Verifying Quantum Proofs with Entangled Games

by

Anand Venkat Natarajan

B.S., Stanford University (2013)
M.S., Stanford University (2013)

Submitted to the Department of Physics
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy in Physics

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

June 2018

Signature redacted

Author .....

Department of Physics
May 25, 2018

Signature redacted

Certified by .....

Aram W. Harrow
Associate Professor of Physics
Thesis Supervisor

Signature redacted

Accepted by .....

Scott Hughes
Interim Associate Head of Physics

Verifying Quantum Proofs with Entangled Games

by

Anand Venkat Natarajan

Submitted to the Department of Physics
on May 25, 2018, in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy in Physics

Abstract

A team of students has been given a challenging physics exam: find the ground energy of a complicated, n-spin system. Even if they succeed, how can the examiners be sure that their answer is correct without physically measuring all n spins of the ground state, or worse, having to read a description of the 2^n components of its wavefunction? The main result of this thesis is a protocol such that, if the examiners are allowed to separately interrogate multiple students, they can be confident that the students possess the n-spin ground state as well as learn its energy to high precision, after exchanging just $O(\log(n))$ bits of classical communication with the students! The protocol and its analysis combine classical computer science techniques for efficiently checking proofs with Bell inequalities.

Stated more formally, the main result of this thesis is a multi-prover interactive proof protocol, in which a classical verifier exchanging only $O(\log(n))$ bits of classical communication with 7 untrusted, entangled provers can certify that they share between them an encoding of an n-qubit quantum state $|\psi\rangle$, and estimate its energy under a local Hamiltonian H to high $(1/\operatorname{poly}(n))$ precision. As a consequence, we show that, under poly-time randomized reductions, it is QMA-hard to estimate the entangled value of a nonlocal game up to constant error, proving the quantum entangled games PCP conjecture of Fitzsimons and Vidick. Our main technical innovations are two constructions of *robust self-tests for entanglement*: two-player nonlocal games where to succeed with probability ε-close to 1, the players must share a state that is $\delta = \operatorname{poly}(\varepsilon)$-close in trace distance to n EPR pairs. These tests are robust in that δ is independent of the number n of EPR pairs being tested. Our techniques draw heavily on the original, "algebraic" proof of the PCP theorem in classical complexity theory, and in particular, each of our robust self-tests is based on a classical locally-testable error correcting code: the first on the Hadamard code and the associated linearity test of Blum, Luby, and Rubinfeld, and the second on Reed-Muller code and the associated low-degree test of Raz and Safra.

Thesis Supervisor: Aram W. Harrow
Title: Associate Professor of Physics

Acknowledgments

This thesis would not have been possible wtithout the help of many teachers, collaborators, and friends. First of all, I would like to thank my advisor, Aram Harrow. I am grateful to Aram not just for always being generous with his time and ideas, and for his hands-on guidance in doing research and writing papers, but for also for giving me a great deal of freedom and encouraging me to attend conferences and workshops, even as a young student with no results to my name. Indeed, the work that became this thesis arose from the first workshop I attended in grad school, held at the Simons Institute at UC Berkeley as part of the spring 2014 program on Hamiltonian complexity. It was at this program that I met Thomas Vidick, the coauthor of most of the papers that became this thesis, and to whom I also owe a great deal: for hosting me at Caltech as a summer student in 2015 and for numerous visits thereafter, and for his guidance throughout our collaboration. I am also grateful to my other coauthors throughout grad school: Xiaodi Wu, Matthew Coudron, Adam Bene Watts, and Gurtej Kanwar. I am particularly grateful to Xiaodi for sharing his insight in how to choose good research problems, and for teaching me a great deal about scientific writing through his thorough and patient revision of our first paper together, which was also my first publication.

In addition to my coauthors I have benefited from many scientific discussions with fellow students as well as more senior researchers at MIT and elsewhere. A (surely incomplete!) list would include (in no particular order) Cyril Stark, Robin Kothari, Lior Eldar, Shalev Ben-David, Adam Bouland, Henry Yuen, Cedric Lin, Bill Fefferman, Shelby Kimmel, David Gossett, Omar Fawzi, Dorit Aharonov, John Preskill, Rolando La Placa, Mehdi Soleimanifar, John Wright, John Napp, Daniel Grier, Luke Schaeffer, Umesh Vazirani, Urmila Mahadev, and Ramis Movassagh. I am particularly grateful to Scott Aaronson and Ike Chuang for teaching me quantum information at MIT, and to Ike, Peter Shor, Eddie Farhi, and Seth Lloyd for serving on my thesis and oral exam committees. I am also grateful for numerous enriching travel opportunities throughout my PhD and to the people and institutions that hosted me: the Simons Institute at Berkeley; the IQIM group at Caltech; the QuICS group at the University of Maryland; Troy Lee at the National University of Singapore; the It From Qubit summer school at the Perimeter Institute; and Stanislaw Szarek, Guillaume Aubrun, and the rest of the organizers of the trimester on quantum information at the Institut Henri Poincaré.

Outside of quantum information, I am thankful to Srivatsan, Nick, Nikhil, Usman, Lina, Ben, Sarah, and the rest of my fellow students in the CTP, for making me feel at home here right from the start of my first year. I am also grateful to Hanzhi, Tony, Lynnelle, Jack, and Shristi for many years of friendship at Stanford and in Cambridge.

Finally, this thesis is dedicated to my parents, who initiated me into the study of math and science and without whose continued and unstinting support I would not be where I am today.

Financial support While performing the research in this thesis, I was financially supported by NSF Grant CCF-1629809, ARO Contract Number W911NF-12-0486, and NSF CAREER Grant CCF-1452616.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

This thesis studies a field of quantum information known as *quantum Hamiltonian complexity*, which, broadly speaking, studies the computational complexity of problems that arise in condensed matter physics. Most of these problems concern properties of low-energy states of complex quantum many-body systems, of which perhaps *the* paradigmatic example is the local Hamiltonian problem: given a Hamiltonian describing a many-body system with local interactions, what is (a good estimate of) its ground energy? Underlying Hamiltonian complexity is the observation that the local Hamiltonian problem is a direct analog of a class of classical computation problems called constraint satisfaction problems (CSPs), for which there exists a rich theory built around the complexity class NP. In the quantum setting, Kitaev generalized the classical theory of NP by defining the its quantum analog: the complexity class QMA. Since then, much work in Hamiltonian complexity has revolved around understanding the difference between QMA and NP, or in physical terms, understanding when there exists a short classical description (or ansatz) for a low-energy state of a quantum system. A major challenge in this direction is the *quantum PCP conjecture*: which would imply the existence of local Hamiltonians for which not just the ground state but all states of low, finite temperature are highly entangled and have no efficient classical description. However, after more than a decade, direct attack on this conjecture has mostly yielded no-go theorems, with only a few positive results known.

This thesis follows a line of work which explores questions in the spirit of the quantum PCP conjecture from a rather different perspective: that of *nonlocal games* or *multiprover interactive proof systems*. These concepts have a long history in computer science, and were crucial to the development of the PCP theorem, often considered the "crown jewel" of the classical theory of CSPs. Perhaps surprisingly, these concepts were foreshadowed in physics several decades before their discovery in computer science by John Bell's pioneering work [Bel64] on the foundations of quantum mechanics. In the rest of this introduction, we will start by reviewing the role played by games and proof systems in classical complexity theory and in quantum foundations. We will then present the main results of this thesis, including a proof of a version of the so-called quantum entangled games PCP conjecture, together with an overview of our techniques and a survey of related works and future directions for research.

1.1 Proof systems, games, and computational complexity

Proof systems have long played a central role in computational complexity theory. Indeed, the class NP, whose study is arguably foundational to the field, is an instance of a proof system: a game played between a polynomial-time *verifier*, and an untrusted *prover* who is allowed unbounded computational resources. For a given instance of a decision problem (whose answer is either YES or NO), the goal of the prover is to convince the verifier that the answer is YES *regardless* of the true answer, while the goal of the verifier is to learn the truth. The game consists of a single turn: the prover comes up with a claimed proof that the answer to the problem is YES, and hands it to the verifier. The verifier then reads the proof and decides—in polynomial time—whether to accept it or reject it. A problem is in NP if for every YES instance, there is some ("honest") proof that the verifier accepts, and for every NO instance, the verifier rejects all claimed (but necessarily false) proofs. The former property is called "completeness" of the proof system, and the latter "soundness."

There are two features of NP that make it a central object of study for complexity theorists. First, NP contains many natural computational problems that arise in practice for which no efficient algorithm is known, despite efforts to find one. Secondly, all problems in NP reduce to the problem of *verifying computational histories*, which in turn can be reduced to *local constraint satisfaction problems* like 3SAT. This is because if an NP problem has a verification algorithm V, which reads as input a claimed proof x, then we can construct a new verifier V' whose input is claimed transcript T_x of the computations V would have executed on x. The verifier V' need only verify that each step in the transcript T_x follows from the previous step, and that the at the end of the transcript, V accepts. Crucially, each check performed by V' is a *local* check that only depends on a constant number of bits of T_x: for instance, if V' is verifying that transcript contains the correct application of an AND gate at time t was correctly applied to two input bits, it need only check the state of the two input bits at time t and the single output bit at time $t+1$. This observation is at the heart of Cook-Levin theorem and the beautiful theory of NP-completeness, and implies that henceforth in understanding NP problems we can restrict our attention to 3SAT.

With this view of NP as a proof system, a natural next question is to ask what happens to the power of the class when the rules of game are modified. The simplest change one can make is to allow the verifier the power of *randomness*: this yields the complexity class known as MA. In the presence of randomness, the definitions of completeness and soundness become probabilistic: we say that a proof system has *completeness parameter* c if for every YES instance, there is some proof it accepts with probability at least c, and *soundness parameter* s if for every NO instance, it accepts no proof with probability more than s. For NP, $c = 1$ and $s = 0$, whereas for MA, we conventionally take $c = 2/3$ and $s = 1/3$, although in fact one obtains the same complexity class for any constant choice of c and s. It turns out that merely adding randomness to the verifier's arsenal does not appear to greatly affect the

power of the proof system: under plausible derandomization conjectures, it is believed that NP = MA. A more consequential change is to allow the prover and the verifier *interaction*, in which the verifier is allowed to send challenges (perhaps generated randomly) to the prover. If polynomially-many rounds of interaction are allowed resulting complexity class, known as IP, was shown to be equal to PSPACE, the class of all computations that can be performed in polynomial space (and up to exponential time). An important feature of this result is that, as PSPACE is not believed to be equal to NP, there is no polynomial-sized certificate of correctness that the verifier can check. Indeed, the key idea enabling the proof of IP=PSPACE is the construction of a robust *encoding* of an *exponentially* large certificate of correctness for a PSPACE computation, in a manner that can be verified by only reading polynomially many bits. The construction of this encoding is algebraic: it relies on a representation of a PSPACE computational as the sum of a multivariate polynomial over variables in $\mathbb{F}_2$, and encodes this computation by extending the polynomial to a finite field extension $\mathbb{F}_{2^t}$ of $\mathbb{F}_2$.

The key challenge in proving a result like IP=PSPACE is establishing *soundness* of the proof protocol: showing that a cheating prover cannot convince a verifier to incorrectly accept. The less the prover's ability to cheat, the greater the power of the proof system. Intuitively, one could view the power of multiple rounds of interaction in these terms as reducing the ability of the prover to cheat: if the prover decides to lie in response to a question from the verifier, the verifier can adjust its follow-up questions to try to catch the prover in an inconsistency. As is familiar from the prisoner's dilemma, another way of catching a liar in an inconsistency is to cross-check its answers against an independent source. This observation motivated the definition of the class MIP of multiprover interactive proofs, in which the verifier is allowed simultaneously interrogate two or more provers who are forbidden from communicating with each other during the interaction (though they may agree on a strategy beforehand). We provide a semi-formal definition below:

Definition 1.1.1. The complexity class $\mathrm{MIP}_m(k, r, c, s)$ consists of all promise problems[1] decidable by a multi-prover interactive proof system with k provers, r rounds of interaction, m bits of communication, completeness c, and soundness s. When the subscript m is omitted it is assumed to be $\mathrm{poly}(n)$, and when c, s are omitted they are assumed to be 1 and 1/2, respectively.

Especially in the case of single-round protocols, we will also refer to multi-prover interactive proof protocols as *nonlocal games*: they are so called because the restriction that the provers cannot communicate can be enforced by spatially separating them. As this thesis will be focusing on MIP and closely related classes, it is worth getting to know this class a little better, by looking at a simple example: a two-prover,

[1]The distinction between promise problems and decision problem is a technical one and can be safely ignored by the non-expert reader. Essentially, to solve a decision problem, an algorithm must output YES or NO correctly for *every* instance ϕ, whereas for a promise problem, the algorithm is required to be correct on some subset of instances (the algorithm is "promised" that the instance comes from this good set).

one-round game for problems in NP. This is the so-called *clause-variable game*, described in Figure 1-1. It is clear that the clause-variable game is a proof system

---

The clause-variable game is a two-prover one-round game. Given is an instance ϕ of 3SAT, consisting of a Boolean formula on n variables $x_1, \ldots x_n$. The verifier starts by permuting the provers at random.

1. The verifier a clause C from ϕ at random, involving the three variables $x_{i_1}, x_{i_2}, x_{i_3}$, and sends to the first prover the tuple of three indices (i_1, i_2, i_3), and to the second prover a single index i drawn randomly from $\{i_1, i_2, i_3\}$.

2. The verifier receives answers $a_{i_1}, a_{i_2}, a_{i_3}$ from the first prover and b_i from the second prover. It accepts if $a_{i_1}, a_{i_2}, a_{i_3}$ are an accepting assignment for the clause C in ϕ, and if $a_i = b_i$.

Figure 1-1: The clause-variable game.

with perfect completeness: if the given 3SAT instance ϕ is satisfiable, then if the provers answer according to a satisfying assignment to the variables, the verifier will accept with probability 1. It is slightly more nontrivial, but still easy, to analyze its soundness. To do so, note that we can assume without loss of generality that both provers play according to a *deterministic* strategy, and so in particular, the second prover answers according to some fixed assignment b. Now, if b is not a satisfying assignment, then it must violate at least one clause of ϕ, and thus the first prover's answers a must either violate this clause as well, or disagree with b, in both cases leading the verifier to reject. The verifier will detect this violated clause with probability $\Omega(1/n)$, so the soundness of the resulting proof system is $1 - \Omega(1/n)$. This result can be encapsulated in the following theorem.

Theorem 1.1.2. *The class* $\mathrm{MIP}_{\log}(2, 1, 1, 1 - \Omega(1/n))$ *of multi-prover interactive proof systems with two provers, one round of interaction,* $O(\log(n))$ *bits of communication, completeness* 1, *and soundness* $1 - \Omega(1/n)$ *is equal to NP.*

Equivalently, we could phrase this as saying that it is NP-complete to approximate the *(classical) value*—the maximum acceptance probability of a (classical) strategy—of a two-prover game up to precision $1/\operatorname{poly}(n)$.

While this result is interesting, it is rather weak, and MIP is much more powerful, exceeding the power of IP. In fact, it was shown by [BFL91] that MIP is equal to NEXP the class of all computations that have an exponentially-large certificate of correctness (NEXP contains PSPACE and the containment is believed to be strict).

Theorem 1.1.3. *The class* $\mathrm{MIP}(2, 1, 1, 1/2)$ *of multi-prover interactive proofs with two provers, one round of interaction,* $\operatorname{poly}(n)$ *bits of communication, completeness* 1, *and soundness* $1/2$ *is equal to* NEXP.

The class NEXP is essentially an exponentially "scaled-up" version of NP, and in this light, the last result can be understood as a "scaled-up" version of Theorem 1.1.2, but with a crucial strengthening: unlike in Theorem 1.1.2, the completeness-soundness gap $c-s$ is a constant independent of the instance size n. This miraculous property is achieved by encoding the exponentially long NEXP proof in a special, highly robust way, and playing a version of the clause-variable game applied to this encoding. As in the case of IP=PSPACE, the main challenge here is showing soundness: if the provers do not honestly answer according to some proof string, their cheating will be caught by the verifier with high probability. A sequence of works [FGL+96, ALM+98, AS98] quantitatively refined this idea to produce a "scaled-down" version of this theorem applicable to NP, known as the Probabilistically Checkable Proofs (PCP) theorem. This theorem, a landmark achievement in complexity theory, showed that every problem in NP has a proof of correctness that can be verified with high confidence simply by reading a few randomly chosen bits from the proof, and has had many applications to areas such as hardness of approximation for various optimization problems. To build intuition, we give three equivalent formulations of this theorem below, the first of which is a direct analog to Theorem 1.1.3, and the last of which recalls our original definition of NP as a *non-interactive* proof system.

Theorem 1.1.4 ([ALM+98, AS98]). *1. The class* $\mathrm{MIP}_{\log}(2,1)$ *of multi-prover interactive proof systems with two provers, a single round of interaction, and* $O(\log(n))$ *bits of communication is equal to* NP.

2. *Equivalently, it is* NP*-complete to approximate the classical value of a game up to constant additive precision.*

3. *Equivalently, for any problem in* NP*, there exists a polynomial-time verifier* V *that, given a problem instance* ϕ *and access to a polynomially long proof string* Π*, flips* $O(\log(n))$ *random coins and reads* $O(\log(n))$ *bits of* Π*, such that if* ϕ *is a YES instance, then there exists some* Π *that makes the verifier accept with probability* 1*, and if* ϕ *is a NO instance, then the verifier accepts with probability at most* $1/2$ *for any* Π.

The equivalence between items 1. and 2. of Theorem 1.1.4 follows immediately from the definitions. The implication from 3. to 1. follows from applying the clause-variable game to the proof Π, and the implication from 1. to 3 follows by taking Π to be a transcript of all possible interactions that could have occurred in the interactive protocol.

The quantum story. Proof systems have played a similarly important role in quantum complexity theory as they have in the classical theory. The central class here is the quantum version of NP, known as QMA[2]:

[2]More accurately, this class is the quantum version of the class MA, which is a probabilistic version of NP.

Definition 1.1.5. The class QMA is the class of all promise problems for which there exists a BQP verification algorithm V taking as input a problem instance H and a quantum proof state $|\psi\rangle$, with the following properties:

1. If H is a YES instance, then there exists a state $|\psi\rangle$ that causes V to accept with probability at least $2/3$.
2. If H is a NO instance, then for any proof state $|\psi\rangle$, V will accept with probability at most $1/3$.

Just as NP can be understood from its most useful complete problem, 3SAT, QMA can be understood from the local Hamiltonian problem, which was shown by Kitaev to be complete for the class.

Definition 1.1.6. A *local Hamiltonian* acting on n qubits is a Hermitian operator H that can be written as

$$H = \frac{1}{m}\sum_{i=1}^{m} H_i,$$

where $m = O(\text{poly}(n))$ and each term H_i is a Hermitian operator acting nontrivially on a constant number of qubits. Moreover, the terms are normalized so that each term H_i has operator norm bounded by $\|H_i\| \leq 1$.

Given parameters $-1 \leq a < b \leq 1$, the *local Hamiltonian problem* is to decide, given a local Hamiltonian H, whether its ground energy λ_{min} is at most a, or at least b, promised that one of these is the case. The quantity $b - a$ is called the *promise gap*.

We remark that, in contrast to the usual convention in physics, our choice of normalization means that the Hamiltonian H is *not* extensive: the total energy is always in the interval $[-1, 1]$, regardless of the system size. This is important to understand the quantitative statements that will follow.

Theorem 1.1.7 (Kitaev [KSV02]). *The local Hamiltonian problem is* QMA*-complete when the promise gap is* $1/O(\text{poly}(n))$.

The fact that the local Hamiltonian problem is complete for QMA indicates that this class roughly captures the worst-case complexity of *condensed-matter physics*, in which we are interested in properties of low-energy states of many-body quantum systems. Thus, the widely-held belief that QMA is more powerful than NP captures the intuition that, in the worst case, there exists no short classical description for the ground state of a many-body quantum system.

Kitaev's result establishes QMA-hardness only in the regime of energies very close to the ground energy, yet Theorem 1.1.4 already implies that the local Hamiltonian problem is at least NP-hard even when the promise gap is taken to be constant, i.e. for energies that are a constant above the ground energy. A natural question to ask is where the transition from "mere" NP-hardness to QMA-hardness occurs. In particular, does there exist some constant promise gap for which the local Hamiltonian problem is QMA-hard?

Conjecture 1.1.8 (Quantum Hamiltonian PCP (qHPCP) conjecture [AN02]). *The local Hamiltonian problem is* QMA*-complete with a promise gap* $b - a = \Omega(1)$.

