A BOUND ON THE QUANTUM VALUE OF ALL COMPILED NONLOCAL GAMES

A. KULPE, G. MALAVOLTA, C. PADDOCK, S. SCHMIDT, AND M. WALTER

Abstract. A compiler introduced by Kalai et al. (STOC'23) converts any nonlocal game into an interactive protocol with a single computationally-bounded prover. Although the compiler is known to be sound in the case of classical provers, as well as complete in the quantum case, quantum soundness has so far only been established for special classes of games.

In this work, we establish a quantum soundness result for all compiled two-player nonlocal games. In particular, we prove that the quantum commuting operator value of the underlying nonlocal game is an upper bound on the quantum value of the compiled game. Our result employs techniques from operator algebras in a computational and cryptographic setting to establish information-theoretic objects in the asymptotic limit of the security parameter. It further relies on a sequential characterization of quantum commuting operator correlations which may be of independent interest.

1. Introduction

A nonlocal game consists of two (or more) non-communicating players interacting with a referee. In the game, the referee samples a question for each player, to which each player replies with an answer. The referee decides if the players win or lose based on the tuple of questions and answers. Since communication is not permitted between players, each player has no information about the questions given to the other players, nor do they know the answers provided to the referee by the other players. Nevertheless, the description of the game is known to the players ahead of time, allowing them to strategize and maximize their probability of winning the game. The *classical value* $\omega_c(\mathcal{G})$ of a nonlocal game $\mathcal{G}$ is the maximum winning probability of players with classical resources (such as shared randomness). On the other hand, the *quantum value* $\omega_q(\mathcal{G})$ represents the maximum winning probability of quantum players sharing a finite amount of quantum resources (such as entangled quantum states, like EPR pairs). In the quantum setting, the no-communication assumption can either be modeled by (i) spatially separating the player so that they act on tensor product subsystems or (ii) requiring that the players' actions commute on the joint system. While these two conditions are equivalent when the state space is finite dimensional, they are not when one allows infinite-dimensional systems. This motivates the study of the *(quantum) commuting operator value* $\omega_{qc}(\mathcal{G})$, which denotes the maximum winning probability over strategies where the measurement operators of the players commute.

Nonlocal games can be viewed as variants of Bell scenarios [Bel64] and been successful in advancing our understanding of entanglement. In particular, have been a productive framework for separating various sets of correlations arising from various physical models. Notably, they have been used to discern the sets of classical and quantum correlations $C_c \subsetneq C_q$ [CHSH69], the sets of quantum correlations and their closure (the quantum approximable correlations) $C_q \subsetneq C_{qa}$ [Slo17], and the sets of quantum approximable and commuting operator correlations $C_{qa} \subsetneq C_{qc}$ [JNV+21]. Along the way, nonlocal games became an important topic in complexity theory, through their connection to multiprover interactive proofs [CHTW04]. More recently, nonlocal games have enabled new protocols to certify quantum computation in the two-prover setting [RUV13, CGJV19, Gri19, JNV+21]. A fundamental question in this area is whether two non-communicating provers are really necessary to build such protocols. The single-prover setting, where a verifier interacts with a single computationally-bounded prover, is both theoretically appealing and practically motivated since the non-communication assumption can be difficult to enforce.

Motivated by this issue, Kalai, Lombardi, Vaikuntanathan, and Yang (KLVY) proposed a generic procedure to transform any nonlocal game into a single-prover protocol, replacing the no-communication assumption between players with a computational assumption on the prover [KLVY23]. For instance, the KLVY compiler translates a two-player game into a four-round game with a single player (prover) and a referee (verifier). Questions are asked and answered sequentially, rather than in parallel, and the leaking of information to the next round is prevented by cryptographic assumptions as signaling in the other direction is prevented by the temporal order of the game. To achieve the desired functionality the construction employs a quantum homomorphic encryption scheme with classical messages [Mah18, Bra18]. This results in a quantum polynomial time (QPT) assumption on the prover, as any prover with greater computational resources could break the security of the QHE scheme, and leak information about the encrypted questions.

In addition to outlining the compilation procedure, Kalai et al. established *classical soundness* and *quantum completeness* of the compiler, meaning that while classical provers cannot exceed the classical value of the corresponding nonlocal game, quantum provers can achieve the quantum value, in the asymptotic limit where the security parameter λ of the underlying quantum homomorphic encryption scheme tends to infinity. In particular this implies that any nonlocal game with $\omega_c < \omega_q$ can be converted into a protocol that classically verifies quantum advantage.

In this work we consider the problem of establishing soundness of the compiler in the quantum setting. Quantum soundness means that the quantum value of the compiled game is suitably bounded above by a quantum value for the original game. A series of subsequent works established upper bounds on the quantum compiled value for the CHSH game [NZ23], the class of XOR games [CMM+24, BVB+24], tilted-CHSH scenarios [MPW24], and for self-tests on Pauli measurements on maximally entangled states [MNZ24]. This enables an alternative and conceptual attractie way to perform verification of BQP and QMA computations with a classical verifier. Despite this progress, a general bound on the quantum value that applies to *all* compiled nonlocal games remained elusive.

1.1. **Main result and techniques.** In this work, we show that the quantum value of any compiled two-player nonlocal game is bounded by the quantum commuting operator value of the underlying nonlocal game.

Theorem (Informal)**.** *For large enough security parameter, no quantum polynomial time prover can win the compiled game with probability exceeding the quantum commuting operator value of the game by any constant.*

In other words, we show that for any nonlocal game $\mathcal{G}$,

$$\omega_{q,\max}(\mathcal{G}_{\text{comp}}) \leq \omega_{qc}(\mathcal{G}),$$

where $\omega_{q,\max}(\mathcal{G}_{\text{comp}})$ denotes the supremum of the winning probability of any quantum polynomial time prover against the compiled game $\mathcal{G}_{\text{comp}}$, in the limit that the security parameter tends to infinity. The definition of $\mathcal{G}_{\text{comp}}$ is given in Definition 4.2 whereas $\omega_{q,\max}(\mathcal{G}_{\text{comp}})$ is defined in Definition 4.4. The formal results are given in Theorem 6.1 and Corollary 6.2. Our theorem establishes quantum commuting operator soundness for all compiled two-player nonlocal games.

Our main result relies on two key ideas. First, we present a new characterization of quantum commuting operator correlations in terms of strategies for a *sequential* game, which serves as an idealization of the compiled game. We show that quantum sequential strategies that satisfy a certain *strong non-signaling property* give rise to quantum commuting operator correlations. We believe this alternative characterization of commuting operator correlations may be of independent interest.

Our second idea concerns the observation that the strong non-signaling property required in the idealized sequential game to obtain commuting operator correlations is obtained only in the limit of the security parameter tending to infinity. To make sense of compiled quantum strategies with respect to this limit we incorporate mathematical tools from operator algebras. Specifically we show that the essential part of the prover's strategies can be captured by states on a *universal C^*-algebra* and use a compactness argument to prove the existence of a limiting state. The limiting state can be then shown to precisely satisfy the aforementioned non-signaling like property, even though for every finite level of the security parameter it only holds for efficient observables. This approach is reminiscent of proofs of completeness for noncommutative optimization hierarchies such as the NPA hierarchy [NPA08].

1.2. **Comparison with prior work.** It is instructive to compare our result with prior works that established quantum soundness in special cases. As mentioned earlier, [NZ23] showed that the compiled value of the CHSH game was bounded by the quantum value. This result was extended to all XOR nonlocal games in [CMM+24, BVB+24]. The fact that these results appear to give tighter bounds on the compiled value by the quantum value ω_q rather than the commuting operator value ω_{qc}, but in fact both values coincide for the XOR case by a result of Tsirelson [Tsi87]. This coincidence is also apparent in the SOS proof techniques in [NZ23, CMM+24, BVB+24], which naturally relate to the commuting operator value rather than the quantum one. Nonlocal games with a sequential (temporal) separation rather than a spatial one have also been investigated in the XOR case [CFE+24].

1.3. **Organization of the paper.** The remainder of the paper is organized as follows: Section 2 covers preliminary material. Section 3 provides an overview of nonlocal games, correlations, and the various values of those games in the spatially separated setting. Section 4 details the KLVY compiler and the description of a compiled nonlocal game, including a discussion of the value of a compiled nonlocal game, and proves a key technical result. Section 5 establishes our equivalent characterization of commuting operator correlations (as well as of classical and quantum correlations) in terms of strategies for a sequential game that satisfy a strong non-signaling property. Section 6 proves of our main result, establishing the upper bound on the quantum value of a compiled nonlocal game.

2. Preliminaries

In this section, we recap some preliminaries from mathematics and computer science as well as fix our notation and conventions.

2.1. **Vectors, operators, quantum mechanics.**

Let $\mathcal{H}$ be a (possibly infinite-dimensional) Hilbert space. Elements of $\mathcal{H}$ are denoted by $|v\rangle \in \mathcal{H}$. The inner product $\langle\cdot|\cdot\rangle$ is linear in the second argument and induces the norm $\|v\| = \sqrt{\langle v|v\rangle}$. We denote by $\mathcal{B}(\mathcal{H})$ be the set of *bounded (linear) operators* on $\mathcal{H}$. We let $\mathbb{1}$ denote the identity operator, and denote the *adjoint* of an operator $A \in \mathcal{B}(\mathcal{H})$ by A^*. The norm on $\mathcal{B}(\mathcal{H})$ is the *operator norm* $\|A\| = \sup_{\|v\|=1}\|Av\|$. For $A, B \in \mathcal{B}(\mathcal{H})$ the *commutator* is denoted $[A, B] = AB - BA$. The *commutant* of a subset $\mathcal{S} \subseteq \mathcal{B}(\mathcal{H})$ is the set $\mathcal{S}' = \{B \in \mathcal{B}(\mathcal{H}) : [B, A] = 0, \text{ for all } A \in \mathcal{S}\}$.

In quantum mechanics, physical systems are often identified with Hilbert spaces $\mathcal{H}$, and the states of the system are identified with positive semidefinite operators ρ with unit trace, called *density operators*. A state is called *pure* if the density operator has rank one, and otherwise it is called *mixed*. Any unit vector $|v\rangle \in \mathcal{H}$ determines a pure state by the formula $\rho = |v\rangle\langle v|$, and conversely any pure state can be written in this way, hence the two concepts are often identified. The *trace distance* is the statistical distance between the distributions associated with two density operators ρ and σ is given by the formula $\frac{1}{2}\|\rho-\sigma\|_1 = \frac{1}{2}\operatorname{tr}(|\rho-\sigma|)$, where $\|\cdot\|_1$ is the Schatten-1 norm and the absolute value of an operator is defined by $|A| := \sqrt{A^*A}$. A *measurement* with a finite outcome set $\mathcal{O}$ is described by a collection of bounded operators $\{A_a\}_{a\in\mathcal{O}}$ acting on $\mathcal{H}$ such that $\sum_{a\in\mathcal{O}} A_a^*A_a = \mathbb{1}$. If the system is in state ρ, then the probability of obtaining outcome a is given by $p(a) = \operatorname{tr}(A_a^*A_a\rho)$, after which the state of the system is described by $A_a\rho A_a^*/p(a)$. The probabilities of measurement outcomes only depend on the operators $M_a := A_a^*A_a$. A collection of operators $\{M_a\}_{a\in\mathcal{O}}$ such as these which satisfy $\sum_{a\in\mathcal{O}} M_a = \mathbb{1}$ is called a *POVM*, which is short for positive operator-valued measure, with outcomes in $\mathcal{O}$. Any POVM arises from a measurement. *Observables* are self-adjoint elements $B = B^* \in \mathcal{B}(H)$, and their *quantum expectation value* with respect to the state ρ is given by $\operatorname{tr}(\rho B)$. This can be related to the preceding if one takes $\mathcal{O}$ to be the set of eigenvalues of B (assuming it is finite) and A_a as the corresponding spectral projections. We will often discuss apparatuses with multiple measurement settings, labeled by some index set $\mathcal{I}$, but the same set of outcomes $\mathcal{O}$ for each setting. This will be denoted by $\{\{M_{ax}\}_{a\in\mathcal{O}} : x \in \mathcal{I}\}$, where $\{M_{xa}\}_{a\in\mathcal{O}}$ is be a POVM (or measurement) with outcomes in $\mathcal{O}$ for each $x \in \mathcal{I}$. We often abbreviate and write this as $\{M_{xa}\}_{a\in\mathcal{O},x\in\mathcal{I}}$ when clear from context.

