THEORY OF COMPUTING, Volume 15 (5), 2019, pp. 1–42
www.theoryofcomputing.org

Classical Verification of Quantum Proofs

Zhengfeng Ji

Received January 30, 2017; Revised March 26, 2018; Published September 15, 2019

Abstract: We present a classical interactive protocol that checks the validity of a quantum witness state for the local Hamiltonian problem. It follows from this protocol that approximating the nonlocal value of a multi-player one-round game to inverse polynomial precision is QMA-hard. Our result makes a connection between the theory of QMA-completeness and Hamiltonian complexity on one hand and the study of nonlocal games and Bell inequalities on the other.

ACM Classification: F.1.2, F.1.3

AMS Classification: 68Q10, 68Q12, 81P40, 81P68

Key words and phrases: quantum interactive proofs, local Hamiltonian problem, nonlocal games, entanglement, Bell inequalities

1 Introduction

The concept of efficient proof verification is of fundamental importance to the theory of computation. The complexity class NP abstracts the notion of checking written proof strings by a polynomial-time deterministic verifier. It is hard to overstate the importance of NP and NP-completeness theory [21, 47, 38] to the development of theoretical computer science in the past several decades.

Interactive models of proof verification were proposed and studied by Babai [7] and Goldwasser, Micali, and Rackoff [29]. They were generalized to the multiple-prover setting by Ben-Or, Goldwasser, Kilian and Wigderson [11]. The efforts to understand these interactive proof systems opened the door to a series of breakthroughs in computational complexity theory (e. g., [48, 64, 8, 6, 5]).

Of particular interest to this paper is the multi-player one-round game, a game theoretical model for interactive proof verification, first studied by Feige and Lovász [24]. In this model, the verifier samples a

An extended abstract of this paper appeared in the Proceedings of the 48th annual ACM Symposium on Theory of Computing (STOC'16) [35].

DOI: 10.4086/toc.2019.v015a005

list of questions and sends them to the players and receives answers back from the players in one round. The players may agree on a particular strategy in advance but are not allowed to communicate with each other during the game. The verifier decides whether to accept or to reject based on the questions and answers. We use both the terms of multi-player one-round games and multi-prover one-round interactive proofs in this paper. A multi-player one-round game is, roughly speaking, a one-round interactive proof for a fixed input instance and can be specified completely by the representation of both its question distribution and the truth table of the verifier predicate.

A method called oracularization [27] that enforces the non-adaptive behavior of the players provides a multi-player-game characterization of NP, in which the questions are bit strings of length logarithmic in the input length and the answers are strings of a constant number of bits. We emphasize that this is an exponential savings in the number of bits communicated from the provers to the verifier compared with the standard method of proof communication in which the prover sends the full proof string to the verifier. This is one of the reasons behind the unexpected power of multi-prover interactive proof systems [8] and the possibility of achieving probabilistically checkable proofs [6, 5, 23].

The study of quantum variants of proof verification systems (see, e. g., [41, 43, 72, 73, 33, 18, 32, 2, 26, 15]) provides both a fruitful way to understand proof verification in the context of quantum computing and an insightful angle to examine unique quantum phenomena such as superposition, entanglement and nonlocality. Interested readers are referred to the recent review article on this topic by Vidick and Watrous [71].

A quantum analog of efficient verification of written proofs was proposed by Kitaev [41, 42, 4]. In this generalization, a quantum witness state plays the role of the written proof and a polynomial-time quantum computer checks whether the witness state is valid for the input. Kitaev introduces the class QMA of problems that admit efficiently verifiable quantum proofs. He also establishes the quantum analog of the Cook-Levin theorem by showing that the local Hamiltonian problem, the natural quantum version of the constraint satisfaction problems, is complete for QMA. The study of local Hamiltonian problems, the structure of entanglement in the ground states of local Hamiltonians, and the quantum PCP conjecture (see, e. g., [2]) form a research direction called Hamiltonian complexity [59, 28].

Quantum interactive proof systems, a model in which a quantum polynomial-time verifier exchanges quantum messages with an all-powerful prover, were first studied by Kitaev and Watrous [43, 72]. It is now known that the class of languages expressible by such proof systems, QIP, is the same as its classical counterpart, IP [33].

In quantum multi-prover interactive proof systems, shared entanglement among the provers plays an essential role. It is known that, without shared entanglement, or with a limited amount of entanglement, the collection of languages that have quantum multi-prover interactive proof systems, QMIP, equals its classical counterpart, MIP [44] (and, hence, also equals NEXP [8]). The classes QMIP^* and MIP^*, corresponding to the collections of languages that have entangled multi-prover interactive proofs with quantum and classical messages respectively, are also known to be the same [63]. There is recent evidence showing that entangled provers may be more powerful than classical provers [26]. But a full understanding of these two complexity classes is still out of reach.

In this article, we focus on multi-prover one-round games with entangled provers. For a multi-player one-round game, its classical value is the maximum acceptance probability that classical strategies can achieve and its nonlocal value is the maximum acceptance probability that entangled players can achieve.

In general, the nonlocal value can be strictly larger than the classical value of a multi-player game. It is pointed out in [18] that this may cause problems in multi-prover interactive proof systems as provers with shared entanglement may break the soundness condition of a classically sound protocol. One striking example is given by the so-called magic square game [53, 60], which has nonlocal value one even though it corresponds to a system of constraints with no classical solution [18]. Strong evidence is also given in that paper that entanglement between the players may indeed weaken the power of two-player XOR games.

Several methods have been proposed to control the cheating ability of entangled provers and recover soundness in certain cases. It is known that approximating the nonlocal value of a multi-player game to inverse-polynomial precision is NP-hard [40, 31], and therefore at least as hard as approximating the classical value [27]. Several natural problems arise from the study of nonlocality, including the binary constraint system game [19], the quantum coloring game [16] and the game corresponding to the Kochen-Specker sets [45], are shown to be NP-hard in [34]. By proving that the multi-linearity test [8] is sound against entangled provers, Ito and Vidick proved the containment of NEXP in MIP^* [32]. This was later improved to the result that three-player XOR games are NP-hard to approximate even to constant precision [70].

In this paper, we present a multi-player one-round game for the local Hamiltonian problem in which the verifier is classical and samples questions of logarithmic size and expects answers of constant size. As a corollary, the problem of approximating the nonlocal value of a multi-prover one-round game is QMA-hard, improving the NP-hardness results in prior work. It makes an interesting connection between the theory of QMA-completeness and Hamiltonian complexity on one hand, and the study of nonlocal games and Bell inequalities on the other. This also provides an example in which a classical verifier can design protocols making essential use of the shared entanglement between the provers and expects them to do things that are impossible for provers without shared entanglement unless $\mathsf{NP} = \mathsf{QMA}$.

Our protocol can be thought of as a de-quantization of the Fitzsimons-Vidick protocol [26] of both the verifier and the messages. The verifier communicates with multiple entangled provers and delegates the quantum verification procedure to the provers. In this sense, this work is also relevant to the developments in the delegation of quantum computation and blind quantum computing [14, 3, 63, 25]. Previous articles usually use a cluster state [62] or EPR states and teleportation to encode quantum computation, while our approach has the additional freedom to encode quantum data directly among the provers. This allows us to go from the delegation of quantum computation to the delegation of quantum proof verification.

The main result of this paper is stated in the following theorem.

Theorem 1.1. *For any integer $r \geq 4$, any promise problem $L = (L_{\text{yes}}, L_{\text{no}})$ in* QMA*, and any instance x of the problem, there exists an r-player one-round game and real numbers $c, s \in [0,1]$, $c - s \geq 1/\operatorname{poly}(|x|)$ such that*

1. *The description of the game and the numbers c, s can be computed in polynomial time given x as input.*
2. *The questions are classical bit strings of length $O(\log(|x|))$.*
3. *The answers are classical bit strings of length $O(1)$.*
4. *If $x \in L_{\text{yes}}$, then the nonlocal value of the game is at least c.*

5. *If $x \in L_{\text{no}}$, then the nonlocal value of the game is at most s.*

A direct corollary is that approximating the nonlocal value of a multi-player game is QMA-hard.

Corollary 1.2. *Given a multi-player one-round game in which the questions are strings of $O(\log n)$ bits and answers are of strings of $O(1)$ bits, it is* QMA*-hard to approximate the nonlocal value of the game to inverse polynomial precision.*

The same problem for the classical value is obviously in NP. This means that the nonlocal value of multi-player one-round games is strictly harder to approximate than the classical value unless $\mathsf{NP} = \mathsf{QMA}$.

Our result has the following consequence for multi-prover interactive proofs with entangled provers by scaling up the problem size. It is a slight improvement of the results obtained in [26]. Let $\mathsf{QMA}_{\mathsf{EXP}}$ be the collection of problems that have quantum witnesses of exponentially many qubits verifiable by a quantum exponential-time machine, and let $\mathsf{MIP}^*(r,t,c,s)$ be the class of languages that have r-prover, t-round interactive proofs with a classical polynomial-time verifier, entangled provers, and completeness c, soundness s.

Corollary 1.3. *For some choices of completeness and soundness c,s and polynomial $p(n)$, with $c-s = \Omega(\exp(-p(n)))$,*

$$\mathsf{QMA}_{\mathsf{EXP}} \subseteq \mathsf{MIP}^*(4,1,c,s),$$

and hence

$$\mathsf{MIP}(4,1,c,s) = \mathsf{MIP} \subsetneq \mathsf{MIP}^*(4,1,c,s)$$

unless $\mathsf{NEXP} = \mathsf{QMA}_{\mathsf{EXP}}$.

1.1 Techniques and proof overview

The main technical difficulty we face is how a classical verifier can check the quantum witness state distributed among a number of players. In a one-round game, the only thing that the classical verifier can collect is some information about the conditional distributions $\Pr(a \mid q)$ for all possible questions q and answers a. Consider the situation of remote state certification, in which two players A and B share a quantum state ρ_{AB} and want to convince the verifier of this fact. If the state ρ_{AB} is an EPR state $(|00\rangle + |11\rangle)/\sqrt{2}$, this is possible in some sense by the verifier playing the CHSH game [17] with the players. The rigidity of the CHSH game [52, 63] implies that if the players win the CHSH game with almost optimal probability, then the state is close to the EPR state up to local isometries. If the state is mixed, however, the situation becomes problematic in a very strong sense. Suppose the two players want to prove that ρ_{AB} is the Werner state [74]

$$\rho_{\mathrm{W}}(\phi) = \frac{(d-\phi)I + (d\phi - 1)\,\mathrm{SWAP}_d}{d^3 - d},$$

where SWAP_d is unitary operator satisfying $\mathrm{SWAP}_d\,|i,j\rangle = |j,i\rangle$ for all $0 \le i,j \le d-1$. It is known [74, 9] that, for some choices of ϕ, the state is an entangled state, but any prescribed local measurement setting on A and B performed on the state ρ_{W} produces distributions $\Pr(a \mid q)$ that have local hidden variable models. That is, the distribution can be exactly reproduced by two classical players with shared randomness and no shared entangled states whatsoever!

It is natural to consider methods from the study of device-independent quantum information processing or self-testing quantum devices (e. g., [49, 67, 54, 50]). For example, such ideas have successful applications in achieving the classical command of quantum systems as shown in [63]. A key ingredient behind such device-independent methods is the rigidity of nonlocal games such as the CHSH game. By the definition of rigidity, however, the players will essentially share a specific entangled state, such as the EPR state or the GHZ state $(|000\rangle+|111\rangle)/\sqrt{2}$, and perform prescribed measurements on the state. This seems contradictory to what we need here—the ability to store the quantum witness state distributed among the players. The quantum witness state is usually an entangled state with complex structures that are far away from what EPR or GHZ states can represent.

Our solution that resolves the above-mentioned difficulties is to encode the quantum witness state by a certain stabilizer code and play a new game, which we call the stabilizer game, defined by the stabilizer. We prove a rigidity theorem for the stabilizer game which roughly states that the only way for the players to win the game with high probability is to share a correctly encoded state of the stabilizer code, perform measurements according to the measurement specifications given in the questions, and respond with the measurement outcome. That is, the stabilizer game we construct provides a device-independent verification of the encoding of the corresponding stabilizer code. Having both the rigidity property and the ability to encode quantum data, the stabilizer game serves as an essential tool for our work and may find other applications in device-independent quantum information processing. For example, in the remote state certification problem discussed above, although it is impossible for the players to certify the Werner state ρ_{W}, the stabilizer games provide a way to certify an *encoded* Werner state using a stabilizer code.

In [26], quantum error correcting codes are also employed in an essential way. The intuition is that, by the quantum error correction property, there will be only one qubit of the player that can pass the encoding check of the error correcting code once the rest of the players respond with the correct qubit. The protocol using quantum error correcting codes proposed in [26] can be thought of as a quantum analog of the oracularization technique [27]—the classical oracularization is based on the classical repetition code in this perspective. One crucial difference between the classical and quantum oracularization techniques is that, in the quantum setting, the referee has to query *all pairs* of qubits in order to be able to argue about the commutativity between observables on different qubits. This is obviously not necessary in the classical setting.

In our case, the stabilizer codes have the same effects but also have an important additional use. Namely, they are responsible for enforcing the players to measure their systems according to the measurement specifications they receive. Instead of using the decoding circuit of the code, we measure the logical X, Z operators on the encoded state. As a result, our proof directly applies to quantum error detecting codes as well.

The proof of rigidity for stabilizer games consists of two steps. In the first step, an idea motivated by the CHSH game is employed and we introduce the special-player stabilizer game. Using similar techniques for proving the rigidity of the CHSH game, we establish a pair of anti-commuting reflections in the strategy for the special player. Then, a quantity called consistency is used to promote this partial rigidity of the special-player stabilizer game to the full rigidity property of the stabilizer game itself. Consistency and another state dependent distance measure of two quantum measurements appeared before in the analysis of nonlocal games and are intensively used in many proofs of this paper.

We then consider the multi-qubit stabilizer game, the nonlocal game version of the stabilizer encoding check in [26]. We prove a partial rigidity theorem for the multi-qubit stabilizer game. This is achieved by establishing the approximate commutativity of reflections corresponding to measurement specifications on different qubits, the proof of which uses the consistency property again in an essential way. Finally, the multi-qubit stabilizer game is performed in the game for the local Hamiltonian problem with high probability to regularize the behavior of the players.

Two additional difficulties arise as the verifier only has limited access to the quantum witness state. First, since the verifier can only enforce Pauli measurements on the witness state, the measurement of the energy of the local Hamiltonian uses Pauli measurements only. This will be less efficient than having the quantum data and measuring directly the POVM corresponding to each term of the Hamiltonian as is done in [26], but there will only be a constant overhead compared to the direct measurement approach.

Second, for convenience, we work with stabilizer codes whose generators are the tensor products of Pauli I, X, Z operators. Alternatively, one may design an extended version of the stabilizer game using ideas from the extended CHSH game proposed in [63] to include Pauli Y operators in the problem. The current form of the stabilizer game is, however, much easier to analyze. As a result, by the rigidity property, the verifier only has access to Pauli X, Z measurements on the quantum witness state. This requires that the Hamiltonian in the local Hamiltonian problem has terms in the real linear span of tensor products of I, X and Z operators. Fortunately, as observed in [13], such a restricted version of the local Hamiltonian problem remains QMA-complete.

1.2 Follow-up work and open problems

There have been several interesting follow-up papers after our manuscript appeared on arXiv. Natarajan and Vidick designed a constant-soundness interactive protocol for the local Hamiltonian problem [56] and later improved their result to achieve robust self-testing for multi-qubit states [57]. The QMA-hardness of nonlocal games has been improved by the author to QMIP^*-completeness (and, hence, NEXP-hardness) in [36].

We briefly mention several related open problems. This paper and the improved results in [36] study the complexity of approximating the nonlocal value to inverse polynomial precision. A natural question to ask is how hard is the constant approximation problem for nonlocal game values. Similarly, one major weakness of our result for the multi-prover interactive proofs with entangled provers in Corollary 1.3 is the exponentially small gap between the completeness and soundness parameters. It is an intriguing and challenging problem to improve this and show, for example, $\mathsf{QMA}_{\mathsf{EXP}}$ is contained in MIP^*.

It is also an interesting question to understand the relationship between the proof checking variant of the quantum PCP conjecture, which asks whether there is a format to encode quantum proofs to allow probabilistic checking, and the multi-player game variant, which asks whether a constant approximation of the nonlocal value is QMA-hard. Our result already demonstrates a connection between Hamiltonian complexity and nonlocal games. But the constant gap will be washed out by the polynomial overhead of the transformation.

1.3 Organization

The rest of the paper is organized as follows. In Section 2, we introduce notation and related concepts used in this paper. Stabilizer games are introduced and analyzed in Section 3. A nonlocal game for the local Hamiltonian problem is given and analyzed in Section 4.