If the qHPCP conjecture is true, then it would imply the existence of Hamiltonians for which *no* state with energy within a constant threshold of the ground energy has an efficient classical description. In particular, for a sufficient low constant temperature T, independent of the system size, the Gibbs state of temperature T would admit no efficient classical description, and thus would have to be highly entangled. So a physical interpretation of the qHPCP conjecture is that, if true, it would imply the existence of highly robust many-body entanglement, in systems with local interactions. This conjecture also has a natural complexity-theoretic motivation: it is, roughly speaking, what we get if we take item 3 of Theorem 1.1.4, and replace NP with QMA, classical proof strings with quantum proof states, and the classical verifier with a quantum verifier. As such, it is one natural quantization of the PCP theorem, thus justifying its name.

Despite much work, the qHPCP conjecture has proven resistant to attack, and indeed it is not clear whether our intuition should be that the conjecture is true or false. The reader is referred to the survey of Aharonov, Arad, and Vidick [AAV13] for a full description of progress up to 2013, including several powerful no-go theorems [BH13, AE15] showing that certain families of Hamiltonians cannot yield qHPCP-type hardness. Since then, perhaps the biggest development has been the work of Eldar and Harrow [EH15], showing lower bounds on the circuit depth required to generate any state from a subset of low-energy states of a particular Hamiltonian. This result would be implied by qHPCP but is much weaker.

The qHPCP conjecture corresponds to one of several equivalent formulations of the classical PCP theorem. Naturally, one might ask whether insight could be gained by considering the "quantization" of one of the other formulations. Indeed, the main focus of this thesis is the quantum version of the interactive-proofs variant of the PCP theorem (items 1 and 2 of Theorem 1.1.4), which we will explore in the following section. While this variant is *not* known to be equivalent to qHPCP, we will see that it is in some ways similar in spirit, and in Section 1.5, we will discuss possibilities for making progress on qHPCP using the ideas we develop.

1.2 Interactive proofs with entangled provers

So far, we have set the stage by discussing classical multi-prover interactive proof systems, and quantum *single*-prover proof system. What about quantum multi-prover proof systems? To do this topic justice, we will have to make a detour to the foundations of quantum mechanics.

1.2.1 Bell inequalities and self-testing

Quite independently of the aforementioned developments in computer science, and indeed several decades prior, the idea of multiprover interactive proofs had already been exploited by John Bell [Bel64], working on quantum foundations. Bell was

not interested in the *computation* power of such proofs, but rather their power to confirm or rule out physical theories. Since the beginnings of quantum mechanics, many physicists, uneasy at the probabilistic nature of the theory, had posited that it was "incomplete," and that the outcomes of measurements were in fact deterministic functions of some hidden variables that had yet to be observed. Einstein, Podolsky, and Rosen, in a famous thought experiment [EPR35], sought to substantiate this view by considering a system of two spatially separated particles (in our language, qubits), in the *EPR state*

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

EPR observed if the first particle is measured in either the Z basis ($\{|0\rangle, |1\rangle\}$) or the X basis ($\{|+\rangle, |-\rangle\}$), the resulting outcome fully determines the outcome of the same measurement applied to the other particle, even though no causal signal could possibly have traveled between the particles. They reasoned from this that each particle carried some *local* hidden variable determining the value of measurements in both the X and Z bases, and that the correlated measurement outcomes between the two particles were caused by purely classical correlations between the local hidden variables.

Bell's achievement was to demonstrate that in fact, the EPR experiment shows the opposite of what its authors claimed: any system that matches the predictions of quantum mechanics for the EPR state *cannot* be described by *any* classical local hidden variable theory. To show this, Bell converted the EPR setup—in which two parties measure halves of an EPR state in either the X or Z basis—into a game pitting two quantum provers against a classical verifier: the quantum provers are supposed each hold one particle from the EPR state. Bell's original game involved the verifier and payers exchanging real numbers, but it was soon simplified by Clauser, Horne, Shimony, and Holt [CHSH69]. This simplified game is described in Figure 1-2. To

---

The CHSH game is played as follows:

1. The verifier chooses bits x, y uniformly at random and sends x to the first prover and y to the second.

2. The provers respond with single-bit answers a and b, respectively. The prover accepts if $xy = a \oplus b$, and rejects otherwise. (Explicitly, if x and y are both 1, then the provers's answers should differ, and otherwise, they should be equal.)

Figure 1-2: The CHSH game is a nonlocal game with 2 provers and 1 round of interaction.

make the connection between the CHSH game and the EPR setup, consider the *EPR strategy* for this game, given in Defintion 1.2.1.

Definition 1.2.1. In the EPR strategy for the CHSH game, the two provers share the

state $|\mathrm{EPR}\rangle$. When the first prover receives an input x, it measures the observable $\tilde{A}_x$ on its half of the state and reports the outcome, where $\tilde{A}_0 = X$ and $\tilde{A}_1 = Z$. The second prover executes a rotated version of this strategy: given input y, it measures the observable $\tilde{B}_y$, where $\tilde{B}_0 = \frac{X+Z}{\sqrt{2}}$ and $\tilde{B}_1 = \frac{X-Z}{\sqrt{2}}$.

It can be checked via explicit calculation that the probability that the EPR strategy described above will be accepted by the verifier ("win" the game) is

$$\omega^*_{\mathrm{CHSH}} = \frac{1}{2} + \frac{\sqrt{2}}{4} \approx 0.85.$$

Bell's remarkable result was to show that the *maximum* probability of winning achievable by *any* strategy that is realizable in a classical hidden variable model is

$$\omega_{\mathrm{CHSH}} = \frac{3}{4}.$$

The proof of this result is very simple: by a convexity argument, one can without loss of generality consider only deterministic strategies for the players. Then, a brute-force enumeration reveals that 3/4 is the maximum achievable. Thus, by executing the CHSH game and measuring the fraction of times that the provers win, one can rule out the existence of a classical hidden variable theory that describes their shared state.

In the language we developed in Section 1.1, the CHSH game can be viewed as a multi-prover interactive proof with completeness ω^*_{CHSH} and soundness 3/4, but with the crucial difference that the provers are allowed (indeed, encouraged!) to share quantum entanglement. In fact, shared entanglement is precisely the property that CHSH certifies: any strategy in which the two provers share a product quantum state would be no better than a classical strategy. Yet there are several puzzling features of the CHSH game: both the number ω^*_{CHSH} and the EPR strategy achieving it seem arbitrary. Might there not be a way to achieve a winning probability of 1 using a larger entangled state, or different measurements? This question was answered in the negative by the famous bound of Tsirelson [Cir80b], which shows that ω^*_{CHSH} is in fact the *optimal* winning probability achievable by any strategy using quantum entanglement, even if the entanglement is infinite dimensional. Moreover, not only is the value ω^*_{CHSH} optimal, but also the strategy that achieves it is essentially unique. This is the *self-testing* property of the CHSH game, first discovered by Summers and Werner [SW88], who showed that for any entangled strategy achieving ω^*_{CHSH}, there exist *local isometries* V_1, V_2, acting separately on the systems of provers 1 and 2 only, that map the state and measurements in this strategy to the EPR strategy described above. Summers and Werner further showed the same result up to finite error: for any strategy achieving a success probability of $\omega^*_{\mathrm{CHSH}} - \varepsilon$, there exist local isometries taking it $\delta(\varepsilon)$-close to the canonical EPR strategy, where δ is a function of ε. This result was rediscovered by the quantum information community and refined in subsequent works (e.g. [MY04, MMMO06a]), culminating the following theorem of McKague, Yang, and Scarani [MYS12a].

Theorem 1.2.2 ([MYS12a]). *Suppose a strategy consisting of a state $|\psi\rangle$ and measurement observables A_0, A_1 for prover 1 and B_0, B_1 for prover 2 achieves success $\omega^*_{\text{CHSH}} - \varepsilon$ in the CHSH game. Then there exist local isometries V_1 and V_2 acting only on prover 1 and prover 2's spaces, respectively, as well as a state $|junk\rangle$, such that for any $x, y \in \{0,1\}$ and any exponents $p, q \in \{0,1\}$,*

$$\|(V_1 \otimes V_2)((A_x)^p \otimes (B_y)^q|\psi\rangle) - ((\tilde{A}_x)^p \otimes (\tilde{B}_y)^q|\text{EPR}\rangle) \otimes |junk\rangle\| \leq O(\varepsilon^{1/4}).$$

Here, $\tilde{A}_x$ and $\tilde{B}_y$ are the observables from the EPR strategy in Definition 1.2.1.

Thus, the CHSH game is a proof system not just for shared entanglement, but a particular entangled state and a particular set of measurements acting on it. (Terminologically, we say that the CHSH game is a *self-test* for this strategy, or more loosely, for the EPR state.) Moreover, it is not the only game to have this property: in fact, another game, called the Magic Square game [Mer90, Per90], is a self-test for the state $|\text{EPR}\rangle^{\otimes 2}$ with perfect completeness, meaning that the optimal success probability achieved using entanglement is equal to 1. The self-testing property of these games is unique to the setting of entangled provers and at first glance seems incomparable to the types of statements we made in Section 1.1, which were about the *computational* power of proof systems. Could self-testing enable proof systems with quantum entangled provers to exceed the power of their classical counterparts?

1.2.2 MIP* and the quantum games PCP conjecture

To formalize the question, we start by defining the class MIP* of multi-prover interactive proofs with shared entanglement.

Definition 1.2.3. The complexity class $\text{MIP}^*_m(k, r, c, s)$ consists of all promise problems decidable by a multi-prover interactive proof system with a classical verifier, k provers who are allowed to share a quantum entangled state of arbitrary dimension, r rounds of purely classical interaction between the verifier and the prover, m classical bits of communication, completeness c, and soundness s. When the parameters m, c, or s are omitted we assume the same default values as in the definition of MIP.

Cleve, Høyer, Toner, and Watrous [CHTW04] made the crucial observation that before we try to show that MIP* is *more* powerful than MIP, we must first answer the highly nontrivial question of whether MIP* is even *at least* as powerful as MIP! The issue is that giving the provers access to a shared entangled state increases their ability to cheat, and thus can ruin the soundness of a the proof protocols that were used to show computational hardness for MIP. Indeed, for the class $\oplus\text{MIP}(2)$ of two-prover proof systems where the verifiers decision to accept or reject depends only on the XOR of the provers' answers, [CHTW04] showed that this collapse of soundness occurs: classically, these proof systems have the full power of NEXP whereas the class $\oplus\text{MIP}^*(2)$ resulting from allowing the provers to share entanglement is contained in EXP. Nevertheless, a series of technically sophisticated works [KKM+11, IKM09, IKP+08] culminating in [IV12, Vid13] were able to show that the classical protocols

(suitably modified) remain sound against entangled provers, and thus that MIP* contains NEXP. In terms of nonlocal games, this means that approximating the entangled value of a nonlocal game to a constant factor is at least NP-hard.

With NP-hardness established and no upper bound known, a natural next step is to conjecture QMA-hardness. This was done by Fitzsimons and Vidick [FV15], who described their conjecture as a type of quantum PCP conjecture.

Conjecture 1.2.4 (Quantum Games PCP (qGPCP) conjecture [FV15]). *The class* $\mathrm{MIP}^*_{\log}(2,1)$ *of multi-prover interactive proof systems with two provers sharing quantum entanglement, a single round of interaction, and* $O(\log(n))$ *bits of (classical) communication contains* QMA.

While no equivalence is known between this conjecture and the qHPCP (Conjecture 1.1.8), there are several reasons that justify the nomenclature. Firstly, the qGPCP conjecture is a natural "quantization" of the interactive-proofs variant of the classical PCP theorem, which was in fact historically prior to the proof-checking variant. In particular, if we take statements 1. and 2. of Theorem 1.1.4 and replace NP and MIP with QMA and MIP* appropriately, we obtain Conjecture 1.2.4. Secondly, both qGPCP and qHPCP are similar in that they explore the difference between QMA and NP by asking whether a problem that we already know is NP-hard is also QMA-hard.

Moreover, the qGPCP conjecture is perhaps more approachable than qHPCP. We saw above that some entangled games possess the property of being *self-tests*, which has no exact classical analog: to win them with close to optimal probability, the players *must* share a particular quantum state. This suggests an approach to prove qGPCP: design a self-test for the witness state of a QMA problem (e.g. the ground state of a local Hamiltonian). Such a self-test would need several properties beyond the examples of the CHSH and Magic Square games we saw above. Firstly, it would need to test for a many-qubit entangled state, whereas CHSH and Magic Square could only test for a constant number of EPR pairs. Secondly, this test would need to have good asymptotic parameters in two ways: the amount of bits of communication in the game must be at most $O(\log n)$ (so that the size of an explicit description of the game remains $\mathrm{poly}(n)$), and the test would need to have a large completeness-soundness gap: we must be able to make non-trivial guarantees on the shared state used by strategies that succeed with probability even constant far from optimal. We refer to the latter property as "robustness" of the test, and as we shall see below, the main technical step in proving qGPCP is designing a robust, communication-efficient self test for n copies of the EPR state.

The first steps towards proving qGPCP using self-testing were already laid by Reichardt, Unger, and Vazirani [RUV13a]. This work was perhaps the first to use self-testing as part of an interactive proof protocol, albeit the motivation of these authors was different: they sought to find interactive proofs for BQP. Moreover, the tests they developed were based on simple repetitions of the CHSH game and as such lacked the crucial robustness parameter. Another first step toward qGPCP was taken by Fitzsimons and Vidick in the paper introducing the conjecture, where they showed the following theorem:

Theorem 1.2.5 ([FV15]). *The class* $\mathrm{QMIP}_{O(\log(n))}(4,1,1,1-\mathrm{poly})$ *of multiprover interactive proofs with shared entanglement as well as quantum messages between the prover and verifier contains* QMA. *Indeed, the inclusion holds when the verifier's questions consist of* $O(\log(n))$ *classical bits, and the provers' responses of* $O(1)$ *quantum bits.*

The key contribution of this result was a method of sharing a copy of a QMA witness state between the provers using error correcting codes (see further discussion in Section 1.4.2). In a subsequent work, Zhengfeng Ji [Ji16a] used a variant of the CHSH game to dequantize the messages in the Fitzsimons-Vidick protocol, obtaining an identical result to Theorem 1.2.5 but for the class MIP* instead of QMIP.

1.3 Results

In this thesis, we develop a series of constructions of games, protocols, and self-tests, leading up to a proof of the qGPCP conjecture (Conjecture 1.2.4). As described above, along the way, the main technical challenge we faced was developing a self-test for many-qubit entangled states with a robust completeness-soundness gap. Our first attempt in this direction was to consider the parallel repetition of the Magic Square game, which, as mentioned above, is a self-test for the state $|\mathrm{EPR}\rangle^{\otimes 2}$. Using fairly standard techniques, we were able to show the following:

Theorem 1.3.1 ([CN16] and Corollary A.4.3 of this thesis). *The n-fold parallel repetition of the Magic Square game is a two-player self-test for the state* $|\mathrm{EPR}\rangle^{\otimes 2n}$ *with*

1. *Completeness: the honest strategy using* $|\mathrm{EPR}\rangle^{\otimes 2n}$ *succeeds with probability* 1.
2. *Soundness: any strategy succeeding with probability at least* $1-\varepsilon$ *must use a shared state that is* $\delta(\varepsilon) = O(n^2\sqrt{\varepsilon})$*-close to* $|\mathrm{EPR}\rangle^{\otimes 2n}$ *up to local isometry. succeeding*

This result is *not* robust: in order to certify the state to constant error δ, one needs to estimate the success probability up to error $\varepsilon = 1/\operatorname{poly}(n)$ and thus perform $\operatorname{poly}(n)$ repetitions of the test. Moreover, it seems impossible to improve this dependence without new techniques in the analysis of the test.

The next result, the first "main" theorem of this thesis, is a self test for many EPR pairs that *does* achieve robustness, based on a new game called the Pauli Braiding Test. This game builds upon the classical linearity test of [BLR93] as well as the Magic Square game.

Theorem 1.3.2 ([NV17a] and Theorem 3.1.1 of this thesis). *The Pauli Braiding Test is a two-player game with* $O(n)$*-bit questions and* $O(1)$*-bit answers, which acts as a self-test for* $|\mathrm{EPR}\rangle^{\otimes n}$ *with*

1. *Completeness: the honest strategy using* $|\mathrm{EPR}\rangle^{\otimes n}$ *succeeds with probability* 1.

2. *Soundness: any strategy succeeding with probability at least* $1 - \varepsilon$ *must use a shared state that is* $\delta(\varepsilon) = \text{poly}(\varepsilon)$*-close to* $|\text{EPR}\rangle^{\otimes n}$ *up to local isometry. Note that* $\delta(\varepsilon)$ *is* independent *of* n.

The analysis of this self-test introduces new techniques, which are described in greater detail in Section 1.4 and Chapter 3; very briefly, the main idea is to use Fourier analysis of matrix-valued functions over the n-qubit Pauli group to analyze nearly-optimal strategies to the test. Using this self-test together with the error-correcting code framework of [FV15], we obtain a game for the local Hamiltonian problem.

Theorem 1.3.3 ([NV17a] and Corollary 3.1.2 of this thesis). *There exists a 7-prover, 1-round* MIP* *protocol for the local Hamiltonian problem for Hamiltonians that can be written as a sum of tensor products of* σ_X *and* σ_Z *operators. For a promise gap* $\Delta = b - a$*, the protocol has* $O(n/\Delta)$*-bit questions and* $O(1)$*-bit answers, and has a constant completeness-soundness gap.*

The local Hamiltonian problem for the class of Hamiltonians that can be written as a tensor product of σ_X and σ_Z operators is QMA-complete, so this implies a protocol for QMA. However, the bits of the communication scale polynomially in n, which is exponentially more than we are allowed by Conjecture 1.2.4. Indeed, if we allow ourselves $O(\text{poly}(n))$-size questions *and* answers, then the complexity theoretic result follows from the inclusion QMA $\subseteq$ NEXP. The large communication cost of this game is inherited from the underlying self-test (Theorem 1.3.2).

In order to have a hope of proving Conjecture 1.2.4, we require a self-test with robust soundness as well as low communication. We achieve this using a test that is similar to the Pauli Braiding Test, but whose classical component is the planes vs. points test for low-degree polynomials of Raz and Safra [RS97]. As a necessary prerequisite, we first show that this test is sound against two entangled provers (for three or more provers, this had been shown by [Vid13])—as a consequence showing that two-player entangled games are NP-hard.

Theorem 1.3.4 ([NV17b] and Theorem 4.1.1 of this thesis). *The Raz-Safra low degree test is sound against two entangled provers. As a consequence, it is* NP*-hard to approximate the entangled value of a nonlocal game with two players up to a constant factor.*

With the classical low-degree test as a key component, we can now design a robust, efficient self-test for many qubits of entanglement. The full theorem statement characterizing this self-test is quite technical; we give an informal version here.

Theorem 1.3.5 ([NV18] and Theorem 5.3.2 in this thesis). *The* quantum low degree test *is a two-player self test for the state* $|\text{EPR}\rangle^{\otimes n}$ *with* $O(\log(n))$*-bit questions and answers and completeness* 1*, and any strategy succeeding with probability* $1 - \varepsilon$ *must use a state that is* $O(\text{poly}(\varepsilon))$*-close to* $|\text{EPR}\rangle^{\otimes n}$ *up to local isometry.*

This self-test finally has parameters that are good enough to enable us to prove Conjecture 1.2.4, bringing us to the final main result of the thesis.

Theorem 1.3.6 ([NV18] and Theorem 5.1.2 in this thesis). *It is* QMA*-hard under poly-time randomized reductions to decide whether the entangled value of a seven-player nonlocal game is* 1 *or at most* $\frac{1}{2}$.

In passing from Theorem 1.3.5 to Theorem 1.3.6, we use similar ideas to the proof of Theorem 1.3.3 from Theorem 1.3.2. However, there are many additional technical subtleties, which result in the appearance of randomized reductions in Theorem 1.3.6. For a more detailed description, see Section 5.1.

1.4 Technical overview

The main technical contribution of this thesis is a proof of the quantum games PCP conjecture, following the lines of the original proof of the classical PCP theorem based on low-degree testing of multivariate polynomials. To explain our approach, it is thus, useful to start with a brief summary of the proof of the classical PCP theorem.

