum games. *Physical Review A 67* (2003), article 022311.

[27] MEYER, D. Quantum strategies. *Physical Review Letters 82*, 5 (1999), 1052–1055.

[28] MOCHON, C. Quantum weak coin-flipping with bias of 0.192. In *45th Annual IEEE Symposium on Foundations of Computer Science* (2004), pp. 2–11.

[29] NESTEROV, Y., AND NEMIROVSKI, A. Interior point polynomial algorithms in convex programming. *SIAM Studies in Applied Mathematics 13* (1994).

[30] NIELSEN, M. A., AND CHUANG, I. L. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[31] ROCKAFELLAR, R. T. *Convex Analysis*. Princeton University Press, 1970.

[32] RÖHRIG, H. *Quantum Query Complexity and Distributed Computing*. PhD thesis, Centrum voor Wiskunde en Informatica, 2004.

[33] VILLE, J. Sur la théorie générale des jeux oú intervient l'habileté des joueurs. *Traité du calcul des probabilités et des applications IV*, 2 (1938), 105–113.

[34] WATROUS, J. PSPACE has constant-round quantum interactive proof systems. *Theoretical Computer Science 292*, 3 (2003), 575–588.