2 Preliminaries

2.1 Concepts and notation

We use calligraphic $\mathcal{H}$ to denote Hilbert spaces, and $\mathrm{D}(\mathcal{H})$, $\mathrm{L}(\mathcal{H})$, $\mathrm{Herm}(\mathcal{H})$, $\mathrm{Pos}(\mathcal{H})$ to denote the set of density operators, bounded linear operators, Hermitian operators and positive semidefinite operators on $\mathcal{H}$. The two-dimensional Hilbert spaces $\mathbb{C}^2$ corresponding to a qubit are denoted by $\mathcal{B}$. For two Hermitian operators $M,N \in \mathrm{Herm}(\mathcal{H})$, we write $M \leq N$ to mean $N - M \in \mathrm{Pos}(\mathcal{H})$. For a matrix M, $|M|$ is defined to be $\sqrt{M^\dagger M}$. For a string x, $|x|$ denotes its length. For a positive integer k, $[k]$ is the abbreviation of the set $\{1,2,\ldots,k\}$. For two complex numbers x, y, we use $x \approx_\varepsilon y$ as a shorthand for $|x-y| \leq O(\varepsilon)$. Two-qubit unitary gates CNOT and SWAP are defined as

$$\mathrm{CNOT}\,|i,j\rangle = |i\rangle|i\oplus j\rangle, \quad \mathrm{SWAP}\,|i,j\rangle = |j,i\rangle,$$

for $i,j \in \{0,1\}$.

Let $\rho \in \mathrm{D}(\mathcal{H})$ be a quantum state on $\mathcal{H}$. For operators $M \in \mathrm{L}(\mathcal{H}), N_0, N_1 \in \mathrm{L}(\mathcal{H},\mathcal{K})$, introduce the following notation:

$$\langle N_0, N_1\rangle = \mathrm{tr}(N_0^\dagger N_1), \tag{2.1a}$$
$$\mathrm{tr}_\rho(M) = \mathrm{tr}(M\rho), \tag{2.1b}$$
$$\langle N_0, N_1\rangle_\rho = \mathrm{tr}_\rho(N_0^\dagger N_1), \tag{2.1c}$$
$$\|N_0\|_\rho = \sqrt{\langle N_0, N_0\rangle_\rho}. \tag{2.1d}$$

It is straightforward to verify that $\langle\cdot,\cdot\rangle_\rho$ is a semi-inner-product, $\|\cdot\|_\rho$ is a seminorm and they become an inner product and a norm, respectively, when ρ is a full-rank state. In particular, the Cauchy-Schwarz inequality holds

$$\left|\langle N_0, N_1\rangle_\rho\right| \leq \|N_0\|_\rho \, \|N_1\|_\rho\,,$$

or more explicitly,

$$\left|\mathrm{tr}_\rho(N_0^\dagger N_1)\right| \leq \left[\mathrm{tr}_\rho(N_0^\dagger N_0)\;\mathrm{tr}_\rho(N_1^\dagger N_1)\right]^{1/2}.$$

For a state $\rho \in \mathrm{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$, and an operator $M \in \mathrm{L}(\mathcal{H}_A)$, we may also write $\mathrm{tr}_\rho(M)$ even though the state ρ and the operator M do not act on the same space. In this case, it is understood that $\mathrm{tr}_\rho(M) = \mathrm{tr}_{\rho_A}(M)$ where ρ_A is the reduced state of ρ on system A. This is one reason that makes $\mathrm{tr}_\rho(\cdot)$ easy to use as it is not necessary to specify the correct reduced state explicitly all the time.

A quantum measurement is described by a collection $M = \{M^a\}$ of measurement operators. These are operators acting on the state space $\mathcal{H}$ of the system being measured. In this paper, we always use superscript to index the measurement outcomes and subscript to index different quantum measurements. The measurement operators satisfy the completeness equation

$$\sum_a (M^a)^\dagger M^a = I.$$

If the state of the system before the measurement is $\rho \in \mathrm{D}(\mathcal{H})$, the probability that outcome a occurs is given by

$$\operatorname{tr}\big((M^a)^\dagger M^a \rho\big) = \|M^a\|_\rho^2\,,$$

and the post-measurement state of the system is

$$\frac{M^a \rho (M^a)^\dagger}{\|M^a\|_\rho^2}.$$

A positive operator valued measure (POVM) is a collection of positive semidefinite operators $\{M^a\}$, such that

$$\sum_a M^a = I.$$

POVMs give descriptions of quantum measurements when the post-measurement state is not important in the analysis. The probability that the measurement has outcome a on state ρ is given by $\operatorname{tr}_\rho(M^a)$.

A projective quantum measurement is described by $\{M^a\}$ where each operator M^a is a projection and $\sum_a M^a = I$. A reflection R is a Hermitian matrix squared to I. It naturally describes a two-outcome projective quantum measurement $\{R^a\}$ where

$$R^a = \frac{I + (-1)^a R}{2},$$

for $a = 0, 1$. The Pauli operators

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},$$

are examples of 2-by-2 reflections. We also use $\sigma_0, \sigma_1, \sigma_2, \sigma_3$ to represent the four Pauli operators. A multi-qubit Pauli operator is of XZ-form if each tensor factor is one of I, X and Z. A Hermitian matrix H is of XZ-form if it is in the real linear span of XZ-form Pauli operators.

Define X' and Z' as

$$X' = \frac{X+Z}{\sqrt{2}}, \qquad Z' = \frac{X-Z}{\sqrt{2}}, \tag{2.2}$$

and W as

$$W = \cos(\pi/8)X + \sin(\pi/8)Z. \tag{2.3}$$

It is easy to verify that W is a reflection and

$$\begin{aligned} X &= WX'W, & X' &= WXW, \\ Z &= WZ'W, & Z' &= WZW. \end{aligned}$$

That is, under the conjugation of W, X' and Z' are mapped to X and Z respectively, and vice versa. The reflections X, Z, X', Z' and W are illustrated in Figure 1. They play an important role in the CHSH game and the stabilizer games introduced in this paper.

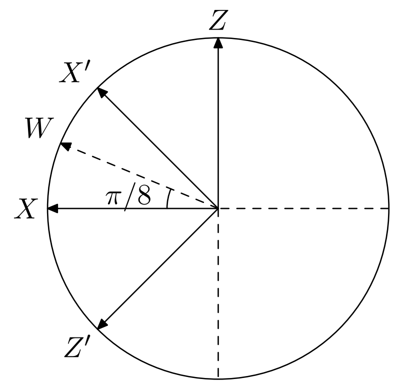

Figure 1: Reflections X, Z, X', Z', W in the x,z-plane of the Bloch sphere.

2.2 Nonlocal games

A multi-player one-round game involves two or more players and a verifier who communicates with the players classically in one round. The verifier samples questions and sends them out to the players and expects to receive answers back. He then decides whether to accept or reject based on the questions and answers. The players are allowed to agree on a strategy before the game starts, but cannot communicate with each other during the game.

Let there be r players, $(1),(2),\ldots,(r)$. Let $\Gamma^{(i)}$ be a finite set of questions for player (i) and $\Lambda^{(i)}$ be a finite set of possible answers from player (i). An r-player game is defined by a distribution π over $\prod_{i=1}^r \Gamma^{(i)}$ and a function $V : \prod_{i=1}^r \Lambda^{(i)} \times \prod_{i=1}^r \Gamma^{(i)} \to [0,1]$, specifying the acceptance probability. By a convexity argument, it suffices to consider the strategy of classical players described by functions $f^{(i)} : \Gamma^{(i)} \to \Lambda^{(i)}$. The value of the strategy is the acceptance probability

$$\omega = \mathop{\mathbb{E}}_{q\sim\pi} V(a(q),q),$$

for $q = (q_1,q_2,\ldots,q_r)$ distributed according to π and $a(q) = \big(f^{(1)}(q_1), f^{(2)}(q_2),\ldots, f^{(r)}(q_r)\big)$. The classical value of the game is the maximum of the values of all classical strategies. An XOR game is a multi-player game in which each player answers a bit a_i and the verifier accepts or rejects depending only on the parity of $\bigoplus_{i=1}^r a_i$. More precisely, there is a function $\hat{V} : \{0,1\} \times \prod_{i=1}^r \Gamma^{(i)} \to [0,1]$ such that

$$V(a,q) = \hat{V}\Big(\bigoplus_{i=1}^r a_i, q\Big),$$

for all $q \in \prod_{i=1}^r \Gamma^{(i)}$, $a \in \prod_{i=1}^r \Lambda^{(i)}$. In most of the games considered in this paper, the verifier accepts or rejects only depending on the parity of some, not all, of the answer bits. We call them generalized XOR games.

In a nonlocal game, the players are allowed to share an arbitrary entangled state before the game starts. A quantum strategy $\mathcal{S}$ for the nonlocal game is described by the shared state ρ, and the measurements

$\{M_{q_i}^{(i)}\}$ that player (i) performs when the question is $q_i \in \Gamma^{(i)}$. The value of the strategy is defined as

$$\omega^*(\mathcal{S}) = \mathop{\mathbb{E}}_{q\sim\pi} \sum_a \Big[\mathrm{tr}_\rho \big(\bigotimes_{i=1}^r M_{q_i}^{(i),a_i} \big) V(a,q) \Big],$$

for $a = (a_1, a_2, \ldots, a_r)$ and $q = (q_1, q_2, \ldots, q_r)$. The nonlocal value of the game is the supremum of the values of all quantum strategies.

The CHSH game [17] is arguably one of the most important nonlocal games. It arises from the study of fundamental questions in quantum mechanics such as entanglement and nonlocality via Bell inequalities [10]. The CHSH game is a two-player XOR game. The verifier samples two bits q_1 and q_2 independently and uniformly at random, sends q_1 to the first player and q_2 to the second player. The verifier accepts if and only if two answer bits a_1 and a_2 satisfy $a_1 \oplus a_2 = q_1 \wedge q_2$. The classical value of the game is $3/4 = 0.75$ and the nonlocal value of the game is $\omega^*_{\mathrm{CHSH}} = (2+\sqrt{2})/4 \approx 0.85$ [66].

In an optimal strategy for the CHSH game, the players share an EPR state $(|00\rangle + |11\rangle)/\sqrt{2}$, and the first player obtains the answer by measuring X (or Z) if the question is 0 (or 1 respectively), while the second player measures X' (or Z') in Equation (2.2) if the question is 0 (or 1). The rigidity property of the CHSH game roughly states that this is essentially the only strategy for the players to achieve the nonlocal value, up to local isometries. Furthermore, any strategy that has a value close to the game value must be close to this optimal strategy in some sense. Rigidity of the CHSH game and other nonlocal games has found interesting applications in certifiable randomness generation (e. g., [20, 61, 68, 55]), device-independent quantum cryptography (e. g., [1, 69, 55]) and classical command of quantum systems [63].

2.3 Quantum proofs and local Hamiltonian problems

The idea of efficient proof verification of NP has a natural quantum generalization given in the following definition.

Definition 2.1. The complexity class QMA is the set of promise problems $L = (L_{\mathrm{yes}}, L_{\mathrm{no}})$ such that there is a polynomial $p(\cdot)$ and a quantum polynomial-time verifier V, and

- *Completeness.* If $x \in L_{\mathrm{yes}}$, there exists a state $|\psi\rangle$ of $p(|x|)$ qubits such that

$$\Pr\big[V \text{ accepts } |x\rangle \otimes |\psi\rangle\big] \geq \frac{2}{3},$$

- *Soundness.* If $x \in L_{\mathrm{no}}$, then for all state $|\psi\rangle$ of $p(|x|)$ qubits,

$$\Pr\big[V \text{ accepts } |x\rangle \otimes |\psi\rangle\big] \leq \frac{1}{3}.$$

Definition 2.2 (Local Hamiltonian Problem)**.** An instance of the k-local Hamiltonian problem of n-qubits is described by the tuple (H, a, b), where the Hamiltonian $H = \sum_{j=1}^m H_j$ and each term H_j acts non-trivially on at most k qubits, H_j is positive semidefinite and $\|H_j\| \leq 1$, $a, b \in \mathbb{R}$ are numbers satisfying $b - a \geq 1/\mathrm{poly}(n)$. Let the ground state energy of the Hamiltonian H be $\lambda_{\min} = \min_{\rho\in\mathrm{D}} \langle H, \rho\rangle$. In the k-local Hamiltonian problem, (H, a, b) is a yes-instance if $\lambda_{\min} \leq am$ and a no-instance if $\lambda_{\min} \geq bm$.

The quantum analog of the Cook-Levin theorem by Kitaev states that the k-local Hamiltonian problem is QMA-complete for $k \geq 5$ [41, 4]. This was later improved to 2-local and more physical Hamiltonians in a series of articles (see e. g., [39, 58, 22]).

2.4 Quantum error correction and stabilizer formalism

A quantum error correcting code encodes a number of qubits, called the logical qubits, into a larger number of physical qubits with the aim of protecting the quantum information in the logical qubits from certain types of noise.

The stabilizer formalism provides a convenient language and a great number of examples of quantum error correcting codes. We present several relevant definitions and facts about stabilizer codes and refer the reader to the thesis of Gottesman [30] for more details. Let $\mathcal{P}_r$ be the group generated by the r-fold tensor product of Pauli operators

$$\mathcal{P}_r = \left\{ \mathrm{e}^{i\phi} \bigotimes_{j=1}^{r} P_j, \text{ for } \phi \in \{0, \pi/2, \pi, 3\pi/2\}, \ P_j \in \{I, X, Y, Z\} \right\}.$$

A stabilizer $\mathfrak{S}$ is an abelian subgroup of $\mathcal{P}_r$ not containing $-I^{\otimes r}$. The stabilizer provides a succinct description of a subspace of $(\mathbb{C}^2)^{\otimes r}$, the simultaneous $+1$-eigenspace of the operators in $\mathfrak{S}$. This subspace is called the code space of the stabilizer. A set of operators in $\mathfrak{S}$ is called the a set of generators of $\mathfrak{S}$ if they generate the group $\mathfrak{S}$.

The weight of an operator in $\mathcal{P}_r$ is the number of non-identity tensor factors in it. Let $C(\mathfrak{S})$ be the centralizer of $\mathfrak{S}$ in $\mathcal{P}_r$, the set of operators in $\mathcal{P}_r$ that commutes with $\mathfrak{S}$. The distance of the stabilizer code is d if there is no operator of weight less than d in $C(\mathfrak{S}) - \mathfrak{S}$. The logical X and Z operators L_X and L_Z are a pair of anti-commuting operators in $C(\mathfrak{S}) - \mathfrak{S}$.

As a simple example, the operators XX and ZZ generate a stabilizer for the EPR state. The famous five-qubit code [46, 12] has a stabilizer representation given in Figure 2a. The five-qubit code encodes one logical qubit in five physical qubits and has distance 3. The logical X and Z operators are $X^{\otimes 5}$ and $Z^{\otimes 5}$. This will be the stabilizer code we use most of the time as an example. Operators $X^{\otimes 4}$ and $Z^{\otimes 4}$ generate the stabilizer for the four-qubit quantum error detecting code. It has distance 2 and encodes two qubits. The operators $XXII$ and $ZIZI$ form a pair of anti-commuting operators and can serve as the logical X and Z operators. There is another pair of logical operators for the other encoded qubit that we do not use.

2.5 State-dependent distance measures of quantum measurements

We introduce a distance measure and a consistency measure of quantum measurements that will be helpful in our treatment of nonlocal games. They grew out of the study of nonlocal games [31, 32, 70] and may be useful in more general contexts. A common feature of them is that they are both state-dependent.

A general question that one usually faces is what the consequences are if a measurement $\{M_1^a\}$ is used in place of $\{M_0^a\}$ in a nonlocal game by one of the players. Will it change the overall analysis significantly? More concretely, suppose that the state of a joint quantum system $\mathcal{H}_A$ and $\mathcal{H}_B$ is ρ and that

$\{M_0^a\}$, $\{M_1^a\}$ are quantum measurements on system A. The post-measurement states are

$$\rho_i = \sum_a |a\rangle\langle a| \otimes M_i^a \rho (M_i^a)^\dagger, \tag{2.4}$$

for $i = 0,1$, respectively, depending on which measurement is performed. By the monotonicity of the trace distance, the difference will be bounded by $D_{\mathrm{tr}}(\rho_0,\rho_1)$ no matter what operation follows the measurement. In particular, in a nonlocal game, if Bob measures on his system $\mathcal{H}_B$ and then the verifier makes the decision, the acceptance probabilities will differ by at most $D_{\mathrm{tr}}(\rho_0,\rho_1)$.

The quantity defined next provides a way to bound the distance $D_{\mathrm{tr}}(\rho_0,\rho_1)$.