1.4.1 The classical PCP theorem: a brief overview

Let L be a language in NP, and suppose we are given an input ϕ and would like to decide whether it lies in L. For concreteness, it may be useful to take L to be the set of satisfiable 3SAT formulas, and ϕ to be a given formula. Since L is in NP, we know that if $\phi \in L$, then there exists some polynomially long proof x certifying this fact (the assignment to the variables of the formula, in our example). However, to verify the proof x will in general require reading all of its bits and performing a polynomial-time computation. The PCP theorem asserts that there exists a special "locally testable" encoding Π_x of the proof x, still consisting of polynomially many bits, and a polynomial-time verification algorithm V with the following properties:

1. The verifier V flips $O(\log(n))$ random coins, and queries $O(\log(n))$ locations in the proof Π.

2. Completeness: if ϕ is in the language L, then V must accept Π_x with high probability—say, certainty.

3. Soundness: if ϕ is *not* in the language L, then for *any* purported proof Π (not necessarily taking the form of a valid encoding Π_ϕ for any ϕ), the verifier must reject with at least a constant probability—say, 1/2.

Roughly speaking, these requirements would be satisfied if Π_x were the encoding of x under an error correcting code with large distance, and for which the checks are local in the sense of acting on only $O(\log n)$ bits each. Moreover, the code should have a good rate, so that the encoding Π_x is only polynomially longer than the unencoded proof x.

As a first attempt, one can try to use a code that has all these properties except for the rate: the Hadamard code. The Hadamard encoding of a string $x \in \mathbb{F}_2^n$ is the truth table of the linear function $f_x : \mathbb{F}_2^n \to \mathbb{F}_2$ defined by $f_x(a) = x \cdot a$, where the

inner product is taken over $\mathbb{F}_2$. The truth table of this function is 2^n bits long, so the encoding is exponentially long. However, this code has a very good distance: if $x \neq x'$, then half of the bits of the encodings of x and x' will differ. Moreover, this code is locally checkable: it was shown by Blum, Luby, and Rubinfeld [BLR93] that one can test whether a given f is a valid codeword by querying it at pointsa, b, and $a + b$ for a randomly chosen $a, b \in \mathbb{F}_2^n$, and verifying that $f(a) + f(b) = f(a + b)$. Any valid codeword will pass the BLR test with certainty, whereas if f differs from any valid codeword on at least a constant fraction of points, then it will be rejected with constant probability by this test. Based on this, one can design the following "exponential PCP":

Theorem 1.4.1 ([ALM+98]). *For any language L in* NP*, there exists a polynomial-time verification algorithm V which, given an instance ϕ and access to an exponentially-long proof string Π, flips* poly(n) *random coins and reads $O(1)$ locations of Π, with the following properties:*

1. *If $\phi \in L$, then there exists a proof Π that is accepted by V with certainty.*
2. *If $\phi \notin L$, then V rejects all proofs Π with probability at least* $1/10$.

The proof string Π is essentially the Hadamard encoding of an NP witness for the instance ϕ, and the test executed by the verifier is the BLR test. The full PCP theorem is obtained by following a similar approach, except using a better error-correcting code: the Reed-Muller code, which encodes a string x into a multivariate low-degree polynomial $g_x(\cdot)$ over a finite field $\mathbb{F}_q$. The role of the BLR test is now played by a test for low-degree polynomials, such as that of Raz and Safra [RS97]. There is a further technical difficulty: directly applying this approach leads to a proof where the verifier needs to read poly $\log(n)$ bits. To reduce this to $O(\log(n))$ bits requires *composing* the

The preceding sketch was presented in terms of the "proof-checking" variant of PCP, but as remarked below Theorem 1.1.4, we can easily pass from this to the multiprover interactive proofs version by using the clause-variable game.

1.4.2 Quantizing the PCP theorem: obstacles and resolutions

We now proceed to the setting of the quantum games PCP, where we start with a promise problem lying in QMA—for concreteness, we may take the local Hamiltonian problem. Then, given an instance H (a local Hamiltonian, in our example), we know that if it is a YES instance of our problem, there exists a quantum proof state $|\psi\rangle$ which certifies this fact (in our example, the ground state of H). However, certifying a given proof state $|\psi\rangle$ requires performing a polynomial-time quantum computation on $|\psi\rangle$—for example, in the local Hamiltonian problem, this is because the verifier needs to measure the energy of $|\psi\rangle$ under H up to inverse-polynomial precision. In proving a quantum games PCP theorem, our goal is to replace this verification procedure by a multiprover protocol in which the verifier is entirely *classical* and exchanges only $O(\log(n))$ classical bits of communication with each prover.

If we try to directly "quantize" the classical proof described in Section 1.4.1, making liberal use of wishful thinking, we might proceed as follows:

1. Hypothesize the existence of a locally-testable encoding $|\Pi\rangle$ of the proof state $|\psi\rangle$, with the property that the energy of $|\psi\rangle$ under H can be estimated up to inverse-polynomial precision by performing a single local measurement on $|\Pi\rangle$.

2. Demand that the two provers each possess a copy of $|\Pi\rangle$. The verifier will then ask each prover to perform, say, up to $O(\log(n))$ local measurements on $|\Pi\rangle$ and return their outcomes, and use these measurements to estimate the energy of $|\psi\rangle$.

3. To ensure soundness, the verifier will check that the provers both share the same state $|\Psi\rangle$, by performing some sort of consistency check between the provers' answers.

Unfortunately, the approach sketched above immediately runs into several serious obstacles. Firstly, the existence of such a locally-testable encoding is itself a long-standing open problem in quantum information theory, which seems to be closely tied to the Hamiltonian formulation of the quantum PCP conjecture [AE13]. Secondly, even accepting that such an encoding exists, it is unclear how to implement the "consistency checks" described above. Generically, $|\Pi\rangle$ will be a highly entangled quantum state, and the reduced state of any small subset of the qubits (which is all that local measurements can access) will be highly mixed and contain little information about the global state. To use an analogy due to John Preskill [Pre18], in a quantum book, every individual page is gibberish, and almost all the information lies in the correlations between pages. Moreover, this approach does not exploit the ability of the provers to share entanglement and is thus doomed to failure, as a protocol where honest provers share no entanglement can only be at most as powerful as NP.

To proceed, we need to modify our approach in several ways. A schematic outline of our protocol is given in Figure 1-3. Below, we explain the main ideas at a high level.

The first change we make is to **replace copying by sharing:** rather than asking each of the k provers to hold a separate copy of some quantum proof state, we will "stretch" the QMA proof state $|\psi\rangle$ into a k-partite entangled state $|\Psi\rangle$, and give each prover a share of it. Concretely, this will be realized by encoding each qubit of $|\psi\rangle$ into a k-qubit error-correcting code $\mathcal{C}$, and distributing one of the qubits to each prover. This idea was introduced by Fitzsimons and Vidick [FV15], and they used it to show (Theorem 1.2.5) the first multi-prover protocol for QMA, albeit with *quantum messages*. The Fitzsimons-Vidick protocol is very simliar to the clause-variable game, except that, in response to an index i, the provers respond with the ith qubit of their share of $|\Psi\rangle$, rather than the ith bit of a classical proof. Instead of checking equality, the verifier checks that the joint state of the qubits is a valid code state of the code $\mathcal{C}$.

The next idea we need is **self-testing**, in order to verify that the provers indeed share a copy of $|\Psi\rangle$. Thus far, we have spoken of self-tests purely in terms of the

state being certified, but actually it is more useful to think of a the test as certifying *measurement operators* acting on the state. Somewhat informally, a test certifies a shared state $|\Psi\rangle$ and a set of measurements operators $\{M_j\}$ on prover i if, for any strategy succeeding with nearly optimal probability, there exists a local isometry under which the provers' shared state is mapped close to $|\Psi\rangle$, *and* for each question j sent to prover i, the post-measurement state after prover i has executed its strategy is close to $M_i \otimes \mathrm{Id}\,|\Psi\rangle$. We often phrase this guarantee more compactly as saying that the measurement operator N_j used by the prover in response to question j must be close to M_i in *state-dependent distance* relative to the state $|\Psi\rangle$. All known analyses of self-tests for states actually proceed by showing a stronger guarantee of this type: for example, Theorem 1.2.2 certifies not just the state $|\mathrm{EPR}\rangle$ but also the single-qubit measurements X, Z, X', Z' from the honest strategy (Definition 1.2.1).

The operator-based perspective on self-testing is useful to us for several reasons. Firstly, since our eventual goal is to certify that $|\Psi\rangle$ is an encoding of a low-energy state of a given Hamiltonian H, we need some method of measuring both H as well as the check operators of the code $\mathcal{C}$ on $|\Psi\rangle$. We can do this with a self-test for a rich enough set of measurements: in particular, the set of all n-qubit tensor products of Pauli σ_X and σ_Z matrices suffice for this purpose, provided we choose H and $\mathcal{C}$ appropriately. The Pauli operators are an especially fortunate choice because they enable us to use the rich theory of stabilizer codes. In particular, we make heavy use of a technique discovered by Ji [Ji16a] that allows us to "lift" any two-player self-test for Pauli operators on the EPR state $|\mathrm{EPR}^{\otimes}\rangle$ to a k-player self-test for codewords of a k-qubit code $\mathcal{C}$. This technique, which we refer to as the idea of a "composite prover,"results in a great conceptual simplification: we have reduced the problem of testing an arbitrary encoded state $|\Psi\rangle$ to testing the fixed state $|\mathrm{EPR}^{\otimes n}\rangle$.

The second main advantage of the operator-based perspective is that it makes it easier for us to transfer insights from the classical proof of the PCP theorem sketched in Section 1.4.1. To see this, let us compare our desired quantum self-test for the X and Z Pauli operators with the example of the Hadamard code. For each string $a \in \mathbb{F}_2^n$, let $X(a)$ be the n-qubit operator obtained by taking the tensor product of σ_X operators acting on locations where a has a 1, and Id where a has a 0, and likewise, let $Z(a)$ be the tensor product of σ_Z and Id defined in the same way. We would like to certify that in response to a certain question, a prover measures the operator $X(a)$ on its share of the state and returns its outcome. We can imagine this measurement as taking place in two stages: first, the prover measures each qubit of its share in the X-basis to obtain a random string x, and then responds with the value of the Hadamard encoding $f_x(a)$ at position a. The same story holds for the operators $Z(a)$, except each qubit is now measured in the Z-basis. This perspective of a **classical locally-testable code applied to quantum measurement outcomes** suggests an approach for testing the tensor Pauli operators $X(a), Z(a)$: we should try to combine the BLR test for the Hadamard code with a test that forces the provers to use the correct X or Z basis. This intuition is the basis for the Pauli Braiding Test (Theorem 1.3.2), and indeed, the analysis of this test is in some sense a "matrix-valued generalization" of Bellare et al.'s Fourier-analytic proof of soundness of the BLR test [BCH+96]. Moreover, the same intuition, applied to the Reed-Muller code

rather than the Hadamard code, enables us to obtain the communication efficient self-test (Theorem 1.3.5) needed for the proof of qGPCP.

---

1. Given an instance H with an n-qubit proof state $|\psi\rangle$, the k honest provers will share amongst themselves a kn-qubit encoded state $|\Psi\rangle = \mathcal{E}(|\psi\rangle)$, obtained by encoding each qubit of $|\psi\rangle$ with a k-qubit quantum error correcting code $\mathcal{C}$. As a result, each prover will be highly entangled with the others. The provers and verifier also agree on a scheme to *amplify* the gap of H, producing a Hamiltonian H' which is a sum of (nonlocal) terms, each of which is a tensor product of Paulis. The goal of the verifier is to estimate the energy of $|\psi\rangle$ under H up to a constant.

2. The verifier performs one of the operations with probability 1/2 each:

   (a) Execute a *robust self-test* between the provers, in which the verifier commands the provers to measure an observable drawn from a set $\mathcal{P}$ of tensor products $\otimes_{i=1}^{n}(\sigma_X)^{a_i}$ or $\otimes_{i=1}^{n}(\sigma_Z)^{a_i}$ of single-qubit Pauli operators. The test verifies that the provers' shared state $|\Psi\rangle$ is a valid code state of the code $\mathcal{C}$, and that each prover applies the measurement observable it was instructed to use.

   (b) Estimate the energy of $|\psi\rangle$ under H' by choosing a single term h from H' at random, and asking each prover to measure an operator from $\mathcal{P}$, such that their product is the logical operator corresponding to h in the code $\mathcal{C}$.

Figure 1-3: A schematic protocol.

Finally, there are two further ideas that play important roles in our constructions. The first was already implicit in the discussion of self-testing above: in order to robustly test a state $|\Psi\rangle$, we must use **nonlocal measurements**. This is reflected in the fact that our self-tests certify high-weight tensor products of Pauli operators, which act on a large fraction of the qubits. A futher way in which we use nonlocality is in **amplifying** the promise gap of the Hamiltonian H we are trying to test. Recall that (short of proving the qHPCP conjecture), we only know QMA-hardness for the local Hamiltonian problem with an an inverse-polynomial promise gap, yet we would like our game to have a *constant* completeness-soundness gap. This means that if the energy of the state $|\Psi\rangle$ is too high by even a very small amount, we should detect this with constant probability. If we were restricted to only making local measurements on $|\Psi\rangle$, we would be stuck, as this is essentially the difficulty of proving qHPCP. However, since in the games setting we can command the provers to perform highly nonlocal measurements, we can use energy amplification techniques

that are far too wasteful for qHPCP: in particular, we make use of a simple tensor-product amplification scheme, asking the provers to measure $H^{\otimes m}$ on many copies of the ground state for $m = \text{poly}(n)$. The second idea that is important in achieving the final parameters of qGPCP is **composition**. This plays a similar role in our proof as it does in the proof of the classical PCP theorem, and we use it in several ways: composition with the quantum Pauli Braiding Test as the inner PCP, as well as composition with the inner PCP being a classical PCP of proximity. One important subtlety that arises in our setting is the need to preserve completeness: classical uses of composition assume that both provers possess a full copy of the entire proof string, whereas in our protocols, each prover only has part of an encoding of the proof state.

1.5 Applications and future work

The classical PCP theorem had far-reaching implications in computer science, such as implying a slew of new hardness of approximation results for combinatorial optimization problems. Although comparatively fewer applications are currently known for qGPCP (or, for that matter, qHPCP), the techniques developed in this thesis have already resulted in progress along an important direction: realistic interactive proof protocols for the class BQP of *polynomial-time* quantum computation. The qualifier "realistic" is important here: since we know that BQP $\subseteq$ PSPACE, one could always apply the IP = PSPACE protocol to verify BQP computations. However, the honest prover in this protocol requires the full prover of PSPACE, whereas we are unlikely to ever build a device more powerful than BQP in the real world. Thus, a "realistic" protocol is one in which the *honest* provers only need the power of BQP (even though soundness would ideally hold against cheating provers without this restriction). Prior to the work in this thesis, there were two results in this area: the pioneering work of Reichardt, Unger, and Vazirani [RUV13a], which obtained a realistic MIP* protocol for BQP with resources scaling polynomially in the size of the circuit being computed, and a paper of Fitzsimons and Hajdušek, which observed that any protocol for the local Hamiltonian problem in which the honest provers need only to perform simple measurements on the ground state immediately implies a protocol for BQP. This follows from the fact that the history state—the QMA witness for a BQP problem—is itself constructible in BQP. This observation, can be immediately combined with our protocols for the local Hamiltonian problem to obtain delegation schemes for BQP. However, these have the undesirable feature of being "post hoc": the entire circuit to be computed must be communicated to the provers before they can prepare their shared entangled state. A subsequent work [CGJV17] removed this obstacle, building on our Pauli Braiding test to introduce nearly optimal protocols for delegated computation of BQP, where the resources of the protocol scale quasi-linearly in the size of the circuit being delegated. In comparison with the original protocol of [RUV13a], the savings achieved by using the Pauli Braiding test are considerable: to delegate a circuit of m gates, the RUV protocol required total resources (i.e. prover and verifier run time and communication) at least m^{8192}, whereas the protocol of [CGJV17] achieve a scaling of $\Theta(m \log m)$.

A second possible application, which remains to be explored, is to quantum cryptography. Already, self-tests have been used to certify the generation of randomness by quantum devices [Col06] and to design "device-independent" protocols for tasks like quantum key distribution [Eke91, BHK05, VV14], for which security holds with minimal assumptions on the devices used to implement the protocol. Could our improved self-tests be used to achieve better results in this space?

In addition, we see several more speculative directions for future research. One particularly exciting direction is to show much stronger lower bounds for MIP*, potentially by combining our results with the "compression" scheme of Ji [Ji16c]. The latter is a method for reducing the communication in any MIP* protocol from $\text{poly}(n)$ to $\log(n)$, albeit at the cost of shrinking the completeness-soundness gap. The compression scheme proceeds by constructing a sort of "generalized Hamiltonian" for the starting MIP* protocol, whose ground states encode transcripts of accepting interactions between the verifier and the provers. The compressed protocol then consists of a self-test akin to the one appearing in [Ji16a], verifying that the provers share a ground state of this generalized Hamiltonian. Could our results enable a version of this compression scheme with no loss in the completeness-soundness gap? As pointed out in [Ji16a], such a result could have interesting consequences if applied recursively to itself, perhaps leading to much stronger lower bounds for MIP* than any known so far. Indeed, as no upper bound is known for this class, the sky is the limit. We also note that showing that MIP* is not decidable would imply the falsehood of Connes' embedding conjecture, a longstanding conjecture in operator algebras [Oza13, FNT14].

1.6 Organization and bibliographical information

In Chapter 2, we introduce basic notation that is used throughout the rest of the thesis. In Chapter 3, we construct a robust self-test for many EPR paris based on linearity testing and the Hadamard code, and use this to construct an exponential quantum games PCP. In Chapter 4, we show that the classical low-degree test of Raz and Safra is sound against two entangled provers. Building on this test as well as our quantum linearity test, in Chapter 5, we give an exponentially more efficient construction of a robust self-test for many EPR pairs. This test enables us in Chapter 6 to prove the quantum entangled games PCP theorem, under randomized reductions. Finally, in Appendix A, to illustrate the difficulties of constructing a robust self-test for many qubits of entanglement, we analyze the parallel repetition of the Magic Square game using prior state-of-the-art self-testing techniques, obtaining only inverse-polynomial (rather than constant) robustness.

The main body of this thesis is based on a series of joint papers with Thomas Vidick: Chapter 3 is based on [NV17a], which was published in the proceedings of STOC'17, Chapter 4 is based on [NV17b], to appear in the proceedings of CCC'18, and Chapters 5 and 6 on [NV18] which is in submission. The appendix is based on a joint work with Matthew Coudron [CN16].

Chapter 2

Preliminaries

We assume basic familiarity with quantum information but give all required definitions. We refer to the standard textbook [NC01] for additional background material.

2.1 Quantum states and measurements

A n-qubit pure quantum state is represented by a unit vector $|\psi\rangle \in \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2 = (\mathbb{C}^2)^{\otimes n} \approx \mathbb{C}^{2^n}$, where the ket notation $|\cdot\rangle$ is used to signify a column vector. A bra $\langle\psi|$ is used for the conjugate-transpose $\langle\psi| = |\psi\rangle^\dagger$, which is a row vector. We use $\||\psi\rangle\|^2 = |\langle\psi|\psi\rangle|$ to denote the Euclidean norm, where $\langle\psi|\phi\rangle$ is the skew-Hermitian inner product between vectors $|\phi\rangle$ and $|\psi\rangle$. A n-qubit mixed state is represented by a density matrix, a positive semi-definite matrix $\rho \in \mathbb{C}^{2^n} \times \mathbb{C}^{2^n}$ of trace 1. The density matrix associated to $|\psi\rangle$ is the rank-1 projection $|\psi\rangle\langle\psi|$. We use $\mathrm{D}(\mathcal{H})$ to denote the set of all density matrices on $\mathcal{H}$.

For a matrix X, $\|X\|$ will refer to the operator norm, the largest singular value. When the Hilbert space can be decomposed as $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ for some $\mathcal{H}_A$ and $\mathcal{H}_B$, and X is an operator on $\mathcal{H}_A$, we often write X as well for the operator $X \otimes \mathrm{Id}_{\mathcal{H}_B}$ on $\mathcal{H}$. It will always be clear from context which space an operator acts on. All Hilbert spaces considered in the thesis are finite dimensional.