2.2. **Algebras and representations.**

An algebra $\mathscr{A}$ over the complex number is called a $*$-*algebra* if it is equipped with an antilinear involution, which for an element $A \in \mathscr{A}$ will always be denoted by A^*, such that $(AB)^* = B^*A^*$ for all $A, B \in \mathscr{A}$. In this work, every algebra we consider is unital, meaning it contains an identity element $\mathbb{1}$. A C^*-*algebra* $\mathscr{A}$ is a $*$-algebra that is complete with respect to a submultiplicative norm $\|\cdot\|$ that satisfies the C^*-identity $\|A^*A\| = \|A\|^2$ for all $A \in \mathscr{A}$. Examples to keep in mind are $\mathcal{B}(\mathcal{H})$ and any $*$-subalgebra of it that is closed with respect to the operator norm, with the adjoint and operator norm as defined above. A more abstract example will be introduced in Section 6 and serve as a key ingredient to the proof of our main result. The commutant $\mathcal{S}'$ of any subset $\mathcal{S} = \mathcal{S}^* \subseteq \mathcal{B}(\mathcal{H})$ is always a C^*-algebra (it is even a von Neumann algebra). An element $A \in \mathscr{A}$ is called *positive*, denoted $A \geq 0$, if it can be written in the form $A = B^*B$ for some $B \in \mathscr{A}$. It is called a *contraction* if $\|A\| \leq 1$; when A is positive this can also be stated as $A \leq \mathbb{1}$. A *positive linear functional* on a C^*-algebra $\mathscr{A}$ is a linear functional $\phi\colon \mathscr{A} \to \mathbb{C}$ such that $\phi(A) \geq 0$ whenever $A \geq 0$. Positive linear functionals are always bounded: it holds that $\|\phi\| = \phi(\mathbb{1})$. Given positive linear functionals ϕ, ψ, we write $\phi \leq \psi$ to denote that $\phi(A) \leq \psi(A)$ for all $A \geq 0$. A *state* on a C^*-algebra $\mathscr{A}$ is a positive linear functional that is also *unital*, meaning that $\phi(\mathbb{1}) = 1$.

The formalism of C^*-algebras generalizes the usual formalism of quantum mechanics outlined above. For example, any density operator ρ acting on a Hilbert space $\mathcal{H}$ gives rise to a state $\phi(\cdot) = \mathrm{tr}(\cdot\rho)$ on the C^*-algebra $\mathscr{A} = \mathcal{B}(\mathcal{H})$. The other concepts of quantum mechanics generalize verbatim. For example, a measurement on $\mathscr{A}$ consists of elements $\{A_a\}_{a\in\mathcal{O}} \subseteq \mathscr{A}$ such that $\sum_a A_a^* A_a = \mathbb{1}$, and so forth. The *Gelfand-Naimark-Segal (GNS) construction* shows that, conversely, the abstract world of C^*-algebras can always be realized concretely on a Hilbert space. It asserts that for every C^*-algebra $\mathscr{A}$ and state $\phi\colon \mathscr{A} \to \mathbb{C}$, there exist a Hilbert space $\mathcal{H}_\phi$, a $*$-homomorphism $\pi_\phi\colon \mathscr{A} \to \mathcal{B}(\mathcal{H}_\phi)$, and a unit vector $|\nu_\phi\rangle \in \mathcal{H}_\phi$ such that

$$\phi(A) = \langle \nu_\phi | \pi_\phi(A) | \nu_\phi \rangle$$

for all $A \in \mathscr{A}$. Moreover, $|\nu_\phi\rangle$ is cyclic (meaning $\overline{\pi_\phi(\mathscr{A})|\nu_\phi\rangle} = \mathcal{H}$) and thereby uniquely determined. We call $(\mathcal{H}_\phi, \pi_\phi, |\nu_\phi\rangle)$ a *GNS triple* associated with ϕ. For more information on C^*-algebras, we refer the reader to [Bla06].

Finally, we recall a result that applies to any normed vector space, but which we will only use for C^*-algebras $\mathscr{A}$. The *Banach–Alaoglu theorem* asserts that the unit ball in the dual space, $\{\phi\colon \mathscr{A} \to \mathbb{C} : \|\phi\| \leq 1\}$, is compact in the weak-* topology. When $\mathscr{A}$ is separable, this unit ball is even sequentially compact in this topology, which concretely means the following: if $\{\phi_n\}_{n\in\mathbb{N}}$ is a sequence of functionals such that $\|\phi_n\| \leq 1$ for all $n \in \mathbb{N}$, then there exists a subsequence $\{\phi_{n_k}\}_{k\in\mathbb{N}}$ and a functional ϕ such that $\lim_{k\to\infty} \phi_{n_k}(A) = \phi(A)$ for all $A \in \mathscr{A}$.

2.3. **Classical and quantum computing.** A function $f\colon \mathbb{N} \to \mathbb{R}$ is called *negligible* if for every $k \in \mathbb{N}$ there exists a $n_0 \in \mathbb{N}$ such that for every $n \geq n_0$ it holds that $f(n) \leq n^{-k}$. The sum of two negligible functions is negligible. Unless stated otherwise, numbers are encoded as bitstrings using their binary representation. To encode a number in unary representation, we use the notation 1^n which refers to the bitstring of length n that only consists of ones. We use the notation $x \leftarrow \mu$ to denote that x is drawn from a probability distribution μ, and $x \leftarrow \mathcal{A}(y)$ to indicate that x is obtained by running an algorithm $\mathcal{A}$ with input y.

A *probabilistic polynomial-time (PPT) algorithm* can be described by a probabilistic Turing machine with a polynomial time bound, meaning that there exists a polynomial p such that for every input $x \in \{0,1\}^*$ the machine halts after at most $p(|x|)$ steps.

For quantum computations, we will use the quantum circuit model. Here, computations correspond to the application of *quantum circuits*, which are unitary operators that operate on the Hilbert space $\mathcal{H} = (\mathbb{C}^2)^{\otimes k}$ of some number k of qubits and are given by the composition of unitary gates that each act nontrivially only on (for definiteness) one or two qubits (taken from some fixed universal gate set). The size of a quantum circuit is the number of gates used in the computation (we assume all qubits are acted upon by at least one gate). The qubits are typically split into input qubits and auxiliary qubits, which are assumed to be initialized in the $|0\rangle$ state, unless stated otherwise. If a classical outcome is desired, a subset of the qubits is measured after the unitary circuit has been applied. A *quantum polynomial-time (QPT) algorithm* consists of family of quantum circuits $\{C_\lambda\}_{\lambda\in\mathbb{N}}$ and a deterministic polynomial-time Turing machine that on input 1^λ outputs a description of C_λ. We can often interpret λ as a problem size or as a security parameter.

Any PPT algorithm can be converted into a QPT algorithm (with C_λ a quantum circuit with λ input qubits that when given as input $|x\rangle$ and if a suitable number of qubits is measured, implements the same behavior as the PPT algorithm on any bitstring x of length $|x| = \lambda$).

3. Nonlocal games and strategies

In this section, we briefly review nonlocal games along with the definitions of classical, quantum, and (quantum) commuting operator strategies, correlations, and values for these games. We also review the definition of non-signaling correlations. Readers familiar with these concepts may proceed directly to Section 4.

3.1. **Nonlocal games.** In the following, let $\mathcal{I}_A, \mathcal{I}_B, \mathcal{O}_A$, and $\mathcal{O}_B$ be finite sets, $\mu\colon \mathcal{I}_A \times \mathcal{I}_B \to \mathbb{R}_{\geq 0}$ be a probability distribution, and $V\colon \mathcal{O}_A \times \mathcal{O}_B \times \mathcal{I}_A \times \mathcal{I}_B \to \{0,1\}$ be a function.

Definition 3.1. A *(two-player) nonlocal game* is a tuple $\mathcal{G} = (\mathcal{I}_A, \mathcal{I}_B, \mathcal{O}_A, \mathcal{O}_B, \mu, V)$ describing a scenario consisting of non-communicating players, Alice and Bob, interacting with a referee. In the game, the referee samples a pair of questions $(x, y) \in \mathcal{I}_A \times \mathcal{I}_B$ according to μ, sending question x to Alice and y to Bob. Then, Alice (resp. Bob) returns answers a (resp. b) to the referee, who computes the rule function V on the question-answer pairs (a, b, x, y) to determine if $V(a, b|x, y) = 1$ they win, or $V(a, b|x, y) = 0$ they lose.[1]

All the information about the game $\mathcal{G}$ is available to the player before the game. This allows them to decide on a strategy beforehand. However, once the game begins the players are not allowed to communicate. To the referee, the behavior of the players can be modeled by the probabilities $p(a, b|x, y)$ of answers a, b given questions x, y as determined by the strategy. The collection of numbers $\{p(a, b|x, y)\}_{a\in\mathcal{O}_A, b\in\mathcal{O}_B, x\in\mathcal{I}_A, y\in\mathcal{I}_B} \in \mathbb{R}^{\mathcal{O}_A\times\mathcal{O}_B\times\mathcal{I}_A\times\mathcal{I}_B}$ is called a *(bipartite) correlation*. Thus, the probability of winning the game $\mathcal{G}$ under a strategy S, with correlations p, is given by

$$\omega(\mathcal{G}, S) = \omega(\mathcal{G}, p) = \sum_{x\in\mathcal{I}_A, y\in\mathcal{I}_B} \sum_{a\in\mathcal{O}_A, b\in\mathcal{O}_B} \mu(x, y) V(a, b|x, y) p(a, b|x, y). \tag{3.1}$$

Observe that the winning probability of a strategy is simply a linear function of the corresponding correlation that it realizes.

Remark 3.2. Nonlocal games can also be viewed in the context of multiprover interactive proofs. Here one thinks of the players as provers and the referee as a verifier in an interactive protocol for a language. The winning probability of the game is the acceptance probability of the verifier.

[1]We use the notation $V(a, b|x, y)$ instead of $V(a, b, x, y)$ to emphasize that this represents the value of answers a, b given questions x, y.

3.2. **Strategies and correlations.** One of the main purposes of nonlocal games was to explore the effect of entangled non-communicating players in contrast to classical players (players with no entanglement). We start with the definition of the latter.

Definition 3.3. A *classical strategy* for a nonlocal game $\mathcal{G}$ consists of

(i) a probability distribution $\gamma\colon \Omega \to \mathbb{R}_{\geq 0}$ on a (without loss of generality) finite probability space Ω, along with
(ii) probability distributions $\{p_\omega(a|x) : x \in \mathcal{I}_A, \omega \in \Omega\}$ with outcomes in $\mathcal{O}_A$ and $\{q_\omega(b|y) : y \in \mathcal{I}_B, \omega \in \Omega\}$ with outcomes in $\mathcal{O}_B$.

A correlation $\{p(a,b|x,y)\}$ for which there is a classical strategy such that

$$p(a,b|x,y) = \sum_{\omega\in\Omega} \gamma(\omega)\, p_\omega(a|x)\, q_\omega(b|y),$$

for all $a \in \mathcal{O}_A, b \in \mathcal{O}_B, x \in \mathcal{I}_A, y \in \mathcal{I}_B$ is called a *classical correlation.* The set of classical correlations is denoted by $C_c(\mathcal{I}_A, \mathcal{I}_B, \mathcal{O}_A, \mathcal{O}_B)$ or simply as C_c when the sets $\mathcal{I}_A, \mathcal{I}_B, \mathcal{O}_A, \mathcal{O}_B$ are clear from context. It is easy to see that $C_c \subseteq \mathbb{R}^{\mathcal{O}_A\times\mathcal{O}_B\times\mathcal{I}_A\times\mathcal{I}_B}$ is a closed convex subset.

In quantum mechanics, spatially separated subsystems are often represented by the tensor product of Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$. The pure states of the joint system are the unit vectors $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$. Furthermore, if $\{X_a\}_{a\in\mathcal{O}_A}$ and $\{Y_b\}_{b\in\mathcal{O}_B}$ are POVMs on $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively, then $\{X_a \otimes Y_b\}_{(a,b)\in\mathcal{O}_A\times\mathcal{O}_B}$ describes the joint measurement, with outcomes in $\mathcal{O}_A \times \mathcal{O}_B$. With this in mind, we can imagine the players in a nonlocal game to be quantum players described in this way. The players start out sharing a joint quantum state and, as they are spatially separated and non-communicating once the game begins, any process by which they use the quantum resource in the game can be modelled by POVMs (which can depend on their given question) that the players employ to obtain their answers. If we assume that the players have finite-dimensional Hilbert spaces at their avail, we arrive at the following definition of a quantum strategy for a nonlocal game.