Definition 2.3. For two quantum measurements $M_i = \{M_i^a\}$ with $i = 0,1$ that have the same set of possible outcomes, define

$$d_\rho(M_0,M_1) = \Big[\sum_a \|M_0^a - M_1^a\|_\rho^2\Big]^{1/2}. \tag{2.5}$$

More explicitly,

$$d_\rho(M_0,M_1) = \Big[2 - 2\,\mathrm{Re}\sum_a \mathrm{tr}_\rho\big((M_0^a)^\dagger M_1^a\big)\Big]^{1/2}. \tag{2.6}$$

Lemma 2.4. *Let $M_i = \{M_i^a\}$ for $i = 0,1$ be two quantum measurements with the same set of possible outcomes, and ρ_i be the post-measurement states in Equation (2.4). Then*

$$D_{\mathrm{tr}}(\rho_0,\rho_1) \le d_\rho(M_0,M_1).$$

Proof. Let $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$ be a purification of ρ. Then

$$\begin{aligned}
D_{\mathrm{tr}}(\rho_0,\rho_1) &\le D_{\mathrm{tr}}\big(\sum_a |a\rangle \otimes (M_0^a|\psi\rangle), \sum_a |a\rangle \otimes (M_1^a|\psi\rangle)\big)\\
&= \Big[1 - \Big|\sum_a \langle\psi|(M_0^a)^\dagger M_1^a|\psi\rangle\Big|^2\Big]^{1/2}\\
&\le \Big[2\Big(1 - \Big|\sum_a \langle\psi|(M_0^a)^\dagger M_1^a|\psi\rangle\Big|\Big)\Big]^{1/2}\\
&\le \Big[2 - 2\,\mathrm{Re}\sum_a \mathrm{tr}_\rho\big((M_0^a)^\dagger M_1^a\big)\Big]^{1/2}\\
&= d_\rho(M_0,M_1).
\end{aligned}$$

The first inequality follows from the monotonicity of the trace distance. The second line follows by a direct calculation of the trace distance for two pure states. The third line is from $1-x^2 \le 2(1-x)$ for $x \in [0,1]$. □

As discussed above, a direct corollary of the above lemma is that when measurement M_0 is replaced with M_1 in a strategy for a nonlocal game using shared state ρ, the acceptance probability change by at most $d_\rho(M_0,M_1)$. This claim works for all types of quantum measurements including the general quantum measurement, POVMs, projective quantum measurements and binary projective measurements described by reflections.

For $M_i = \{M_i^a\}$, $i = 0, 1$, describing two POVMs that satisfy $\sum_a M_i^a = I$, we define the corresponding distance as

$$d_\rho(M_0, M_1) = \inf_{N_i = \{N_i^a\}} d_\rho(N_0, N_1),$$

where the infimum is taken over all possible measurement operators N_i^a such that $M_i^a = (N_i^a)^\dagger N_i^a$. The inclusion of all possible measurement operators in the definition makes it technically easier to establish upper bounds on the distance. For projective measurements $M_i = \{M_i^a\}$, define

$$d_\rho(M_0, M_1) = \left[2 - 2\,\mathrm{Re} \sum_a \mathrm{tr}_\rho \left(M_0^a M_1^a\right)\right]^{1/2}.$$

Finally, for reflections R_0, R_1, let

$$R_i^a = \frac{I + (-1)^a R_i}{2}$$

be the projective measurement operators corresponding to R_i. Define

$$\begin{aligned} d_\rho(R_0, R_1) &= d_\rho(\{R_0^a\}, \{R_1^a\}) \\ &= \left[2 - 2\,\mathrm{Re} \sum_a \mathrm{tr}_\rho \left(\frac{I + (-1)^a R_0}{2} \frac{I + (-1)^a R_1}{2}\right)\right]^{1/2} \\ &= \left[1 - \mathrm{Re}\ \mathrm{tr}_\rho \left(R_0 R_1\right)\right]^{1/2}. \end{aligned}$$

It is easy to verify that d_ρ satisfies the triangle inequality.

Lemma 2.5. *Let M_0, M_1, M_2 be three measurements on state ρ. Then*

$$d_\rho(M_0, M_2) \leq d_\rho(M_0, M_1) + d_\rho(M_1, M_2).$$

The next important quantity measures the consistency of two quantum measurements.

Definition 2.6. Let $\rho \in \mathrm{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$ be the shared state between system A and B, let $M = \{M^a\}$, $N = \{N^a\}$ be POVMs on system A and B respectively having the same set of possible outcomes. Define the consistency of M, N on state ρ as

$$C_\rho(M, N) = \sum_a \mathrm{tr}_\rho (M^a \otimes N^a). \tag{2.7}$$

M and N are called ε-consistent on state ρ if $C_\rho(M, N) \geq 1 - \varepsilon$.

For two reflections R, S, let $\{R^a\}$, $\{S^a\}$ be their corresponding projective measurements. Define

$$C_\rho(R, S) = C_\rho(\{R^a\}, \{S^a\}) = \frac{1 + \mathrm{tr}_\rho (R \otimes S)}{2}. \tag{2.8}$$

The condition $\operatorname{tr}_\rho(R \otimes S) \approx_\varepsilon 1$, or equivalently, R, S are $O(\varepsilon)$-consistent on ρ, can be thought of as a quantitative way of saying that ρ is approximately stabilized by $R \otimes S$.

The consistency of measurements puts strong structural constraints on the strategies of nonlocal games. It will be a key ingredient in our proof of the main result. In the following lemma, it is proved that if two measurements M_0, M_1 are consistent with the same measurement N, then M_0, M_1 must be close to each other in terms of the distance d_ρ.

Lemma 2.7. *Let $\rho \in \mathrm{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$ be a state on system A and B. Let $M_i = \{M_i^a\}$ for $i = 0, 1$ be POVMs on system A, $N = \{N^a\}$ be a POVM on system B. If*

$$C_\rho(M_i, N) \geq 1 - \varepsilon,$$

for $i = 0, 1$, then

$$d_\rho(M_0, M_1) \leq O(\sqrt{\varepsilon}).$$

Proof. First prove that

$$\sum_a \operatorname{tr}_\rho \left[\left(1 - \sqrt{M_0^a}\right)\left(1 - \sqrt{M_1^a}\right) \otimes N^a \right] \approx_\varepsilon 0. \tag{2.9}$$

By the Cauchy-Schwarz inequality, the absolute value of the left hand side is at most

$$\begin{aligned}
&\sum_a \sqrt{\operatorname{tr}_\rho \left[\left(1 - \sqrt{M_0^a}\right)^2 \otimes N^a \right] \operatorname{tr}_\rho \left[\left(1 - \sqrt{M_1^a}\right)^2 \otimes N^a \right]} \\
&\leq \sum_a \sqrt{\operatorname{tr}_\rho \left[\left(1 - M_0^a\right) \otimes N^a \right] \operatorname{tr}_\rho \left[\left(1 - M_1^a\right) \otimes N^a \right]} \\
&\leq \sqrt{\sum_a \operatorname{tr}_\rho \left[\left(1 - M_0^a\right) \otimes N^a \right] \sum_a \operatorname{tr}_\rho \left[\left(1 - M_1^a\right) \otimes N^a \right]} \\
&\leq \varepsilon,
\end{aligned}$$

where the first inequality follows from the fact that $(1 - \sqrt{x})^2 \leq 1 - x$ for $x \in [0, 1]$, the second inequality is another Cauchy-Schwarz inequality and the last inequality follows from the condition that $C_\rho(M_i, N) \geq 1 - \varepsilon$.

Similarly, by using the Cauchy-Schwarz inequality twice, we have

$$\sum_a \operatorname{tr}_\rho \left[\sqrt{M_0^a}\sqrt{M_1^a} \otimes \left(1 - N^a\right) \right] \approx_\varepsilon 0. \tag{2.10}$$

Adding Equations (2.9) and (2.10) gives

$$\begin{aligned}
\sum_a \operatorname{tr}_\rho \left[\sqrt{M_0^a}\sqrt{M_1^a} \right] &\approx_\varepsilon \sum_a \operatorname{tr}_\rho \left[\sqrt{M_0^a} \otimes N^a \right] + \sum_a \operatorname{tr}_\rho \left[\sqrt{M_1^a} \otimes N^a \right] - 1 \\
&\approx_\varepsilon 1 + 1 - 1 = 1.
\end{aligned}$$

The lemma follows by the definition of d_ρ for POVMs. $\square$

In the analysis, it is useful to have a quantity characterizing the approximate commutativity of two projective measurements $M = \{M^a\}$ and $N = \{N^a\}$ on a state ρ. The quantity we choose is

$$\sum_a \|[M^a, N^a]\|_\rho^2 .$$

For reflections R, S, let $\{R^a\}$ and $\{S^a\}$ be the projective measurements corresponding to R and S respectively. The commutativity of these two measurements on state ρ is

$$\begin{aligned}\sum_{a\in\{0,1\}} \|[R^a, S^a]\|_\rho^2 &= \sum_{a\in\{0,1\}} \left\| \left[\frac{I + (-1)^a R}{2}, \frac{I + (-1)^a S}{2} \right] \right\|_\rho^2 \\ &= \frac{1}{8} \|[R,S]\|_\rho^2 .\end{aligned}$$

For this reason, $\|[R,S]\|_\rho^2$ equivalently serves as a bound on the approximate commutativity of the two projective measurements defined by R, S.

3 Stabilizer games and rigidity

3.1 CHSH game revisited

Before introducing stabilizer games, it is beneficial to revisit the CHSH game in the stabilizer formalism.

Recall that the EPR state $|\Phi\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ is a stabilizer state defined by two generators $g_1 = XX$ and $g_2 = ZZ$, and the eigenstate of eigenvalue 2 of the operator $g_1 + g_2$. If a verifier has trusted measuring devices, it suffices to perform the projective measurements associated with the reflections g_1, g_2 to check whether the state is an EPR state. However, this simple measurement setting does not correspond to any non-trivial schemes that allow device-independent certification of the EPR state.

In the CHSH game, one of the two players is asked to measure her share of $|\Phi\rangle$ with X, Z, while the other is asked to measure X', Z' in Equation (2.2), the $\pi/4$ rotated versions of X, Z. This motivates us to consider the generators $g_1' = XX'$ and $g_2' = ZZ'$. By the conjugation relation of X, Z and X', Z', they generate a stabilizer for the state $|\Phi'\rangle = I \otimes W |\Phi\rangle$ and

$$\left\langle \Phi' \middle| \sum_{i=1}^{2} g_i' \middle| \Phi' \right\rangle = 2. \tag{3.1}$$

Expanding X' and Z' in g_1' and g_2' using X and Z gives four operators

$$h_1 = XX, \quad h_2 = XZ, \quad h_3 = ZX, \quad h_4 = -ZZ, \tag{3.2}$$

such that $h_1 + h_2 = \sqrt{2} g_1'$ and $h_3 + h_4 = \sqrt{2} g_2'$. The four operators h_i in Equation (3.2) recover exactly the CHSH game by encoding the Pauli operators X, Z in h_i as questions $0, 1$ and the sign ± 1 of h_i as the expected parity of answers. Equation (3.1) becomes

$$\left\langle \Phi' \middle| \sum_{i=1}^{4} h_i \middle| \Phi' \right\rangle = 2\sqrt{2},$$

which is an explanation of the $\sqrt{2}$ quantum advantage in the CHSH game.

3.2 Special-player stabilizer game

In this section, we introduce stabilizer games with a special player. The construction works with any non-trivial stabilizer code that has a set of generators all in the tensor product form of I, X, Z.

Consider the generators of the stabilizer group for the five-qubit quantum code in Figure 2a. Its code space is the two-dimensional eigenspace of eigenvalue 4 of the operator $\sum_{j=1}^{4} g_j$, where the g_j operators are defined in Figure 2a.

Name	Operator
g_1	$IXZZX$
g_2	$XIXZZ$
g_3	$ZXIXZ$
g_4	$ZZXIX$

(a) Standard generators

Name	Operator
g'_1	$IXZZX'$
g'_2	$XIXZZ'$
g'_3	$ZXIXZ'$
g'_4	$ZZXIX'$

(b) Generators with the last qubit rotated.

Figure 2: Stabilizer generators for the five-qubit code.

Motivated by the CHSH game, we apply the $\pi/4$-trick to the last column of the four generators in Figure 2a. That is, we replace X and Z in the last column with X' and Z' in Equation (2.2). This gives us another set of generators, as in Figure 2b, which generates the stabilizer for the five-qubit code with the last qubit rotated by the single-qubit unitary W in Equation (2.3). If $|\psi\rangle$ is in the code space of the five-qubit code, the state

$$|\psi'\rangle = (I \otimes W)|\psi\rangle \tag{3.3}$$

is in the eigenspace of $\sum_{j=1}^{4} g'_j$ with eigenvalue 4.

Expanding the primed X, Z operators in each of the generators in Figure 2b into X, Z, we get a set of eight operators h_j as in Figure 3a. For state $|\psi'\rangle$ in Equation (3.3),

$$\left\langle \psi' \right| \sum_{j=1}^{8} h_j \left| \psi' \right\rangle = 4\sqrt{2}. \tag{3.4}$$

The table in Figure 3b is obtained by translating the operators I, X, Z in Figure 3a to the questions in the alphabet of $*, 0, 1, 2, 3$. The I operator is always translated to $*$, which denotes a null question. The verifier will not send anything to the player and does not expect any answers if the question is the null question $*$. For convenience, we sometimes assume that the verifier will replace $*$ with either 0 or 1 as the question and ignore the answers corresponding to this question. The operators X, Z are translated to 0, 1 respectively in the first four columns and to 2, 3 respectively in the last column. One can of course also use 0, 1 in the last column and the change is only for later convenience. Finally, the parity column is read off from the ± 1 signs in the h_i operators.

The table in Figure 3b specifies a five-player game in Figure 4 called the *Special-Player Stabilizer Game*. In the game, the verifier randomly selects four players each time, asks a question encoded with a single bit and expects a single bit answer. He accepts or rejects depending on the parity of the answers received. The fifth player is special because of the $\pi/4$-rotation applied on the fifth column of the

Name	Operator
h_1	$IXZZX$
h_2	$IXZZZ$
h_3	$XIXZX$
h_4	$-XIXZZ$
h_5	$ZXIXX$
h_6	$-ZXIXZ$
h_7	$ZZXIX$
h_8	$ZZXIZ$

(a) Eight operators obtained from Figure 2b.

Parity	Question
0	$*$ 0 1 1 2
0	$*$ 0 1 1 3
0	0 $*$ 0 1 2
1	0 $*$ 0 1 3
0	1 0 $*$ 0 2
1	1 0 $*$ 0 3
0	1 1 0 $*$ 2
0	1 1 0 $*$ 3

(b) The table for the game with a special player.

Figure 3: Translation from measurement operators to game specifications.

stabilizer generators. This breaks the translation invariance of the five-qubit code and, in the honest strategy, the fifth player performs differently from other players.

Special-Player Stabilizer Game

Let $s_1, \dots, s_8$ be the eight entries in the parity column of Figure 3b and let $w_j = (w_{j,i})$ be the j-th row of the question column. The verifier does the following:

1. Select an index $j \in [8]$ uniformly at random.
2. For $i \in [5]$, send $w_{j,i}$ in Figure 3b to the player (i) if $w_{j,i}$ is not $*$, the null question.
3. Receive a bit $a^{(i)}$ from player (i) if she was asked a question.
4. Accept if and only if the parity of the answers $\bigoplus_i a^{(i)}$ equals s_j.

Figure 4: Special-player stabilizer game for the five-qubit code. The fifth player is the special player.

It turns out that the special-player stabilizer game in Figure 4 has nonlocal value

$$\omega^*_{\mathrm{SPS}} = \frac{2+\sqrt{2}}{4}, \tag{3.5}$$

the same as that of the CHSH game. The following strategy achieves the value. The five players share the state $|\psi'\rangle$ as in Equation (3.3) and measure X (or Z) if the question is even (or odd, respectively) and reply with the outcome. Let $h_{j,i}$ be the i-th Pauli operator of h_j. The value this strategy achieves is

$$\begin{aligned}\omega^*_{\mathrm{SPS}} &= \mathop{\mathbb{E}}_{j} \frac{1+(-1)^{s_j}\langle\psi'|\left(\bigotimes_{i=1}^5 h_{j,i}\right)|\psi'\rangle}{2} \\ &= \frac{1+\mathbb{E}_j\langle\psi'|h_j|\psi'\rangle}{2},\end{aligned} \tag{3.6}$$

which gives the desired value using Equation (3.4). It is beneficial to restate the above optimal strategy using $|\psi\rangle$ instead of $|\psi'\rangle$. By the conjugation relation between X, Z and X' and Z', the fifth player essentially measures X' and Z' on the state $|\psi\rangle$ in the code space when the question is $2,3$ respectively. If we think of questions $0,1,2,3$ as measurement specifications of X, Z, X', Z', then players who honestly follow the measurement instructions on an encoded state have acceptance probability ω^*_{SPS}. We mention without proof that the classical value of the game is $3/4$, again the same as that of the CHSH game.

We have seen a strategy for the game with value $(2+\sqrt{2})/4$. The fact that this value is optimal is given in the following theorem. The theorem also proves an important structural result about strategies that almost achieve the nonlocal value of the game. Namely, the special player (the fifth player) must measure honestly the X' and Z' measurements up to an isometry. It is a partial rigidity property of the special-player stabilizer games. It will be technically convenient to apply Naimark's theorem and assume without loss of generality that the measurement operators considered in this paper are projective and have the same rank. By this assumption, it suffices to consider players that use *traceless* reflections in their strategies.