We use $\mathrm{Pos}(\mathcal{H})$ to denote the set of positive semidefinite operators on $\mathcal{H}$. A n-qubit measurement (also called POVM, for projective operator-valued measurement) with k outcomes is specified by k positive matrices $M = \{M_1, \ldots, M_k\} \subseteq \mathrm{Pos}(\mathbb{C}^{2^n})$ such that $\sum_i M_i = \mathrm{Id}$. The measurement is *projective* if each M_i is a projector, i.e. $M_i^2 = M_i$. The probability of obtaining the i-th outcome when measuring state ρ with M is $\mathrm{Tr}(M_i\rho)$. By Naimark's dilation theorem, any POVM can be simulated by a projective measurement acting on an enlarged state; that is, for every POVM $M = \{M_i\}_i$ acting on state $|\psi\rangle \in \mathcal{H}$ there exists a projective measurement $M' = \{P_i\}_i$ and a state $|\psi\rangle \otimes |\phi\rangle \in \mathcal{H} \otimes \mathcal{H}_{\text{ancilla}}$ with the same outcome probabilities as M. Moreover, the post-measurement state after performing M is the same as the *reduced* post-measurement state obtained after performing M' and tracing out the ancilla subsystem $\mathcal{H}_{\text{ancilla}}$.

An n-qubit observable is a Hermitian matrix $O \in \mathbb{C}^{2^n} \times \mathbb{C}^{2^n}$ that squares to

identity. We use $\mathrm{Obs}(\mathcal{H})$ to denote the set of observables acting on $\mathcal{H}$. $O \in \mathrm{Obs}(\mathcal{H})$ is diagonalizable with eigenvalues ± 1, $O = P_+ - P_-$, and $P = \{P_+, P_-\}$ is a projective measurement. For any state ρ, $\mathrm{Tr}(O\rho)$ is the expectation of the ± 1 outcome obtained when measuring ρ with P. If $\rho = |\psi\rangle\langle\psi|$ we abbreviate this quantity, $\mathrm{Tr}(O\rho) = \mathrm{Tr}(P_+\rho) - \mathrm{Tr}(P_-\rho) = \langle\psi|O|\psi\rangle$ as $\langle P\rangle_\psi$.

A convenient orthogonal basis for the real vector space of n-qubit observables is given by the set $\{I, \sigma_X, \sigma_Y, \sigma_Z\}^{\otimes n}$, where $\{I, \sigma_X, \sigma_Y, \sigma_Z\}$ are the four single-qubit Pauli observables

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{2.1}$$

We call the eigenbasis of σ_X (resp. σ_Z) the X-basis (resp. Z-basis). We often consider operators that are tensor products of just I and σ_X, or just I and σ_Z. We denote these by $\sigma_X(a), \sigma_Z(b)$, where the strings $a, b \in \{0,1\}^n$ indicate which qubits to apply the σ_X or σ_Z operators to: a 0 in position i indicates an I on qubit i, and a 1 indicates an σ_X or σ_Z. We denote by

$$|\mathrm{EPR}\rangle = \frac{1}{\sqrt{2}}|0\rangle|0\rangle + \frac{1}{\sqrt{2}}|1\rangle|1\rangle$$

the unique state stabilized by both $\sigma_X \otimes \sigma_X$ and $\sigma_Z \otimes \sigma_Z$.

2.2 Stabilizer codes

Stabilizer codes are the quantum analogue of linear codes. For an introduction to the theory of stabilizer codes we refer to [Got97]. We will only use very elementary properties of such codes.

The codes we consider are *Calderbank-Shor-Steane (CSS) codes* [CS96, Ste96]. For an r-qubit code the codespace, the vector space of all valid codewords, is the subspace of $(\mathbb{C}^2)^{\otimes r}$ that is the simultaneous $+1$ eigenspace of a set $\{S_1, \ldots, S_k\}$ of r-qubit pairwise commuting Pauli observables called the stabilizers of the code. The stabilizers form a group under multiplication. Unitary operations, such as a Pauli X or Z operators, on the logical qubit are implemented on the codespace by logical operators $X_{logical}$ and $Z_{logical}$. The smallest CSS code is Steane's 7-qubit code [Ste96]. Table 2.1 lists a set of stabilizers that generate the stabilizer group of the code.

Every CSS code satisfies certain properties which will be useful for us. Firstly, both the stabilizer generators and the logical operators can be written as tensor products of only I, σ_X, and σ_Z operators — there are no σ_Y. This simplifies our protocol, allowing us to consider only two distinct basis settings. Secondly, every CSS code has the following symmetry: for every index $i \in [r]$ there exists stabilizers S_X, S_Z such that S_X is a tensor product of only σ_X and I operators and has an σ_X at position i, and S_Z is equal to S_X with all σ_X operators replaced by σ_Z operators.

These properties imply the following simple observation, which will be important for us. For every Pauli operator $P \in \{I, \sigma_X, \sigma_Z\}$ acting on the i-th qubit of the code

	1	2	3	4	5	6	7
Stabilizers	I	I	I	σ_X	σ_X	σ_X	σ_X
	I	σ_X	σ_X	I	I	σ_X	σ_X
	σ_X	I	σ_X	I	σ_X	I	σ_X
	I	I	I	σ_Z	σ_Z	σ_Z	σ_Z
	I	σ_Z	σ_Z	I	I	σ_Z	σ_Z
	σ_Z	I	σ_Z	I	σ_Z	I	σ_Z
Logical X	σ_X	σ_X	σ_X	σ_X	σ_X	σ_X	σ_X
Logical Z	σ_Z	σ_Z	σ_Z	σ_Z	σ_Z	σ_Z	σ_Z

Table 2.1: Stabilizer table for the 7-qubit Steane code

there is a tensor product $\bar{P}$ of Paulis acting on the remaining $(r-1)$ qubits such that $P \otimes \bar{P}$ is a stabilizer operator on the whole state, and moreover each term in the tensor product is either identity or P. Indeed, the choice of $\bar{P}$ is not unique. Henceforth, we use the notion $\bar{P}$ to denote *any* such operator, unless otherwise specified.

2.3 Local Hamiltonians

A n-qubit local Hamiltonian is a Hermitian, positive semidefinite operator H on $(\mathbb{C}^2)^{\otimes n}$ that can be decomposed as a sum $H = \sum_{i=1}^{m} H_i$ with each H_i is local, i.e. H_i can be written as $H_i = I \otimes \cdots I \otimes h_i \otimes I \otimes \cdots \otimes I$, where h_i is a Hermitian operator on $(\mathbb{C}^2)^{\otimes k}$ with norm (largest singular value) at most 1. The smallest k for which H admits such a decomposition is called the locality of H. The terms are normalized such that $\|H_i\| \leq 1$ for all i. A family of Hamiltonians $\{H_i\}$ acting on increasing numbers of qubits is called local if all H_i are k-local for some k independent of n (for us k will always be 2).

The local Hamiltonian problem is the prototypical QMA-complete problem, as 3SAT is for NP.

Definition 2.3.1. Let $k \geq 2$ be an integer. The *k-local Hamiltonian problem* is to decide, given a family of k-local Hamiltonians $\{H_n\}_{n \in \mathbb{N}}$ such that H_n acts on n qubits, and functions $a, b : \mathbb{N} \to (0,1)$ such that $b - a = \Omega(\text{poly}^{-1}(n))$, if the smallest eigenvalue of H_n is less than $a(n)$ or greater than $b(n)$.

Here we restrict our attention to Hamiltonians

$$H = \frac{1}{m} \sum_{i=1}^{m} H_i,$$

for which each term H_i can be written as a linear combination of tensor products of Pauli I, σ_X and σ_Z observables only. Such Hamiltonians are known to be QMA complete for some constant k (see Lemma 22 of [Ji16a] for a proof).

2.4 State-dependent distance measure and approximations

We make extensive use of a state-dependent distance between measurements that has been frequently used in the context of entangled-prover interactive proof systems (see e.g. [IV12, Ji16a]). For ρ a positive semidefinite matrix and X any linear operator define

$$\mathrm{Tr}_\rho(X) = \mathrm{Tr}(\rho X).$$

For any two operators S, T, define the *state-dependent distance* between S an T on a ρ as

$$\mathrm{d}_\rho(S,T) := \sqrt{\mathrm{Tr}_\rho\left((S-T)^\dagger(S-T)\rho\right)}.$$

Based on the state-dependent distance we define a distance between POVMs, given by summing the state-dependent distance between the square roots of the POVM elements. Let $\{M^a\}$ and $\{N^a\}$ be two POVMs with the same number of outcomes, indexed by a, and let $|\psi\rangle$ be a quantum state. Then the state-dependent distance between the POVMs M and N on ρ is denoted as $\mathrm{d}_\rho(\sqrt{M}, \sqrt{N})$ and defined as

$$\mathrm{d}_\rho(\sqrt{M}, \sqrt{N}) = \Big(\sum_a \mathrm{d}_\rho\left(\sqrt{M^a}, \sqrt{N^a}\right)^2\Big)^{1/2}.$$

While this notation is ambiguous (since the sum over outcomes is not explicitly indicated), context will always make it clear which notion of d_ρ is intended. We will also drop the square roots in the case of POVMs that are projective measurements.

To simplify the notation, let $A^a = \sqrt{M^a}$ and $B^a = \sqrt{N^a}$. Then this distance can be rewritten as:

$$\begin{aligned}\mathrm{d}_\rho(\sqrt{M}, \sqrt{N})^2 &= \sum_a \mathrm{Tr}_\rho\left((A^a - B^a)^2\rho\right) \\ &= 2 - \sum_a \Re\,\mathrm{Tr}_\rho\left(A^a B^a\right), \end{aligned} \tag{2.2}$$

where we used the fact that A^a and B^a are Hermitian and their squares sum to identity. If we specialize to the case of projective measurements with binary outcomes, we get the following relations (here $A = A^1 - A^{-1}$ and $B = B^1 - B^{-1}$ are the observables associated to the measurements):

$$\begin{aligned}\mathrm{d}_\rho(\sqrt{M}, \sqrt{N})^2 &= 2 - \mathrm{Tr}_\rho\left(A^1B^1 + A^{-1}B^{-1} + B^1A^1 + B^{-1}A^{-1}\right) \\ &= 2 - \frac{1}{4}\mathrm{Tr}_\rho\left((\mathrm{Id}+A)(\mathrm{Id}+B) + (\mathrm{Id}-A)(\mathrm{Id}-B) + (\mathrm{Id}+B)(\mathrm{Id}+A)\right. \\ &\quad \left. + (\mathrm{Id}-B)(\mathrm{Id}-A)\right)|\psi\rangle \\ &= 2 - \frac{1}{4}\mathrm{Tr}_\rho\left(4\,\mathrm{Id} + 2AB + 2BA\right) \\ &= 1 - \frac{1}{2}\mathrm{Tr}_\rho\left(AB + BA\right)\end{aligned}$$

$$= \frac{1}{2}\operatorname{Tr}_\rho\left((A-B)^2\right) \tag{2.3}$$
$$= \mathrm{d}_\rho(A,B)^2.$$

This distance measure has the following useful property:

Lemma 2.4.1. *Let ρ be positive semidefinite, C be a linear operator such that $\|CC^\dagger\| \leq K$ and S, T linear operators. Then*

$$\left|\operatorname{Tr}_\rho(CS) - \operatorname{Tr}_\rho(CT)\right| \leq \sqrt{2K}\,\mathrm{d}_\rho(S,T).$$

Likewise, if $\{C_a\}$ a family of operators such that $\|\sum_a C_a C_a^\dagger\| \leq K$ and $\{M^a\}$ and $\{N^a\}$ POVMs. Then

$$\left|\sum_a \operatorname{Tr}_\rho\left(C_a\sqrt{M^a}\right) - \sum_a \operatorname{Tr}_\rho\left(C_a\sqrt{N^a}\right)\right| \leq \sqrt{K}\,\mathrm{d}_\rho(\sqrt{M},\sqrt{N}).$$

Proof. The proof of both results is identical, and uses the Cauchy-Schwarz inequality; we show only the proof of the second. Let $A^a = \sqrt{M^a}$ and $B^a = \sqrt{N^a}$. Applying the Cauchy-Schwarz inequality,

$$\begin{aligned}\left|\sum_a \operatorname{Tr}_\rho\left(C_a(A^a - B^a)\right)\right| &\leq \left|\operatorname{Tr}_\rho\Big(\sum_a C_a C_a^\dagger\Big)\right|^{1/2}\left|\operatorname{Tr}_\rho\Big(\sum_a (A^a-B^a)^2\Big)\right|^{1/2} \\ &\leq \sqrt{K}\,\mathrm{d}_\rho(\sqrt{M},\sqrt{N}),\end{aligned}$$

as claimed. □

A second measure of proximity that is often convenient is the *consistency*. As before, let $\{M^a\}$ and $\{N^a\}$ be POVMs with the same number of outcomes. Then their consistency is defined as

$$\mathrm{C}_\rho(M,N) = \Re\Big(\sum_a \operatorname{Tr}_\rho\left(M^a N^a\right)\Big),$$

so that by (2.2) we have

$$\mathrm{d}_\rho(\sqrt{M},\sqrt{N})^2 = 2 - 2\,\mathrm{C}_\rho(\sqrt{M},\sqrt{N}). \tag{2.4}$$

For collections of binary observables $\{A(a)\}$ and $\{B(a)\}$ we use

$$\begin{aligned}\mathrm{C}_\rho(A,B) &= \sum_a \Re\Big(\sum_{c\in\{0,1\}} \frac{1}{4}\operatorname{Tr}_\rho\left((\mathrm{Id}+(-1)^c A(a))(\mathrm{Id}+(-1)^c B(a))\right)\Big) \\ &= \frac{1}{2}\Re\Big(1 + \sum_a \operatorname{Tr}_\rho\left(A(a)B(a)\right)\Big).\end{aligned}$$

A useful property of the consistency is that if M and N are POVMs acting on two separate subsystems of ρ, applying Naimark dilation to each of them results in projective measurements M' and N' and a state ρ' such that $\mathrm{C}_\rho(M,N) = \mathrm{C}_{\rho'}(M',N')$.

Given two observables A and B, the product AB is an observable if and only if A and B commute. The following lemma shows how to define a "product" observable C when A and B commute only approximately in state-dependent distance, such that the action of C on the state is close to AB (and BA).

Lemma 2.4.2. *Let ρ be a density matrix and A, B observables such that the bound $\mathrm{d}_\rho(AB, BA) \leq \delta$ holds for some $\delta \geq 0$. Let C be the observable defined by*

$$C = \frac{AB + BA}{|AB + BA|},$$

where we use the convention that $M/|M|$ is defined as the identity on the kernel of M. Then

$$\max\Big\{ \mathrm{d}_\rho(C, AB),\, \mathrm{d}_\rho(C, BA)\Big\} \leq \frac{\sqrt{2}}{2}\delta.$$

Proof. It is clear from the definition that C is Hermitian and an observable (i.e. all its eigenvalues are ± 1). Evaluate

$$\mathrm{d}_\rho(AB, C)^2 = 2 - \mathrm{Tr}_\rho\Big(\frac{AB + BA}{|AB + BA|}AB + BA\frac{AB + BA}{|AB + BA|}\Big).$$

Notice that AB and BA both commute with $(AB + BA)$ and hence with $(AB + BA)/|AB + BA|$. Thus the above expression simplifies to

$$\begin{aligned}
\mathrm{d}_\rho(AB, C)^2 &= 2 - \mathrm{Tr}_\rho\Big(\frac{(AB + BA)^2}{|AB + BA|}\Big) \\
&\leq 2 - \mathrm{Tr}_\rho |AB + BA| \\
&\leq 2 - \frac{1}{2}\mathrm{Tr}_\rho\big((AB + BA)^2\big) \\
&= 2 - \frac{1}{2}\mathrm{Tr}_\rho\big(2\,\mathrm{Id} + ABAB + BABA\big).
\end{aligned}$$

From the assumption, $\mathrm{d}_\rho(AB, BA)^2 = \mathrm{Tr}_\rho(2\,\mathrm{Id} - ABAB - BABA) \leq \delta^2$. Substituting in the above, we get $\mathrm{d}_\rho(AB, C)^2 \leq \delta^2/2$, as desired □

Our calculations will often require estimates of the form $\mathbf{E}_x\, \mathrm{d}_\rho(A_x, B_x)^2 = O(\varepsilon)$ where the expectation is taken according to some distribution on x (always over a finite set) that will be clear from context. We introduce the following notation to represent the same estimate:

$$A_x|\psi\rangle \approx^x_\varepsilon B_x|\psi\rangle.$$

Here $|\psi\rangle$ can be understood as any purification of ρ, with the usual convention that operators are extended to act as identity on spaces on which they are not defined. If

the symbol x is omitted then the distribution should be clear from context. If it needs to be specified we may write e.g. $A_x|\psi\rangle \approx_\varepsilon^{x|x_1=0} B_x|\psi\rangle$, meaning that the distribution on x is the one clear from context (typically, uniform on $\{0,1\}^n$), conditioned on the first bit of x being a 0. Although the notation can be ambiguous when taken out of context we hope that it will help make some of the more cumbersome derivations more transparent.

2.5 Nonlocal games

In the thesis we formulate a number of tests meant to be executed between a verifier and r players (sometimes also called provers), for $r \geq 1$ an integer. These tests all take the form of a classical one-round interaction: the verifier samples an r-tuple of questions and sends one question to each player; the players each provide an answer to the verifier, who decides to accept or reject. If the verifier accepts the players are said to win the game.

We call a tuple $(N, |\psi\rangle)$, where $|\psi\rangle \in \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_r$ is an entangled state on the joint space of all r players, and N a collection of POVM for each player and possible question to the player, a *strategy* for the players in G. Note that we may always assume $|\psi\rangle$ is a pure state and all POVM are projective.

Given a game G we denote by $\omega^*(G)$ the highest probability of winning that can be achieved by r players sharing quantum entanglement. For a more thorough introduction to nonlocal games in a similar framework as used here we refer to e.g. [Ji16a].

One of our tests uses nonlocal games as a means to enforce anticommutation relations between a player's observables. Towards this we introduce the following definition.

Definition 2.5.1 (Anticommutation game)**.** Let $\omega_{\text{ac}}^* \in (0,1]$ and $\delta : [0,1] \to [0,1]$ a continuous function such that $\delta(0) = 0$. A two-player game G is called a $(\omega_{\text{ac}}^*, \delta)$ anticommutation game if $\omega^*(G) \geq \omega_{\text{ac}}^*$ and moreover there exists questions q_X, q_Z (called *special questions*) to the second player and $\{\pm 1\}$-valued functions f_X, f_Z defined on the player's set of possible answers to questions q_X, q_Z respectively such that the following two properties hold:

1. *Completeness:* There exists a strategy using the state $|\text{EPR}\rangle_{AB}^{\otimes m}$ for some $m \geq 1$ and projective measurements that achieves the optimal success probability ω_{ac}^*, and is uch that measurement operators $\{A_q^a\} \in \text{Pos}(\mathcal{H}_A)$ for the second player satisfy $\sum_a f_X(a) A_{a_X}^a = \sigma_X \otimes \text{Id}$ and $\sum_a f_Z(a) A_{q_Z}^a = \sigma_Z \otimes \text{Id}$, where σ_X and σ_Z act on the first EPR pair and the identity on the remaining EPR pairs. Moreover, for every quesion q received by the second player and answer a, the projector A_q^a can be written as $A_q^a = \sum_j \Pi_j$ where each Π_j is the projector onto an eigenspace of a tensor product of σ_X, σ_Z and Id.[1] We call such a strategy an *honest strategy* for G.

[1]This seemingly ad-hoc condition is needed for the use of the anticommutation game in the Hamiltonian self-test described in Section 3.4, but not in the Pauli braiding test from Section 3.3.

2. Soundness: Let a projective strategy for the players in G be given such that the strategy uses entangled state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ and measurement operators $\{A_q^a\} \in \mathrm{Pos}(\mathcal{H}_A)$ for the second player. Then for any $\varepsilon > 0$, provided the strategy has success probability at least $\omega_{\mathrm{ac}}^* - \varepsilon$ in G, there exists isometries $U : \mathcal{H}_A \to \mathbb{C}^2 \otimes \mathcal{H}_{A'}$ and $V : \mathcal{H}_B \to \mathbb{C}^2 \otimes \mathcal{H}_{B'}$ and a state $|\psi'\rangle \in \mathcal{H}_{A'} \otimes \mathcal{H}_{B'}$ such that if

$$X = \sum_a f_X(a) A_{qX}^a \qquad \text{and} \qquad Z = \sum_a f_Z(a) A_{qZ}^a \tag{2.5}$$

then the following bounds hold:

$$\begin{aligned} \left\| U \otimes V |\psi\rangle - |\mathrm{EPR}\rangle \otimes |\psi'\rangle \right\| &\leq \delta \\ \max\left\{ \mathrm{d}_\rho(X, U^\dagger(\sigma_X \otimes \mathrm{Id}_{A'})U),\ \mathrm{d}_\rho(Z, V^\dagger(\sigma_Z \otimes \mathrm{Id}_{B'})V) \right\} &\leq \delta. \end{aligned}$$

The CHSH game [CHSH69] and the Mermin-Peres Magic Square game [Mer90, Per90] are both known to be anti-commutation games. For the former, see e.g. [MYS12a] and for the latter, [WBMS16a, CN16]. The advantage of the CHSH game is that there is an optimal strategy which only requires a single EPR pair of entanglement. The Magic Square has the advantage of having value 1, but an optimal strategy requires two EPR pairs.