Definition 3.4. A *quantum strategy* for a nonlocal game $\mathcal{G}$ consists of

(i) Finite-dimensional Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$,
(ii) a (without loss of generality) pure quantum state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$, along with
(iii) POVMs $\{\{M_{xa} : a \in \mathcal{O}_A\} : x \in \mathcal{I}_A\}$ acting on $\mathcal{H}_A$ and POVMs $\{\{N_{yb} : b \in \mathcal{O}_B\} : y \in \mathcal{I}_B\}$ acting on $\mathcal{H}_B$.

A correlation $\{p(a,b|x,y)\}$ for which there exists a quantum strategy such that

$$p(a,b|x,y) = \langle\psi|M_{xa} \otimes N_{yb}|\psi\rangle$$

for all $a \in \mathcal{O}_A, b \in \mathcal{O}_B, x \in \mathcal{I}_A, y \in \mathcal{I}_B$ is called a *quantum correlation.* The set of quantum correlations is denoted by $C_q(\mathcal{I}_A, \mathcal{I}_B, \mathcal{O}_A, \mathcal{O}_B)$ or simply C_q.

Quantum strategies of particular interest are the *entangled strategies.* This is because if the state in the quantum strategy is *unentangled*, then the resulting correlation is always classical. It is easy to see that $C_c \subseteq C_q$, and the inclusion is in general strict, as follows from the existence of nontrivial Bell inequalities [CHSH69, Mer90, Per90].

The restriction to finite-dimensional quantum systems is not the only model. If one allows the Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ to be infinite-dimensional, one gets the set of *spatial* quantum correlations C_{qs}. Clearly, $C_q \subseteq C_{qs}$, and both sets are convex subsets $\mathbb{R}^{\mathcal{O}_A\times\mathcal{O}_B\times\mathcal{I}_A\times\mathcal{I}_B}$. It turns out that in general, the inclusion is strict [CS20] and neither set is closed [Slo17, DPP19, Col20, MR20, Bei21]. Moreover, both sets have the same closure, denoted by C_{qa} and named the set of *quantum approximable correlations*.

Another assumption that is not always warranted is the tensor product structure $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ of the joint Hilbert space. For instance, spatially separated quantum systems in quantum field theory need not correspond to a tensor product factorization, but are rather modelled mathematically by commuting subalgebras $\mathscr{A}, \mathscr{B} \subseteq \mathcal{B}(\mathcal{H})$ of observables on a single joint Hilbert space $\mathcal{H}$. This perspective gives rise to the following class of strategies.

Definition 3.5. A *(quantum) commuting operator strategy*[2] for a nonlocal game $\mathcal{G}$ consists of

(i) a Hilbert space $\mathcal{H}$,
(ii) a (without loss of generality) pure quantum state $|\psi\rangle \in \mathcal{H}$, along with
(iii) POVMs $\{\{M_{xa} : a \in \mathcal{O}_A\} : x \in \mathcal{I}_A\}$ and $\{\{N_{yb} : b \in \mathcal{O}_B\} : y \in \mathcal{I}_B\}$ acting on $\mathcal{H}$, such that $[M_{xa}, N_{yb}] = 0$ for all $a \in \mathcal{O}_A$, $b \in \mathcal{O}_B$, $x \in \mathcal{I}_A$, $y \in \mathcal{I}_B$.

A correlation $\{p(a, b|x, y)\}$ for which there exists a commuting operator strategy such that

$$p(a, b|x, y) = \langle\psi|M_{xa}N_{yb}|\psi\rangle$$

for all $a \in \mathcal{O}_A, b \in \mathcal{O}_B, x \in \mathcal{I}_A, y \in \mathcal{I}_B$ is called a *commuting operator correlation*. The set of *commuting operator correlations* is denoted by $C_{qc}(\mathcal{I}_A, \mathcal{I}_B, \mathcal{O}_A, \mathcal{O}_B)$ or C_{qc}.

The set of commuting operator correlations $C_{qc} \subseteq \mathbb{R}^{\mathcal{O}_A\times\mathcal{O}_B\times\mathcal{I}_A\times\mathcal{I}_B}$ is always a closed convex subset [Fri12]. Since every quantum strategy is a commuting operator strategy by properties of the tensor product, it follows that $C_{qa} \subseteq C_{qc}$. When the Hilbert space $\mathcal{H}$ is finite-dimensional then any commuting operator strategy can also be seen as an ordinary quantum strategy, but in general, this is not so. In fact there exist commuting operator correlations which have no realization as a quantum strategy, and hence $C_q \subsetneq C_{qc}$ [Slo16]. Whether the correlation sets C_{qa} and C_{qc} were the same became known as Tsirelson's Problem. This was recently resolved in the celebrated work $\mathsf{MIP}^* = \mathsf{RE}$ [JNV+21] by the construction of a correlation in C_{qc} with no realization in C_{qa}. In turn, this implied a negative resolution to Connes' Embedding Problem, following [Oza13, JNP+11].

Given that there are different models of physical correlations, it is interesting to ask for conditions that any correlation should satisfy so that it can reasonably be interpreted as a strategy of non-communicating players. One such condition is known as the *non-signaling* property: it asserts that the marginal distribution of either player's answers must be independent of the other player's question. Non-signaling is easily verified to hold for all correlations defined so far.

Definition 3.6. A correlation $p(a, b|x, y)$ is *non-signaling* if for all $x, x' \in \mathcal{I}_A$, $y \in \mathcal{I}_B$, and $b \in \mathcal{O}_B$, it holds that

$$\sum_{a\in\mathcal{O}_A} p(a, b|x, y) = \sum_{a\in\mathcal{O}_A} p(a, b|x', y)$$

[2]These are also called quantum commuting strategies in part of the literature.

and moreover for all $x \in \mathcal{I}_A$, $y, y' \in \mathcal{I}_B$, and $a \in \mathcal{O}_A$, it holds that

$$\sum_{b \in \mathcal{O}_B} p(a, b|x, y) = \sum_{b \in \mathcal{O}_B} p(a, b|x, y').$$

The set of *non-signaling correlations* is denoted by $C_{ns}(\mathcal{I}_A, \mathcal{I}_B, \mathcal{O}_A, \mathcal{O}_B)$ or C_{ns}.

To summarize, we have the following inclusion of convex sets, all of which are known to be strict in general:

$$C_c \subsetneq C_q \subsetneq C_{qs} \subsetneq C_{qa} \subsetneq C_{qc} \subsetneq C_{ns}$$

Moreover, $C_c, C_{qa}, C_{qc}, C_{ns}$ are all closed, while C_q and C_{qa} are in general not.

3.3. **Values of games.** One of the original motivations for studying nonlocal games was to understand when different types of strategies achieve different maximal winning probabilities, as this can provide separations between the various correlation sets. To this end, one defines the value of a game as the highest winning probability for a given class of strategies or, equivalently, correlations.

Definition 3.7. Given a nonlocal game $\mathcal{G}$ and $\star \in \{c, q, qc, ns\}$, we define

$$\omega_\star(\mathcal{G}) = \sup_{p \in C_\star} \omega(\mathcal{G}, p).$$

The quantity $\omega_c(\mathcal{G})$ is called the *classical value* of the game, $\omega_q(\mathcal{G})$ its *quantum value*, $\omega_{qc}(\mathcal{G})$ its *commuting operator value*, and $\omega_{ns}(\mathcal{G})$ its non-signaling value.

Clearly, the value only depends on the closure of the corresponding set of correlations. In particular, ω_q can equivalently be defined in terms of C_{qs} or C_{qa}. Given a nonlocal game $\mathcal{G}$ it is immediate that

$$\omega_c(\mathcal{G}) \leq \omega_q(\mathcal{G}) \leq \omega_{qc}(\mathcal{G}) \leq \omega_{ns}(\mathcal{G}).$$

However, there also exist games $\mathcal{G}$ for which each of these inequalities is strict. Indeed, the latter is equivalent to the statement that the closed convex sets $C_c \subsetneq C_{qa} \subsetneq C_{qc} \subsetneq C_{ns}$ are in general distinct, as discussed above.[3]

4. Compiled nonlocal games

In this section we will review the construction from [KLVY23] that allows compiling any multi-player nonlocal game into a single-prover interactive protocol, along with the required cryptography. We will then prove a technical result that will be key to our later analysis. It states that as the security parameter tends to infinity, the average state of the prover after the first round of protocol becomes independent of the first round's challenge (question) in a precise sense (Proposition 4.6).

4.1. **Quantum homomorphic encryption.** We now define the notion of a quantum homomorphic encryption scheme, which is the central component of the KLVY compiler. For the purposes of their construction, only classical messages need to be encrypted, and all ciphertexts should be classical. Moreover, one requires the capability to apply quantum circuits to homomorphically compute on such ciphertexts, and in addition to the classical input and output, these quantum circuits may also act on auxiliary input qubits (which are not encrypted).

[3]Veritably, the existence of certain nonlocal games $\mathcal{G}$ is how several of the strict inclusions $C_c \subsetneq C_{qa} \subsetneq C_{qc} \subsetneq C_{ns}$ were established.

Because in this work we do not discuss families of games and their interplay with the security parameter, we can assume that the set of allowed classical messages (which will later correspond to Alice's questions and answers) is a fixed finite set, independent of the security parameter. We will denote this message set by M and assume without loss of generality that it consists of bitstrings of some fixed length $\ell \in \mathbb{N}$. Similarly, we may assume that the set of allowed quantum circuits, which we denote by $\mathcal{C}$, is a fixed (but possibly infinite) set independent of the security parameter. Each circuit $C \in \mathcal{C}$ takes as input some number $\ell + a_C$ of input qubits, with the first ℓ qubits corresponding to the classical message (encoded in the computational basis) and the remaining a_C qubits serving as the auxiliary input mentioned above. In the following definition, we also denote by SK the set of classical secret keys and by CT the set of classical ciphertexts; both sets consist of bitstrings.

Definition 4.1. Given sets of classical messages M and of quantum circuits $\mathcal{C}$ as above, a *quantum homomorphic encryption scheme* is a tuple

$$\mathsf{QHE} = (\mathsf{Gen}, \mathsf{Enc}, \{\mathsf{Eval}^C\}_{C\in\mathcal{C}}, \mathsf{Dec})$$

consisting of algorithms with the following description:

- *Key generation:* $\mathsf{Gen}\colon \{1^\lambda\}_{\lambda\in\mathbb{N}} \to \mathsf{SK}$ is a QPT algorithm that takes as input the security parameter λ in unary, and returns a secret key.
- *Encryption:* $\mathsf{Enc}\colon \mathsf{SK} \times \mathsf{M} \to \mathsf{CT}$ is a QPT algorithm that takes as input a secret key and a message, and returns a ciphertext.
- *Homomorphic evaluation:* For every quantum circuit $C \in \mathcal{C}$, there is a QPT algorithm $\mathsf{Eval}^C\colon \mathsf{CT} \times (\mathbb{C}^2)^{\otimes a_C} \to \mathsf{CT}$ that takes as input a ciphertext and a quantum register on a_C qubits, and returns a ciphertext.
- *Decryption:* $\mathsf{Dec} : \mathsf{SK} \times \mathsf{CT} \to \mathsf{M}$ is a QPT algorithm that takes as input a secret key and a ciphertext, and returns a message.

We require that the following two properties hold:

- *Correctness with auxiliary input:* Recall that each circuit $C \in \mathcal{C}$ acts on a Hilbert space of the form $\mathcal{H}_M \otimes \mathcal{H}_A$, where $\mathcal{H}_M = (\mathbb{C}^2)^{\otimes \ell}$ and $\mathcal{H}_A = (\mathbb{C}^2)^{\otimes a_C}$. For every quantum circuit $C \in \mathcal{C}$, for every message $m \in \mathsf{M}$, for every Hilbert space $\mathcal{H}_B$, and for every quantum state $|\psi\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$, there should be a negligible function η of the security parameter such that the states returned by the following two games have trace distance at most $\eta(\lambda)$, for all λ:
  - Game 1: Apply $C_{MA} \otimes \mathbb{1}_B$ to $|m\rangle_M \otimes |\psi\rangle_{AB}$. Measure register M to obtain a bitstring m'. Return m' and register B.
  - Game 2: Sample a key $\mathsf{sk} \leftarrow \mathsf{Gen}(1^\lambda)$ and encrypt using $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{sk}, m)$. Apply $\mathsf{Eval}^C(\mathsf{ct}, \cdot) \otimes \mathbb{1}_B$ to $|\psi\rangle_{AB}$ to obtain a ciphertext ct'. Decrypt using $m' \leftarrow \mathsf{Dec}(\mathsf{sk}, \mathsf{ct}')$. Return m' and register B.
- *Security against quantum distinguishers:* For any QPT algorithm $\mathcal{A} = \{\mathcal{A}_\lambda\}$ and any two messages $m, m' \in \mathsf{M}$, there is a negligible function η such that

$$\left| \Pr\left[1 \leftarrow \mathcal{A}_\lambda(\mathsf{ct})^{\mathsf{Enc}(\mathsf{sk},\cdot)} \;\middle|\; \begin{array}{l} \mathsf{sk} \leftarrow \mathsf{Gen}(1^\lambda) \\ \mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{sk}, m) \end{array} \right] - \Pr\left[1 \leftarrow \mathcal{A}_\lambda(\mathsf{ct})^{\mathsf{Enc}(\mathsf{sk},\cdot)} \;\middle|\; \begin{array}{l} \mathsf{sk} \leftarrow \mathsf{Gen}(1^\lambda) \\ \mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{sk}, m') \end{array} \right] \right| \leq \eta(\lambda)$$

  for all λ.