Theorem 3.1. *Let $\mathcal{S} = \big(\rho, \{R_w^{(i)}\}\big)$ be a strategy for the special-player stabilizer game in Figure 4 for the five-qubit code, where ρ is the state shared between the players before the game starts and $R_w^{(i)}$ is the traceless reflection on Hilbert space $\mathcal{H}_i$ describing the projective measurements the player (i) performs when receiving question $w \in \{0,1,2,3\}$. Then the value of the strategy $\mathcal{S}$ is at most ω^*_{SPS} given in Equation (3.5). Furthermore, if the value is at least $\omega^*_{\mathrm{SPS}} - \varepsilon$, then there exists a unitary operator $V \in \mathrm{L}(\mathcal{H}_5, \mathcal{B}\otimes\hat{\mathcal{H}}_5)$ such that $R_3^{(5)} = V^\dagger (Z\otimes I) V$, and*

$$d_\rho\big(R_2^{(5)}, V^\dagger (X\otimes I)V\big) \le O(\sqrt{\varepsilon}).$$

We note that some previous papers use different distance measures for measurements in the statement of rigidity theorem. For example, the quantity $\|(R-S)\otimes I|\psi\rangle\|$ is used in [63] for reflections R, S on state $|\psi\rangle$. It is easy to verify that this is the same as our distance measure $d_\rho(R,S)$ up to a constant for $\rho = |\psi\rangle\langle\psi|$.

The proof of the above theorem relies on the following lemmas.

Lemma 3.2 (Jordan's Lemma [37])**.** *For any two reflections R_0, R_1 acting on a finite dimensional Hilbert space $\mathcal{H}$, there exists a decomposition of $\mathcal{H}$ into orthogonal one- and two-dimensional subspaces invariant under both R_0 and R_1.*

Lemma 3.3. *Let R be a reflection and H be a Hermitian matrix. Then*

$$\big|\mathrm{tr}_\rho(R\otimes H)\big| \le \mathrm{tr}_\rho |H|.$$

Proof. We first prove that

$$\mathrm{tr}_\rho(R\otimes H) \le \mathrm{tr}_\rho |H|.$$

Let H^+ and H^- be the positive and negative part of $H = H^+ - H^-$ for positive semidefinite H^+ and H^-. The claim follows by a direct calculation

$$\begin{aligned} &\mathrm{tr}_\rho(R\otimes H) - \mathrm{tr}_\rho |H| \\ =&\mathrm{tr}_\rho(R\otimes(H^+ - H^-)) - \mathrm{tr}_\rho(I\otimes(H^+ + H^-)) \\ =&-\mathrm{tr}_\rho((I-R)\otimes H^+) - \mathrm{tr}_\rho((I+R)\otimes H^-) \le 0. \end{aligned}$$

A similar argument establishes

$$\operatorname{tr}_\rho(R \otimes H) \geq -\operatorname{tr}_\rho |H|,$$

which completes the proof. ☐

Lemma 3.4. *For $\theta_l \in [0,\pi]$, $C_l = \cos\theta_l$, $S_l = \sin\theta_l$, and any probability distribution over l, if*

$$\mathop{\mathbb{E}}_l \left(\sqrt{1+C_l} - 1\right)^2 \leq \varepsilon,$$

then

$$\mathop{\mathbb{E}}_l S_l \geq 1 - O(\varepsilon).$$

Proof. Let ε_l be $(\sqrt{1+C_l}-1)^2$. Then $\mathbb{E}_l \varepsilon_l \leq \varepsilon$. For each l, $\varepsilon_l \leq 1$. We claim that for all l, $S_l \geq 1 - 9\varepsilon_l$. This will obviously finish the proof.

As

$$-2\sqrt{\varepsilon_l} \leq C_l = \varepsilon_l \pm 2\sqrt{\varepsilon_l} \leq 3\sqrt{\varepsilon_l},$$

it follows that $C_l^2 \leq 9\varepsilon_l$. If $\varepsilon_l \geq 1/9$, the claim is trivial since $\theta_l \in [0,\pi]$ and $S_l \geq 0$. Otherwise,

$$S_l = \sqrt{1-C_l^2} \geq \sqrt{1-9\varepsilon_l} \geq 1 - 9\varepsilon_l.$$ ☐

Proof of Theorem 3.1. We first give an expression of the game value for the strategy $\mathcal{S}$. For each operator h_j in Figure 3a, define $h_j(\mathcal{S})$ as the operator obtained by substituting the X, Z operators in h_j with the players' corresponding reflections in the strategy $\mathcal{S}$. That is

$$h_j(\mathcal{S}) = (-1)^{s_j} \bigotimes_{i=1}^{5} R^{(i)}_{w_{j,i}},$$

where s_j, $w_{j,i}$ are defined in Figure 4 and $R^{(i)}_*$ is defined to be I. Following similar steps as in Equation (3.6), the value of $\mathcal{S}$ is computed as

$$\omega^*(\mathcal{S}) = \frac{1 + \mathbb{E}_j \operatorname{tr}_\rho(h_j(\mathcal{S}))}{2}.$$

Consider four matrices

$$\Delta_1(\mathcal{S}) = I \otimes R_0^{(2)} \otimes R_1^{(3)} \otimes R_1^{(4)} \otimes I - I^{\otimes 4} \otimes \frac{R_2^{(5)} + R_3^{(5)}}{\sqrt{2}}, \tag{3.7a}$$

$$\Delta_2(\mathcal{S}) = R_0^{(1)} \otimes I \otimes R_0^{(3)} \otimes R_1^{(4)} \otimes I - I^{\otimes 4} \otimes \frac{R_2^{(5)} - R_3^{(5)}}{\sqrt{2}}, \tag{3.7b}$$

$$\Delta_3(\mathcal{S}) = R_1^{(1)} \otimes R_0^{(2)} \otimes I \otimes R_0^{(4)} \otimes I - I^{\otimes 4} \otimes \frac{R_2^{(5)} - R_3^{(5)}}{\sqrt{2}}, \tag{3.7c}$$

$$\Delta_4(\mathcal{S}) = R_1^{(1)} \otimes R_1^{(2)} \otimes R_0^{(3)} \otimes I \otimes I - I^{\otimes 4} \otimes \frac{R_2^{(5)} + R_3^{(5)}}{\sqrt{2}}. \tag{3.7d}$$

In the following, we write them as Δ_l and hide their dependence on the strategy $\mathcal{S}$ when there is no ambiguity. The sum-of-squares of the four matrices is

$$\sum_{l=1}^{4} \Delta_l^2 = 8I - \sqrt{2}\sum_j h_j(\mathcal{S}).$$

This gives the following expression for the game value

$$\omega^*(\mathcal{S}) = \frac{1}{2} + \frac{8\sqrt{2} - \sqrt{2}\sum_{l=1}^{4} \operatorname{tr}_\rho(\Delta_l^2)}{32},$$

from which the optimality of ω^*_{SPS} is obvious. It also implies that for any strategy $\mathcal{S}$ having value at least $\omega^*_{\mathrm{SPS}} - \varepsilon$,

$$\operatorname{tr}_\rho(\Delta_1^2) \le \sum_{l=1}^{4} \operatorname{tr}_\rho(\Delta_l^2) \le O(\varepsilon). \tag{3.8}$$

We remark that the definition of the matrices Δ_l and the sum of square conditions are motivated by similar analysis for the CHSH rigidity in [63] and are generalized here to the four-player stabilizer game.

For simplicity, let R_2 and R_3 be shorthand for $R_2^{(5)}$ and $R_3^{(5)}$ for the remainder of the proof. Following a similar truncation argument as in [63], we may assume without loss of generality that the underlying Hilbert spaces of the players are finite dimensional so that Jordan's Lemma applies. By Jordan's lemma, one obtains simultaneous 2-by-2 block diagonalizations of R_2 and R_3 such that each 2-by-2 block is a reflection having both ± 1 eigenvalues. Hence, there is a unitary operator $V \in \mathrm{L}(\mathcal{H}_5, \mathcal{B} \otimes \hat{\mathcal{H}}_5)$ such that

$$R_3 = V^\dagger (Z \otimes I) V,$$

and

$$R_2 = V^\dagger \sum_l \left[\begin{pmatrix} C_l & S_l \\ S_l & -C_l \end{pmatrix} \otimes |l\rangle\langle l| \right] V,$$

where $C_l = \cos\theta_l, S_l = \sin\theta_l$ for $\theta_l \in [0,\pi]$ and l is the index of the two-dimensional invariant subspaces obtained by Jordan's lemma.

Substituting the expression for R_2 and R_3 in Equation (3.8),

$$\begin{aligned}
O(\varepsilon) \ge \operatorname{tr}_\rho(\Delta_1^2) &= 2 + \frac{1}{2}\operatorname{tr}_\rho(R_2R_3 + R_3R_2) + \sqrt{2}\operatorname{tr}_\rho\big(R \otimes (R_2 + R_3)\big) \\
&\ge 2 + \frac{1}{2}\operatorname{tr}_\rho(R_2R_3 + R_3R_2) - \sqrt{2}\operatorname{tr}_\rho |R_2 + R_3| \\
&= 2 + \frac{1}{2}\operatorname{tr}_{\tilde\rho}\left[\sum_l \begin{pmatrix} 2C_l & 0 \\ 0 & 2C_l \end{pmatrix} \otimes |l\rangle\langle l|\right] - 2\operatorname{tr}_{\tilde\rho}\big(\sum_l \sqrt{1+C_l}\, I \otimes |l\rangle\langle l|\big) \\
&= \mathop{\mathbb{E}}_l (\sqrt{1+C_l} - 1)^2,
\end{aligned} \tag{3.9}$$

where R is the reflection $I \otimes R_0^{(2)} \otimes R_1^{(3)} \otimes R_1^{(4)}$, the second line follows from Lemma 3.3, $\tilde\rho = V\rho V^\dagger$, and the expectation $\mathbb{E}_l$ is over the probability distribution $\Pr(l) = \operatorname{tr}_{\tilde\rho}(I \otimes |l\rangle\langle l|)$.

To complete the proof, consider the state dependent distance between reflections R_2 and $V^\dagger(X\otimes I)V$

$$\begin{aligned} d_\rho\big(R_2, V^\dagger(X\otimes I)V\big) &= \big[1-\operatorname{Re}\operatorname{tr}_\rho\big(R_2V^\dagger(X\otimes I)V\big)\big]^{\frac{1}{2}} \\ &= \big(1-\mathop{\mathbb{E}}_{l} S_l\big)^{\frac{1}{2}}. \end{aligned}$$

This equation and Equation (3.9) together with Lemma 3.4 give the second part in the theorem. $\square$

In the above discussion, the fifth player plays the role of the special player in the game. It is natural to generalize this to a game with player (t) as the special player. The five-qubit code game with special player (t) is the game defined by the table in Figure 3b after a cyclic rotation of the question columns such that the special column becomes the t-th one. This makes use of the translation invariance of the five-qubit code.

For a general r-qubit stabilizer $\mathfrak{S}$ that has a set of XZ-form generators $g_1, g_2, \ldots, g_l$, we need to select two generators $g_X^{(t)}$, $g_Z^{(t)}$ among $g_1, \ldots, g_l$ for each qubit $t\in[r]$ such that $g_X^{(t)}$ has X operator on the t-th qubit and $g_Z^{(t)}$ has Z operator on the t-th qubit. This is possible in most cases as long as the distance of the stabilizer is larger than or equal to 2 and the t-th qubit is not fixed to a pure state for all code states. We call a stabilizer non-trivial if such choices of a pair of generators are possible for all $t\in[r]$. The choice of $g_X^{(t)}$ and $g_Z^{(t)}$ may not be unique, but any such choice will work. To play the special player stabilizer game with special player (t), we follow the procedure in Figure 4 with generators $g_X^{(t)}$ and $g_Z^{(t)}$. Even though the game may not essentially depend on all the generators, the proof of partial rigidity still follows in this general case.

More specifically, for $t\in[r]$, let $g_X^{(t)}$ and $g_Z^{(t)}$ be generators that have X and Z on the t-th qubit respectively. Following the idea in the design of the game for the five-qubit code, define four operators obtained by doing the $\pi/4$-trick on the t-th qubit to this pair of generators

$$h_1^{(t)} = g_X^{(t)}, \quad h_2^{(t)} = g_{X\mapsto Z}^{(t)}, \quad h_3^{(t)} = g_{Z\mapsto X}^{(t)}, \quad h_4^{(t)} = -g_Z^{(t)}, \tag{3.10}$$

where $g_{X\mapsto Z}^{(t)}$ is the operator obtained by changing the X operator of the t-th qubit of $g_X^{(t)}$ to Z and, similarly, $g_{Z\mapsto X}^{(t)}$ is the operator obtained by changing the Z on t-th qubit of $g_Z^{(t)}$ to X.

As in the case for the five-qubit code game, we translate the operators $h_j^{(t)}$ to questions $w_j = (w_{j,i})$ where $w_{j,i}$ is in $\{*,0,1,2,3\}$. Following the translation rule, $w_{j,i}$ is $*$ if the i-th tensor factor of h_j is I. It is 0, 1 if $i\neq t$ and the corresponding tensor factor is X, Z respectively, and it is 2, 3 if $i=t$ and the tensor factor is X, Z respectively. Similarly, define s_j to be 0 or 1 if the sign of $h_j^{(t)}$ is 1 or -1 respectively.

The stabilizer game with special player (t) is the game defined as in Figure 5.

3.3 Stabilizer game

The partial rigidity of the special-player stabilizer game applies only to the measurements performed by the special player. It essentially forces the special player to measure X' and Z' on her system. There are, however, no rigidity results known for the other players' measurements and nothing is proved about the shared state of the strategy. The stabilizer game uses the special-player stabilizer game as a sub-module to achieve the full rigidity properties for all players.

Special-Player Stabilizer Game (General Case)

For a stabilizer $\mathfrak{S}$ with XZ-form generators, let $w_{j,i}$ and s_j be the questions and parities defined by the operators $h_j^{(t)}$ in Equation (3.10) for $j \in [4]$. In the special-player stabilizer game with player (t) as the special player, the verifier performs the following steps:

1. Select an index $j \in [4]$ uniformly at random.
2. For $i \in [r]$, send $w_{j,i}$ in Figure 3b to the player (i) if $w_{j,i}$ is not $*$, the null question.
3. Receive a bit $a^{(i)}$ from player (i) if she was asked a question.
4. Accept if and only if the parity of the answers $\bigoplus_i a^{(i)}$ equals s_j.

Figure 5: Special-player stabilizer game.

The specification of the *Stabilizer Game* is given in Figure 6. It is defined by the r-qubit stabilizer $\mathfrak{S}$ with XZ-form generators. It also implicitly depends on a fixed choice of generators $g_X^{(t)}, g_Z^{(t)}$ for each $t \in [r]$ in order to perform the second test. The game involves r players, each of whom may receive a question of two bits, and is required to answer one bit. The verifier's decision depends only on the parity of some of the answer bits, so that game is a generalized XOR game. In this paper, the number r of qubits of the stabilizer is always assumed to be a constant, and it may be subsumed by the Big-O notation in the rest of the paper.

Stabilizer Game

For an r-qubit non-trivial stabilizer $\mathfrak{S}$ with XZ-form generators $g_1, g_2, \ldots, g_l$, define the stabilizer game of $\mathfrak{S}$ as follows. Let $w_{j,i}$ for $j \in [l]$, $i \in [r]$ be $*$, 0, or 1 if g_j has I, X, or Z on the i-th qubit respectively. Let s_j for $j \in [l]$ be the 0, 1 if the sign of g_j is 1, -1 respectively. The verifier performs the following two tests with equal probability:

1. Select an index $j \in [l]$ uniformly at random. Send $w_{j,i}$ to the player (i) if $w_{j,i} \neq *$. Receives a bit from each player. Accept if the answers not corresponding to the null questions have the same parity as s_j. Reject otherwise.
2. Select $t \in [r]$ uniformly at random. Play the special-player stabilizer game with special player (t) in Figure 5.

Figure 6: Stabilizer game for a stabilizer $\mathfrak{S}$.

The nonlocal value of the game is

$$\omega_{\mathrm{S}}^* = \frac{1+\omega_{\mathrm{SPS}}^*}{2} = \frac{6+\sqrt{2}}{8},$$

which can be achieved by players who share an encoded state of the stabilizer code and measures X, Z, X', Z' when receiving $0,1,2,3$, respectively. This value is easily seen to be optimal as it saturates the winning probability in both tests of the stabilizer game.

The stabilizer game has the following rigidity property. We remark that it is important for us to obtain rigidity not only for the X' and Z' operators but for the X and Z operators as well which are used later to construct the energy checks by the measuring the logical operators of the four qubit code. The error dependence on ε may be improved and we did not try to optimize it as this will not be important for our final result.