Lemma 2.5.2. *The CHSH game is a* $(\cos^2 \pi/8, O(\sqrt{\varepsilon}))$ *anticommutation game. The Magic Square game is a* $(1, O(\sqrt{\varepsilon}))$ *anticommutation game.*

Chapter 3

A quantum linearity test, and an exponential quantum PCP

In this chapter, we introduce a simple two-player test which certifies that the players apply tensor products of Pauli σ_X and σ_Z observables on the tensor product of n EPR pairs. The test has constant robustness: any strategy achieving success probability within an additive ε of the optimal must be poly(ε)-close, in the appropriate distance measure, to the honest n-qubit strategy. The test involves $2n$-bit questions and 2-bit answers. The key technical ingredient is a quantum version of the classical linearity test of Blum, Luby, and Rubinfeld.

As applications of our result we give (i) the first robust self-test for n EPR pairs; (ii) a quantum multiprover interactive proof system for the local Hamiltonian problem with a constant number of provers and classical questions and answers, and a constant completeness-soundness gap independent of system size; (iii) a robust protocol for delegated quantum computation.

3.1 Introduction

Quantum non-local games lie at the intersection of several areas of quantum information. They provide a natural approach to *device-independent certification* or *self-testing* of unknown quantum states. Device-independent certification has applications to quantum cryptography, from quantum key distribution [VV14, MS14] to delegated computation [RUV13a, FH15]. The key idea behind these applications is that certain nonlocal games, such as the CHSH game [CHSH69], provide natural statistical tests that can be used to certify that an arbitrary quantum device implements a certain "strategy" specified by local measurements on an entangled state (e.g. an EPR pair).

A common weakness of all existing self-testing results is that their performance scales poorly with the number of qubits of the state that is being tested. Given a self-test, define (somewhat informally) its robustness as the largest $\varepsilon = \varepsilon(\delta)$ such that a success probability at least $\omega^*_{\text{opt}} - \varepsilon$ in the test certifies the target state up to error (in trace distance and up to local isometries) at most δ, where ω^*_{opt} is the success probability achieved by an ideal strategy. All previously known tests for n-qubit

states required $\varepsilon \ll \text{poly}(\delta, 1/n)$.

Our main result is a form of robust self-test for any state that can be characterized via expectation values of tensor products of standard Pauli σ_X or σ_Z observables. (This includes a tensor product of n EPR pairs; see below.)

Theorem 3.1.1 (simplified[1]). *Let $\mathcal{P}$ be a set of n-qubit observables, each of which is a tensor product of single-qubit Pauli σ_X, σ_Z or $\pm I$, and $\lambda_{\max} = \|\mathbf{E}_{P\sim\mathcal{P}}[P]\|$. For any $\eta \geq 0$ there exists a $p = p(\eta) = \Theta(\eta^c)$, where $0 < c < 1$ is a universal constant, and a 7-player nonlocal game with $O(n)$-bit questions and $O(1)$-bit answers such that*

$$\omega^*_{\text{opt}} = \frac{1}{2} + p\,\lambda_{\max} \pm \eta.$$

We view the theorem as a robust self-test in the following sense. Suppose a many-qubit state $|\psi\rangle$ can be characterized as the leading eigenvector of an operator $O = \mathbf{E}_{P\sim\mathcal{P}}[P]$ obtained as the average of n-qubit Pauli operators, with associated eigenvalue $\lambda_{\max} \in [-1, 1]$. For example, if $\mathcal{P}$ is the uniform distribution over $\{\sigma_X \otimes \sigma_X, \sigma_Z \otimes \sigma_Z\}^{\otimes n}$ then $\lambda_{\max} = 1$ and the leading eigenvector is the tensor product of n EPR pairs. More generally, if H is a local Hamiltonian with m local XZ terms we can take $\mathcal{P}$ to be Id with probability $1/2$ and the negation of a random term of H with probability $1/2$. Then $\lambda_{\max} = \frac{1}{2} - \frac{1}{2m}\lambda_{\min}(H)$ and the leading eigenvector is a ground state of H.

Theorem 3.1.1 provides a nonlocal game such that the optimal success probability in the game is directly related to $\lambda_{\max}$, thereby providing a test distinguishing between small and large $\lambda_{\max}$. In fact the complete statement of the theorem (see Theorem 3.4.4 in Section 3.4) says much more. In particular, we provide a complete characterization (up to local isometries) of strategies achieving a success probability at least $\omega^*_{\text{opt}} - \varepsilon$, for ε sufficiently small but independent of n, showing that such strategies must be based on a particular encoding (based on a simple, fixed error-correcting code) of an eigenvector associated to $\lambda_{\max}$.

3.1.1 Applications

Before giving an overview of the proof of the theorem we discuss some consequences of the theorem that help underscore its generality.

Hamiltonian complexity. A first consequence of Theorem 3.1.1 is that the ground state energy of a local Hamiltonian can be certified via a non-local game with questions of polynomial length and constant-length answers.

Corollary 3.1.2. *Let H be an n-qubit Hamiltonian that can be expressed as a weighted sum, with real coefficients, of tensor products of σ_X and σ_Z operators on a subset of the qubits, and normalize H such that $\|H\| \leq 1$. Suppose it is given that $\lambda_{\min}(H) \leq a$ or $\lambda_{\min}(H) \geq b$ for some $0 \leq a < b \leq 1$. There exists a one-round interactive proof*

[1]The complete statement of the theorem says much more, and provides a characterization of near-optimal strategies.

protocol between a classical polynomial-time verifier and 7 entangled provers where the verifier's (classical) questions are $O(n/(b-a))$ bits long, the provers' (classical) answers are $O(1)$ bits each, and the maximum probability that the verifier accepts is

$$\lambda_{\min} \leq a \implies \omega^*_{\text{opt}} \geq p_{\text{c}} := \frac{1}{2} + 2\,\eta_0, \qquad \lambda_{\min} \geq b \implies \omega^*_{\text{opt}} \leq p_{\text{s}} := \frac{1}{2} + \eta_0,$$

where $\eta_0 > 0$ is a small (universal) constant.

Since the class of Hamiltonians considered in Corollary 3.1.2 has been shown to be QMA-complete [CM14], the corollary can be viewed as a quantum analogue of the (games variant of the) exponentially long PCP based on the linearity test of Blum, Luby and Rubinfeld [BLR93]. Indeed, observe that the game constructed in the corollary has an efficient verifier, polynomial-length questions, and a constant completeness-soundness gap η_0 as soon as the original promise on the ground state energy for the Hamiltonian exhibits an inverse-polynomial completeness-soundness gap. The derivation of Corollary 3.1.2 from Theorem 3.1.1 involves a step of gap amplification via tensoring, and relies on the fact that Theorem 3.1.1 allows any XZ-Hamiltonian with no requirement on locality.

A similar result to Corollary 3.1.2 was obtained by Ji [Ji16a], and we build on Ji's techniques. The results are incomparable: on the one hand, the question size in our protocol is much larger (poly(n) bits instead of $O(\log n)$ for [Ji16a]); on the other hand, the dependence of the verifier's acceptance probability on the ground state energy is much better, as in [Ji16a] the completeness-soundness gap remains inverse polynomial.

An exponential quantum PCP. The expert reader may already have noted that the complexity-theoretic formulation of Corollary 3.1.2 described above already follows from known results in quantum complexity. Indeed, recall that the class QMA is in PSPACE, and that single-round multiprover interactive proof systems for PSPACE (and even NEXP) follow from the results in [IV12, Vid13]. Another possible proof approach for the same result could be obtained by repeating the protocol in [Ji16a] a polynomial number of times; provided there existed an appropriate parallel repetition theorem this would amplify the soundness to a constant (although the answer length would now be polynomial). In fact, based on a recent result by Ji [Ji16c] it seems likely that both approaches, based either on our results or parallel repetition of [Ji16c], could lead to an exponential "quantum-games" PCP for all languages in NEXP (instead of just QMA). Even though in purely complexity-theoretic terms the result would still not be new, we believe that the techniques from Hamiltonian complexity developed to obtain it show good promise for further extensions.

Indeed our protocol has some advantages over the generic sequence of known reductions. One is efficiency: in our protocol the provers merely need access to a ground state of the given local Hamiltonian and the ability to perform constant-depth quantum circuits. It is this property that enables our application to delegated quantum computing (see below for more on this). Answers in our protocol are a constant number of bits; the reductions mentioned above would require soundness

amplification via parallel repetition, which would lead to answers of (at least) linear length.

Even though they may not provide the most immediately compelling application of Theorem 3.1.1, the complexity-theoretic consequences of Corollary 3.1.2 tie our results to one of their primary motivations, the *quantum PCP conjecture*. Broadly speaking, the quantum PCP research program is concerned with finding a robust analog of the Cook-Levin theorem for the class QMA. The "games variant" of this conjecture states that estimating the optimal winning probability of entangled players in a multiplayer nonlocal game, up to an additive constant, is QMA-hard. In other words, that there exists an MIP* protocol for QMA with $O(\log(n))$-bit messages and constant completeness-soundness gap. The best progress to date in this direction is the work of Ji [Ji16a], which gives a five-prover one-round MIP* protocol with $O(\log(n))$-bit messages for the local Hamiltonian problem such that the verifier's maximum acceptance probability is $a - b\lambda_{min}(H)n^{-c}$ for positive constants a, b, c. This falls short of the games PCP conjecture in that the completeness-soundness gap is inverse polynomial in n, rather than constant.[2]

Our results suggest an approach to the problem from a different angle: we provide a "gap preserving" protocol, in the sense that the completeness-soundness gap is a polynomial function of the underlying promise gap of the Hamiltonian, but *independent* of the system size n. However, this occurs at the cost of much longer messages — polynomial instead of logarithmic.

Dimension witnesses. Consider the operator $O = (\frac{1}{2}(\sigma^X \otimes \sigma^X + \sigma^Z \otimes \sigma^Z))^{\otimes n}$. This operator has largest eigenvalue 1 with associated eigenvector $|\mathrm{EPR}\rangle^{\otimes n}$, where $|\mathrm{EPR}\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$. In this case the proof of Theorem 3.1.1 allows us to obtain the following robust self-test for $|\mathrm{EPR}\rangle^{\otimes n}$:

Corollary 3.1.3. *For any integer n there is a two-player game with $O(n)$-bit questions and $O(1)$-bit answers such that (i) there is a strategy with optimal winning probability ω^* that uses $|\mathrm{EPR}\rangle^{\otimes n}$ as entangled state; (ii) for any $\varepsilon > 0$, any strategy with success probability at least $\omega^* - \varepsilon$ must be based on an entangled state which is (up to local isometries) within distance $\delta = \mathrm{poly}(\varepsilon)$ of $|\mathrm{EPR}\rangle^{\otimes n}$.*

The game whose properties are summarized in Corollary 3.1.3 is based on the CHSH game. By using the Magic Square game instead, it is possible to devise a test with perfect completeness, $\omega^* = 1$, which can be achieved using an honest strategy based on the use of $(n+1)$ EPR pairs.

To the best of our knowledge, all prior self-tests for any family of states had a robustness guarantee going to 0 inverse polynomially fast with the number of qubits tested (see Section 3.1.3 below for a more thorough comparison with related works).

Delegated computation. It was noticed in [FH15] that an interactive proof system for the local Hamiltonian problem can also be used for delegated quantum computa-

[2]Here again we point the interested reader to the recent [Ji16c], which obtains a protocol with similar parameters, involving 8 provers, for all languages in NEXP.

tion with so-called *post-hoc* verification. The key idea is to use the Feynman-Kitaev construction to produce a Hamiltonian encoding the desired computation; measuring the ground energy of this Hamiltonian reveals whether the computation accepts or rejects. Following the same connection, we are able to give a post-hoc verifiable delegated computation scheme with a purely classical verifier and a constant number of provers. The provers only need the power of BQP. The scheme has a constant completeness-soundness gap independent of the size of the circuit to be computed, unlike the scheme of [FH15] and the classical scheme of [RUV13a], which both have inverse-polynomial gaps. However, unlike the scheme of [RUV13a], our protocol is not *blind*: the verifier must reveal the entire circuit to be computed to all the provers before the verification process starts. We refer to Section 3.5 for more details on this application.

3.1.2 Proof overview

The proof of Theorem 3.1.1 builds on ideas from complexity theory and quantum information. We draw inspiration from classical ideas in the closely related areas of probabilistically checakble proofs, locally testable codes, and property testing. The link between these areas and quantum self-testing is the idea of verifying a *global* property of an unknown object using only limited measurements. The two most important components of the proof are a "locally verifiable" encoding of arbitrary n-qubit quantum states [FV15], and a quantum analogue of the linearity test of Blum et al. [BLR93]. Since the second component is the more novel we explain it first.

Linearity testing of quantum observables. The simplest instantiation of the classical PCP theorem relies on the Hadamard code to robustly encode an n-bit string (e.g. an assignment to an instance of 3-SAT). Under this code, a string $u \in \{0,1\}^n$ is encoded as the 2^n-bit long truth table of the function $f_u : \{0,1\}^n \to \{-1,1\}$ given by $f_u(x) = (-1)^{u \cdot x}$, where $\cdot$ is the bitwise inner product. The function $f_u(x)$ is said to be *linear*, since $f_u(x+y) = f_u(x)f_u(y)$. The key property of the Hadamard code which makes it useful in this context is that it is locally testable. A local test is given by the BLR linearity test: given query access to a function $f : \{0,1\}^n \to \{-1,1\}$, by checking that $f(x+y) = f(x)f(y)$ at randomly chosen x, y the test certifies that any f that is accepted with probability at least $1-\varepsilon$ has the form $f \approx_\varepsilon f_u$ for some $u \in \{0,1\}^n$, where $f_u : a \mapsto (-1)^{u \cdot a}$ and $\approx_\varepsilon$ designates equality on an $(1 - O(\varepsilon))$ fraction of inputs.

Here is a "quantum" reformulation of this test as a nonlocal game: instead of querying an oracle for f at three points, play a three-player nonlocal game where each player is asked for the value at a point. This test is sound even if the players share an entangled quantum state [IV12], but success in the test does not certify quantum behavior: the players could win with certainty just by sharing a description of a classical linear function f_u; indeed, the main point of the analysis in [IV12] is precisely to ensure that provers sharing entanglement have no more freedom than to use it as shared randomness in selecting u.

In contrast, we seek an extension of the test which certifies a very specific type of quantum behavior that could not be emulated by classical means alone: specifically, that the observable O_x measured by a player upon receiving question x itself is (up to a change of basis, and in the appropriate "state-dependent" norm) close to $\otimes_i \sigma_X^{x_i}$. We give a test which achieves this. The test performs a combination of a linearity test in the X-basis and a linearity test in the Z-basis; an "anticommutation game" (which can be taken to be a version of the CHSH or Magic Square games) is used to constrain how the results of the two linearity tests relate to each other.

Theorem 3.1.4 (Pauli braiding test, informal). *There exists a two-player nonlocal game, based on the combination of (i) a linearity test in the X basis (questions $x \in \{0,1\}^n$); (ii) a linearity test in the Z basis (questions $z \in \{0,1\}^n$; (iii) an "anticommutation game" (based on e.g. the CHSH or Magic Square games) designed to test for generalized anti-commutation relations (questions $(x,z) \in \{0,1\}^{2n}$), such that any strategy that has success probability $\omega^*_{\text{opt}} - \varepsilon$ for some $\varepsilon > 0$ must be based on observables $A(x), A(z), A(x,z)$ and an entangled state $|\psi\rangle_{AB}$ such that up to local isometries*

$$A(x) \approx_\delta \otimes_i \sigma_X^{x_i}, \qquad A(z) \approx_\delta \otimes_i \sigma_Z^{z_i}, \qquad \text{and} \qquad |\psi\rangle_{AB} \approx_\delta |\text{EPR}\rangle_{AB}^{\otimes n},$$

where $\delta = \text{poly}(\varepsilon)$.

Neither the linearity test nor the anticommutation test *alone* would be sufficient to achieve the conclusion: as noted above, the linearity test can be passed even by classical provers, and our anticommutation test can be fooled if the provers share just one EPR pair. Rather, it is the guarantees provided by these tests together that enable us to create a tensor-product structure in the provers' Hilbert space.

To gain intuition on the test one may think of it in the following way. A standard approach to self-testing n EPR pairs is to fix a decomposition of the Hilbert space as

$$\mathcal{H} = \mathbb{C}^{2^n} \approx \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2, \tag{3.1}$$

and perform the CHSH (or Magic Square) test "in parallel", on each copy of $\mathbb{C}^2$. To the best of our knowledge such test only leads to robustness bounds with a polynomial dependence in n. In contrast the test on which Theorem 3.1.4 is based relies on the observation that the decomposition (3.1) need not be rigidly fixed a priori; indeed there are many bases in which such decomposition of $\mathbb{C}^{2^n}$ in tensor factors can be performed. In particular, *any* pair of anti-commuting observables on $\mathcal{H}$ suffices to specify a copy of $\mathbb{C}^2$, on which a CHSH test can in principle be performed (here we crucially rely on rotation invariance of the 2^n-dimensional maximally entangled state). Our test leverages this observation by performing a CHSH test for each possible pair of Pauli operators $(\sigma_X(a), \sigma_Z(b))$, where $a, b \in \{0,1\}^n$ are such that $a \cdot b = 1$. Each of these tests amounts to identifying a copy of $\mathbb{C}^2$ and performing the CHSH test on it. Contrary to the parallel-repeated CHSH test these copies are not independent, and this is what makes our test much more robust.

Encoding quantum states. The second component of the proof of Theorem 3.1.1 is a procedure, first introduced in [FV15, Ji16a], for encoding an n-qubit quantum state in a constant number of n-qubit shares such that certain properties of the encoded state (such as expectation values of local Pauli observables) can be verified through a classical interaction with provers each holding one of the shares. This is akin to how the "games" variant of the classical PCP theorem is derived from the "proof-checking" variant: while in the classical setting a proof can be directly shared across multiple provers, in the quantum setting we use a form of secret-sharing code that allows for distributing quantum information.

This procedure is efficient in that the total number of tests that can be performed (equivalently, the number of questions) is polynomial in n. However, the test in [FV15, Ji16a] is not robust, and is only able to provide meaningful results for values of ε that scale inverse-polynomially with n. By extending the Pauli braiding test, Theorem 3.1.4, to the stabilizer framework of [Ji16a] we obtain a procedure which is meaningful for constant ε. The drawback is that the provers may now be asked to measure all their qubits, and questions have length linear in n; however the total effort required of the classical verifier (and of provers given access to the state) remains polynomial in the size of the instance.

3.1.3 Related work

We build on a number of previous works in quantum information and complexity theory. Motivation for the problem we consider goes back to a question of Aharonov and Ben-Or (personal communication, 2013), who asked how a quantum generalization of the exponential classical PCP could look like if it was not derived through the "circuitous route" obtained as the compilation of known but complex results from the theory of classical and quantum interactive proof systems (as described earlier). In this respect we point to [AAV13, Section 5] for a very different approach to the same question based on a "quantum take" on the arithmetization technique.

More directly, our work builds on the already-mentioned works [FV15, Ji16a] initiating the study of entangled-prover interactive proof systems for the local Hamiltonian problem. The idea of using a distributed encoding of the ground state in order to obtain a multiprover interactive proof system for the ground state energy is introduced in [FV15]. In that work the protocol required the provers to return qubits; the possibility for making the protocol purely classical was uncovered by Ji [Ji16a]. Our use of stabilizer codes, and the stabilizer test which forms part of our protocol, originate in his work. In addition we borrow from ideas introduced in the study of quantum multiprover interactive proofs with entangled provers [KM03, CHTW04], and especially the three-prover linearity test of [IV12] and the use of oracularization from [IKM09] to make it into a two-prover test.