It follows from [KLVY23, NZ23] that the quantum fully homomorphic encryption schemes of [Mah20, Bra18] can be used to define QHE schemes in the sense of the above definition (note that we require correctness only for a single $C \in \mathcal{C}$ at a time, as the security parameter tends to infinity).

We allow all subroutines to be QPT even if they only have classical input and output. This is not important for our result and only makes it stronger, since we prove a bound that applies to any such scheme. We also note that while the Eval^C algorithms and the correctness with auxiliary input property are required to describe the KLVY compiler and prove its correctness, they have no relevance to our result.

The security property demands that no adversary described by a QPT algorithm[4] can distinguish between the encryption of any two fixed messages, with non-negligible probability, even when given access to an encryption oracle. This in fact implies a (seemingly stronger) security property, called *parallel repeated IND-CPA security*, where the adversary can choose the two messages and also receives a polynomial number of ciphertexts [NZ23].

4.2. **The KLVY compiler.** We now describe the compiler of [KLVY23]. It takes as its input a nonlocal game (Definition 3.1) and a QHE scheme (Definition 4.1). We assume from here onwards that the question and answer sets of the game are encoded as bitstrings of some fixed length.

Definition 4.2 ([KLVY23])**.** Consider a nonlocal game $\mathcal{G} = (\mathcal{I}_A, \mathcal{I}_B, \mathcal{O}_A, \mathcal{O}_B, \mu, V)$ and a quantum homomorphic encryption scheme $\mathsf{QHE} = (\mathsf{Gen}, \mathsf{Enc}, \{\mathsf{Eval}^C\}_{C\in\mathcal{C}}, \mathsf{Dec})$ with message set $\mathsf{M} \supseteq \mathcal{I}_A \cup \mathcal{O}_A$. The corresponding *compiled nonlocal game* $\mathcal{G}_{\mathrm{comp}}$ describes an interactive protocol between a verifier and a prover exchanging classical messages. They get as input the security parameter, encoded in unary, and proceed as follows:

1. The verifier samples a question pair $(x, y) \leftarrow \mu$ and a secret key $\mathsf{sk} \leftarrow \mathsf{Gen}(1^\lambda)$. They encrypt Alice's question by $\xi \leftarrow \mathsf{Enc}(\mathsf{sk}, x)$ and send the classical ciphertext ξ to the prover.
2. The prover replies with some classical message α.
3. The verifier sends y unencrypted to prover.
4. The prover replies with another classical message b.
5. The verifier interprets α as a ciphertext and decrypts it as $a \leftarrow \mathsf{Dec}(\mathsf{sk}, \alpha)$. They accept if $a \in \mathcal{O}_A$, $b \in \mathcal{O}_B$, and $V(a, b|x, y) = 1$.

We only described the compiled version of a two-player nonlocal game, which is the focus of the present work, but the compiler generalizes straightforwardly to any game with k players (in which case $2k$ rounds of communication are required) [KLVY23].

In the compiled game, the verifier plays the role of the referee and the prover plays the role of both Alice and Bob. In analogy to the nonlocal game, we will denote by $\omega_\lambda(\mathcal{G}_{\mathrm{comp}}, S)$ the probability that the verifier accepts for a given value of the security parameter $\lambda \in \mathbb{N}$ when interacting with a prover described by a strategy $S = \{S_\lambda\}$, where S_λ denotes the strategy for fixed λ. Using (3.1), this can also be written as

$$\omega_\lambda(\mathcal{G}_{\mathrm{comp}}, S) = \omega(\mathcal{G}, p_\lambda) = \sum_{x\in\mathcal{I}_A, y\in\mathcal{I}_B} \sum_{a\in\mathcal{O}_A, b\in\mathcal{O}_B} \mu(x, y)V(a, b|x, y)p_\lambda(a, b|x, y), \tag{4.1}$$

[4] QPT algorithms as defined in Section 2 are a uniform notion. A stronger requirement is security against *non-uniform* QPT quantum adversaries, in which case one can also hope to get stronger conclusions. This is indeed the case and we return to this point in Remark 4.5 below.

where $p_\lambda(a,b|x,y)$ denotes the probability that the prover's first reply under S_λ decrypts to a and that their second reply is b, conditional on question pair (x,y).

Since a single prover plays the role of both Alice and Bob, this appears to be in stark contraction to the no-communication requirement of nonlocal games. The intuition that the compiled game can still be meaningful is as follows: because we use encryption for Alice's part but not for Bob's, the prover should not be able to usefully "correlate" the two messages, and might therefore be forced to act like a pair of non-communicating players. Because the security of the cryptographic scheme only applies to efficient adversaries, this can only be true if we similarly constrain the prover's computational power.

Just like in the case of the nonlocal games, there are different scenarios, depending on whether we consider classical or quantum provers. Here we focus on the quantum scenario, since [KLVY23] already proved that no classical efficient prover can exceed the classical value of the nonlocal game. The following definition describes the behavior of an efficient quantum prover in the compiled setting, analogously to Definition 3.4 in the nonlocal setting.

Definition 4.3. A *QPT strategy* $S = \{(V_\lambda, W_\lambda)\}_{\lambda\in\mathbb{N}}$ for a compiled game $\mathcal{G}_{\mathrm{comp}}$ consists of two QPT algorithms $\{V_\lambda\}_{\lambda\in\mathbb{N}}$ and $\{W_\lambda\}_{\lambda\in\mathbb{N}}$. It describes a quantum prover that behaves as follows:

1. When receiving the ciphertext $\xi \in \mathsf{CT}$, the prover applies V_λ to $|\xi\rangle$ along with a suitable number of $|0\rangle$ states. They then measure a suitable number of qubits and respond with the measurement outcome α.
2. When receiving the question $y \in \mathcal{I}_B$, the prover applies W_λ to $|y\rangle$ along with the post-measurement state of the preceding step. They again measure a suitable number of qubits and respond with the measurement outcome b.

This definition is perhaps more precise, but also more cumbersome to work with than the notation used in prior works, which instead described QPT strategies by families $\{(\mathcal{H}_\lambda, |\psi_\lambda\rangle, \{A^\lambda_{\xi\alpha}\}, \{B^\lambda_{yb}\})\}_{\lambda\in\mathbb{N}}$, consisting of

- Hilbert spaces $\mathcal{H}_\lambda$,
- states $|\psi_\lambda\rangle \in \mathcal{H}_\lambda$,
- measurement operators of the form $A^\lambda_{\xi\alpha} = U^\lambda_{\xi\alpha} P^\lambda_{\xi\alpha}$, where all $U^\lambda_{\xi\alpha}$ are unitaries on $\mathcal{H}_\lambda$ and $\{P^\lambda_{\xi\alpha}\}_{\alpha\in\mathsf{CT}}$ is a projective measurement for any $\xi \in \mathsf{CT}$,
- POVMs or projective measurements $\{B^\lambda_{yb}\}_{b\in\mathcal{O}_B}$ for each $y \in \mathcal{I}_B$,

subject to QPT assumptions that are less straightforward to state than above. The relation is immediate: we take $|\psi_\lambda\rangle$ to be the all-zeros states on a suitable multi-qubit Hilbert space $\mathcal{H}_\lambda$ (but it can be any state that can be prepared by a QPT algorithm), the projective measurements $P^\lambda_{\xi\alpha}$ correspond to the first part of Definition 4.3, the unitaries $U^\lambda_{\xi\alpha}$ can be taken as the identity,[5] and the operators B^λ_{yb} correspond to the second part of Definition 4.3, that is,

$$B^\lambda_{yb} = (\langle y| \otimes \mathbb{1}) W^*_\lambda (|b\rangle\langle b| \otimes \mathbb{1}) W_\lambda (|y\rangle \otimes \mathbb{1}). \tag{4.2}$$

We emphasize that unlike in the nonlocal case, there are *no* commutation conditions imposed on the operators $A^\lambda_{\xi\alpha}$ and B^λ_{yb}, nor is there any tensor product structure of

[5]This is without loss of generality: the unitaries $U^\lambda_{\xi\alpha}$ can always be absorbed into the second POVM, as $|\alpha\rangle$ is part of the post-measurement state and we can also keep a copy of $|\xi\rangle$ in it.

the Hilbert spaces $\mathcal{H}_\lambda$. Using this notation, the probabilities p_λ in (4.1) take the following form for a QPT strategy:

$$p_\lambda(a,b|x,y) = \mathop{\mathbb{E}}_{\mathsf{sk}\leftarrow\mathsf{Gen}(1^\lambda)} \mathop{\mathbb{E}}_{\xi\leftarrow\mathsf{Enc}(\mathsf{sk},x)} \sum_{\alpha\in\mathsf{CT}} \Pr(a\leftarrow\mathsf{Dec}(\mathsf{sk},\alpha))\,\langle\psi^\lambda|\,(A^\lambda_{\xi\alpha})^* B^\lambda_{yb} A^\lambda_{\xi\alpha}|\psi^\lambda\rangle$$

Introducing positive (semidefinite) operators

$$\sigma^\lambda_{xa} = \mathop{\mathbb{E}}_{\mathsf{sk}\leftarrow\mathsf{Gen}(1^\lambda)} \mathop{\mathbb{E}}_{\xi\leftarrow\mathsf{Enc}(\mathsf{sk},x)} \sum_{\alpha\in\mathsf{CT}} \Pr(a\leftarrow\mathsf{Dec}(\mathsf{sk},\alpha))\, A^\lambda_{\xi\alpha}|\psi^\lambda\rangle\langle\psi^\lambda|(A^\lambda_{\xi\alpha})^*, \tag{4.3}$$

the correlations can also be written as

$$p_\lambda(a,b|x,y) = \operatorname{tr}(\sigma^\lambda_{xa} B^\lambda_{yb}). \tag{4.4}$$

We note that $\operatorname{tr}(\sigma^\lambda_{xa})$ is the probability that the first part of the prover replies with a ciphertext that decrypts to $a \in \mathcal{O}_A$ when given an encryption of $x \in \mathcal{I}_A$, and $\sigma^\lambda_{xa}/\operatorname{tr}(\sigma^\lambda_{xa})$ is its post-measurement state in this case.

As in the nonlocal case, we can also define the value of a compiled game by taking the maximum (supremum) over all possible QPT strategies. Any quantum strategy $S = \{S_\lambda\}$ gives rise to a *sequence* of acceptance probabilities $\{\omega_\lambda(\mathcal{G}_{\mathrm{comp}}, S)\}$ as in Eq. (4.1). If we would like to define a single value then there are at least two natural definitions.

Definition 4.4. Then we associate to of a compiled game $\mathcal{G}$ the following *minimal and maximal quantum values*:

$$\omega_{q,\min}(\mathcal{G}_{\mathrm{comp}}) = \sup\left\{ \liminf_{\lambda\to\infty} \omega_\lambda(\mathcal{G}_{\mathrm{comp}}, S) \;\middle|\; S = \{S_\lambda\} \text{ a QPT strategy for } \mathcal{G}_{\mathrm{comp}} \right\},$$
$$\omega_{q,\max}(\mathcal{G}_{\mathrm{comp}}) = \sup\left\{ \limsup_{\lambda\to\infty} \omega_\lambda(\mathcal{G}_{\mathrm{comp}}, S) \;\middle|\; S = \{S_\lambda\} \text{ a QPT strategy for } \mathcal{G}_{\mathrm{comp}} \right\}.$$

Both quantities are meaningful. A bound of the form $\omega_{q,\min}(\mathcal{G}_{\mathrm{comp}}) \geq \theta$ shows that efficient quantum provers are able to *achieve* an acceptance probability arbitrarily close to θ, while $\omega_{q,\max}(\mathcal{G}_{\mathrm{comp}}, S) \leq \theta$ means that no quantum prover can *exceed* this acceptance probability by any constant, for large enough security parameter. Clearly, $\omega_{q,\min}(\mathcal{G}_{\mathrm{comp}}) \leq \omega_{q,\max}(\mathcal{G}_{\mathrm{comp}})$.