Theorem 3.5. *For any non-trivial r-qubit stabilizer with XZ-form generators, the stabilizer game in Figure 6 has the following rigidity property. For any strategy $\mathcal{S}$ of the game specified by Hilbert spaces $\{\mathcal{H}_i\}_{i=1}^r$, a state $\rho \in \mathrm{D}(\bigotimes_{i=1}^r \mathcal{H}_i)$, and traceless reflections $R_w^{(i)}$ on $\mathcal{H}_i$ for $i \in [r]$, $w \in \{0,1,2,3\}$, if the value of the strategy is at least $\omega_{\mathrm{S}}^* - \varepsilon$, then there are unitary operators $V_i \in \mathrm{L}(\mathcal{H}_i, \mathcal{B} \otimes \hat{\mathcal{H}}_i)$ for $i \in [r]$ such that the following properties hold:*

- *For all $i \in [r]$, $R_3^{(i)} = V_i^\dagger (Z' \otimes I) V_i$ and*

$$d_\rho\big(R_2^{(i)}, V_i^\dagger (X' \otimes I) V_i\big) \le O(\varepsilon^{1/2}), \tag{3.11a}$$
$$d_\rho\big(R_1^{(i)}, V_i^\dagger (Z \otimes I) V_i\big) \le O(\varepsilon^{1/4}), \tag{3.11b}$$
$$d_\rho\big(R_0^{(i)}, V_i^\dagger (X \otimes I) V_i\big) \le O(\varepsilon^{1/4}), \tag{3.11c}$$

  where X', Z' are defined in Equation (2.2).

- *Let Π be the projection to the code space of the stabilizer code of $\mathfrak{S}$, and let V be the unitary operator $\bigotimes_{i=1}^r V_i$. It holds that*

$$\big\langle \Pi \otimes I, V \rho V^\dagger \big\rangle \ge 1 - O(\varepsilon^{1/4}),$$

  where Π acts on the r qubits, each of which is the first qubit of each player after the application of V.

Proof. By the symmetry of the game, it suffices to prove the statement for one of the players, say, the player (r). For simplicity, use R_w to represent the reflection $R_w^{(r)}$ of player (r). It is easy to see that strategy $\mathcal{S}$ wins the special-player stabilizer game of special player (r) with probability $\omega_{\mathrm{SPS}}^* - O(\varepsilon)$. By Theorem 3.1, there exists a unitary operator V such that $R_3 = V^\dagger (Z \otimes I) V$ and

$$d_\rho\big(R_2, V^\dagger (X \otimes I) V\big) \le O(\varepsilon^{1/2}).$$

Taking $V_r = (W \otimes I) V$, we get the first two conditions in the first item of the theorem, where W is the reflection defined in Equation (2.3).

Next, we prove the claim in Equations (3.11b) and (3.11c). For any XZ-form Pauli operator g, define $g(\mathcal{S})$ to be the operator obtained by replacing X with $R_0^{(i)}$ and Z with $R_1^{(i)}$. Let R be the product of the first $r-1$ tensor factors of $g_X^{(r)}(\mathcal{S})$. Here, $g_X^{(r)}$ is the chosen generator that has X on the r-th qubit in the stabilizer game with special player (r). As the strategy $\mathcal{S}$ has value at least $\omega_{\mathrm{S}}^* - \varepsilon$, it has value at least $1-O(\varepsilon)$ for the first test of the stabilizer game, and therefore,

$$\operatorname{tr}_\rho(R\otimes R_0) = \operatorname{tr}_\rho\big(g_X^{(r)}(\mathcal{S})\big) \geq 1-O(\varepsilon). \tag{3.12}$$

In other words, the reflection R_0 is $O(\varepsilon)$-consistent with R on ρ. We emphasize that the reflection R acts on the joint system of the first $r-1$ players. This does not cause any problem as it is only used for our proof and is never actually measured on the joint system.

Consider a new strategy $\hat{\mathcal{S}}$ modified from strategy $\mathcal{S}$ by changing R_2 in the strategy $\mathcal{S}$ to $V_r^\dagger(X'\otimes I)V_r$. This new strategy has value at least $\omega_{\mathrm{S}}^* - O(\sqrt{\varepsilon})$ by Lemma 2.4. Consider the matrix Δ_1 for strategy $\hat{\mathcal{S}}$, as in Equation (3.7),

$$\begin{aligned}\Delta_1(\hat{\mathcal{S}}) &= R\otimes I - I\otimes\Big[V_r^\dagger\big(\frac{X'+Z'}{\sqrt{2}}\otimes I\big)V_r\Big],\\ &= R\otimes I - I\otimes V_r^\dagger(X\otimes I)V_r.\end{aligned}$$

By a similar argument that gives Equation (3.8) and the fact that $\hat{\mathcal{S}}$ has value at least $\omega_{\mathrm{SPS}}^* - O(\sqrt{\varepsilon})$ in the second part of the game, we have

$$\operatorname{tr}_\rho(\Delta_1^2(\hat{\mathcal{S}})) \leq O(\sqrt{\varepsilon}).$$

This gives

$$\operatorname{tr}_\rho(R\otimes V_r^\dagger(X\otimes I)V_r) \geq 1-O(\sqrt{\varepsilon}), \tag{3.13}$$

which proves the $O(\sqrt{\varepsilon})$-consistency of $V_r^\dagger(X\otimes I)V_r$ and R on ρ.

Equations (3.12) and (3.13) and Lemma 2.7 imply that

$$d_\rho\big(R_0, V_r^\dagger(X\otimes I)V_r\big) \leq O(\varepsilon^{1/4}).$$

This completes the proof for Equation (3.11c). A similar argument establishes Equation (3.11b).

Finally, to prove the second item of the theorem, consider a strategy $\tilde{\mathcal{S}}$ that uses the same state ρ and reflections

$$\begin{aligned} R_0^{(i)} &= V_i^\dagger(X\otimes I)V_i, & R_2^{(i)} &= V_i^\dagger(X'\otimes I)V_i,\\ R_1^{(i)} &= V_i^\dagger(Z\otimes I)V_i, & R_3^{(i)} &= V_i^\dagger(Z'\otimes I)V_i.\end{aligned}$$

By Lemma 2.4 and the first part of the theorem, strategy $\tilde{\mathcal{S}}$ has value at least $\omega_{\mathrm{S}}^* - O(\varepsilon^{1/4})$. Hence, it has acceptance probability at least $1-O(\varepsilon^{1/4})$ in the first test of the stabilizer game. This means that

$$\frac{1+\mathbb{E}_j \operatorname{tr}_{\tilde{\rho}}(g_j)}{2} = 1-O(\varepsilon^{1/4}),$$

where j is uniformly random over $[l]$, the g_j operators are the generators of the stabilizer, and $\tilde{\rho} = V^\dagger \rho V$. This is equivalent to

$$\mathrm{tr}_{\tilde{\rho}}\big(\sum_{j=1}^{l} g_j\big) = l - O(\varepsilon^{1/4}). \tag{3.14}$$

Operator $\sum_{j=1}^{l} g_j$ has eigenvalues in $\{-l, -l+2, \ldots, l-2, l\}$ and Π projects to the eigenspace of eigenvalue l. Hence

$$\sum_{j=1}^{l} g_j \leq l\Pi + (l-2)(I-\Pi) = (l-2)I + 2\Pi.$$

This, together with Equation (3.14), implies that

$$\mathrm{tr}_{\tilde{\rho}}(\Pi) = 1 - O(\varepsilon^{1/4}),$$

which is equivalent to the second part of the theorem. □

3.4 Multi-qubit stabilizer game

In this section, we consider a multi-qubit variant of the stabilizer game called the (k,n)-stabilizer game. It is a nonlocal game implementation of the stabilizer check of the Fitzsimons-Vidick protocol [26]. Instead of asking for the qubits and performing an encoding check on them, the verifier sends the measurement instructions on the corresponding qubits to the players. The optimal strategy of the game is to encode each qubit with the stabilizer code and measure X, Z, X' and Z' honestly on the encoded data on corresponding qubits. We prove a partial rigidity theorem for the multi-qubit stabilizer game, which suffices for our purpose. In particular, we only prove the rigidity for the reflections corresponding to questions in $0,1$. The full rigidity properties can be proved with some extra effort. The overall proof idea is similar to that of [26] which extracts the qubits one by one sequentially, but our proof provided here is more modularized.

The (k,n)-stabilizer game is given in Figure 7. For simplicity, we assume in the multi-qubit stabilizer game that, when the question is $*$, the verifier replaces it with either 0 or 1 and ignores the corresponding answer. With this convention, each player will either see a question of the form (u,w) for $u \in [n]$ and $w = 0,1,2,3$ or a tuple of k such questions. Answers are either a single bit or a string of k-bits correspondingly. The verifier accepts or rejects depending on the parity of some of the answer bits.

It is easy to see that the nonlocal value ω^*_{MQS} of the (k,n)-stabilizer game in Figure 7 equals the value of the stabilizer game ω^*_{S}. Let $\mathcal{H}_i$ be the state space of player (i). A strategy for the k-qubit stabilizer game,

$$\mathcal{S} = \big(\rho, \{R_q^{(i)}\}, \{M_{\vec{q}}^{(i)}\}\big),$$

consists of a state $\rho \in \mathrm{D}\big(\bigotimes_{i=1}^{r} \mathcal{H}_i\big)$, reflections $R_q^{(i)}$ the players measure for question q and measurements $M_{\vec{q}}^{(i)}$ with k-bit outcomes for question $\vec{q}$. The superscripts of the measurements indexing the players are sometimes omitted if there will be no ambiguity.

Without loss of generality, it is assumed that the measurements $M_{\vec{q}}$ are projective measurements of the same rank. For each q that occurs as the i-th entry in the tuple $\vec{q}$, define a reflection

$$S_{q|\vec{q}} = \sum_{b \in \{0,1\}^k} (-1)^{b_i} M_{\vec{q}}^{b}.$$

Multi-Qubit Stabilizer Game

Let $\mathfrak{S}$ be a non-trivial r-qubit stabilizer with a set of generators of XZ-form. Let $[n]$ be the index of n qubits and let $k \geq 2$ be a constant. The (k,n)-stabilizer game for $\mathfrak{S}$ is an r-player nonlocal game where the verifier does the following with equal probability:

1. Select a subset $J \subset [n]$ of size k, an index $u \in J$, and a player $t \in [r]$, all uniformly at random. For each qubit $v \in J$, randomly select questions $w_v = (w_{v,i})$, where $w_{v,i} \in \{0,1,2,3\}$ and each w_v is sampled as in the stabilizer game. Define $q_v^{(i)} = (v, w_{v,i})$ for $i \in [r]$ and $v \in J$. Send $q_u^{(i)}$ to player (i) and receive an answer bit $a^{(i)}$ if $i \neq t$. Send $\vec{q} = \left(q_v^{(t)}\right)_{v \in J}$ to player (t), and receive a k-bit string $b = (b_v)_{v \in J}$. Define $a^{(t)} = b_u$ and $a = (a^{(1)}, a^{(2)}, \ldots, a^{(r)})$. The verifier accepts if and only if the verifier for the stabilizer game accepts when the questions are w_u and answers are a.
2. Select a qubit $u \in [n]$ uniformly at random. Play the stabilizer game on qubit u. That is, the verifier samples $w = (w_i)$ as in the stabilizer game. Define $q^{(i)} = (u, w_i)$ for $i \in [r]$. Send $q^{(i)}$ to player (i) and receive an answer bit $a^{(i)}$. The verifier accepts if the verifier for the stabilizer game accepts on questions w and answers $a = (a^{(i)})$.

Figure 7: Multi-qubit stabilizer game.

The reflections R_q and $S_{q|\vec{q}}$ are all traceless. For $\vec{q} = (q_1, q_2, \ldots, q_k)$, the measurement $M_{\vec{q}}$ has a one-to-one correspondence with the collection of k pairwise commuting reflections

$$\left\{S_{q_s|\vec{q}}\right\}_{s=1}^{k},$$

and we refer to these reflections as the reflections associated with the projective measurement $M_{\vec{q}}$. We also write $S_{q|\vec{q}}$ as $S_{u,w|\vec{q}}$ for $q = (u,w)$. On the other hand, for any collection of k pairwise commuting reflections, there associates a projective measurement with k-bit outcome as the repeated application of the two-outcome measurements defined by the reflections.

We prove the following partial rigidity property of the (k,n)-stabilizer game.

Theorem 3.6. *For any constant integer $k \geq 2$, there exists a constant $\kappa > 0$ that depends only on k such that the (k,n)-stabilizer game in Figure 7 has the following rigidity property. For any quantum strategy $\mathcal{S} = \left(\rho, \left\{R_q^{(i)}\right\}, \left\{M_{\vec{q}}^{(i)}\right\}\right)$ that has value at least $\omega_{\mathcal{S}}^* - \varepsilon$, there are isometries $V_i \in \mathrm{L}(\mathcal{H}_i, \mathcal{B}^{\otimes n} \otimes \hat{\mathcal{H}}_i)$, such that the following properties hold*

- *For all $i \in [r]$, all $q = (u,w)$, $q_s = (u_s, w_s)$ with $u \in [n]$, $u_s \in [n]$, $w \in \{0,1\}$, $w_s \in \{0,1\}$, $s \in [k]$, and $\vec{q} = (q_1, q_2, \ldots, q_k)$,*

$$d_\rho\left(R_q^{(i)}, V_i^\dagger D_q V_i\right) \leq O(n^\kappa \varepsilon^{1/\kappa}), \tag{3.15a}$$

$$d_\rho\left(M_{\vec{q}}^{(i)}, N_{\vec{q}}^{(i)}\right) \leq O(n^\kappa \varepsilon^{1/\kappa}), \tag{3.15b}$$

where D_q is the X, Z operator on the u-th qubit for $w = 0,1$ respectively, and $N_{\vec{q}}^{(i)}$ is the measurement that measures D_{q_s} for $s = 1,2,\ldots,k$ sequentially after the application of V_i.

- *Let Π be the projection to the code space of the stabilizer code, V be the isometry $\bigotimes_{i=1}^{r} V_i$, then*

$$\left\langle \Pi^{\otimes n} \otimes I, V\rho V^{\dagger} \right\rangle \geq 1 - O(n^{\kappa}\varepsilon^{1/\kappa}), \tag{3.16}$$

where the t-th tensor factor of $\Pi^{\otimes n}$ acts on r qubits, each of which is the t-th qubit of each player's system after the application of V.

The proof of Theorem 3.6 relies on the following lemmas.

Lemma 3.7. *Let $\rho \in \mathrm{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$ be a state on systems A and B. Let M_0, M_1, N_0, N_1 be four projective measurements on $\mathcal{H}_A$ such that M_1^a, N_1^a commute for all a. Let M, N be two projective measurements on $\mathcal{H}_B$. Suppose that M_0, M_1 are both ε-consistent with M, and N_0, N_1 are both ε-consistent with N on state ρ. Then*

$$\sum_a \| [M_0^a, N_0^a] \|_\rho^2 \leq O(\sqrt{\varepsilon}).$$

Proof. We first prove that

$$\sum_a \mathrm{tr}_\rho \left(M_0^a N_0^a M_0^a N_0^a \right) \approx_{\sqrt{\varepsilon}} \sum_a \mathrm{tr}_\rho \left(N_0^a M_0^a N_0^a M_1^a \right).$$

Namely, we can move operator M_0^a in the front to the end of the product and change it to M_1^a without incurring too much error in the expression.