Our results are related to work in quantum self-testing, in particular testing EPR pairs [MYS12a] and more general entangled states [McK14]. A sequence of results has established that the presence of n EPR pairs between two provers can be certified via a protocol using queries and answers of length polynomial in n, with inverse-polynomial completeness-soundness gap. This was first achieved by [RUV13a] for a

test based on serial repetition of the CHSH game, and subsequently by [McK15a] for a single-round test based on CHSH, by [OV16] for an XOR game based on CHSH, and by [CN16] and [Col16] independently for the parallel-repeated Magic Square game. Viewed in the context of these results our work is the only one to provide a test whose robustness does not depend on the number of EPR pairs being tested. The reason this can be achieved is the linearity test(s) performed as part of the Pauli braiding test, which we see as a major innovation of our work.

3.1.4 Open questions and future directions

In our opinion the most important direction for future work is to improve the efficiency of the Pauli braiding test in terms of the number of questions required. This is carried out in the subsequent chapters of this thesis, using ideas based on low-degree polynomial encodings that are key to the classical PCP theorem, and we will not discuss this applicaiton any further here.

Aside from this direction, there are several open questions that we find interesting and may be more approachable.

1. In the classical PCP setting, the Hadamard code and the BLR linearity test can be used for *alphabet reduction*: converting a PCP or MIP protocol with large answer alphabet into one with a binary alphabet. This is a key step in Dinur's proof of the PCP theorem [Din07]. Can the linearity test also be used for alphabet reduction of MIP* protocols? The difficulty is to preserve completeness; if the optimal honest strategy uses a maximally entangled state then the adaptation should be straightforward, but if not it may be more challenging — perhaps ideas similar to our protocol for ground states of XZ Hamiltonians can be used.

2. An obvious application for many EPR pairs is quantum key distribution (QKD). A major contribution of [RUV13a] was to show that the sequential self-test for many EPR pairs obtained in that paper could be leveraged into a scheme for quantum key distribution (QKD) that is secure in the device-independent (DI) model of security. We believe it should be possible to use the Pauli braiding test to develop a DIQKD protocol in which the interaction with the devices can be executed in parallel, but we leave this possibility for future work.

3. The energy test can be viewed as a "device independent property test" for any property of a quantum state that can be suitably expressed as a Hamiltonian. Are there other device-independent property tests that can be formulated in our framework? It would be interesting to see which results from the survey of Montanaro and de Wolf on quantum property testing [MdW13] can be generalized to the device-independent setting.

Organization of this chapter. Throughout this chapter, we make use of notation and basic definitions from Chapter 2. In Section 3.2, we establish an important technical component of our results, the linearity test and its quantum analysis. We

expand this into a two-prover self-test for the Pauli group on n-qubits in Section 3.3, which forms the basis for our main result. In Section 3.4 we extend this test to handle more than two provers and show how it can be combined with an energy measurement test to devise a game for the local Hamiltonian problem. In Section 3.5 we discuss the application of our protocol to delegated computation.

3.2 The linearity test

We state and analyze a variant of the classic 3-query linearity test of Blum, Luby, and Rubinfeld [BLR93] (BLR) that can be played with two entangled players. The two-player test is based on the idea of oracularization with a dummy question introduced in [IKM09]. Our analysis builds on [IV12], who analyze a 3-player variant. Their proof is an extension of the Fourier-analytic proof due to Håstad to the matrix-valued setting. We analyze the two-player variant using similar techniques.

We note that the use of two players, rather than three as in the original test, is essential for our applications to self-testing. Ultimately we will require the provers to succeed in a linearity test performed in either of two mutually incompatible bases (e.g. the X and Z bases). Two provers can achieve this by sharing a maximally entangled state, but there is no tripartite state that would allow three entangled provers to obtain consistent answers whenever they measure their share of the state in either the X or the Z basis. (Formulated differently, $\sigma_X \otimes \sigma_X$ and $\sigma_Z \otimes \sigma_Z$ share a common $+1$ eigenvector, the EPR pair; $\sigma_X \otimes \sigma_X \otimes \sigma_X$ and $\sigma_Z \otimes \sigma_Z \otimes \sigma_Z$ do not. This is a manifestation of entanglement monogamy.)

We show the result in two steps. First we show that any set of quantum observables satisfying linearity relations approximately in expectation can be "rounded" to a nearby set of observables satisfying these relations exactly.

Theorem 3.2.1. *Suppose there exist observables* $\{A(a)\}_{a\in\{0,1\}^n}$ *in* $\mathrm{Obs}(\mathcal{H})$ *acting on a state* $\rho \in \mathrm{D}(\mathcal{H})$ *such that*

$$\mathbf{E}_{a,b} \operatorname{Tr}_\rho \big(A(a)A(b)A(a+b)\big) \geq 1 - \delta. \tag{3.2}$$

Then there exists an extended state $\rho' = \rho \otimes |\mathrm{anc}\rangle\langle\mathrm{anc}| \in \mathrm{D}(\mathcal{H} \otimes \mathcal{H}')$ *and observables* $\{\mathcal{A}(a)\}$ *in* $\mathrm{Obs}(\mathcal{H} \otimes \mathcal{H}')$ *such that*

$$\mathcal{A}(a)\mathcal{A}(b) = \mathcal{A}(a+b) \quad \forall a, b \in \{0,1\}^n \qquad \textit{and} \qquad \mathbf{E}_a \, \mathrm{d}_{\rho'}(\mathcal{A}(a), A(a))^2 \leq \delta. \tag{3.3}$$

Here, and throughout this chapter, the notation $a + b$ denotes the bitwise XOR of a and b, i.e. the sum of a and b viewed as elements of the additive group $\mathbb{Z}_2^n$. We call observables $\{\mathcal{A}(a)\}$ satisfying the first set of relations in (3.3) *exactly linear*.

Proof. For every $u \in \{0,1\}^n$ consider the Fourier transform $\hat{A}^u = \mathbf{E}_a (-1)^{a\cdot u} A(a)$. Define measurement operators $B^u = (\hat{A}^u)^2$. By Parseval's identity, these operators form a POVM. Using Naimark's theorem there exists an ancilla space $\mathcal{H}'$, $|\mathrm{anc}\rangle\langle\mathrm{anc}| \in$

$\mathrm{D}(\mathcal{H}')$, and a projective measurement $\{C^u\}$ on $\mathcal{H}\otimes\mathcal{H}'$ that simulates $\{B^u\}$. Introduce observables

$$\mathcal{A}(a) = \sum_u (-1)^{u\cdot a} C^u.$$

From the orthogonality of the projectors C^u it follows that $\mathcal{A}(a)\mathcal{A}(b) = \mathcal{A}(a+b)$. Write

$$\begin{aligned}
\mathbf{E}_a \, \mathrm{C}_{\rho'}(A(a), \mathcal{A}(a)) &= \frac{1}{2} + \frac{1}{2} \mathbf{E}_a \, \Re \mathrm{Tr}_{\rho'}\big(A(a)\mathcal{A}(a)\big) \\
&= \frac{1}{2} + \frac{1}{2} \mathbf{E}_a \, \Re\Big(\sum_u \mathrm{Tr}_\rho \left((-1)^{u\cdot a} A(a) (\hat{A}^u)^2 \right) \Big) \\
&= \frac{1}{2} + \frac{1}{2} \sum_u \mathrm{Tr}_\rho \left((\hat{A}^u)^3 \right).
\end{aligned}$$

To conclude, note that $\sum_u \mathrm{Tr}_\rho((\hat{A}^u)^3) = \mathbf{E}_{ab} \, \mathrm{Tr}_\rho(A(a)A(b)A(a+b))$, and use the assumption made in the theorem and the relation between $\mathrm{C}_{\rho'}$ and $\mathrm{d}^2_{\rho'}$. □

Next we exhibit a two-player game such that any strategy which succeeds with probability at least $1-\varepsilon$ in the game must satisfy the assumption (3.2) of Theorem 3.2.1 for some $\delta = O(\sqrt{\varepsilon})$.

The verifier performs the following one-round interaction with two players. He starts by choosing one of the players at random and labels her Alice; the other player is labeled Bob. In each test each player is sent a pair of n-bit strings. The n-bit strings are always assumed to be sent in lexicographic order.

1. Choose two strings $a, b \in \{0,1\}^n$ uniformly at random. Send (a, b) to Alice.
2. Let c be with equal probability either a, b, or $a+b$, and let $c' \in \{0,1\}^n$ be chosen uniformly at random. Send (c, c') to Bob.
3. The players reply with $\alpha, \beta \in \{\pm 1\}$ and $\gamma, \gamma' \in \{\pm 1\}$ respectively. Depending on the value of c the verifier performs one of the following two tests:
   (a) *Consistency test*: if $c = a$ (resp. b), accept if and only if both players return the same value as their answer to that question: $\gamma = \alpha$ (resp. $\gamma = \beta$).
   (b) *Linearity test*: if $c = a + b$, accept if and only if $\gamma = \alpha\beta$.

Figure 3-1: The two-player linearity test

Theorem 3.2.2. *Suppose two players Alice and Bob succeed in the linearity test of Figure 3-1 with probability at least* $1-\varepsilon$, *using a shared state* $|\psi\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$

and projective measurements $\{M_{a,b}^{\alpha,\beta}\}_{\alpha,\beta} \in \mathrm{Pos}(\mathcal{H}_A)$ *and* $\{N_{a,b}^{\alpha,\beta}\}_{\alpha,\beta} \in \mathrm{Pos}(\mathcal{H}_B)$ *respectively. Consider the POVM* $\{\tilde{M}_a^\alpha\}_\alpha$ *whose elements are given by* $\tilde{M}_a^\alpha := \mathbf{E}_b \sum_\beta M_{a,b}^{\alpha,\beta}$, *and let* $\{A_a^\alpha\}_\alpha \in \mathrm{Pos}(\mathcal{H}_A \otimes \mathcal{H}_{A'})$ *be the projective measurement obtained by Naimark dilation of* $\tilde{M}$.

Then the observables $A(a) := A_a^0 - A_a^1$ *satisfy*

$$\mathbf{E}_{a,b} \operatorname{Tr}_{\rho'}(A(a)A(b)A(a+b)) = 1 - O(\sqrt{\varepsilon}),$$

where $\rho' = |\psi\rangle\langle\psi| \otimes |\mathrm{anc}\rangle\langle\mathrm{anc}|_{\mathcal{H}_{A'}}$.

Proof of Theorem 3.2.2. Introduce the following conditional measurement operator on $\mathcal{H}_B$,

$$N_{a|ab}^\alpha = \sum_\beta N_{ab}^{\alpha\beta}.$$

Note that for every a, b and α, $N_{a|ab}^\alpha$ is a projector since we assumed each $M_{ab}^{\alpha\beta}$ is as well. Suppose that the players' acceptance probability conditioned on the verifier performing the consistency part of the test (i.e. $c = a$ or $c = b$) is $1 - \varepsilon_c$, while conditioned on the verifier performing the linearity part of the test (i.e. $c = a + b$) it is $1 - \varepsilon_l$, so that $\varepsilon = 2\varepsilon_c/3 + \varepsilon_l/3$. Let $\rho = |\psi\rangle\langle\psi|_{AB}$. By definition of the consistency test,

$$1 - \varepsilon_c = \mathbf{E}_{ab} \, \mathrm{C}_\rho \left(\tilde{M}_a, N_{a|ab}\right). \tag{3.4}$$

Using Naimark's dilation theorem there is an ancilla space $\mathcal{H}_{A'}$ and $|\mathrm{anc}\rangle\langle\mathrm{anc}| \in \mathrm{D}(\mathcal{H}'_{\mathrm{A}})$ such that the POVM $\{\tilde{M}_a^\alpha\}$ acting on $\mathcal{H}_A$ can be simulated by a projective measurement $\{A_a^\alpha\}$ acting on $\rho' = \rho \otimes |\mathrm{anc}\rangle\langle\mathrm{anc}|_{\mathcal{H}_{A'}}$. Let $d(a|ab) = \mathrm{d}_{\rho'}\left(A_a, N_{a|ab}\right)$, so that by Jensen's inequality, (2.4) and (3.4),

$$\begin{aligned}
\mathbf{E}_{ab} \, d(a|ab) &\leq \sqrt{\mathbf{E}_{ab} \, d(a|ab)^2} \\
&= O\Big(\sqrt{\mathbf{E}_{ab} \, \mathrm{C}_\rho(\tilde{M}_a, N_{a|ab})}\Big) \\
&= O(\sqrt{\varepsilon_c}).
\end{aligned} \tag{3.5}$$

Now compute

$$\begin{aligned}
\mathbf{E}_{ab} \operatorname{Tr}_{\rho'}\big(A(a)A(b)A(a+b)\big) &= \mathbf{E}_{ab} \sum_{\alpha\beta} \operatorname{Tr}_{\rho'}\big(A_a^\alpha A_b^\beta A_{a+b}^{\alpha\beta} - A_a^\alpha A_b^\beta A_{a+b}^{-\alpha\beta}\big) \\
&= 2\,\mathbf{E}_{ab} \sum_{\alpha\beta} \operatorname{Tr}_{\rho'}\big(A_a^\alpha A_b^\beta A_{a+b}^{\alpha\beta}\big) - 1 \\
&\geq 2\,\mathbf{E}_{ab} \Big(\sum_{\alpha\beta} \operatorname{Tr}_{\rho'}\big(A_{a+b}^{\alpha\beta} N_{a|ab}^\alpha N_{b|ab}^\beta\big) - O\big(d(a|ab) + d(b|ab)\big)\Big) \\
&\quad - 1 \\
&= 1 - O\big(\varepsilon_l + \sqrt{\varepsilon_c}\big),
\end{aligned}$$

where the inequality uses Lemma 2.4.1 and the last line is by (3.5) and, by definition of the linearity test,

$$\begin{aligned} 1-\varepsilon_l &= \mathbf{E}_{ab} \sum_{\alpha,\beta} \mathrm{Tr}_\rho \left(\tilde{M}_{a+b}^{(\alpha\beta)} N_{ab}^{\alpha\beta} \right) \\ &= \mathbf{E}_{ab} \sum_{\alpha,\beta} \mathrm{Tr}_\rho \left(\tilde{M}_{a+b}^{(\alpha\beta)} N_{a|ab}^{\alpha} N_{b|ab}^{\beta} \right), \end{aligned}$$

since the POVM elements $N_{a|b}^{\alpha\beta}$ are projectors. □

3.3 The Pauli braiding test

In this section we combine the linearity test with an anticommutation test based on any anticommutation game G_{ac} satisfying Definition 2.5.1 to devise a two-player test for which the honest strategy consists of applying tensor products of single-qubit observables in the set $\{\sigma_X(a)\sigma_Z(b),\, a,b \in \{0,1\}\}$. We show that for any strategy with near-optimal success probability there exists a (local) isometry under which the players' observables are close (in the state-dependent distance) on average to operators satisfying the Pauli commutation and anti-commutation ("braiding") relations perfectly.

3.3.1 The protocol

The protocol for the Pauli braiding test is described in Figure 3-2. In the protocol there are several possible types of queries that each player may receive. For convenience we give them the following names:

1. A *W-query*, represented by (W, a, b), where $W \in \{X, Z\}$ and a, b are uniformly random strings in $\{0,1\}^n$. The expected answer is two bits $\alpha, \beta \in \{-1, 1\}$.

2. A *G-query*, represented by (q, a, b) where q is a question in G_{ac} and a, b are uniformly random strings in $\{0,1\}^n$. The expected answer is a single value α taken from the answer alphabet in G.

To each query is associated an intended behavior of the player, which is specified as part of the *honest strategy* given in the following definition.

Definition 3.3.1. The *honest strategy* for the two players in the Pauli braiding test consists of the following. Let U, V be unitaries to an optimal strategy in G_{ac} as in Definition 2.5.1, and recall that by the completeness property this strategy can be implemented by sharing m EPR pairs of entanglement.

The players share the state $|\psi\rangle_{AB} = |\mathrm{EPR}\rangle_{AB}^{\otimes n} \otimes |\mathrm{EPR}\rangle_{A'B'}^{\otimes(m-1)}$. Upon receiving a query, a player performs the following depending on the type of the query:

- W-query (W, a, b), for $W \in \{X, Z\}$: measure the compatible observables $\sigma_W(a)$ and $\sigma_W(b)$ on its share of $|\mathrm{EPR}\rangle_{AB}^{\otimes n}$, and return the two outcomes.

Let G_{ac} be a two-player anticommutation game, with special questions q_X, q_Z. The verifier performs the following one-round interaction with two players. He starts by choosing one of the players at random and labels them Alice; the other player is labeled Bob. In each test a player will be sent a label and a pair of n-bit strings. The n-bit strings are always assumed to be sent in lexicographic order.

1. **Linearity test:** The verifier chooses a basis setting $W \in \{X, Z\}$ and sends it to both players. He executes the two-player linearity test with the players.

2. **Anticommutation test:** The verifier chooses two strings $a, b \in \{0,1\}^n$ such that $a \cdot b = 1 \mod 2$ uniformly at random, and sends (a, b) to both players. He executes the game G_{ac} with the players and accepts if and only if they succeed.

3. **Consistency test:** The verifier chooses two strings $a, b \in \{0,1\}^n$ such that $a \cdot b = 1 \mod 2$ uniformly at random, and a basis setting $W \in \{X, Z\}$. He sends (W, a, b) to Alice. With probability 1/2 each,

   - He samples a question q from the second player's distribution in G_{ac} and sends (q, a, b) to Bob. If $q = q_X$ (resp. $q = q_Z$) he accepts if and only if Alice's answer associated to a (resp. b) equals $f_W(\alpha)$, where α is Bob's answer and f_W the function from Definition 2.5.1. Otherwise, he accepts automatically.
   - He selects a uniformly random $c \in \{0,1\}^n$ and sends (N, a, c) to Bob. He accepts if and only if the product of Alice and Bob's answers associated to the query string a is $+1$.

Figure 3-2: The two-player Pauli braiding test

- G-query (q, a, b). Suppose the query is sent to Alice, the case of Bob being treated symmetrically. Let $W_{a,b} : \mathbb{C}^{2^n} \to \mathbb{C}^{2^n}$ be a unitary such that $W_{a,b}\sigma_X(a)W_{a,b}^\dagger = \mathrm{Id}_{\mathbb{C}^{2^{n-1}}} \otimes \sigma_X$ and $W_{a,b}\sigma_Z(b)W_{a,b}^\dagger = \mathrm{Id}_{\mathbb{C}^{2^{n-1}}} \otimes \sigma_Z$. (Such a $W_{a,b}$ exists and can be agreed upon by the players since in a G-query it is always the case that $a \cdot b = 1 \mod 2$, and both players are sent the same pair (a, b).) Let $\{A_q^\alpha\}_\alpha$ be the projective measurement on $\mathbb{C}^2 \otimes \mathcal{H}_{A'}$ associated with the first player in a honest strategy in G. Then Alice performs the projective measurement
$$\left\{(W_{a,b}^\dagger \otimes \mathrm{Id}_{A'})(\mathrm{Id}_{\mathbb{C}^{2^{n-1}}} \otimes A_q^\alpha)(W_{a,b} \otimes \mathrm{Id}_{A'})\right\}_\alpha$$
and returns the outcome.

Having defined the honest strategy for the players we introduce some notation associated with arbitrary strategies in the protocol. We specify a strategy using the shorthand $(N, |\psi\rangle_{AB})$. Here $|\psi\rangle_{AB}$ denotes the bipartite state shared by the players, and N the collection of POVM that the players apply in response to the different types

of queries they can be asked. Using Naimark's theorem we may assume without loss of generality that $|\psi\rangle_{AB}$ is a pure state and each player's POVM is projective.

Given a query (X, a, b) (resp. (Z, a, b)), we denote by $\{N_{ab}^{\alpha\beta}\}_{\alpha,\beta}$ (resp. $\{M_{ab}^{\alpha\beta}\}_{\alpha,\beta}$) the two-outcome projective measurement that is applied by a given player. Since the protocol treats the players symmetrically we may assume that these operators are the same for both Alice and Bob (see e.g. [Vid13, Lemma 2.5]). By taking appropriate marginals over the answers we define associated observables for the players, $X^A(a)$ and $Z^A(b)$ for the first player and $X^B(a)$ and $Z^B(b)$ for the second, as

$$X^A(a) = \frac{1}{2^n} \sum_{b\in\{0,1\}^n} \sum_{\beta\in\{\pm 1\}} \left(N_{ab}^{1\beta} - N_{ab}^{-1\beta}\right), \qquad Z^A(b) = \frac{1}{2^n} \sum_{a\in\{0,1\}^n} \sum_{\alpha\in\{\pm 1\}} \left(M_{ab}^{\alpha 1} - M_{a,b}^{\alpha -1}\right). \tag{3.6}$$

Observables $X^B(a)$ and $Z^B(b)$ for the second player are defined similarly.