Any strategy for the nonlocal game can be converted into a prover for the compiled game by using the homomorphic evaluation functionality of the encryption (assuming it supports evaluating the necessary quantum circuits). Thus, for every quantum strategy S for the nonlocal game $\mathcal{G}$, there exists a QPT strategy $S_{\mathrm{comp}} = \{S^\lambda_{\mathrm{comp}}\}$ and a negligible function η such that $\omega_\lambda(\mathcal{G}_{\mathrm{comp}}, S_{\mathrm{comp}}) \geq \omega(\mathcal{G}, S) - \eta(\lambda)$ for all $\lambda \in \mathbb{N}$. This is one half of the main result [KLVY23, Thm. 3.2], and it implies that in particular $\omega_{q,\min}(\mathcal{G}_{\mathrm{comp}}) \geq \omega_q(\mathcal{G})$. The other half of their theorem states that efficient classical provers cannot exceed the classical value $\omega_c(\mathcal{G})$ by a non-negligible amount, as already mentioned earlier.

Remark 4.5. In this section, we consider quantum strategies that are defined in terms of (uniform) QPT algorithms, in line with the prior works [NZ23, CMM+24] and to emphasize that all reductions that will be discussed in the following are uniform as well. In cryptography, one can also model adversaries by *non-uniform* QPT algorithms, as mentioned earlier, and one can similarly define non-uniform QPT strategies. It is easy to see that all our results hold verbatim for such strategies, provided the QHE scheme is secure against non-uniform QPT adversaries.

We note that while in this setting the appropriate definition of $\omega_{q,\max}$ is by optimizing over non-uniform QPT strategies, $\omega_{q,\min}$ is still most naturally defined in terms of uniform QPT strategies since this is the appropriate notion for an honest prover to achieve a desired functionality.

4.3. **Asymptotic security for any noncommutative polynomial.** In the compiled game the prover gets Bob's question after giving Alice's answer. This implies that the correlations $p_\lambda(a,b|x,y)$ are necessarily non-signaling *from Bob to Alice*, i.e. $\sum_{b\in\mathcal{O}_B} p_\lambda(a,b|x,y) = \sum_{b\in\mathcal{O}_B} p_\lambda(a,b|x,y')$ for all $x\in\mathcal{I}_A$ and $y,y'\in\mathcal{I}_B$. Unlike in the nonlocal case, however, it is not a priori clear to which extent these correlations are non-signaling *from Alice to Bob*. However, the security property of the QHE scheme readily implies that the post-measurement states (4.3) are computationally indistinguishable when averaged over the possible measurement outcomes α. That is, if we define the quantum states

$$\sigma_x^\lambda = \sum_{a\in\mathcal{O}_A} \sigma_{xa}^\lambda = \mathop{\mathbb{E}}_{\mathsf{sk}\leftarrow\mathsf{Gen}(1^\lambda)} \mathop{\mathbb{E}}_{\xi\leftarrow\mathsf{Enc}(\mathsf{sk},x)} \sum_{\alpha\in\mathsf{CT}} A_{\xi\alpha}^\lambda |\psi^\lambda\rangle\langle\psi^\lambda| (A_{\xi\alpha}^\lambda)^*. \tag{4.5}$$

then $\{\sigma_x^\lambda\}$ and $\{\sigma_{x'}^\lambda\}$ are computationally indistinguishable for any $x,x'\in\mathcal{I}_A$, meaning that no QPT algorithm can distinguish them with non-negligible probability. This, in particular, implies that the correlations $p_\lambda(a,b|x,y)$ become non-signaling from Alice to Bob in the limit $\lambda\to\infty$. That is, for any $x,x'\in\mathcal{I}_A$ and $y\in\mathcal{I}_B$, there exists a negligible function η such that, for all λ,

$$\Big|\sum_{a\in\mathcal{O}_A} p_\lambda(a,b|x,y) - \sum_{a\in\mathcal{O}_A} p_\lambda(a,b|x',y)\Big| = \Big|\mathrm{tr}(\sigma_x^\lambda B_{yb}^\lambda) - \mathrm{tr}(\sigma_{x'}^\lambda B_{yb}^\lambda)\Big| \le \eta(\lambda),$$

because the POVM $\{B_{yb}^\lambda\}$ is implemented by a QPT algorithm for every $y\in\mathcal{I}_B$.

However, the security property of the encryption scheme implies a much stronger notion of computational non-signaling from Alice to Bob, as it makes a statement about any efficient algorithm. In particular, we can prove the following result.

Proposition 4.6. *Consider any compiled game and QPT strategy. Let $x,x'\in\mathcal{I}_A$, and let $P = P(\{B_{yb}\})$ be a polynomial in noncommuting variables $\{B_{yb}\}_{y\in\mathcal{I}_B,b\in\mathcal{O}_B}$. Then there exists a negligible function η such that, for all $\lambda\in\mathbb{N}$,*

$$\big|\mathrm{tr}\big(\sigma_x^\lambda\, P(\{B_{yb}^\lambda\})\big) - \mathrm{tr}\big(\sigma_{x'}^\lambda\, P(\{B_{yb}^\lambda\})\big)\big| \le \eta(\lambda),$$

where σ_x^λ is the prover's average state after its first reply when given an encryption of $x\in\mathcal{I}_A$, see (4.5), and where $\{B_{yb}^\lambda\}_{b\in\mathcal{O}_B}$ are POVMs for $y\in\mathcal{I}_B$, corresponding to the measurements that lead to the prover's second reply, as defined in (4.2).

Proposition 4.6 is a generalization of [CMM+24, Lem. 21] and is proved in a similar fashion, by using block encodings.

Definition 4.7. A *block encoding* of an operator M on $(\mathbb{C}^2)^{\otimes n}$ is a unitary U on $(\mathbb{C}^2)^{\otimes(m+n)}$, for some additional number of qubits $m\in\mathbb{N}$, such that

$$tH = \big(\langle 0|^{\otimes m}\otimes \mathbb{1}\big)\, U\, \big(|0\rangle^{\otimes m}\otimes \mathbb{1}\big), \quad \text{i.e.} \quad U = \begin{pmatrix} tH & * \\ * & * \end{pmatrix}$$

for some $t>0$ called the *scale factor* of the block encoding.

A *QPT block encoding* of a family of operators $\{M_\lambda\}$ is a QPT algorithm $\{U_\lambda\}$ such that each U_λ is a block encoding of M_λ, with t and m independent of λ.

The significance of this definition is as follows. On the one hand, the quantum expectation value of an observable that admits a QPT block encoding can be measured to any inverse polynomial precision, by a QPT quantum algorithm that takes polynomially many copies of the state. Together with the security property of the QHE scheme this implies the following.

Lemma 4.8 ([CMM+24, Lem 2.21], cf. [NZ23, Lem. 15-17])**.** *Consider any compiled game and QPT strategy. Let $x, x' \in \mathcal{I}_A$, and let $\{M_\lambda\}_{\lambda\in\mathbb{N}}$ be a family of observables that admit a QPT block encoding and such that $\sup_\lambda \|M_\lambda\| < \infty$. Then there exists a negligible function η such that, for all $\lambda \in \mathbb{N}$,*

$$\left|\mathrm{tr}\big(\sigma_x^\lambda\, M_\lambda\big) - \mathrm{tr}\big(\sigma_{x'}^\lambda\, M_\lambda\big)\right| \le \eta(\lambda),$$

where the states σ_x^λ are defined as in (4.5).

On the other hand, one can show that the families of POVM elements $\{B_{yb}^\lambda\}_{\lambda\in\mathbb{N}}$ have natural QPT block encodings, and moreover that the existence of QPT block encoding is preserved by multiplication and taking linear combinations. This implies that the family of operators defined by $M_\lambda = P(\{B_{yb}^\lambda\})$ has a QPT block encoding, which in view of the preceding lemma essentially establishes the proposition. The following proof makes this reasoning precise.

Proof of Proposition 4.6. It suffices to prove the claim for monomials since any noncommutative polynomial is a finite linear combination of monomials.

We first note that for any fixed $y \in \mathcal{I}_B$ and $b \in \mathcal{O}_B$, the POVM elements $\{B_{yb}^\lambda\}$ have a natural QPT block encoding. This follows from equation (4.2), by the same reasoning as in [GSLW19, Lem. 26], which also shows that the resulting block encodings have parameter $t = 1$ and $m = N$, where N denotes the total number of bits in the binary representation of y and b.

Now suppose that P is a monomial of degree D and let $M_\lambda = P(\{B_{yb}^\lambda\})$. It follows from [GSLW19, Lem. 30] that $\{M_\lambda\}$ admits a QPT block encoding with $t = 1$ and $m = DN$, simply by concatenating the individual block encodings in a suitable way (cf. [CMM+24, Lem 2.18]). Even though each POVM element is an observable, the operators M_λ need not be Hermitian, so we cannot apply Lemma 4.8 directly. Instead, we observe that it suffices to prove the claim for the observables $\mathrm{Re}(M_\lambda) = (M_\lambda + M_\lambda^*)/2$ and $\mathrm{Im}(M_\lambda) = (M_\lambda - M_\lambda^*)/(2\imath)$. To this end, we first note that $\{M_\lambda^*\}$ also admits a QPT block encoding with the same parameters as $\{M_\lambda\}$, as the former family corresponds to the monomial obtained by reversing P. Then it follows from [GSLW19, Lem. 29], by taking the controlled unitaries corresponding to these QPT block encodings, along with fixed state-preparation pairs for the two desired linear combinations, that the two families $\{\mathrm{Re}(M_\lambda)\}$ and $\{\mathrm{Im}(M_\lambda)\}$ admit QPT block encodings (cf. [CMM+24, Lem 2.17]). Now the claim follows from Lemma 4.8, the triangle inequality, and the fact that nonnegative linear combinations of negligible functions are negligible. ∎

5. Sequential characterizations of nonlocal correlations

Motivated by the two-round structure of a compiled game, we consider sequential games and strategies. Without further constraints, the resulting correlations can even be signaling, but we identify an information-theoretic property motivated by Proposition 4.6 that ensures that the resulting correlations are exactly quantum (in the finite-dimensional case) respectively commuting operator correlations (in the infinite-dimensional case). We also give a classical version of this result.

5.1. **Sequential games.** We consider sequential games that are parameterized by nonlocal games (Definition 3.1). Unlike in the nonlocal game, there is a single player that plays the roles of both Alice and Bob.

Definition 5.1. Consider a nonlocal game $\mathcal{G} = (\mathcal{I}_A, \mathcal{I}_B, \mathcal{O}_A, \mathcal{O}_B, \mu, V)$. The corresponding *sequential game* $\mathcal{G}_{\mathrm{seq}}$ describes a scenario of a single player interacting with a referee. In the game, the referee samples a pair of questions $(x, y) \in \mathcal{I}_A \times \mathcal{I}_B$ according to μ and sends question x to the player. The player returns an answer $a \in \mathcal{O}_A$. Then the referee sends y to the player, who replies with an answer $b \in \mathcal{O}_B$. Finally the referee computes $V(a, b|x, y)$ to determine if the player wins or loses.

Remark 5.2. A sequential game can also be interpreted as a *two-player* game where the first player can pass some information (depending on their question) to the second player before the latter has to respond with their answer.

As in the nonlocal case, we can describe the player's behavior by strategies that determine the probabilities $p(a, b|x, y)$ of answers a, b given questions x, y. Thus, the probability of winning the game $\mathcal{G}_{\mathrm{seq}}$ under a sequential strategy S, with correlations $p = \{p(a, b|x, y)\}$, will be denoted by

$$\omega(\mathcal{G}_{\mathrm{seq}}, S) = \omega(\mathcal{G}, p) = \sum_{x \in \mathcal{I}_A, y \in \mathcal{I}_B} \sum_{a \in \mathcal{O}_A, b \in \mathcal{O}_B} \mu(x, y) V(a, b|x, y) p(a, b|x, y).$$

Because of the temporal order in the sequential game, these correlations should be non-signaling from Bob to Alice, meaning that for all $x \in \mathcal{I}_A$, $y, y' \in \mathcal{I}_B$, and $a \in \mathcal{O}_A$, it should hold that

$$\sum_{b \in \mathcal{O}_B} p(a, b|x, y) = \sum_{b \in \mathcal{O}_B} p(a, b|x, y').$$

On the other hand, there is nothing imposed that prevents Alice from signaling Bob.