By ε-consistency between M_0 and M,

$$\sum_a \mathrm{tr}_\rho \left(M_0^a N_0^a M_0^a N_0^a \right) \approx_{\sqrt{\varepsilon}} \sum_a \mathrm{tr}_\rho \left(M_0^a N_0^a M_0^a N_0^a \otimes M^a \right),$$

as the absolute value of the difference on the two sides is

$$\begin{aligned} &\left| \sum_a \mathrm{tr}_\rho \left(M_0^a N_0^a M_0^a N_0^a \otimes (1 - M^a) \right) \right| \\ \leq &\sqrt{\sum_a \mathrm{tr}_\rho \left(M_0^a \otimes (1 - M^a) \right) \sum_a \mathrm{tr}_\rho \left(N_0^a M_0^a N_0^a M_0^a N_0^a \right)} \\ \leq &\sqrt{\varepsilon}. \end{aligned}$$

By similar arguments,

$$\begin{aligned} \sum_a \mathrm{tr}_\rho \left(M_0^a N_0^a M_0^a N_0^a \otimes M^a \right) &\approx_{\sqrt{\varepsilon}} \sum_a \mathrm{tr}_\rho \left(N_0^a M_0^a N_0^a \otimes M^a \right) \\ &\approx_{\sqrt{\varepsilon}} \sum_a \mathrm{tr}_\rho \left(N_0^a M_0^a N_0^a M_1^a \otimes M^a \right) \\ &\approx_{\sqrt{\varepsilon}} \sum_a \mathrm{tr}_\rho \left(N_0^a M_0^a N_0^a M_1^a \right). \end{aligned}$$

This proves our claim about moving and changing M_0^a to M_1^a. We do this for the four operators in the product sequentially,

$$\sum_a \operatorname{tr}_\rho\left(M_0^a N_0^a M_0^a N_0^a\right) \approx_{\sqrt{\varepsilon}} \sum_a \operatorname{tr}_\rho\left(M_1^a N_1^a M_1^a N_1^a\right).$$

Expand the ρ-norm in left-hand side of the claim in the lemma,

$$\sum_a \|[M_0^a, N_0^a]\|_\rho^2 = \sum_a \operatorname{tr}_\rho\left[M_0^a N_0^a M_0^a + N_0^a M_0^a N_0^a - M_0^a N_0^a M_0^a N_0^a - N_0^a M_0^a N_0^a M_0^a\right].$$

Now the proof follows by applying the above operator moving procedure to each of the four terms in the expansion and the condition that M_1^a commutes with N_1^a for all a. □

Lemma 3.8. *Let $\mathcal{B}_1$, $\mathcal{B}_{1'}$, $\mathcal{B}$ be two-dimensional Hilbert spaces. Let $V \in \mathrm{L}(\mathcal{H}, \mathcal{B} \otimes \hat{\mathcal{H}})$ be an isometry, $R \in \mathrm{L}(\mathcal{H})$ be an operator and $|\Phi\rangle$ be the EPR state on $\mathcal{B}_1 \otimes \mathcal{B}_{1'}$. Define isometry $C \in \mathrm{L}(\mathcal{H}, \mathcal{B}_1 \otimes \mathcal{B}_{1'} \otimes \mathcal{H})$ as*

$$C = (I \otimes V^\dagger)\,\mathrm{SWAP}(|\Phi\rangle \otimes V),$$

where the SWAP *acts on $\mathcal{B}_1$ and $\mathcal{B}$. Then*

$$C^\dagger R C = \mathop{\mathbb{E}}_{j=0,1,2,3} \big(V^\dagger \sigma_j V\big) R \big(V^\dagger \sigma_j V\big),$$

where σ_j are Pauli operators.

Proof. This follows by substituting the two SWAP gates using the identity

$$\mathrm{SWAP} = \frac{I + XX + YY + ZZ}{2},$$

and a direct calculation. □

Lemma 3.9. *Let $\rho \in \mathrm{D}(\mathcal{H} \otimes \mathcal{H}')$ be a state, $T \in \mathrm{L}(\mathcal{H})$ be an operator with constant operator norm, R be a reflection on $\mathcal{H}$ that has an ε-consistent reflection S on $\mathcal{H}'$. Then*

$$\operatorname{tr}_\rho(RTR) \approx_{\sqrt{\varepsilon}} \operatorname{tr}_\rho(T).$$

Proof. We first prove that

$$\operatorname{tr}_\rho(RT) \approx_{\sqrt{\varepsilon}} \operatorname{tr}_\rho(T \otimes S). \tag{3.17}$$

By consistency of R and S, we have

$$\begin{aligned}
\operatorname{tr}_\rho(RT) &= \sum_{a\in\{0,1\}} \operatorname{tr}_\rho(R^a (-1)^a T) \\
&\approx_{\sqrt{\varepsilon}} \sum_{a\in\{0,1\}} \operatorname{tr}_\rho(R^a (-1)^a T \otimes S^a) \\
&\approx_{\sqrt{\varepsilon}} \sum_{a\in\{0,1\}} \operatorname{tr}_\rho((-1)^a T \otimes S^a) \\
&= \operatorname{tr}_\rho(T \otimes S).
\end{aligned}$$

Similarly,

$$\mathrm{tr}_\rho(TR) \approx_{\sqrt{\varepsilon}} \mathrm{tr}_\rho(T \otimes S). \tag{3.18}$$

Taking $T = TR$ in Equations (3.17) and (3.18), we have $\mathrm{tr}_\rho(RTR) \approx_{\sqrt{\varepsilon}} \mathrm{tr}_\rho(TR \otimes S)$, and

$$\mathrm{tr}_\rho(T) = \mathrm{tr}_\rho(TRR) \approx_{\sqrt{\varepsilon}} \mathrm{tr}_\rho(TR \otimes S).$$

This completes the proof. □

Lemma 3.10. *Let $M = \{M^a\}$ be a projective measurement having k-bit outcomes on quantum system A and let $R_1, R_2, \ldots, R_k$ be the associated reflections. Let $N = \{N^a\}$ be a projective measurement having k-bit outcomes on quantum system B and let $S_1, S_2, \ldots, S_k$ be its associated reflections. Let $V \in \mathrm{L}(\mathcal{H}_A, \mathcal{H}_B)$ be an isometry and $\rho \in \mathrm{D}(\mathcal{H}_A \otimes \mathcal{H}_C)$ a quantum state. For $i \in [k]$, define $\check{S}_i = V^\dagger S_i V \in \mathrm{Herm}(\mathcal{H}_A)$. Let $\check{N}$ be the quantum measurement that measures N after the application of isometry V.*

If both R_i and $\check{S}_i$ have ε-consistent reflections on $\mathcal{H}_C$ for $i \in [k]$, then

$$d_\rho(M, \check{N}) \le O(\varepsilon^{1/2}).$$

Proof. The measurement $\check{N}$ is a POVM with measurement operators

$$\begin{aligned}\check{N}^a &= V^\dagger \left[\prod_{i=1}^k \frac{I + (-1)^{a_i} S_i}{2}\right] V \\ &= \frac{1}{2^k} \sum_{x \in \{0,1\}^k} (-1)^{\langle a,x\rangle} V^\dagger \left(\prod_{i=1}^k S_i^{x_i}\right) V.\end{aligned}$$

This implies that

$$\begin{aligned}\sum_a \mathrm{Re}\,\mathrm{tr}_\rho(M^a \check{N}^a) &= \frac{1}{2^{2k}} \sum_{a,x,y} (-1)^{\langle a, x\oplus y\rangle} \mathrm{Re}\,\mathrm{tr}_\rho\left[\left(\prod_{i=1}^k R_i^{x_i}\right)\left(V^\dagger \prod_{i=1}^k S_i^{y_i} V\right)\right] \\ &= \frac{1}{2^k} \sum_x \mathrm{Re}\,\mathrm{tr}_\rho\left[\left(\prod_{i=1}^k R_i^{x_i}\right) V^\dagger \left(\prod_{i=1}^k S_i^{x_i}\right) V\right].\end{aligned}$$

In this proof, the superscript of an operator represents the corresponding power of the operator and is not the index for measurement outcome as in the other parts of the paper.

We claim that for all $x \in \{0,1\}^k$, the term in the summand

$$\mathrm{Re}\,\mathrm{tr}_\rho\left[\left(\prod_{i=1}^k R_i^{x_i}\right) V^\dagger \left(\prod_{i=1}^k S_i^{x_i}\right) V\right] \approx_\varepsilon 1.$$

This will conclude the proof by the definition of d_ρ for POVMs by choosing $\{VM^a\}$ and $\{N^a V\}$ as the measurement operators for the two POVMs M and $\check{N}$ respectively.

We prove this claim by an induction on k. For $k=1$, the claim follows from Lemma 2.7 and the consistency conditions. Assume now the claim holds for $k-1$. We have

$$\operatorname{Re}\operatorname{tr}_\rho\left[\Big(\prod_{i=1}^{k} R_i^{x_i}\Big)V^\dagger\Big(\prod_{i=1}^{k-1} S_i^{x_i}\Big)VR_k^{x_k}\right]\approx_\varepsilon 1, \tag{3.19a}$$

$$\operatorname{Re}\operatorname{tr}_\rho\left[\Big(\prod_{i=1}^{k} R_i^{x_i}\Big)V^\dagger\Big(\prod_{i=1}^{k-1} S_i^{x_i}\Big)V\check{S}_k^{x_k}\right]\approx_\varepsilon 1, \tag{3.19b}$$

where the approximations follow from the induction hypothesis, the consistency conditions and the Cauchy-Schwarz inequality. Then, we use the Cauchy-Schwarz inequality again to remove the $VV^\dagger$, and it follows that

$$\operatorname{Re}\operatorname{tr}_\rho\left[\Big(\prod_{i=1}^{k} R_i^{x_i}\Big)V^\dagger\Big(\prod_{i=1}^{k} S_i^{x_i}\Big)V\right]\approx_\varepsilon 1. \qquad\square$$

Proof of Theorem 3.6. Consider first the claim in Equation (3.15a) of the theorem for $i=r$.

In the proof, D_w denotes X, Z for $w=0,1$ respectively, and D_q denotes D_w acting on the u-th qubit if $q=(u,w)$. Let δ be $n\varepsilon$ and δ_k be $n^k\varepsilon$. For simplicity, we omit the superscript (r) in the reflections for player (r).

Since the strategy $\mathcal{S}$ has value at least $\omega_{\mathcal{S}}^*-\varepsilon$ for the (k,n)-stabilizer game, it must have value at least $\omega_{\mathcal{S}}^*-O(\delta)$ for the stabilizer games for each $u\in[n]$ in the second part of the game. More precisely, $\mathcal{S}_u=\big(\rho,\{R_{u,w}^{(i)}\}\big)$ forms a strategy for the stabilizer game with value at least $\omega_{\mathcal{S}}^*-O(\delta)$.

By Theorem 3.5, for all $u\in[n]$, there exist a unitary operators $V_u\in \mathrm{L}(\mathcal{H}_r,\mathcal{B}\otimes\tilde{\mathcal{H}}_r)$ such that

$$d_\rho\big(R_{u,w},V_u^\dagger(D_w\otimes I)V_u\big)\le O(\delta^{1/4}).$$

Define $\hat{R}_{u,w}=V_u^\dagger(D_w\otimes I)V_u$. The above equation becomes

$$d_\rho\big(R_{u,w},\hat{R}_{u,w}\big)\le O(\delta^{1/4}). \tag{3.20}$$

Similarly, for all $J\subseteq[n]$ and $u\in J$, all choices of w_v for $v\in J$ and $v\ne u$, consider state ρ, reflections $R_{u,w}^{(i)}$ for $i\in[r-1]$ and $S_{u,w|\vec{q}}$ for player (r). They form a strategy for the stabilizer game with value at least $\omega_{\mathcal{S}}^*-O(\delta_k)$ for $q_u=(u,w)$, $q_v=(v,w_v)$ and $\vec{q}=(q_v)_{v\in J}$. We clarify that only w is the index of questions for the stabilizer game in this strategy and everything else in the subscripts are fixed.

By Equations (3.12) and (3.13), reflections $S_{u,w|\vec{q}}$ and $\hat{R}_{u,w}$ have the same $O(\sqrt{\delta_k})$-consistent measurement on ρ. Let (u,w) and (v,w') be two entries of $\vec{q}$, then the reflections $\hat{R}_{u,w}$, $S_{u,w|\vec{q}}$, $S_{v,w'|\vec{q}}$, $\hat{R}_{v,w'}$ correspond to measurements that satisfy the conditions for M_0,M_1,N_1,N_0 in Lemma 3.7. Hence,

$$\big\|\big[\hat{R}_{u,w},\hat{R}_{v,w'}\big]\big\|_\rho^2\le O(\delta_k^{1/4}), \tag{3.21}$$

for all $u\ne v\in[n]$.

Consider $2n$ two-dimensional Hilbert spaces $\mathcal{B}_u$, $\mathcal{B}_{u'}$ for $u\in[n]$. Denote $\mathcal{H}_{[n]}=\bigotimes_{u=1}^n\mathcal{B}_u$ and $\mathcal{H}_{[n]'}=\bigotimes_{u=1}^n\mathcal{B}_{u'}$. We sometimes call the system of $\mathcal{B}_u$ the u-th qubit. Let $|\Phi\rangle_{u,u'}$ be the EPR state on systems $\mathcal{B}_u,\mathcal{B}_{u'}$. For each $u\in[n]$, define isometry $C_u\in\mathrm{L}(\mathcal{H},\mathcal{B}_u\otimes\mathcal{B}_{u'}\otimes\mathcal{H})$ as

$$C_u=(I\otimes V_u^\dagger)\,\mathrm{SWAP}_u(|\Phi\rangle_{u,u'}\otimes V_u),$$

where SWAP_u is the SWAP gate acting on the u-th qubit and the first output qubit of V_u. This isometry was previously used in [51, 26, 36] in related contexts.

Define isometry $V \in \mathrm{L}\big(\mathcal{H}_r, \mathcal{H}_{[n]} \otimes \mathcal{H}_{[n]'} \otimes \mathcal{H}_r\big)$ as the sequential application of $C_1, C_2, \ldots, C_n$,

$$V = C_n C_{n-1} \cdots C_1. \tag{3.22}$$

We claim that this choice of V works for the claims of the theorem by taking $\hat{\mathcal{H}}_r$ to be $\mathcal{H}_{[n]'} \otimes \mathcal{H}_r$. Define

$$\tilde{R}_q = V^\dagger D_q V,$$

for $q = (u, w)$. There are single-qubit Pauli X, Z operators that are close to the reflections used by in the strategy and help us to establish the rigidity theorem.

Define a quantum channel

$$\mathcal{T}_u(\rho) = \mathop{\mathbb{E}}_{i \in \{0,1,2,3\}} T_{u,i} \rho T_{u,i}^\dagger,$$

where

$$T_{u,0} = I, \quad T_{u,1} = \hat{R}_{u,0}, \quad T_{u,2} = \hat{R}_{u,0} \hat{R}_{u,1}, \quad T_{u,3} = \hat{R}_{u,1}. \tag{3.23}$$

Recalling the definition of $\hat{R}_q$, the action of quantum channel $\mathcal{T}_u$ essentially traces out the qubit corresponding to $\hat{R}_{u,0}, \hat{R}_{u,1}$, the Pauli X, Z operators up to the unitary operator V_u.

As D_q and C_v commute for all $v > u$ and $q = (u, w)$, we have

$$\tilde{R}_q = C_1^\dagger C_2^\dagger \ldots C_{u-1}^\dagger \hat{R}_q C_{u-1} C_{u-2} \ldots C_1.$$

A series of applications of Lemma 3.8 gives the expression of $\tilde{R}_q$ for $q = (u, w)$,

$$\tilde{R}_q = \mathcal{T}_1 \circ \mathcal{T}_2 \circ \cdots \circ \mathcal{T}_{u-1}(\hat{R}_q).$$

This gives a useful alternative representation for $\tilde{R}_q$ in terms of operators $\hat{R}_{u,w}$ and the corresponding trace-out channels.

The aim is to first prove that

$$d_\rho(\hat{R}_q, \tilde{R}_q) \leq O(n^\kappa \varepsilon^{1/\kappa}).$$

For convenience, define

$$R = \mathcal{T}_2 \circ \cdots \circ \mathcal{T}_{u-1}(\hat{R}_q).$$

Then

$$\tilde{R}_q = \mathop{\mathbb{E}}_{i \in \{0,1,2,3\}} T_{1,i} R T_{1,i}^\dagger,$$

and

$$\mathrm{tr}_\rho\big(\tilde{R}_q \hat{R}_q\big) = \mathop{\mathbb{E}}_{i \in \{0,1,2,3\}} \mathrm{tr}_\rho\big(T_{1,i} R T_{1,i}^\dagger \hat{R}_q\big).$$

For each of the four cases for i, it is claimed that $\mathrm{tr}_\rho\big(T_{1,i} R T_{1,i}^\dagger \hat{R}_q\big)$ is close to $\mathrm{tr}_\rho(R\hat{R}_q)$. In words, removing the superoperator $\mathcal{T}_{1,s_1}$ induces a bounded error in the expression.

Consider the case $i = 1$ first. In this case

$$\begin{aligned}\operatorname{tr}_\rho\big(T_{1,1}(R)T_{1,1}^\dagger \hat{R}_q\big) &= \operatorname{tr}_\rho\big(\hat{R}_{1,0}R\hat{R}_{1,0}\hat{R}_q\big)\\ &\approx_{\delta_k^{1/8}} \operatorname{tr}_\rho\big(\hat{R}_{1,0}R\hat{R}_q\hat{R}_{1,0}\big)\\ &\approx_{\delta^{1/4}} \operatorname{tr}_\rho(R\hat{R}_q),\end{aligned}$$

where the first approximation follows from Equation (3.21) and Cauchy-Schwarz inequality, and the second approximation follows from Lemma 3.9 and the fact that $\hat{R}_{1,0}$ has an $O(\delta^{1/2})$-consistency reflection on ρ by Equation (3.13).