Finally we use $X'^A(a, b)$ and $Z'^A(a, b)$ to denote the observables defined via (2.5) from Alice's strategy upon questions (q_X, a, b) and (q_Z, a, b) respectively.

3.3.2 Statement of results

We state the analysis of the Pauli braiding test in two parts: first we show that success in the test implies that observables (3.6) constructed from Alice and Bob's measurement operators approximately obey certain relations; then we show that these relations imply the existence of a local isometry under which the operators are close to operators satisfying the relations exactly.

Theorem 3.3.2. *Suppose a strategy $(N, |\psi\rangle_{AB})$ succeeds in the Pauli braiding test (Figure 3-2) with probability at least $\omega^*_{\text{pauli}} - \varepsilon$, when the game G_{ac} is an $(\omega^*_{\text{ac}}, \delta)$ anticommutation game. Then the following approximate relations hold, where operators W^D are defined in (3.6) for $W \in \{X, Z\}$ and $D \in \{A, B\}$ and $\rho = |\psi\rangle\langle\psi|$.*

1. *(Approximate consistency) For $W \in \{X, Z\}$,*

$$\mathbf{E}_a \, \mathrm{d}_\rho(W^A(a), W^B(a))^2 = O(\varepsilon);$$

2. *(Approximate linearity) For $W \in \{X, Z\}$,*

$$\mathbf{E}_{a,b} \, \mathrm{d}_\rho(W^A(a)W^A(b), W^A(a+b))^2 = O(\sqrt{\varepsilon});$$

3. *(Approximate anticommutation)*

$$\mathbf{E}_{a,b|a\cdot b=1} \, \mathrm{d}_\rho(X^A(a)Z^A(b), -Z^A(b)X^A(a))^2 = O(\delta(\varepsilon));$$

4. *(Approximate commutation)*

$$\mathbf{E}_{a,b|a\cdot b=0} \, \mathrm{d}_\rho(X^A(a)Z^A(b), Z^A(b)X^A(a))^2 = O(\varepsilon^{1/4} + \delta(\varepsilon)^{1/2}).$$

We note that the constant ω^*_{pauli} is given by

$$\omega^*_{\text{pauli}} = \frac{2}{3} + \frac{1}{3}\omega^*_{\text{ac}}, \tag{3.7}$$

where $\omega^*_{\text{ac}} \in (0,1]$ is the winning parameter associated with the $(\omega^*_{\text{ac}}, \delta)$ anticommutation game G_{ac} used in the protocol. Thus if $\omega^*_{\text{ac}} = 1$ then $\omega^*_{\text{pauli}} = 1$ as well.

Theorem 3.3.3. *Suppose given a bipartite state $|\psi\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$, and observables $\{X^A(a)\}_{a\in\{0,1\}^n}$, $\{Z^A(b)\}_{b\in\{0,1\}^n}$ on $\mathcal{H}_A$ and $\{X^B(a)\}_{a\in\{0,1\}^n}, \{Z^B(b)\}_{b\in\{0,1\}^n}$ on $\mathcal{H}_B$ such that conditions 1.,2. and 3. in Theorem 3.3.2 are satisfied, for some $\varepsilon > 0$ and $\delta(\varepsilon) = O(\sqrt{\varepsilon})$.[3] Then there exists a state*

$$|\Psi\rangle_{AB} = |\psi\rangle_{AB} \otimes |\text{EPR}\rangle_{A'A''} \otimes |\text{EPR}\rangle_{B'B''} \in \big(\mathcal{H}_A \otimes (\mathbb{C}^2_{A'} \otimes \mathbb{C}^2_{A''})^{\otimes n}\big) \otimes \big(\mathcal{H}_B \otimes (\mathbb{C}^2_{B'} \otimes \mathbb{C}^2_{B''})^{\otimes n}\big)$$

and observables $\{P^A(a,b)\}$ on $AA'A''$ such that, if $\rho = |\Psi\rangle\langle\Psi|$,

(a) (Approximate consistency) The following consistency relations hold:

$$\begin{aligned} \mathbf{E}_a \, \mathrm{d}_\rho(P^A(a,0), X^A(a) \otimes \mathrm{Id}_{A'A''})^2 &= O(\varepsilon^{1/8}) \\ \mathbf{E}_b \, \mathrm{d}_\rho(P^A(0,b), Z^A(b) \otimes \mathrm{Id}_{A'A''})^2 &= O(\varepsilon^{1/8}). \end{aligned}$$

(b) (Pauli braiding) For all $a, b, a', b' \in \{0,1\}^n$,

$$P^A(a,b)P^A(a',b') = (-1)^{a'\cdot b} P^A(a+a', b+b').$$

Likewise, there exist observables $\{P^B(a,b)\}$ on $BB'B''$ satisfying analogous relations.

We note that the Pauli braiding relations expressed in (b) imply the existence of an isomorphism such that the operators $P^A(a,b)$ (resp. $P^B(a,b)$) are mapped to "true" Pauli operators $\sigma^A_X(a)\sigma^A_Z(b)$ (resp. $\sigma^B_X(a)\sigma^B_Z(b)$).

The proofs of Theorem 3.3.2 and Theorem 3.3.3 are given in Sections 3.3.3 and Section 3.3.4 respectively. Before moving to the proofs we state an immediate, but powerful, application of the theorems to the problem of establishing dimension witnesses. For this it is sufficient to note the following well-known fact:

Fact 3.3.4. *Let ρ be a density matrix on $\mathbb{C}^{\otimes n} \otimes \mathbb{C}^{\otimes n}$ and $\varepsilon > 0$ such that*

$$\frac{1}{2^n} \sum_{P\in\{X,Z\}^n} \mathrm{Tr}((\sigma_P \otimes \sigma_P)\rho) \geq 1 - \varepsilon,$$

where $\sigma_P = \sigma_{P_1} \otimes \cdots \otimes \sigma_{P_n}$. Then

$$\langle \text{EPR}|^{\otimes n} \, \rho \, |\text{EPR}\rangle^{\otimes n} \geq 1 - \varepsilon.$$

[3]The restriction on δ is not necessary, but it is satisfied for both the CHSH and Magic Square games, and simplifies the presentation.

Proof. Observe that $|\mathrm{EPR}\rangle\langle\mathrm{EPR}| \geq \frac{1}{2}(\sigma_X \otimes \sigma_X + \sigma_Z \otimes \sigma_Z)$. □

Combining this fact and Theorems 3.3.2 and 3.3.3 gives the following consequence: a robust self-test for n EPR pairs.

Corollary 3.3.5. *Suppose given a strategy $(N, |\psi\rangle_{AB})$ for the players in the Pauli braiding test (Figure 3-2) with success probability $\omega^*_{\text{pauli}} - \varepsilon$, for some $\varepsilon > 0$. Then there exists a local isometry $\Phi = (\Phi^A : \mathcal{H}_A \to \mathcal{H}_{A'} \otimes \mathcal{H}_{A''}, \Phi^B : \mathcal{H}_B \to \mathcal{H}_{B'} \otimes \mathcal{H}_{B''})$ such that*

$$\mathrm{Tr}\Big(\big(\langle\mathrm{EPR}|^{\otimes n}_{A'B'} \otimes \mathrm{Id}_{A''B''}\big)\big(\Phi^A \otimes \Phi^B(|\psi\rangle\langle\psi|_{AB})\big)\big(|\mathrm{EPR}\rangle^{\otimes n}_{A'B'} \otimes \mathrm{Id}_{A''B''}\big)\Big) = 1 - O\big(\varepsilon^{1/8}\big).$$

By instantiating the anticommutation game G_{ac} used in the test with the Magic Square game we obtain a robust self-test for n EPR pairs in which the optimal strategy only requires the use of $(n+1)$ EPR pairs and is accepted with probability 1.[4]

3.3.3 Proof of Theorem 3.3.2

The proof of Theorem 3.3.2 proceeds by analyzing each of the three subtests performed in the Pauli braiding test separately, and then putting them together to establish the three conditions claimed in the theorem. We give the proof of the theorem now, assuming the results on each subtest established in Lemma 3.3.6, Lemma 3.3.7 and Lemma 3.3.8 below.

Proof of Theorem 3.3.2. Given a strategy $(N, |\psi\rangle_{AB})$ for the players, define observables $X^A(a), Z^A(b)$ and $X^B(a), Z^B(b)$ as in (3.6). Property 1. of approximate consistency is established by the consistency test (Lemma 3.3.6). Property 2. of approximate linearity follows from the Linearity Test (Theorem 3.2.2). When $a \cdot b = 1 \mod 2$, the approximate anticommutation property is established by the anticommutation test (Lemma 3.3.7). When $a \cdot b = 0 \mod 2$ the corresponding commutation is proved in Lemma 3.3.8. □

Consistency Test

The following lemma states consequences of the consistency test we will use.

Lemma 3.3.6. *Suppose the strategy $(N, |\psi\rangle)$ succeeds in the consistency test with probability $1 - \varepsilon$. Then there exists $\varepsilon_{\text{stab}} = O(\varepsilon)$ such that*

$$\mathbf{E}_a \, \mathrm{d}_\rho(X^A(a), X^B(a))^2 \leq \varepsilon_{stab}$$
$$\mathbf{E}_b \, \mathrm{d}_\rho(Z^A(b), Z^B(b))^2 \leq \varepsilon_{stab},$$

and

$$\mathbf{E}_{a,b|a\cdot b=1} \, \mathrm{d}_\rho(X^A(a), X'^B(a,b))^2 \leq \varepsilon_{stab}$$

[4] In fact, for the case of the Magic Square game it is not hard to see that there always exists an optimal strategy in the test using $\max(2, n)$ EPR pairs.

$$\mathbf{E}_{a,b|a\cdot b=1}\, \mathrm{d}_\rho(Z^A(b), Z'^B(a,b))^2 \leq \varepsilon_{stab}.$$

Moreover, the honest strategy succeeds in the test with probability 1.

Proof. It follows from the definition of C_ρ that any strategy $(N, |\psi\rangle)$ succeeding in the test with probability $1-\varepsilon$ satisfies

$$\frac{1}{2}\Big(\mathbf{E}_{a,b|a\cdot b=1}\, \mathrm{C}_\rho(X^A(a), X'^B(a,b)) + \mathbf{E}_a\, \mathrm{C}_\rho(X^A(a), X^B(a))\Big) = 1 - O(\varepsilon)$$
$$\frac{1}{2}\Big(\mathbf{E}_{a,b|a\cdot b=1}\, \mathrm{C}_\rho(Z^A(b), Z'^B(a,b)) + \mathbf{E}_b\, \mathrm{C}_\rho(Z^A(b), Z^B(b))\Big) = 1 - O(\varepsilon).$$

The first part of the lemma follows directly by applying (2.4) to the above relations. The second part follows from the definition of the honest strategy and the fact that

$$\sigma_X \otimes \sigma_X |\mathrm{EPR}\rangle = \sigma_Z \otimes \sigma_Z |\mathrm{EPR}\rangle = |\mathrm{EPR}\rangle.$$

□

Anticommutation test

The (approximate) Pauli braiding relations state that

$$X^A(a)Z^A(b)|\psi\rangle \approx (-1)^{a\cdot b} Z^A(a)X^A(b)|\psi\rangle.$$

There are two cases: if $a \cdot b = 0 \mod 2$ then the two operators should commute; otherwise, they should anti-commute. The anticommutation test enforces the latter property. In Section 3.3.3 we show how the former can be derived as a consequence.

Lemma 3.3.7. *Suppose the game G_{ac} used in the anticommutation test is an $(\omega^*_{\mathrm{ac}}, \delta)$ anticommutation game. Suppose the strategy $(N, |\psi\rangle)$ succeeds in the anticommutation test with probability $\omega^*_{\mathrm{ac}} - \varepsilon_{\mathrm{ac}}$ and in the consistency test with probability $1 - \varepsilon_{\mathrm{stab}}$. Then*

$$\mathbf{E}_{a,b:a\cdot b=1}\, \mathrm{d}_\rho(X^A(a)Z^A(b), (-1)^{a\cdot b} Z^A(b)X^A(a))^2 = O(\delta(\varepsilon_{\mathrm{ac}})) + O(\sqrt{\varepsilon_{\mathrm{stab}}}).$$

Moreover, the honest strategy succeeds in this test with probability ω^*_{ac}.

Proof. By definition of the soundness condition of an $(\omega^*_{\mathrm{ac}}, \delta)$ anticommutation game, the observables $X'^A(a,b)$ and $Z'^A(a,b)$ satisfy

$$\mathbf{E}_{a,b:a\cdot b=1}\, \mathrm{d}_\rho(X'^A(a,b)Z'^A(a,b), (-1)^{a\cdot b} Z'^A(a,b)X'^A(a,b))^2 = O(\delta(\varepsilon_{\mathrm{ac}})).$$

Using the triangle inequality, Lemma 3.3.6 (note that under the uniform distribution $a \cdot b = 1$ with probability at least 1/4) and Lemma 2.4.1,

$$\mathbf{E}_{a,b:a\cdot b=1}\, \mathrm{d}_\rho(X^B(a)Z^B(b), (-1)^{a\cdot b} Z^B(b)X^B(a))^2 = O(\delta(\varepsilon_{\mathrm{ac}})) + O(\sqrt{\varepsilon_{\mathrm{stab}}}),$$

and analogue relations hold for observables on Alice, using again Lemma 3.3.6. □

Commutation

The protocol does not involve a test for commutation, as the required property can be derived as a consequence of the existing tests.

Lemma 3.3.8. *Suppose the strategy $(N, |\psi\rangle)$ succeeds in the linearity and consistency tests with probability at least $1-\varepsilon_{\text{stab}}$ and in the anticommutation test with probability at least $\omega^*_{\text{ac}} - \varepsilon_{\text{ac}}$. Then*

$$\mathbf{E}_{a,b:a\cdot b=0} \, \mathrm{d}_\rho(X^A(a)Z^A(b) - Z^A(b)X^A(a))^2 = O(\delta(\varepsilon_{\text{ac}})^{1/2}) + O({\varepsilon_{\text{stab}}}^{1/4}).$$

Proof. We combine the anticommutation, linearity, and consistency tests through the following sequence of approximate identities. Note the approximations are taken under the uniform distribution on n-bit strings a, b such that $a \cdot b = 0 \mod 2$. Since this event occurs with probability at least $1/2$ for uniform a, b, the conditioning does not affect any of the approximations used by more than a multiplicative factor 2.

Start by applying approximate linearity (guaranteed by Theorem 3.2.2) of Z to express $Z(b)$ as a product $Z(c)Z(c+b)$, for uniformly random c such that $c \cdot a = 1 \mod 2$:

$$X^A(a)Z^A(b)|\psi\rangle \approx^{a,b,c|a\cdot b=0,c\cdot a=1}_{\varepsilon_{\text{stab}}^{1/4}} X^A(a)Z^A(c)Z^A(c+b)|\psi\rangle$$

Next use approximate consistency (Lemma 3.3.6), to exchange $Z^B(c+b)$ for $Z^A(c+b)$:

$$\approx^{a,b,c|a\cdot b=0,c\cdot a=1}_{\sqrt{\varepsilon_{\text{stab}}}} Z^B(c+b)X^A(a)Z^A(c)|\psi\rangle$$

Next, apply approximate anticommutation (Lemma 3.3.7) to anti-commute $X^A(a)$ and $Z^A(c)$:

$$\approx^{a,b,c|a\cdot b=0,c\cdot a=1}_{\delta^{1/2}+\varepsilon_{\text{stab}}^{1/4}} -Z^B(c+b)Z^A(c)X^A(a)|\psi\rangle$$

Applying Lemma 3.3.6 again, transfer $Z^B(c+b)$ back to Alice:

$$\approx^{a,b,c|a\cdot b=0,c\cdot a=1}_{\sqrt{\varepsilon_{\text{stab}}}} -Z^A(c)X^A(a)Z^A(c+b)|\psi\rangle$$

Applying Lemma 3.3.7 anti-commutes $Z^A(c+b)$ and $X^A(a)$:

$$\approx^{a,b,c|a\cdot b=0,c\cdot a=1}_{\delta^{1/2}+\varepsilon_{\text{stab}}^{1/4}} Z^A(c)Z^A(c+b)X^A(a)|\psi\rangle$$

Use Lemma 3.3.6 to transfer $X^A(a)$ to Bob:

$$\approx^{a,b,c|a\cdot b=0,c\cdot a=1}_{\sqrt{\varepsilon_{\text{stab}}}} X^B(a)Z^A(c)Z^A(c+b)|\psi\rangle$$

Finally apply Theorem 3.2.2 to combine the Z operators, and then Lemma 3.3.6 to move the X operator back to Alice:

$$\approx^{a,b,c|a\cdot b=0,c\cdot a=1}_{\varepsilon_{\text{stab}}{}^{1/4}} X^B(a)Z^A(b)|\psi\rangle$$
$$\approx^{a,b,c|a\cdot b=0,c\cdot a=1}_{\sqrt{\varepsilon_{\text{stab}}}} Z^A(b)X^B(a)|\psi\rangle.$$

□

3.3.4 Proof of Theorem 3.3.3

We give the proof of Theorem 3.3.3.

Proof of Theorem 3.3.3. Adjoin two n-qubit registers A' and A'' to Alice's system, and initialize them in the state $|\text{EPR}\rangle^{\otimes n}_{A'A''}$. Define new observables $X'(a) := X^A(a) \otimes \sigma_X(a)_{A'} \otimes \text{Id}_{A''}$ and $Z'(b) := Z^A(b) \otimes \sigma_Z(b)_{A'} \otimes \text{Id}_{A''}$. Further define observables

$$C(a,b) := \frac{X'(a)Z'(b) + Z'(b)X'(a)}{|X'(a)Z'(b) + Z'(b)X'(a)|},$$

where the notation $|\cdot|$ denotes the matrix absolute value and we use the convention $0/0 = 1$. We use the assumptions made in the theorem (i.e. properties 1, 2 and 3 in Theorem 3.3.2) to show that $C(a,b)$ satisfies approximate linearity over $\mathbb{Z}_2^{2n}$, i.e. that $C(a,b)C(a',b')|\Psi\rangle \approx^{a,b,a',b'} C(a+a',b+b')|\Psi\rangle$. First, by property 3 (approximate anticommutation), $X^A(a)Z^A(b)|\Psi\rangle \approx^{a,b}_{\varepsilon^{1/4}} (-1)^{a\cdot b}Z^A(a)X^A(a)|\Psi\rangle$, and thus $X'(a)Z'(b)|\Psi\rangle \approx^{a,b}_{\varepsilon^{1/4}} Z'(b)X'(a)|\Psi\rangle$. Hence, by Lemma 2.4.2 it follows that $C(a,b)|\Psi\rangle \approx^{a,b}_{\varepsilon^{1/4}} X'(a)Z'(b)|\Psi\rangle$. Using this relation, we consider the product of two C operators.

$$C(a,b)C(a',b')|\Psi\rangle$$
$$\approx^{a,b}_{\varepsilon^{1/8}} C(a,b)X^A(a')Z^A(b') \otimes \sigma_X(a')\sigma_Z(b')|\Psi\rangle.$$

By property 1 (approximate consistency), we can switch the X^A and Z^A operators to Bob, and switch the σ_X, σ_Z operators to the other half of the ancilla. Then, we relate $C(a,b)$ to $X^A(a)Z^A(b)$.

$$\approx^{a,b,a',b'}_{\varepsilon^{1/4}} Z^B(b')X^B(a')C(a,b) \otimes \sigma_Z(b')_{A''}\sigma_X(a')_{A''}|\Psi\rangle$$
$$\approx^{a,b,a',b'}_{\varepsilon^{1/8}} Z^B(b')X^B(a')X^A(a)Z^A(b) \otimes \sigma_Z(b')_{A''}\sigma_X(a')_{A''}\sigma_X(a)\sigma_Z(b)|\Psi\rangle.$$

Switching Z^BX^B back to Alice, and $\sigma_Z\sigma_X$ back to the other half of the ancilla,

$$\approx^{a,b,a',b'}_{\varepsilon^{1/4}} X^A(a)Z^A(b)X^A(a')Z^A(b') \otimes \sigma_X(a)\sigma_Z(b)\sigma_X(a')\sigma_Z(b')|\Psi\rangle.$$

By the properties of the exact Pauli operators,

$$=^{a,b,a',b'} (-1)^{a'\cdot b} X^A(a) Z^A(b) X^A(a') Z^A(b') \otimes \sigma_X(a+a') \sigma_Z(b+b') |\Psi\rangle.$$

Applying property 3 (approximate anticommutation),

$$\approx^{a,b,a',b'}_{\varepsilon^{1/8}} (-1)^{a'\cdot(b+b')} X^A(a) Z^A(b) Z^A(b') X^A(a') \otimes \sigma_X(a+a') \sigma_Z(b+b') |\Psi\rangle.$$

Applying property 1 (approximate consistency) to $X^Z(a')$, and then property 2 (approximate linearity) to combine $Z^A(b)$ with $Z^A(b')$, we get

$$\approx^{a,b,a',b'}_{\varepsilon^{1/4}} (-1)^{a'\cdot(b+b')} X^B(a') X^A(a) Z^A(b+b') \otimes \sigma_X(a+a') \sigma_Z(b+b') |\Psi\rangle.$$

Applying property 3 (approximate anticomutation) to $Z^A(b+b')$ and $X^A(a)$,

$$\approx^{a,b,a',b'}_{\varepsilon^{1/8}} (-1)^{(a+a')\cdot(b+b')} X^B(a') Z^A(b+b') X^A(a) \otimes \sigma_X(a+a') \sigma_Z(b+b') |\Psi\rangle.$$

Applying property 1 (approximate consistency) to move $X^B(a')$ back to Alice, and then applying property 2 (approximate linearity) to combine $X^A(a')$ with $X^A(a)$,

$$\approx^{a,b,a',b'}_{\varepsilon^{1/4}} (-1)^{(a+a')\cdot(b+b')} Z^A(b+b') X^A(a+a') \otimes \sigma_X(a+a') \sigma_Z(b+b') |\Psi\rangle.$$

Finally, applying property 3 (approximate anticommutation) to interchange $X^A(a+a')$ and $Z^A(b+b')$,

$$\begin{aligned} &\approx^{a,b,a',b'}_{\varepsilon^{1/8}} X^A(a+a') Z^A(b+b') \otimes \sigma_X(a+a') \sigma_Z(b+b') |\Psi\rangle \\ &\approx^{a,b,a',b'}_{\varepsilon^{1/8}} C(a+a', b+b') |\Psi\rangle. \end{aligned}$$

Applying Theorem 3.2.1 (over $\{0,1\}^{2n}$), we conclude that there exist observables $D(a,b)$ acting on an extension of Alice's system by an ancilla state, satisfying

$$D(a,b) D(a',b') = D(a+a', b+b') \quad \text{and} \quad \mathbf{E}_{a,b} \, \mathrm{d}_\rho(D(a,b), C(a,b))^2 = O(\varepsilon^{1/8}).$$

Set

$$P^A(a,b) := D(a,b) \otimes \sigma_X(a)_{A''} \sigma_Z(b)_{A''}.$$

We claim that $P^A(a,b)$ satisfies the desired properties.