5.2. **Classical strategies and correlations.** While our main interest are quantum strategies, we first discuss the classical case to build some intuition.

Definition 5.3. A *classical strategy* for the sequential game $\mathcal{G}_{\mathrm{seq}}$ consists of

(i) probability distributions $\{p(a, \omega|x) : x \in \mathcal{I}_A\}$ with outcomes in $\mathcal{I}_A \times \Omega$, where Ω is a (without loss of generality) finite set,
(ii) probability distributions $\{q_\omega(b|y) : y \in \mathcal{I}_B, \omega \in \Omega\}$ with outcomes in $\mathcal{O}_B$.

Such a classical strategy gives rise to a correlation

$$p(a, b|x, y) = \sum_{\omega \in \Omega} p(a, \omega|x)\, q_\omega(b|y),$$

where $a \in \mathcal{O}_A, b \in \mathcal{O}_B, x \in \mathcal{I}_A, y \in \mathcal{I}_B$.

We note that $\omega \in \Omega$ models the information that is preserved between the two rounds of the game. While classical strategies for sequential games are always non-signaling from Bob to Alice, they may even be signaling from Alice to Bob. However, we can identify a natural property that ensures that the resulting correlations are not only non-signaling, but in fact nonlocal classical correlations in the sense of Definition 3.3: the distribution of ω should be independent of x.

Proposition 5.4. *Consider a classical strategy for $\mathcal{G}_{\mathrm{seq}}$ and suppose that the distributions $p(\omega|x) = \sum_{a\in\mathcal{O}_A} p(a,\omega|x)$ are the same for all $x \in \mathcal{I}_A$. Then the resulting correlation is a nonlocal classical correlation, that is, in C_c.*

Proof. Define a probability distribution $\gamma(\omega) := p(\omega|x)$, which by assumption does not depend on $x \in \mathcal{I}_A$, as well as probability distribution $p_\omega(a|x) := p(a,\omega|x)/\gamma(\omega)$ for $x \in \mathcal{I}_A$ and $\omega \in \Omega$ (for $\gamma(\omega) = 0$ the corresponding distributions p_ω can be defined arbitrarily). Then it holds that

$$p(a,b|x,y) = \sum_{\omega\in\Omega} p(a,\omega|x)\, q_\omega(b|y) = \sum_{\omega\in\Omega} \gamma(\omega)\, p_\omega(a|x)\, q_\omega(b|y),$$

which is precisely the form of a classical correlation. □

Conversely, any classical strategy for the nonlocal game (Definition 3.3) gives rise to one for the sequential game that satisfies the hypotheses of Proposition 5.4. Simply set $p(a,\omega|x) := \gamma(\omega)p_\omega(a|x)$ and use the same $q_\omega(b|y)$ as in the nonlocal strategy.

Corollary 5.5. *The classical correlation set C_c consists precisely of the correlations produced by classical sequential strategies satisfying the condition in Proposition 5.4.*

Remark 5.6. The condition identified in Proposition 5.4 does not refer to the Bob part of the strategy. If one takes Bob's strategy into account then one can give a sharper criterion – the distributions $p(\omega|x)$ should coincide when restricted to the σ-algebra generated by the functions $\{\omega \mapsto q_\omega(b|y)\}_{b\in\mathcal{O}_B, y\in\mathcal{I}_B}$. In the classical case, the simpler condition is without loss of generality, but not so in the (infinite-dimensional) quantum case.

5.3. **Quantum strategies and correlations.** Next, we move on to the quantum case. We give a definition that applies in finite as well as infinite dimensions.

Definition 5.7. A *quantum strategy* for the sequential game $\mathcal{G}_{\mathrm{seq}}$ consists of

(i) a Hilbert space $\mathcal{H}$,
(ii) positive (semidefinite) operators $\{\sigma_{xa}\}_{x\in\mathcal{I}_A, a\in\mathcal{O}_A}$ such that $\sigma_x := \sum_{a\in\mathcal{O}_A} \sigma_{xa}$ is a density operator (i.e., has unit trace) for every $x \in \mathcal{I}_A$, along with
(iii) POVMs $\{\{B_{yb} : b \in \mathcal{O}_B\} : y \in \mathcal{I}_B\}$ acting on $\mathcal{H}$.

Such a quantum strategy gives rise to a correlation

$$p(a,b|x,y) = \mathrm{tr}(\sigma_{xa} B_{yb})$$

where $a \in \mathcal{O}_A, b \in \mathcal{O}_B, x \in \mathcal{I}_A, y \in \mathcal{I}_B$.

Note that this formula is precisely the same expression as in (4.4) for the correlation determined by a QPT strategy.

Operators as in (ii) naturally arise as unnormalized post-measurement states for quantum measurements. For example, given a state ρ and a collection of measurements $\{\{A_{xa}\}_{a\in\mathcal{O}_A}\}_{x\in\mathcal{I}}$, the operators $\sigma_{xa} = A_{xa}\rho A_{xa}^*$ satisfy the assumption, as do the operators $\{\sigma_{xa}^\lambda\}$ defined in (4.3) for the compiled game (for any fixed λ). This is immediate, but can also be verified by the following lemma.

Lemma 5.8. *Let $\mathcal{H}$ be a Hilbert space, ρ be a state on $\mathcal{H}$, and $\{\Phi_{xa}\}_{x\in\mathcal{I}_A, a\in\mathcal{O}_A}$ be a collection of completely positive maps such that $\sum_{a\in\mathcal{O}_A} \Phi_{xa}$ is trace-preserving for* *every $x \in \mathcal{I}_A$.*[6] *Then the operators $\sigma_{xa} = \Phi_{xa}(\rho)$ satisfy the assumptions in (ii) of Definition 5.7. Conversely, any collection of operators as in (ii) arises in this way.*

Proof. The first claim follows directly from the trace-preserving assumption. For the converse, take ρ to be an arbitrary state and define $\Phi_{xa}(\cdot) = \operatorname{tr}(\cdot)\,\sigma_{xa}$. □

Correlations produced by quantum strategies for sequential games are always non-signaling from Bob to Alice, but not necessarily from Alice to Bob. We now state the key property that allows us to ensure that the correlations are in fact quantum respective commuting operator correlations for the nonlocal game, in the sense of Definitions 3.4 and 3.5. As the states σ_x are analogous to the marginal distributions $p(\omega|x)$ in the classical case, it is natural to demand that they are identical in a suitable sense.

Definition 5.9. A quantum strategy for $\mathcal{G}_{\mathrm{seq}}$ is *strongly non-signaling* if there exists a C^*-algebra $\mathscr{B} \subseteq \mathcal{B}(\mathcal{H})$ containing the operators $\{B_{yb}\}_{y\in\mathcal{I}_B, b\in\mathcal{O}_B}$ such that the following condition holds: for all $x, x' \in \mathcal{I}_A$ and for all $B \in \mathscr{B}$, we have

$$\operatorname{tr}(\sigma_x B) = \operatorname{tr}(\sigma_{x'} B). \tag{5.1}$$

We can always take $\mathscr{B}$ to be the C^*-algebra generated by the operators $\{B_{yb}\}$, because it is contained in any other C^*-algebra that contains these elements. Moreover, by continuity it suffices to verify (5.1) on the dense set of noncommutative polynomials in these operators.[7] We record this useful observation.

Lemma 5.10. *A quantum sequential strategy is strongly non-signaling if, and only if, for every $x, x' \in \mathcal{I}_A$ and for every noncommutative polynomial $P(\{B_{yb}\})$ in the operators $\{B_{yb}\}_{y\in\mathcal{I}_B, b\in\mathcal{O}_B}$, it holds that*

$$\operatorname{tr}\big(\sigma_x\, P(\{B_{yb}\})\big) = \operatorname{tr}\big(\sigma_{x'}\, P(\{B_{yb}\})\big). \tag{5.2}$$

Note the similarity between the characterization in Lemma 5.10 and the statement of Proposition 4.6. In Section 6 we will show how to connect the two in a precise way. Because we will need to take the limit where the security parameter tends to infinity, this will require us to consider infinite-dimensional strategies.

However, to build intuition we first consider finite-dimensional quantum sequential strategies. In this case we can prove that the strong non-signaling property ensures that these give rise to nonlocal quantum correlations in the sense of Definition 3.4.

Proposition 5.11. *Consider a quantum strategy for $\mathcal{G}_{\mathrm{seq}}$ that satisfies the strong non-signaling condition. If $\dim(\mathcal{H}) < \infty$, then the resulting correlation is a nonlocal quantum correlation, that is, in C_q.*

Proof. As explained in Remark 5.17 we may assume that $\mathscr{B} = \mathcal{B}(\mathcal{H})$ and hence $\sigma_x = \sigma_{x'}$ for all $x, x' \in \mathcal{I}_A$, and therefore we let $\sigma = \sigma_x$. Let $\mathcal{H}_A := \mathbb{C}^{\mathcal{O}_A} \otimes \mathcal{H}_{A'}$ and $\mathcal{H}_{A'} := \mathcal{H}_B := \mathcal{H}$. We think of the operators σ_{xa} as acting on $\mathcal{H}_B$ and choose purifications $|\psi_{xa}\rangle \in \mathcal{H}_{A'} \otimes \mathcal{H}_B$ for each $x \in \mathcal{I}_A$ and $a \in \mathcal{O}_A$. Then the states

$$|\psi_x\rangle := \sum_{a\in\mathcal{O}_A} |a\rangle \otimes |\psi_{xa}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$$

[6] A collection of completely positive maps $\{\Psi_a\}_{a\in\mathcal{O}}$ such that $\sum_{a\in\mathcal{O}_A} \Psi_{xa}$ is trace-preserving is called a *quantum instrument*. It describes the most general quantum evolution that has a classical outcome (measurement result) as well as a quantum one (post-measurement state) [Wil17, §4.6.8].

[7] However, it does *not* suffice to only require that (5.1) holds for the generators $B \in \{B_{yb}\}_{y\in\mathcal{I}_B, b\in\mathcal{O}_B}$.

are purifications of the same operator σ, which implies that there exist unitaries $U_{xx'}$ on $\mathcal{H}_A$ such that $|\psi_x\rangle = (U_{xx'} \otimes \mathbb{1}_B)|\psi_{x'}\rangle$. Defining $P_a := |a\rangle\langle a| \otimes \mathbb{1}_{A'}$ gives a projective measurement $\{P_a\}_{a\in\mathcal{O}_A}$ on $\mathcal{H}_A$. Fixing some $x_0 \in \mathcal{I}_A$, we observe that

$$p(a,b|x,y) = \mathrm{tr}(\sigma_{xa}B_{yb}) = \langle\psi_x|P_a \otimes B_{yb}|\psi_x\rangle = \langle\psi_{x_0}|U^*_{xx_0}P_aU_{xx_0} \otimes B_{yb}|\psi_{x_0}\rangle,$$

which shows that $p(a,b|x,y)$ is a quantum correlation, with Hilbert spaces $\mathcal{H}_A, \mathcal{H}_B$, initial state $|\psi_{x_0}\rangle$, and POVM elements $A_{xa} := U^*_{xx_0}P_aU_{xx_0}$ and B_{yb} for all $a \in \mathcal{O}_A, b \in \mathcal{O}_B, x \in \mathcal{I}_A$, and $y \in \mathcal{I}_B$. □

Conversely, any quantum strategy for the nonlocal game (Definition 3.4) gives rise to one for the sequential game that satisfies the hypotheses of Proposition 5.11. Simply let $\mathcal{H} = \mathcal{H}_B$, $\sigma_{xa} = \mathrm{tr}_A((M_{xa}\otimes\mathbb{1}_B)|\psi\rangle\langle\psi|)$, and use the operators $B_{yb} = N_{yb}$. Then strong non-signaling is satisfied, e.g., for $\mathscr{B} = \mathcal{B}(\mathcal{H})$.

Corollary 5.12. *The quantum correlation set C_q consists precisely of the correlations produced by* finite-dimensional *quantum sequential strategies satisfying the strong non-signaling condition of Definition 5.9.*

If we do not require the Hilbert space to be finite dimensional, we find that the strong non-signaling condition precisely characterizes the *commuting operator correlations* in the sense of Definition 3.5. To establish this result, it is useful to define the following equivalent C^*-algebraic model.