A similar argument applies for the other cases of i. Repeating this procedure of removing the quantum channel $\mathcal{T}_j$ one by one, we have

$$\operatorname{tr}_\rho(\tilde{R}_q, \hat{R}_q) \approx_{u\,\delta_k^{1/8}} \operatorname{tr}_\rho(\hat{R}_q, \hat{R}_q) = 1,$$

and

$$d_\rho(\tilde{R}_q, \hat{R}_q) \le O\big(\sqrt{u\,\delta_k^{1/8}}\big) \le O\big(n^{1/2}\delta_k^{1/16}\big).$$

By the triangle inequality of d_ρ and Equation (3.20)

$$d_\rho(\tilde{R}_q, R_q) \le O\big(n^{1/2}\delta_k^{1/16}\big). \tag{3.24}$$

This proves the bound in Equation (3.15a) by choosing κ sufficiently large.

Recall that there exists a reflection R that is δ_k-consistent with both R_q and $S_{q|\vec{q}}$ on ρ. By the bound in Equation (3.24) and Lemma 2.4,

$$C_\rho(R, \tilde{R}_q) \ge 1 - O\big(n^{1/2}\delta_k^{1/16}\big).$$

The bounds in Equation (3.15b) follow from Lemma 3.10 and the consistency of $\tilde{R}_q$, $S_{q|\vec{q}}$ with the same reflection R on the first $r-1$ players' systems.

The second part of the theorem follows by a similar argument used to prove the second part of Theorem 3.5. □

4 Nonlocal games for local Hamiltonian problems

In this section, we give the nonlocal game for the local Hamiltonian problem. Consider a restricted form of the local Hamiltonian problem in the following definition.

Definition 4.1. For a k-local Hamiltonian of m terms on n qubits $H = \sum_{j=1}^m H_j$, where $0 \le H_j \le I$ acts on at most k qubits, the Hamiltonian H is in XZ-form if H_j is a real linear combination of tensor products of I, X, Z for each j.

Lemma 4.2. *There exists a constant k such that the XZ-form k-local Hamiltonian problem is* QMA-*complete.*

Proof. This is a simple corollary of the results in [13]. The gate set $\{\text{CNOT}, X, W = \cos(\pi/8)X + \sin(\pi/8)Z\}$ is known to be universal by the result of Shi [65] and each gate U_t in the gate set is of XZ-form and $U_t = U_t^\dagger$. Start with a circuit using this particular set of gates and perform the circuit to Hamiltonian construction of Kitaev. The 5-local terms resulting from the construction will have the XZ-form. For example, the term checking the propagation of the t-th step of the circuit is

$$\begin{aligned}H_{\text{prop},t} =& I \otimes |100\rangle\langle 100|_{t-1,t,t+1} - U_t \otimes |110\rangle\langle 100|_{t-1,t,t+1} \\ & - U_t^\dagger \otimes |100\rangle\langle 110|_{t-1,t,t+1} + I \otimes |110\rangle\langle 110|_{t-1,t,t+1} \\ =& \frac{I - Z_{(t-1)}}{2} \otimes \frac{I + Z_{(t+1)}}{2} - U_t \otimes \frac{I - Z_{(t-1)}}{2} \otimes X_{(t)} \otimes \frac{1 + Z_{(t+1)}}{2},\end{aligned}$$

which is easily seen to have XZ-form for U_t in the chosen gate set. Other terms in the construction can be checked similarly. This proves the claim for $k = 5$.

Using more advanced results from [22], such as their Lemma 22, one can prove the claim for $k = 2$ and the two-local terms H_j have the form $\alpha_j(XZ - ZX)$. □

Let $H = \sum_{j=1}^m H_j$ be the Hamiltonian and assume that $0 \leq H_j \leq I$. We will consider two different types of energy measurements for a k-local Hamiltonian H on a state ρ. The first type of measurement is the one used in [26] and does the following. The verifier randomly selects $j \in [m]$ and gets the k-qubit state ρ_j on which H_j acts. Then the verifier measures the POVM $\{H_j, I - H_j\}$ and rejects when the measurement result is 'H_j'. It is easy to see that the verifier rejects with probability

$$\frac{1}{m}\sum_{j=1}^m \langle H_j, \rho\rangle = \frac{1}{m}\langle H, \rho\rangle.$$

In the second type of energy measurement, we only measure Pauli operators. Let $\mathcal{P}_{XZ}$ be the set of the 3^k k-fold tensor products of I, X, Z operators. For XZ-form Hamiltonians, it suffices to measure the Pauli operators in $\mathcal{P}_{XZ}$ only. Expand each term

$$H_j = \sum_{P \in \mathcal{P}_{XZ}} \alpha_{j,P} P. \tag{4.1}$$

Computing the trace of squared operators on both sides of Equation (4.1), we have

$$\sum_{P \in \mathcal{P}_{XZ}} \alpha_{j,P}^2 \leq 1.$$

The verifier randomly selects $j \in [m]$ and gets the k-qubit state ρ_j on which H_j acts. He then chooses P uniformly at random and measures P on ρ_j. The verifier rejects with probability $|\alpha_{j,P}|$ if either $\alpha_{j,P} > 0$ and the measurement result is $+1$, or $\alpha_{j,P} < 0$ and the measurement result is -1. The probability of rejection is computed as

$$\frac{1}{3^k m}\sum_j \sum_P \frac{|\alpha_{j,P}| + \alpha_{j,P}\langle P, \rho_j\rangle}{2} = \frac{\alpha m + \langle H, \rho\rangle}{2 \cdot 3^k m},$$

where

$$\alpha = \frac{1}{m} \sum_{j,P} \left| \alpha_{j,P} \right| \tag{4.2}$$

is a constant determined by the Hamiltonian.

We note that the second type of the energy measurement is less efficient but the probabilities of rejection in these two settings are linearly related. In fact, it is easy to see that the rejection probability in the first setting is p if and only if the rejection probability of the second setting is

$$\frac{\alpha + p}{2 \cdot 3^k}.$$

We now give the nonlocal game for the local Hamiltonian problem as in Figure 8. To measure the energy, we further assume that the stabilizer $\mathfrak{S}$ used in the game has the logical X, Z operators L_X and L_Z that are products of I, X, Z. This is the case for both the five-qubit code and the four-qubit quantum error detecting code.

<u>Nonlocal Game for The Local Hamiltonian Problem</u>

Let $\mathfrak{S}$ be a non-trivial r-qubit stabilizer code with XZ-form generators that encodes at least one qubit and has a pair of logical L_X, L_Z operators of XZ-form. Define two question vectors $w_X = (w_{X,i})$ and $w_Z = (w_{Z,i})$ as follows. The entry $w_{D,i}$ is $*$, 0, or 1, if the i-th Pauli factor of the logical operator L_D is I, X, Z respectively for $D = X, Z$. For an XZ-form, k-local Hamiltonian problem (H, a, b), and a small probability p chosen later, we consider the following multi-player nonlocal game. It involves a classical verifier and r players (i) for $i \in [r]$. The verifier performs the first test with probability p, and the second test with probability $1 - p$:

1. *Energy Check*. Select $j \in [m]$ uniformly at random. Expand H_j as

$$H_j = \sum_{P \in \mathcal{P}_{XZ}} \alpha_{j,P} P,$$

and let $J \subset [n]$ be the set of k qubits H_j acts on non-trivially. Select an operator P in $\mathcal{P}_{XZ}$ uniformly at random. For each $u \in J$, define $w_{u,i}$ to be $w_{X,i}$ or $w_{Z,i}$ if the tensor factor in P acting on qubit u is X or Z, respectively. Define $q_u^{(i)} = (u, w_{u,i})$ and $\vec{q} = \left(q_u^{(i)}\right)_{u \in J}$. Send the question $\vec{q}$ to the r players. Receive a k-bit answer $a^{(i)} = \left(a_u^{(i)}\right)$ from each player. The verifier rejects with probability $\left|\alpha_{j,P}\right|$ if either the parity of the answer bits not corresponding to the null question is even and $\alpha_{j,P} > 0$, or the parity is odd and $\alpha_{j,P} < 0$.
2. *Encoding Check*. Play the (k, n)-stabilizer game.

Figure 8: The nonlocal game for local Hamiltonian problems

Theorem 4.3. *There exist constants C and κ such that the following holds. If p in the r-player game for an XZ-form, k-local Hamiltonian problem in Figure 8 is chosen to be $C(b-a)^\kappa/n^\kappa$, and α is defined as in Equation (4.2), then*

1. *For yes-instances of the k-local Hamiltonian problem, the nonlocal value of the game is at least*
$$(1-p)\omega_{\mathrm{S}}^* + p\left(1 - \frac{\alpha+a}{2\cdot 3^k}\right).$$
2. *For no-instances of the k-local Hamiltonian problem, the nonlocal value of the game is at most*
$$(1-p)\omega_{\mathrm{S}}^* + p\left(1 - \frac{\alpha+(a+b)/2}{2\cdot 3^k}\right).$$

Proof. First consider the completeness of the game. If the local Hamiltonian problem is a yes-instance, there exists a quantum witness state $|\psi\rangle \in \mathcal{B}^{\otimes n}$ such that
$$\langle\psi|H|\psi\rangle \le am.$$
We construct the strategy for the r players as follows. For each qubit u of $|\psi\rangle$, we encode it with the stabilizer code $\mathfrak{S}$ and let player (i) hold the i-th encoded qubit of u. When receiving the question (u,w) from the verifier, the players measure their share of qubit u with X, Z, X', Z' correspondingly if $w = 0,1,2,3$.

For this strategy, the players can win the *Encoding Check* part with optimal probability ω_{S}^*. In the *Energy Check* part of the game, the measurement of the logical X and logical Z is essentially an implementation of the second type of energy measurement on the state ψ. The rejection probability in this part is
$$\frac{\alpha m + \langle H, |\psi\rangle\langle\psi|\rangle}{2\cdot 3^k m}.$$
Therefore, the acceptance probability of the game ω^* is at least
$$(1-p)\omega_{\mathrm{S}}^* + p\left(1 - \frac{\alpha+a}{2\cdot 3^k}\right).$$

Next, we prove the soundness of the game. If the local Hamiltonian problem defined by (H,a,b) is a no-instance, we need to prove an upper bound of the nonlocal value of the game.

Consider any strategy $\mathcal{S}$ that has acceptance probability $\omega_{\mathrm{S}}^* - \varepsilon$ in the *Encoding Check* part of the game. Theorem 3.6 states that there are isometries $V_i \in \mathrm{L}(\mathcal{H}_i, \mathcal{B}^{\otimes n} \otimes \hat{\mathcal{H}}_i)$, measurements $N_{\vec{q}}$ associated with $\left\{V_i^\dagger D_{q_s} V_i\right\}_{s=1}^k$, such that
$$d_\rho(M_{\vec{q}}, N_{\vec{q}}) \le O(n^\kappa \varepsilon^{1/\kappa}).$$

Consider the strategy $\tilde{\mathcal{S}} = (\rho, \{R_q\}, \{N_{\vec{q}}\})$. The values of $\mathcal{S}$ and $\tilde{\mathcal{S}}$ for the *Energy Check* differ at most by $O(n^\kappa \varepsilon^{1/\kappa})$ by Lemma 2.4.

Strategy $\tilde{\mathcal{S}}$ uses honest X, Z measurement on the logical space of the error correcting code and we claim that it must have value at most
$$1 - \frac{\alpha+b}{2\cdot 3^k},$$

in the *Energy Check* part. Otherwise, the state of the first rn qubits after the application of $\bigotimes_i V_i$ has rejection probability at most $(\alpha+b)/(2\cdot 3^k)$ in the energy measurement using logical X, Z operators L_X, L_Z. This implies the existence of n-qubit state that has rejection probability at most $(\alpha+b)/(2\cdot 3^k)$ in the second type energy measurement, which is a contradiction to the no-instance condition of the local Hamiltonian problem.

Therefore, the value of strategy $\mathcal{S}$ is at most

$$(1-p)(\omega_{\mathrm{S}}^* - \varepsilon) + p\big(1 - \frac{\alpha+b}{2\cdot 3^k} + cn^{\kappa}\varepsilon^{1/\kappa}\big), \tag{4.3}$$

for constants c, κ large enough.

Maximizing the expression as a function of ε, it is easy to see that the maximum value is achieved at

$$\varepsilon = \Big(\frac{pcn^{\kappa}}{(1-p)\kappa}\Big)^{\kappa/(\kappa-1)}.$$

Substituting this into Equation (4.3), $\omega^*(\mathcal{S})$ is upper bounded by

$$(1-p)\omega_{\mathrm{S}}^* + p\big(1 - \frac{\alpha+b}{2\cdot 3^k} + \Delta\big),$$

for

$$\Delta = \big(1-\frac{1}{\kappa}\big)cn^{\kappa}\Big(\frac{pcn^{\kappa}}{(1-p)\kappa}\Big)^{1/(\kappa-1)}.$$

Choosing κ large and p small such that $(1-p)\kappa \geq 1$, we can bound Δ as

$$\Delta \leq cn^{\kappa}(pcn^{\kappa})^{1/(\kappa-1)} = \big(pc^{\kappa}n^{\kappa^2}\big)^{1/(\kappa-1)}.$$

Finally, if we choose a constant C small enough and

$$p = C(b-a)^{\kappa-1}/n^{\kappa^2},$$

we have

$$\Delta \leq \frac{b-a}{4\cdot 3^k},$$

and

$$\omega^*(\mathcal{S}) \leq (1-p)\omega_{\mathrm{S}}^* + p\big(1 - \frac{\alpha+(a+b)/2}{2\cdot 3^k}\big).$$

This concludes the proof of the theorem by choosing κ large enough. □

Finally, Theorem 1.1 follows by using the stabilizer for the four-qubit error detecting code in the game and noticing that the completeness and soundness have an inverse polynomial gap in Theorem 4.3.

Acknowledgments

The author acknowledges helpful discussions with Richard Cleve, Debbie Leung, Fang Song, Thomas Vidick, Guoming Wang, John Watrous, Xiaodi Wu and Bei Zeng on related problems. The major part of the paper was done while the author was with the Institute for Quantum Computing, University of Waterloo.

References

[1] ANTONIO ACÍN, NICOLAS BRUNNER, NICOLAS GISIN, SERGE MASSAR, STEFANO PIRONIO, AND VALERIO SCARANI: Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.*, 98(23):230501, 2007. [doi:10.1103/PhysRevLett.98.230501, arXiv:quant-ph/0702152] 10

[2] DORIT AHARONOV, ITAI ARAD, AND THOMAS VIDICK: Guest Column: The Quantum PCP Conjecture. *SIGACT News*, 44(2):47–79, 2013. [doi:10.1145/2491533.2491549] 2

[3] DORIT AHARONOV, MICHAEL BEN-OR, ELAD EBAN, AND URMILA MAHADEV: Interactive proofs for quantum computations. 2017. Preliminary version in ICS'10, see arXiv:0810.5375. [arXiv:1704.04487] 3

[4] DORIT AHARONOV AND TOMER NAVEH: Quantum NP - a survey, 2002. [arXiv:quant-ph/0210077] 2, 11

[5] SANJEEV ARORA, CARSTEN LUND, RAJEEV MOTWANI, MADHU SUDAN, AND MARIO SZEGEDY: Proof verification and the hardness of approximation problems. *J. ACM*, 45(3):501–555, 1998. Preliminary version in FOCS'92. [doi:10.1145/278298.278306] 1, 2

[6] SANJEEV ARORA AND SHMUEL SAFRA: Probabilistic checking of proofs: a new characterization of NP. *J. ACM*, 45(1):70–122, 1998. Preliminary version in FOCS'92. [doi:10.1145/273865.273901] 1, 2

[7] LÁSZLÓ BABAI: Trading group theory for randomness. In *Proc. 17th STOC*, pp. 421–429. ACM Press, 1985. [doi:10.1145/22145.22192] 1

[8] LÁSZLÓ BABAI, LANCE FORTNOW, AND CARSTEN LUND: Nondeterministic exponential time has two-prover interactive protocols. *Comput. Complexity*, 1(1):3–40, 1991. Preliminary version in FOCS'90. [doi:10.1007/BF01200056] 1, 2, 3

[9] JONATHAN BARRETT: Nonsequential positive-operator-valued measurements on entangled mixed states do not always violate a Bell inequality. *Phys. Rev. A*, 65(4):042302, 2002. [doi:10.1103/PhysRevA.65.042302, arXiv:quant-ph/0107045] 4

[10] JOHN S. BELL: On the Einstein Podolsky Rosen paradox. *Physics Physique Fizika*, 1(3):195–200, 1964. [doi:10.1103/PhysicsPhysiqueFizika.1.195] 10

[11] MICHAEL BEN-OR, SHAFI GOLDWASSER, JOE KILIAN, AND AVI WIGDERSON: Multi-prover interactive proofs: How to remove intractability assumptions. In *Proc. 20th STOC*, pp. 113–131. ACM Press, 1988. [doi:10.1145/62212.62223] 1

[12] CHARLES H. BENNETT, DAVID P. DIVINCENZO, JOHN A. SMOLIN, AND WILLIAM K. WOOTTERS: Mixed-state entanglement and quantum error correction. *Phys. Rev. A*, 54(5):3824–3851, 1996. [doi:10.1103/PhysRevA.54.3824, arXiv:quant-ph/9604024] 11