Definition 5.13. A *strongly non-signaling algebraic strategy* for $\mathcal{G}_{\mathrm{seq}}$ consists of

(i) a C^*-algebra $\mathscr{B}$,
(ii) positive linear functionals $\phi_{xa}\colon \mathscr{B} \to \mathbb{C}$ for $x \in \mathcal{I}_A$ and $a \in \mathcal{O}_A$, along with
(iii) POVMs $\{B_{yb}\}_{b\in\mathcal{O}_B}$ in $\mathscr{B}$ with outcomes in $\mathcal{O}_B$ for every $y \in \mathcal{I}_B$,

such that there exists a state $\phi\colon \mathscr{B} \to \mathbb{C}$ such that $\sum_{a\in\mathcal{O}_A} \phi_{xa} = \phi$ for every $x \in \mathcal{I}_A$. Such a strategy gives rise to a correlation

$$p(a,b|x,y) = \phi_{xa}(B_{yb})$$

where $a \in \mathcal{O}_A, b \in \mathcal{O}_B, x \in \mathcal{I}_A, y \in \mathcal{I}_B$.

Any quantum strategy for $\mathcal{G}$ can be converted into such an algebraic strategy, provided it satisfies the strong non-signaling property for a C^*-algebra $\mathscr{B}$. Simply define the positive linear functionals ϕ_{xa} by $\phi_{xa}(B) := \mathrm{tr}(\sigma_{xa}B)$ for all $B \in \mathscr{B}$. Thus the algebraic model is at least as general.

We now state the key result of this section. We will use it as an important component in the proof of our main result in Section 6.

Theorem 5.14. *For any strongly non-signaling algebraic strategy, the resulting correlation is a nonlocal commuting operator correlation, that is, in C_{qc}.*

In the proof of the theorem we will use the following version of the Radon-Nikodyme theorem for C^*-algebras, which is well-known to experts in operator algebras. We refer the reader to Section 2.2 for the concepts used in its statement.

Proposition 5.15 (Radon-Nikodyme theorem for C^*-algebras)**.** *Let ϕ and ψ be positive linear functionals on a unital C^*-algebra $\mathscr{B}$ with $\psi \leq \phi$. Then there exists a unique operator $T \in \pi_\phi(\mathscr{B})' \in \mathcal{B}(\mathcal{H}_\phi)$, with $0 \leq T \leq \mathbb{1}$, such that*

$$\psi(B) = \langle\nu_\phi|T\pi_\phi(B)|\nu_\phi\rangle,$$

for all $B \in \mathscr{B}$, where $(\mathcal{H}_\phi, \pi_\phi, |\nu_\phi\rangle)$ is any GNS triple associated with ϕ.

The version stated here is [Bla06, Prop. II.6.4.6] and we refer to this reference for a concise proof.

Proof of Theorem 5.14. Observe that $\phi_{xa} \leq \phi$ for all $x \in \mathcal{I}_A$ and $a \in \mathcal{O}_A$. Let $(\mathcal{H}_\phi, \pi_\phi, |\nu_\phi\rangle)$ be a GNS triple associated with ϕ. Then, by Proposition 5.15, for each pair (x, a) there exists an operator $M_{xa} \in \pi_\phi(\mathscr{B})'$ (in the commutant) such that $0 \leq M_{xa} \leq \mathbb{1}$ and we have $\phi_{xa}(B) = \langle \nu_\phi | M_{xa} \pi_\phi(B) | \nu_\phi \rangle$ for all $B \in \mathscr{B}$. Because $B_{yb} \in \mathscr{B}$ for all y, b, it follows that, for all x, y, a, b,

$$p(a, b|x, y) = \phi_{xa}(B_{yb}) = \langle \nu_\phi | M_{xa} \pi_\phi(B_{yb}) | \nu_\phi \rangle = \langle \nu_\phi | M_{xa} N_{yb} | \nu_\phi \rangle$$

where $N_{yb} := \pi_\phi(B_{yb}) \in \pi_\phi(\mathscr{B})$. Moreover, $[M_{xa}, N_{yb}] = 0$ because $M_{xa} \in \pi_\phi(\mathscr{B})'$.

To conclude that $p(a, b|x, y)$ is a commuting operator correlation, it remains to argue that $\{M_{xa}\}_{a \in \mathcal{O}_A}$ is a POVMs for each $x \in \mathcal{I}_A$ and $\{N_{yb}\}_{b \in \mathcal{O}_B}$ is a POVM for each $y \in \mathcal{I}_B$. The latter follows from the fact that each $\{B_{yb}\}_{b \in \mathcal{O}_B}$ is a POVM and π_ϕ is a $*$-homomorphism. For the former, it suffices to prove that $\sum_{a \in \mathcal{O}_A} M_{xa} = \mathbb{1}$ for every $x \in \mathcal{I}_A$ because we already know that the operators M_{xa} are positive. To this end, we observe that for any two elements $E, F \in \mathscr{B}$, it holds that

$$\begin{aligned}
\langle \nu_\phi | \pi_\phi(E^*) \sum_{a \in \mathcal{O}_A} M_{xa} \pi_\phi(F) | \nu_\phi \rangle &= \sum_{a \in \mathcal{O}_A} \langle \nu_\phi | M_{xa} \pi_\phi(E^* F) | \nu_\phi \rangle \\
&= \sum_{a \in \mathcal{O}_A} \phi_{xa}(E^* F) \\
&= \phi(E^* F) = \langle \nu_\phi | \phi(E^*) \phi(F) | \nu_\phi \rangle
\end{aligned}$$

where we used that $M_{xa} \in \pi_\phi(\mathscr{B})'$ and that π_ϕ is a $*$-homomorphism. Thus we have $\langle \nu_\phi | \pi_\phi(E^*) (\sum_{a \in \mathcal{O}_A} M_{xa} - \mathbb{1}) \pi_\phi(F) | \nu_\phi \rangle = 0$ for all $E, F \in \mathscr{B}$. Since $\pi_\phi(\mathscr{B}) |\nu_\phi\rangle$ is dense in $\mathcal{H}_\phi$, we deduce that $\sum_{a \in \mathcal{O}_A} M_{xa} = \mathbb{1}$, as desired, concluding the proof. □

Finally, any commuting operator strategy for the nonlocal game (Definition 3.5) gives rise to a strongly non-signaling quantum strategy for the sequential game. Simply use the same Hilbert space $\mathcal{H}$, $\sigma_{xa} = \sqrt{M_{xa}} |\psi\rangle\langle\psi| \sqrt{M_{xa}}$, the operators $B_{yb} = N_{yb}$, and let $\mathscr{B}$ denote the C^*-algebra generated by the operators $\{B_{yb}\}_{b \in \mathcal{O}_B, y \in \mathcal{I}_B}$. Then it is easily verified that strong non-signaling holds for $\mathscr{B}$, noting that $M_{xa} \in \mathscr{B}'$ (as we started from a commuting operator strategy) and hence the same is true for its positive square roots $\sqrt{M_{xa}}$. Altogether we obtain the following corollary which may be of independent interest.

Corollary 5.16. *The commuting operator correlation set C_{qc} is equal to the correlations produced by strongly non-signaling algebraic sequential strategies (Definition 5.13), as well as to the correlations produced by (possibly infinite-dimensional) strongly non-signaling quantum sequential strategies (Definition 5.9).*

Remark 5.17. Clearly, a quantum strategy is strongly non-signaling (Definition 5.9) if $\sigma_x = \sigma_{x'}$ for all $x, x' \in \mathcal{I}_A$. This condition is analogous to the one that we gave in the classical case. If $\mathcal{H}$ is finite-dimensional then we can always reduce to this situation, by replacing each σ_{xa} by its twirl over the unitary group of the commutant of the C^*-algebra generated by the POVM elements. When $\mathcal{H}$ is infinite-dimensional such a reduction is not possible, but the C^*-algebraic model described in Definition 5.13 can serve as a useful substitute. We note that when $\mathscr{B}$ is finite-dimensional and *commutative*, the latter reduces to the situation of Proposition 5.4.

6. Upper bound on the quantum value of compiled nonlocal games

In this section we prove that the (maximal) quantum value of a compiled game never exceeds the commuting operator value of the corresponding nonlocal game. The basic idea is as follows. In Section 4, we showed that any QPT strategy of a nonlocal game satisfies an analogue of the strong non-signaling condition discussed in Section 5. More precisely, Proposition 4.6 states that (5.2) holds to arbitrary precision when the security parameter tends to infinity, for any fixed polynomial in the Bob POVMs. We would like to take a limit, but as the Hilbert spaces will depend on the security parameter, we instead work with a single *universal* C^*-algebra. We can then define a sequence of states on this algebra, which captures precisely all information that can be accessed using the Bob POVMs, for every value of the security parameter, and use compactness of the state space of a C^*-algebra to define a limit where the strong non-signaling condition holds exactly. The result then follows from Theorem 5.14.

We now describe the required C^*-algebra, which is often called the *POVM algebra*, denoted $\mathscr{A}^{\mathcal{I},\mathcal{O}}_{\mathrm{POVM}}$, for finite sets $\mathcal{I}$ and $\mathcal{O}$ [PSZZ23]. It has elements $\{B_{xa}\}_{x\in\mathcal{I},a\in\mathcal{O}}$ which satisfy the relations $0 \leq B_{xa} \leq \mathbb{1}$ and $\sum_{a\in\mathcal{O}} B_{xa} = 1$ for each $x \in \mathcal{I}$. Importantly, it satisfies the following *universal property*: for any Hilbert space $\tilde{\mathcal{H}}$ and any collection of POVMs $\{\tilde{B}_{xa}\}$ on $\tilde{\mathcal{H}}$, there exists a unique $*$-homomorphism $\theta\colon \mathscr{A}^{\mathcal{I},\mathcal{O}}_{\mathrm{POVM}} \to \mathcal{B}(\tilde{\mathcal{H}})$ sending $B_{xa} \mapsto \tilde{B}_{xa}$ for all $x \in \mathcal{I}$ and $a \in \mathcal{O}$. The POVM C^*-algebras are separable as they are finitely generated.

Theorem 6.1. *Let $\mathcal{G}$ be any two-player nonlocal game and let S be any QPT strategy for the compiled game $\mathcal{G}_{\mathrm{comp}}$. Then it holds that*

$$\limsup_{\lambda\to\infty} \omega_\lambda(\mathcal{G}_{\mathrm{comp}}, S) \leq \omega_{qc}(\mathcal{G})$$

As a direct consequence, we obtain the following upper bound on the (maximal) quantum value of any compiled game (Definition 4.4).

Corollary 6.2. *For any two-player nonlocal game $\mathcal{G}$, we have $\omega_{q,\max}(\mathcal{G}_{\mathrm{comp}}) \leq \omega_{qc}(\mathcal{G})$.*

We now prove the theorem.

Proof of Theorem 6.1. Recall from Eq. (4.4) that for each value of the security parameter $\lambda \in \mathbb{N}$ there exists a Hilbert space $\mathcal{H}_\lambda$, positive operators σ^λ_{xa} for $x \in \mathcal{I}_A$ and $a \in \mathcal{O}_A$ such that each $\sigma^\lambda_x := \sum_{a\in\mathcal{O}_A} \sigma^\lambda_{xa}$ is a state, and POVMs $\{B^\lambda_{yb}\}_{b\in\mathcal{O}_B}$ for all $y \in \mathcal{I}_B$, such that the correlations take the following form:

$$p_\lambda(a,b|x,y) = \mathrm{tr}(\sigma^\lambda_{xa} B^\lambda_{yb})$$

After passing to a subsequence, we may assume that the limit

$$\lim_{\lambda\to\infty} \omega_\lambda(\mathcal{G}_{\mathrm{comp}}, S)$$

exists and is equal to the lim sup of the original sequence.

The theorem follows if we can show that there exists a further subsequence $\{\lambda_k\}_{k\in\mathbb{N}}$ such that the correlations p_{λ_k} converge to a commuting operator correlation. To this end, let $\mathscr{A}^{\mathcal{I}_B,\mathcal{O}_B}_{\mathrm{POVM}}$ denote the POVM C^*-algebra described above, with its generators $\{B_{yb}\}$. By the universal property, there exist $*$-homomorphisms

$$\vartheta_\lambda\colon \mathscr{A}^{\mathcal{I}_B,\mathcal{O}_B}_{\mathrm{POVM}} \to \mathcal{B}(\mathcal{H}_\lambda)$$

such that $\vartheta_\lambda(B_{yb}) = B^\lambda_{yb}$ for all λ, y, b. We can use these to define linear functionals

$$\phi^\lambda_{xa} \colon \mathscr{A}^{\mathcal{I}_B,\mathcal{O}_B}_{\mathrm{POVM}} \to \mathbb{C}, \quad \phi^\lambda_{xa}(\cdot) = \mathrm{tr}(\sigma^\lambda_{xa}\vartheta_\lambda(\cdot)). \tag{6.1}$$

Observe that each ϕ^λ_{xa} is a positive linear functional of norm $\|\phi^\lambda_{xa}\| = \phi^\lambda_{xa}(\mathbb{1}) = \mathrm{tr}(\sigma^\lambda_{xa}) \leq 1$. Thus we can apply the Banach–Alaoglu theorem (Section 2.2) to deduce that, for each $x \in \mathcal{I}_A, a \in \mathcal{O}_A$, the sequence $\{\phi^\lambda_{xa}\}_{\lambda\in\mathbb{N}}$ (and any subsequence thereof) has a weak-$*$ convergent subsequence. By iteratively passing to convergent subsequences (recall that $\mathcal{I}_A$ and $\mathcal{O}_A$ are finite sets), we obtain a strictly increasing subsequence $\{\lambda_k\}_{k\in\mathbb{N}}$ and positive linear functionals $\phi_{xa} \colon \mathscr{A}^{\mathcal{I}_B,\mathcal{O}_B}_{\mathrm{POVM}} \to \mathbb{C}$ such that

$$\lim_{k\to\infty} \phi^{\lambda_k}_{xa}(B) = \phi_{xa}(B) \tag{6.2}$$

for every $x \in \mathcal{I}_A$, $a \in \mathcal{O}_A$, and $B \in \mathscr{A}^{\mathcal{I}_B,\mathcal{O}_B}_{\mathrm{POVM}}$. Let $\phi_x := \sum_{a\in\mathcal{O}_A} \phi_{xa}$. These are states, because $\sum_{a\in\mathcal{O}_A} \phi^\lambda_{xa}(\mathbb{1}) = \mathrm{tr}(\sigma^\lambda_x) = 1$ and hence also $\phi_x(\mathbb{1}) = 1$, by (6.2). We now show that $\phi_x = \phi_{x'}$ for all $x, x' \in \mathcal{I}_A$. To this end, take any fixed polynomial $P(\{B_{yb}\})$ in the generators B_{yb} of $\mathscr{A}^{\mathcal{I}_B,\mathcal{O}_B}_{\mathrm{POVM}}$. Using Eqs. (6.1) and (6.2),

$$\begin{aligned}
\phi_{xa}(P(\{B_{yb}\})) &= \lim_{k\to\infty} \phi^{\lambda_k}_{xa}(P(\{B_{yb}\})) \\
&= \lim_{k\to\infty} \mathrm{tr}\big(\sigma^{\lambda_k}_{xa}\, \vartheta_{\lambda_k}(P(\{B_{yb}\}))\big) \\
&= \lim_{k\to\infty} \mathrm{tr}\Big(\sigma^{\lambda_k}_{xa}\, P(\{B^{\lambda_k}_{yb}\})\Big)
\end{aligned}$$

and hence

$$\phi_x(P(\{B_{yb}\})) = \lim_{k\to\infty} \mathrm{tr}\Big(\sigma^{\lambda_k}_x\, P(\{B^{\lambda_k}_{yb}\})\Big).$$

Now Proposition 4.6 implies that $\phi_x(B) = \phi_{x'}(B)$ for all $x, x' \in \mathcal{I}_A$ and any element of the form $B = P(\{B_{yb}\})$. Since these elements are dense in $\mathscr{A}^{\mathcal{I}_B,\mathcal{O}_B}_{\mathrm{POVM}}$, it follows that $\phi_x = \phi_{x'}$ for all $x, x' \in \mathcal{I}_A$. Thus we have proved that the C^*-algebra $\mathscr{A}^{\mathcal{I}_B,\mathcal{O}_B}_{\mathrm{POVM}}$ along with the functionals $\{\phi_{xa}\}$ and the operators $\{B_{yb}\}$ constitute a strongly non-signaling algebraic strategy for the sequential game $\mathcal{G}_{\mathrm{seq}}$. Using Theorem 5.14, we obtain that

$$p(a, b|x, y) = \phi_{xa}(B_{yb})$$

is a commuting operator correlation. On the other hand, Eq. (6.2) implies that

$$\lim_{k\to\infty} p_{\lambda_k}(a, b|x, y) = p(a, b|x, y)$$

for all a, b, x, y. It follows that

$$\lim_{\lambda\to\infty} \omega_\lambda(\mathcal{G}_{\mathrm{comp}}, S) = \lim_{k\to\infty} \omega_{\lambda_k}(\mathcal{G}_{\mathrm{comp}}, S) = \lim_{k\to\infty} \omega(\mathcal{G}, p_{\lambda_k}) = \omega(\mathcal{G}, p) \leq \omega_{qc}(\mathcal{G}),$$

and this concludes the proof of the theorem. □

Acknowledgements

CP thanks the hospitality at RUB for a productive visit. CP acknowledges funding support from the Natural Sciences and Engineering Research Council of Canada (NSERC). AK, GM, SS and MW acknowledge support by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy - EXC 2092 CASA - 390781972. GM is also supported by the European Research Council through an ERC Starting Grant (Grant agreement No. 101077455, ObfusQation). MW is supported by the European Research Council through an ERC Starting Grant (Grant agreement No. 101040907, SYMOPTIC), by the NWO through grant OCENW.KLEIN.267, and by the BMBF through project Quantum Methods and Benchmarks for Resource Allocation (QuBRA).

References

[Bei21] Salman Beigi. Separation of quantum, spatial quantum, and approximate quantum correlations. *Quantum*, 5:389, 2021.

[Bel64] John S Bell. On the Einstein Podolsky Rosen paradox. *Physics Physique Fizika*, 1(3):195, 1964.

[Bla06] Bruce Blackadar. *Operator Algebras: Theory of C^*-Algebras and von Neumann Algebras*, volume 122. Springer Science & Business Media, 2006.

[Bra18] Zvika Brakerski. Quantum FHE (almost) as secure as classical. In *Annual International Cryptology Conference*, pages 67–95. Springer, 2018.

[BVB+24] Matilde Baroni, Quoc-Huy Vu, Boris Bourdoncle, Eleni Diamanti, Damian Markham, and Ivan Šupić. Quantum bounds for compiled XOR games and d-outcome CHSH games. *preprint arXiv:2403.05502*, 2024.

[CFE+24] Lorenzo Catani, Ricardo Faleiro, Pierre-Emmanuel Emeriau, Shane Mansfield, and Anna Pappa. Connecting XOR and XOR* games. *Physical Review A*, 109(1):012427, 2024.

[CGJV19] Andrea Coladangelo, Alex B Grilo, Stacey Jeffery, and Thomas Vidick. Verifier-on-a-leash: new schemes for verifiable delegated quantum computation, with quasilinear resources. In *Annual international conference on the theory and applications of cryptographic techniques*, pages 247–277. Springer, 2019.

[CHSH69] John F Clauser, Michael A Horne, Abner Shimony, and Richard A Holt. Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, 23(15):880, 1969.

[CHTW04] R. Cleve, P. Hoyer, B. Toner, and J. Watrous. Consequences and limits of nonlocal strategies. In *Proceedings. 19th IEEE Annual Conference on Computational Complexity, 2004.*, pages 236–249, 2004.

[CMM+24] David Cui, Giulio Malavolta, Arthur Mehta, Anand Natarajan, Connor Paddock, Simon Schmidt, Michael Walter, and Tina Zhang. A computational Tsirelson's theorem for the value of compiled XOR games, 2024. Accepted at TQC 2024.

[Col20] Andrea Coladangelo. A two-player dimension witness based on embezzlement, and an elementary proof of the non-closure of the set of quantum correlations. *Quantum*, 4:282, 2020.

[CS20] Andrea Coladangelo and Jalex Stark. An inherently infinite-dimensional quantum correlation. *Nature communications*, 11(1):3335, 2020.

[DPP19] Ken Dykema, Vern I Paulsen, and Jitendra Prakash. Non-closure of the set of quantum correlations via graphs. *Communications in Mathematical Physics*, 365:1125–1142, 2019.

[Fri12] Tobias Fritz. Tsirelson's problem and Kirchberg's conjecture. *Reviews in Mathematical Physics*, 24(05):1250012, 2012.

[Gri19] Alex B. Grilo. A simple protocol for verifiable delegation of quantum computation in one round. In Christel Baier, Ioannis Chatzigiannakis, Paola Flocchini, and Stefano Leonardi, editors, *46th International Colloquium on Automata, Languages, and Programming (ICALP 2019)*, volume 132 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 28:1–28:13, Dagstuhl, Germany, 2019. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

[GSLW19] András Gilyén, Yuan Su, Guang Hao Low, and Nathan Wiebe. Quantum singular value transformation and beyond: exponential improvements for quantum matrix arithmetics. In *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2019, page 193'204, New York, NY, USA, 2019.

[JNP+11] Marius Junge, Miguel Navascues, Carlos Palazuelos, David Perez-Garcia, Volkher B Scholz, and Reinhard F Werner. Connes' embedding problem and Tsirelson's problem. *Journal of Mathematical Physics*, 52(1), 2011.

[JNV+21] Zhengfeng Ji, Anand Natarajan, Thomas Vidick, John Wright, and Henry Yuen. MIP* = RE. *Communications of the ACM*, 64(11):131–138, 2021.

[KLVY23] Yael Kalai, Alex Lombardi, Vinod Vaikuntanathan, and Lisa Yang. Quantum advantage from any non-local game. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing (STOC)*, pages 1617–1628, 2023.

[Mah18] Urmila Mahadev. Classical verification of quantum computations. In *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 259–267. IEEE, 2018.

[Mah20] Urmila Mahadev. Classical homomorphic encryption for quantum circuits. *SIAM Journal on Computing*, pages FOCS18–189, 2020.

[Mer90] N. David Mermin. Simple unified form for the major no-hidden-variables theorems. *Phys. Rev. Lett.*, 65:3373–3376, Dec 1990.

[MNZ24] Tony Metger, Anand Natarajan, and Tina Zhang. Succinct arguments for QMA from standard assumptions via compiled nonlocal games. *preprint arXiv:2404.19754*, 2024.

[MPW24] Arthur Mehta, Connor Paddock, and Lewis Wooltorton. Self-testing in the compiled setting via tilted-CHSH inequalities. *preprint arXiv:2406.04986*, 2024.

[MR20] Magdalena Musat and Mikael Rørdam. Non-closure of quantum correlation matrices and factorizable channels that require infinite dimensional ancilla (with an appendix by Narutaka Ozawa). *Communications in Mathematical Physics*, 375(3):1761–1776, 2020.

[NPA08] Miguel Navascués, Stefano Pironio, and Antonio Acín. A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. *New Journal of Physics*, 10(7):073013, 2008.

[NZ23] Anand Natarajan and Tina Zhang. Bounding the quantum value of compiled nonlocal games: from CHSH to BQP verification. In *2023 IEEE 64th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 1342–1348. IEEE, 2023.

[Oza13] Narutaka Ozawa. About the Connes embedding conjecture. *Japanese Journal of Mathematics*, 8(1):147–183, 2013.

[Per90] Asher Peres. Incompatible results of quantum measurements. *Physics Letters A*, 151(3):107–108, 1990.

[PSZZ23] Connor Paddock, William Slofstra, Yuming Zhao, and Yangchen Zhou. An operator-algebraic formulation of self-testing. In *Annales Henri Poincaré*, pages 1–37. Springer, 2023.

[RUV13] Ben W Reichardt, Falk Unger, and Umesh Vazirani. Classical command of quantum systems. *Nature*, 496(7446):456–460, 2013.

[Slo16] William Slofstra. Tsirelson's problem and an embedding theorem for groups arising from non-local games. *Journal of the American Mathematical Society*, 2016.

[Slo17] William Slofstra. The set of quantum correlations is not closed. *Forum of Mathematics, Pi*, 7, 2017.

[Tsi87] Boris Tsirelson. Quantum analogues of the Bell inequalities: The case of two spatially separated domains. *Journal of Soviet Mathematics*, 36:557–570, 1987.

[Wil17] Mark M. Wilde. *Quantum Information Theory.* Cambridge University Press, 2017.

Alexander Kulpe, Faculty of Computer Science, Ruhr University Bochum, Germany
Email address: `alexander.kulpe@rub.de`

Giulio Malavolta, Department of Computing Sciences, Bocconi University, Italy and Max Planck Institute for Security and Privacy
Email address: `giulio.malavolta@unibocconi.it`

Connor Paddock, Department of Mathematics & Statistics, University of Ottawa, Canada
Email address: `cpaulpad@uottawa.ca`

Simon Schmidt, Faculty of Computer Science, Ruhr University Bochum, Germany
Email address: `s.schmidt@rub.de`

Michael Walter, Faculty of Computer Science, Ruhr University Bochum, Germany
Email address: `michael.walter@rub.de`