[13] JACOB D. BIAMONTE AND PETER J. LOVE: Realizable Hamiltonians for universal adiabatic quantum computers. *Phys. Rev. A*, 78(1):012352, 2008. [doi:10.1103/PhysRevA.78.012352, arXiv:0704.1287] 6, 33

[14] ANNE BROADBENT, JOSEPH FITZSIMONS, AND ELHAM KASHEFI: Universal blind quantum computation. In *Proc. 50th FOCS*, pp. 517–526. IEEE Comp. Soc. Press, 2009. [doi:10.1109/FOCS.2009.36, arXiv:0807.4154] 3

[15] ANNE BROADBENT, ZHENGFENG JI, FANG SONG, AND JOHN WATROUS: Zero-knowledge proof systems for QMA. In *Proc. 57th FOCS*, pp. 31–40. IEEE Comp. Soc. Press, 2016. [doi:10.1109/FOCS.2016.13, arXiv:1604.02804] 2

[16] PETER J. CAMERON, ASHLEY MONTANARO, MICHAEL W. NEWMAN, SIMONE SEVERINI, AND ANDREAS WINTER: On the quantum chromatic number of a graph. *Electronic J. Combinatorics*, 14:R81, 2007. [arXiv:quant-ph/0608016] 3

[17] JOHN F. CLAUSER, MICHAEL A. HORNE, ABNER SHIMONY, AND RICHARD A. HOLT: Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23(15):880–884, 1969. [doi:10.1103/PhysRevLett.23.880] 4, 10

[18] RICHARD CLEVE, PETER HØYER, BENJAMIN TONER, AND JOHN WATROUS: Consequences and limits of nonlocal strategies. In *Proc. 19th IEEE Conf. on Computational Complexity (CCC'04)*, pp. 236–249. IEEE Comp. Soc. Press, 2004. [doi:10.1109/CCC.2004.1313847, arXiv:quant-ph/0404076] 2, 3

[19] RICHARD CLEVE AND RAJAT MITTAL: Characterization of binary constraint system games. In *Proc. 41st Internat. Colloq. on Automata, Languages and Programming (ICALP'14)*, pp. 320–331. Springer, 2014. [doi:10.1007/978-3-662-43948-7_27, arXiv:1209.2729] 3

[20] ROGER COLBECK: *Quantum And Relativistic Protocols For Secure Multi-Party Computation*. Ph. D. thesis, University of Cambridge, 2006. [arXiv:0911.3814] 10

[21] STEPHEN A. COOK: The complexity of theorem-proving procedures. In *Proc. 3rd STOC*, pp. 151–158. ACM Press, 1971. [doi:10.1145/800157.805047] 1

[22] TOBY S. CUBITT AND ASHLEY MONTANARO: Complexity classification of local Hamiltonian problems. *SIAM J. Comput.*, 45(2):268–316, 2016. Preliminary version in FOCS'14. [doi:10.1137/140998287, arXiv:1311.3161] 11, 33

[23] IRIT DINUR: The PCP theorem by gap amplification. *J. ACM*, 54(3):12:1–12:44, 2007. Preliminary version in STOC'06. [doi:10.1145/1236457.1236459] 2

[24] URI FEIGE AND LÁSZLÓ LOVÁSZ: Two-prover one-round proof systems: their power and their problems. In *Proc. 24th STOC*, pp. 733–744. ACM Press, 1992. [doi:10.1145/129712.129783] 1

[25] JOSEPH F. FITZSIMONS AND ELHAM KASHEFI: Unconditionally verifiable blind computation. *Phys. Rev. A*, 96(1):012303, 2017. [doi:10.1103/PhysRevA.96.012303, arXiv:1203.5217] 3

[26] JOSEPH F. FITZSIMONS AND THOMAS VIDICK: A multiprover interactive proof system for the local Hamiltonian problem. In *Proc. 6th Innovations in Theoretical Computer Science Conf. (ITCS'15)*, pp. 103–112. ACM Press, 2015. [doi:10.1145/2688073.2688094, arXiv:1409.0260] 2, 3, 4, 5, 6, 25, 31, 33

[27] LANCE FORTNOW, JOHN ROMPEL, AND MICHAEL SIPSER: On the power of multi-prover interactive protocols. *Theoret. Comput. Sci.*, 134(2):545–557, 1994. Preliminary version in SCT'88. [doi:10.1016/0304-3975(94)90251-8] 2, 3, 5

[28] SEVAG GHARIBIAN, YICHEN HUANG, ZEPH LANDAU, AND SEUNG WOO SHIN: Quantum Hamiltonian complexity. *Foundations and Trends in Theoretical Computer Science*, 10(3):159–282, 2014. [doi:10.1561/0400000066, arXiv:1401.3916] 2

[29] SHAFI GOLDWASSER, SILVIO MICALI, AND CHARLES RACKOFF: The knowledge complexity of interactive proof-systems. *SIAM J. Comput.*, 18(1):186–208, 1989. Preliminary version in STOC'85. [doi:10.1137/0218012] 1

[30] DANIEL GOTTESMAN: *Stabilizer Codes and Quantum Error Correction*. Ph. D. thesis, California Institute of Technology, 1997. [arXiv:quant-ph/9705052] 11

[31] TSUYOSHI ITO, HIROTADA KOBAYASHI, AND KEIJI MATSUMOTO: Oracularization and two-prover one-round interactive proofs against nonlocal strategies. In *Proc. 24th IEEE Conf. on Computational Complexity (CCC'09)*, pp. 217–228. IEEE Comp. Soc. Press, 2009. [doi:10.1109/CCC.2009.22, arXiv:0810.0693] 3, 11

[32] TSUYOSHI ITO AND THOMAS VIDICK: A multi-prover interactive proof for NEXP sound against entangled provers. In *Proc. 53th FOCS*, pp. 243–252. IEEE Comp. Soc. Press, 2012. [doi:10.1109/FOCS.2012.11, arXiv:1207.0550] 2, 3, 11

[33] RAHUL JAIN, ZHENGFENG JI, SARVAGYA UPADHYAY, AND JOHN WATROUS: QIP = PSPACE. *J. ACM*, 58(6):30:1–30:XX, 2011. Preliminary version in STOC'10. [doi:10.1145/2049697.2049704, arXiv:0907.4737] 2

[34] ZHENGFENG JI: Binary constraint system games and locally commutative reductions, 2013. [arXiv:1310.3794] 3

[35] ZHENGFENG JI: Classical verification of quantum proofs. In *Proc. 48th STOC*, pp. 885–898. ACM Press, 2016. [doi:10.1145/2897518.2897634, arXiv:1505.07432] 1

[36] ZHENGFENG JI: Compression of quantum multi-prover interactive proofs. In *Proc. 49th STOC*, pp. 289–302. ACM Press, 2017. [doi:10.1145/3055399.3055441, arXiv:1610.03133] 6, 31

[37] CAMILLE JORDAN: Essai sur la géométrie à *n* dimensions. *Bull. de la Soc. Math. de France*, 3:103–174, 1875. [doi:10.24033/bsmf.90] 18

[38] RICHARD M. KARP: Reducibility among combinatorial problems. In *Proc. Symp. Complexity of Computer Computations*, pp. 85–103. Springer, 1972. [doi:10.1007/978-1-4684-2001-2_9] 1

[39] JULIA KEMPE, ALEXEI KITAEV, AND ODED REGEV: The complexity of the local Hamiltonian problem. *SIAM J. Comput.*, 35(5):1070–1097, 2006. Preliminary version in FSTTCS'04. [doi:10.1137/S0097539704445226, arXiv:quant-ph/0406180] 11

[40] JULIA KEMPE, HIROTADA KOBAYASHI, KEIJI MATSUMOTO, BEN TONER, AND THOMAS VIDICK: Entangled games are hard to approximate. *SIAM J. Comput.*, 40(3):848–877, 2011. Preliminary version in FOCS'08. [doi:10.1137/090751293, arXiv:0704.2903] 3

[41] ALEXEI Y. KITAEV: Lecture given in Hebrew University, Jerusalem, Israel, 1999. 2, 11

[42] ALEXEI Y. KITAEV, ALEXANDER H. SHEN, AND MIKHAIL. N. VYALYI: *Classical and Quantum Computation*. American Mathematical Society, 2002. 2

[43] ALEXEI Y. KITAEV AND JOHN WATROUS: Parallelization, amplification, and exponential time simulation of quantum interactive proof systems. In *Proc. 32nd STOC*, pp. 608–617. ACM Press, 2000. [doi:10.1145/335305.335387] 2

[44] HIROTADA KOBAYASHI AND KEIJI MATSUMOTO: Quantum multi-prover interactive proof systems with limited prior entanglement. *J. Comput. System Sci.*, 66(3):429–450, 2003. Preliminary version in ISAAC'02. [doi:10.1016/S0022-0000(03)00035-7, arXiv:cs/0102013] 2

[45] SIMON B. KOCHEN AND ERNST SPECKER: The problem of hidden variables in quantum mechanics. *J. Math. Mech.*, 17(1):59–87, 1967. JSTOR. 3

[46] RAYMOND LAFLAMME, CESAR MIQUEL, JUAN PABLO PAZ, AND WOJCIECH HUBERT ZUREK: Perfect quantum error correcting code. *Phys. Rev. Lett.*, 77(1):198–201, 1996. [doi:10.1103/PhysRevLett.77.198, arXiv:quant-ph/9602019] 11

[47] LEONID LEVIN: Universal search problems. *Problems of Information Transmission*, 9(3):115–116, 1973. 1

[48] CARSTEN LUND, LANCE FORTNOW, HOWARD KARLOFF, AND NOAM NISAN: Algebraic methods for interactive proof systems. *J. ACM*, 39(4):859–868, 1992. Preliminary version in FOCS'90. [doi:10.1145/146585.146605] 1

[49] DOMINIC MAYERS AND ANDREW YAO: Quantum cryptography with imperfect apparatus. In *Proc. 39th FOCS*, p. 503. IEEE Comp. Soc. Press, 1998. [doi:10.1109/SFCS.1998.743501] 5

[50] MATTHEW MCKAGUE: Self-testing graph states. In *Proc. 6th Conf. Quantum Computation, Communication, and Cryptography (TQC'11)*, pp. 104–120. Springer, 2014. [doi:10.1007/978-3-642-54429-3_7, arXiv:1010.1989] 5

[51] MATTHEW MCKAGUE: Interactive proofs for BQP via self-tested graph states. *Theory of Computing*, 12(3):1–42, 2016. [doi:10.4086/toc.2016.v012a003, arXiv:1309.5675] 31

[52] MATTHEW MCKAGUE, TZYH HAUR YANG, AND VALERIO SCARANI: Robust self-testing of the singlet. *Journal of Physics A: Mathematical and Theoretical*, 45(45):455304, 2012. [doi:10.1088/1751-8113/45/45/455304, arXiv:1203.2976] 4

[53] NATHANIEL DAVID MERMIN: Simple unified form for the major no-hidden-variables theorems. *Phys. Rev. Lett.*, 65(27):3373–3376, 1990. [doi:10.1103/PhysRevLett.65.3373] 3

[54] CARL A. MILLER AND YAOYUN SHI: Optimal robust self-testing by binary nonlocal XOR games. In *Proc. 8th Conf. Quantum Computation, Communication, and Cryptography (TQC'13)*, pp. 254–262. Springer, 2013. [doi:10.4230/LIPIcs.TQC.2013.254] 5

[55] CARL A. MILLER AND YAOYUN SHI: Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices. *J. ACM*, 63(4):33, 2016. Preliminary version in STOC'14. [doi:10.1145/2885493, arXiv:1402.0489] 10

[56] ANAND NATARAJAN AND THOMAS VIDICK: Constant-soundness interactive proofs for local Hamiltonians, 2015. [arXiv:1512.02090] 6

[57] ANAND NATARAJAN AND THOMAS VIDICK: Robust self-testing of many-qubit states, 2016. Conference version STOC'17. [arXiv:1610.03574] 6

[58] ROBERTO OLIVEIRA AND BARBARA M. TERHAL: The complexity of quantum spin systems on a two-dimensional square lattice. *Quantum Inf. Comput.*, 8(10):900–924, 2008. [arXiv:quant-ph/0504050] 11

[59] TOBIAS J. OSBORNE: Hamiltonian complexity. *Reports on Progress in Physics*, 75(2):022001, 2012. [doi:10.1088/0034-4885/75/2/022001, arXiv:1106.5875] 2

[60] ASHER PERES: Incompatible results of quantum measurements. *Physics Letters A*, 151(3–4):107–108, 1990. [doi:10.1016/0375-9601(90)90172-K] 3

[61] S. PIRONIO, A. ACÍN, S. MASSAR, A. BOYER DE LA GIRODAY, D. N. MATSUKEVICH, P. MAUNZ, S. OLMSCHENK, D. HAYES, L. LUO, T. A. MANNING, AND C. MONROE: Random numbers certified by Bell's theorem. *Nature*, 464(7291):1021–1024, 2010. [doi:10.1038/nature09008, arXiv:0911.3427] 10

[62] ROBERT RAUSSENDORF, DANIEL E. BROWNE, AND HANS J. BRIEGEL: Measurement-based quantum computation on cluster states. *Phys. Rev. A*, 68(2):022312, 2003. [doi:10.1103/PhysRevA.68.022312, arXiv:quant-ph/0301052] 3

[63] BEN W. REICHARDT, FALK UNGER, AND UMESH VAZIRANI: Classical command of quantum systems. *Nature*, 496(7446):456–460, 2013. [doi:10.1038/nature12035] 2, 3, 4, 5, 6, 10, 18, 20

[64] ADI SHAMIR: IP = PSPACE. *J. ACM*, 39(4):869–877, 1992. Preliminary version in FOCS'90. [doi:10.1145/146585.146609] 1

[65] YAOYUN SHI: Both Toffoli and controlled-NOT need little help to do universal quantum computing. *Quantum Inf. Comput.*, 3(1):84–92, 2003. [arXiv:quant-ph/0205115] 33

[66] BORIS S. TSIREL'SON: Quantum generalizations of Bell's inequality. *Letters in Mathematical Physics*, 4(2):93–100, 1980. [doi:10.1007/BF00417500] 10

[67] WIM VAN DAM, FRÉDÉIC MAGNIEZ, MICHELE MOSCA, AND MIKLOS SANTHA: Self-testing of universal and fault-tolerant sets of quantum gates. *SIAM J. Comput.*, 37(2):611–629, 2007. Preliminary version in STOC'00. [doi:10.1137/S0097539702404377, arXiv:quant-ph/9904108] 5

[68] UMESH VAZIRANI AND THOMAS VIDICK: Certifiable quantum dice: or, true random number generation secure against quantum adversaries. In *Proc. 44th STOC*, pp. 61–76. ACM Press, 2012. [doi:10.1145/2213977.2213984, arXiv:1111.6054] 10

[69] UMESH VAZIRANI AND THOMAS VIDICK: Fully device-independent quantum key distribution. *Phys. Rev. Lett.*, 113(14):140501, 2014. Conference version in ITCS'14. [doi:10.1103/PhysRevLett.113.140501, arXiv:1210.1810] 10

[70] THOMAS VIDICK: Three-player entangled XOR games are NP-hard to approximate. *SIAM J. Comput.*, 45(3):1007–1063, 2016. Preliminary version in FOCS'13. [doi:10.1137/140956622, arXiv:1302.1242] 3, 11

[71] THOMAS VIDICK AND JOHN WATROUS: Quantum proofs. *Foundations and Trends in Theoretical Computer Science*, 11(1–2):1–215, 2015. [doi:10.1561/0400000068, arXiv:1610.01664] 2

[72] JOHN WATROUS: PSPACE has constant-round quantum interactive proof systems. *Theoret. Comput. Sci.*, 292(3):575–588, 2003. Preliminary version in FOCS'99. [doi:10.1016/S0304-3975(01)00375-9] 2

[73] JOHN WATROUS: Zero-knowledge against quantum attacks. *SIAM J. Comput.*, 39(1):25–58, 2009. Preliminary version in STOC'06. [doi:10.1137/060670997, arXiv:quant-ph/0511020] 2

[74] REINHARD F. WERNER: Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model. *Phys. Rev. A*, 40(8):4277–4281, 1989. [doi:10.1103/PhysRevA.40.4277] 4

AUTHOR

Zhengfeng Ji
Centre for Quantum Software and Information
School of Software
Faculty of Engineering and Information Technology
University of Technology Sydney, NSW, Australia
Zhengfeng.Ji@uts.edu.au
`http://www.uts.edu.au/staff/zhengfeng.ji`

ABOUT THE AUTHOR

ZHENGFENG JI graduated from Tsinghua University in 2007; his advisor was Mingsheng Ying. His interests in the theory of quantum multiprover interactive proof systems and nonlocal games were influenced by Richard Cleve and John Watrous, from the Institute for Quantum Computing (IQC) at the University of Waterloo, while he was a postdoctoral fellow at IQC.