(b) Pauli braiding: This follows from linearity of $D(a,b)$:

$$\begin{aligned} P^A(a,b) P^A(a',b') &= D(a,b) D(a',b') \otimes \sigma_X(a)_{A''} \sigma_Z(b)_{A''} \sigma_X(a')_{A''} \sigma_Z(b')_{A''} \\ &= D(a+a', b+b') \otimes (-1)^{a'\cdot b} \sigma_X(a+a')_{A''} \sigma_Z(b+b')_{A''} \\ &= (-1)^{a'\cdot b} P^A(a+a', b+b'). \end{aligned}$$

(a) Approximate consistency: We establish this in two steps. First, note that $D(a,b)$ is approximately consistent with $C(a,b)$, so

$$\begin{aligned} P^A_{a,b}|\Psi\rangle &=^{a,b} D(a,b) \otimes \sigma_X(a)_{A''}\sigma_Z(b)_{A''}|\Psi\rangle \\ &\approx^{a,b}_{\varepsilon^{1/8}} C(a,b) \otimes \sigma_X(a)_{A''}\sigma_Z(b)_{A''}|\Psi\rangle \\ &\approx^{a,b}_{\varepsilon^{1/4}} X^A(a)Z^A(b) \otimes \sigma_X(a)_{A'}\sigma_Z(b)_{A'} \otimes \sigma_X(a)_{A''}\sigma_Z(b)_{A''}|\Psi\rangle \\ &=^{a,b} X^A(a)Z^A(b) \otimes \mathrm{Id}_{A'A''}\,|\Psi\rangle, \end{aligned}$$

where the last line follows since both $\sigma_X \otimes \sigma_X$ and $\sigma_Z \otimes \sigma_Z$ stabilize $|\mathrm{EPR}\rangle$.

Finally, to establish consistency for the operators $P^A(a,0)$ where one coordinate is fixed to 0, we exploit the exact Pauli braiding relation:

$$P^A(a,0)|\Psi\rangle =^{a,c,d} (-1)^{d\cdot c}P^A(a+c,d)P^A(c,d)|\Psi\rangle$$

By approximate consistency of P^A,

$$\approx^{a,c,d}_{\varepsilon^{1/8}} (-1)^{d\cdot c}P^A(a+c,d)X^A(c)Z^A(d)|\Psi\rangle$$

Applying property 1 (approximate consistency) twice, first to $Z^A(d)$ and then to $X^A(c)$, we shift them to Bob's space:

$$\approx^{a,c,d}_{\sqrt{\varepsilon}} (-1)^{d\cdot c}Z^B(d)X^B(c)P^A(a+c,d)|\Psi\rangle$$

Now we apply approximate consistency of P^A again:

$$\approx^{a,c,d}_{\varepsilon^{1/8}} Z^B(d)X^B(c)X^A(a+c)Z^A(d)|\Psi\rangle$$

Applying property 3 (approximate anticommutation) to $X^A(a+c)$ and $Z^A(d)$, and then property 1 (approximate consistency) to $X^B(c)$, we get

$$\approx^{a,c,d}_{\varepsilon^{1/8}} (-1)^{a\cdot d}Z^B(d)Z^A(d)X^A(a+c)X^A(c)|\Psi\rangle$$

We use property 2 (approximate linearity) to combine $X^A(a+c)$ and $X^A(c)$:

$$\approx^{a,c,d}_{\varepsilon^{1/4}} (-1)^{a\cdot d}Z^B(d)Z^A(d)X^A(a)|\Psi\rangle$$

Now, applying property 3 (approximate anticommutation), we get,

$$\approx^{a,c,d}_{\varepsilon^{1/8}} Z^B(d)X^A(a)Z^A(d)|\Psi\rangle.$$

Finally, use property 1 (approximate consistency), and the fact that $Z^A(d)$ is an observable to get

$$\begin{aligned}&\approx_{\sqrt{\varepsilon}}^{a,c,d} X^A(a)Z^A(d)Z^A(d)|\Psi\rangle \\ &=^{a,c,d} X^A(a)|\Psi\rangle.\end{aligned}$$

□

3.4 The Hamiltonian Self-Test

In this section, we build on the Pauli braiding test to construct a test that distinguishes between the cases when a Hamiltonian given as input has ground state energy below, or higher than, pre-specified thresholds (i.e. in the former case the players will have a strategy with high success probability in the protocol, whereas in the latter any strategy will have low success probability). Due to the nature of our tests we restrict attention to n-qubit Hamiltonians specified by a linear combination of m terms, each of which is a tensor product of single-qubit I, σ_X or σ_Z Pauli operators.

Recall the Pauli braiding test analyzed in the previous section. As we saw (Corollary 3.3.5) this test can be used as a robust self-test for an n-qubit maximally entangled state. In order to test non-maximally entangled states, we proceed as in [FV15, Ji16a] by requiring the (honest) players to share a qubit-by-qubit encoding of the ground state of the Hamiltonian, where each qubit is encoded using a simple r-qubit CSS code. As elucidated in [Ji16a], any code state, thought of as a bipartite entangled state across any one of its qubits and the others, is maximally entangled. This allows us to lift the two-player tests which constitute the Pauli braiding test to r-player tests, where each player holds one qubit ("share") of the encoding of each qubit of the ground state, and one of the players (to be called the *special player*) plays the role of Alice while the remaining $(r-1)$ players (to be called the *composite player*) play the role of Bob.

The essential property of the consituent tests of the Pauli braiding test that permit this lifting is that all of the measurements performed by Bob in the honest strategy can be implemented by measuring the tensor product of Pauli operators σ_X, σ_Z, and Id on a state of n EPR pairs. (For the anticommutation test, this is ensured by the completeness condition in Definition 2.5.1, and for the other tests, it can be seen to hold for both Alice and Bob's measurements). These operators can be implemented transversally in any CSS code, and moreover in a way such that marginal distribution of queries received by the special player and each of the composite players is identical, as we show below.

3.4.1 The protocol

We describe the protocol in detail. The input is an n-qubit local Hamiltonian H that can be expressed as

$$H = \frac{1}{m}\sum_{\ell=1}^{m} H_\ell, \qquad H_\ell = \alpha_\ell \, \sigma_X(a_\ell)\sigma_Z(b_\ell), \tag{3.8}$$

for $\alpha_\ell \in [-1, 1]$ and $a_\ell, b_\ell \in \{0,1\}^n$ such that $a_\ell \wedge b_\ell = 0^n$ for all $\ell \in \{1, \ldots, m\}$. The verifier interacts with r players, where r is the number of qubits of codewords in the CSS code chosen for the protocol (such as Steane's 7-qubit code, as described in Section 2.2, in which case $r = 7$).

Although the protocol is to be performed with r "physical" players, part of the protocol consists in applying the Pauli braiding test, which is formulated as a two-player test in the previous section. To translate between the r players and the two players in the Pauli braiding test we introduce two "logical" players. A query to the logical players (as specified in the Pauli braiding test) is mapped to a query to the r physical players as follows. One of the physical players is chosen at random to play the role of the first logical player (Alice), called the *special player*. The remaining $(r-1)$ physical players together play the role of the second logical player (Bob), called the *composite player*.[5] For a given query Q to the special player of a type among those specified in the Pauli braiding test we define a *complementary query* $\overline{Q}$ for the composite player as per the following lemma.

Lemma 3.4.1. *For any X-query or Z-query, there exists a complementary query $\overline{Q}$ such that*

1. *The query associated to each physical player forming the composite player in $\overline{Q}$ is of the same type as Q. In particular the distribution on query strings is as specified by the query type.*

2. *If all players apply the honest strategy and provide answers α, β to Q and $\overline{\alpha}, \overline{\beta}$ to $\overline{Q}$ respectively, where $\overline{\alpha}$ and $\overline{\beta}$ are each obtained as the product of the answer to the corresponding query coming from each of the physical players making up the composite player, it holds that $\alpha\overline{\alpha} = \beta\overline{\beta} = +1$.*

Proof. Both items follow from the properties of CSS codes described in Section 2.2. We give the proof for an X-query (X, a, b). Let the index of the special player be $i \in \{1, \ldots, r\}$, and let S_X be a stabilizer of the code, such that S_X consists only of I and σ_X Paulis and has a σ_X in position i. For each physical player $j \neq i$ associated with the composite player, if the operator in position j of S_X is σ_X, player j is sent the query (X, a, b). Otherwise, player j is sent a uniformly random X-query (X, c, d).

[5]The physical players remain isolated throughout the protocol and are never allowed to communicate; it is only for purposes of analysis that we group $(r-1)$ physical players into a single logical player. In particular the physical players are never told which logical player they are associated with, and the distribution of queries to any physical player is the same whether it plays the role of the special or composite player.

Composite answers $\overline{\alpha}, \overline{\beta}$ to the complementary query are determined by taking the product of the answers from all players who did not receive random strings; using that S_X is a stabilizer of the code ensures that item 2 is satisfied.

In the composite query, for a given choice of S_X each player receives a query that is either identical to the original query, or is a uniformly random string; since the original query is chosen at random this is also the case for each of the physical players associated with the composite player. This proves item 1. □

We can then define associated observables for the players, $\hat{X}(a)$ and $\hat{Z}(b)$ for the special player and $\overline{X}(a)$ and $\overline{Z}(b)$ for the composite player, exactly as in (3.6).

Definition 3.4.2. Let $\{\hat{M}_{a,b}^{\alpha\beta}\}$ (resp. $\{\overline{M}_{a,b}^{\alpha\beta}\}$) be the POVM implemented by the special player (resp. composite player) when asked a query (W, a, b) (resp $(\overline{W}, a, b)$; see Lemma 3.4.1), for $W = X$ or Z. Define observables

$$\hat{W}(a) = \frac{1}{2^n} \sum_{b\in\{0,1\}^n} \sum_{\beta\in\{\pm 1\}} \left(\hat{M}_{a,b}^{1\beta} - \hat{M}_{a,b}^{-1\beta}\right), \qquad \overline{W}(a) = \frac{1}{2^n} \sum_{b\in\{0,1\}^n} \sum_{\beta\in\{\pm 1\}} \left(\overline{M}_{a,b}^{1\beta} - \overline{M}_{a,b}^{-1\beta}\right).$$

Aside from the Pauli braiding test, the protocol considers two other tests called the *energy test* and the *energy consistency test.* In the energy test, the verifier asks the players to measure a randomly chosen term in the Hamiltonian. The consistency test is needed to relate the operators applied in the energy test to those applied in the Pauli braiding test. The energy test uses an additional query type, which differs from the types of queries used in the Pauli braiding test:

3. An *XZ-query* is represented by (XZ, a, b) where $a, b \in \{0,1\}^n$ are such that $a \wedge b = 0^n$. Note that here, in contrast to $X-$ or $Z-$queries, the strings a and b are ordered. The distribution on a and b depends on the Hamiltonian. The expected answer is two bits $\alpha, \beta \in \{-1, 1\}$.

The honest strategy for the players in the Hamiltonian self-test (Figure 3-3) consists of applying the honest strategy defined for the Pauli braiding test (Definition 3.3.1) whenever the query is of X, Z, or G type, and the following strategy when it is of XZ type:

Definition 3.4.3. In the honest strategy, a player answers an XZ-query (XZ, a, b) by measuring the compatible observables $\sigma_X(a)$ and $\sigma_Z(b)$ and returning both outcomes.

3.4.2 Statement of results

Our main result regarding the Hamiltonian self-test is given in the following theorem, which states the completeness and soundness guarantees of the protocol described in Figure 3-3.

Theorem 3.4.4. *There exists a constant $0 < d < 1$ such that the following holds. Let H be a (not necessarily local) Hamiltonian with m terms over n qubits of the form (3.8), and $\lambda_{\min}(H)$ the smallest eigenvalue of H. Then for every $\eta > 0$ there is*

a choice $p = \Theta(\eta^{1-d})$ for the probability of performing the energy test in Protocol 3-3 such that the maximum probability $\omega^*(H)$ with which any r-player strategy succeeds in the protocol satisfies

$$1 - \frac{p}{8}\Big(\lambda_{min}(H) + \frac{2}{m}\sum_{\ell=1}^{m}|\alpha_l|\Big) \leq \omega^*(H) \leq 1 - \frac{p}{8}\Big(\lambda_{min}(H) + \frac{2}{m}\sum_{\ell=1}^{m}|\alpha_l|\Big) + \eta.$$

Corollary 3.1.2 follows from Theorem 3.4.4 by an amplification step described in Section 3.4.5. The proof of the theorem relies on the analysis of the energy test and the energy consistency test, given in Section 3.4.3 and Section 3.4.4 respectively, together with the analysis of the Pauli braiding test given in Section 3.3.2.

Proof of Theorem 3.4.4. First we establish the lower bound. An honest quantum strategy (as described in Definition 3.3.1 and Definition 3.4.3) acting on an encoded ground state $|\Gamma\rangle$ of H, together with an encoding of the additional EPR pairs $|\mathrm{EPR}\rangle_{A'B'}^{\otimes(m-1)}$ required to implement an optimal strategy in the anticommutation game G_{ac} (recall we take $G_{\mathrm{ac}} = \mathrm{MS}$ in this section, so $\omega_{\mathrm{ac}}^* = 1$, $\delta(\varepsilon) = O(\sqrt{\varepsilon})$, and $m = 2$) succeeds in the protocol with probability $\omega_{\mathrm{honest}}(H) = (1-p) + p\,\omega_{\mathrm{ENERGY}}^*(H)$, where

$$\omega_{\mathrm{ENERGY}}^*(H) = \frac{1}{2} + \frac{1}{2}\Big(1 - \frac{1}{4}\lambda_{\min}(H) - \frac{1}{2m}\sum_{\ell=1}^{m}|\alpha_\ell|\Big)$$

denotes the probability of the honest strategy to pass in the energy and consistency tests, each executed with probability 1/2; the analysis of the energy test is from Lemma 3.4.5.

Next we establish the upper bound. Suppose a strategy for the players succeeds with overall probability ω_{cheat}, passes the Pauli braiding test with probability $1-\varepsilon$, and passes the energy and consistency tests with probability ω_{ENERGY}; thus $\omega_{\mathrm{cheat}} = (1-p)(1-\varepsilon) + p\,\omega_{\mathrm{ENERGY}}$. Applying the combination of Theorem 3.3.2 and Theorem 3.3.3 there exists an (rn)-qubit state $|\varphi_1\rangle$ on which the action of the Pauli operators σ_X, σ_Z is $O(\varepsilon^{1/8})$-consistent with the action of the players' operators X, Z in the cheating strategy. Further, Lemma 3.4.6 shows that the measurements performed in the energy test are $O(\varepsilon^d)$-consistent, for some $0 < d < 1$, with the corresponding product of players' X and Z operators from the Pauli test. Combining these two statements we deduce that an *honest* strategy using the shared state $|\varphi_1\rangle$ will succeed in the Pauli braiding test with probability 1 (since it is honest and $\omega_{\mathrm{ac}}^* = 1$), and in the energy test with probability at least $\omega_{\mathrm{ENERGY}} - O(\varepsilon^d)$. Since this strategy implements valid logical X and Z operators in the energy test, by lemma 3.4.5 it passes the test with probability at most $\omega_{\mathrm{ENERGY}}^*(H)$. Thus $\omega_{\mathrm{ENERGY}} \leq \omega_{\mathrm{ENERGY}}^*(H) + O(\varepsilon^d)$, and

$$\begin{aligned}\omega_{\mathrm{cheat}} &= (1-p)(1-\varepsilon) + p\,\omega_{\mathrm{ENERGY}} \\ &\leq (1-p)(1-\varepsilon) + p\,\omega_{\mathrm{ENERGY}}^*(H) + O(p\,\varepsilon^d) \\ &\leq \omega_{\mathrm{honest}}(H) - (1-p)\varepsilon + O(p\,\varepsilon^d).\end{aligned}$$

Choosing p to be a sufficiently small constant times η^{1-d}, for all $0 \leq \varepsilon \leq 1$ this

expression is less than or equal to $\omega_{\text{honest}}(H) + \eta$. □

3.4.3 Analysis of the energy test

The goal of the energy test is to estimate the energy of a randomly chosen term in the Hamiltonian.

Lemma 3.4.5. *Given a Hamiltonian H as in (3.8), the acceptance probability of the energy test, when the correct Pauli operators are applied by each player on its respective register of the (rn)-qubit encoding of an n-qubit state $|\psi\rangle$, is*

$$\begin{aligned}\omega^*_{\text{ENERGY}}(H, |\psi\rangle) &= 1 - \Big(\frac{1}{2m}\sum_{\ell=1}^{m} \frac{|\alpha_\ell| + \alpha_\ell \langle\psi|H_\ell|\psi\rangle}{2}\Big) \\ &= 1 - \Big(\frac{1}{4}\langle\psi|H|\psi\rangle + \frac{1}{2m}\sum_{\ell} |\alpha_\ell|\Big),\end{aligned}$$

where $H_\ell = \sigma_X(a_\ell)\sigma_Z(b_\ell)$ is the ℓ-th term in the Hamiltonian.

Proof. The proof is a simple calculation in all points similar to that performed in [Ji16a, Section 4]; see in particular the discussion that precedes Theorem 23 in that paper. We omit the details. □

3.4.4 Analysis of the consistency test

The goal of the energy consistency test is to guarantee that operators used by the special player on XZ-type queries are consistent with those used on other types of queries.

Lemma 3.4.6. *Suppose the strategy $(N, |\psi\rangle)$ for the players succeeds in the energy consistency test and the Pauli braiding test with probability $1 - \varepsilon$ each. Then*

$$\frac{1}{m}\sum_{\ell=1}^{m} \big\|(\hat{H}_\ell - \hat{X}(a)\hat{Z}(b))|\psi\rangle\big\|^2 = O\big(\varepsilon^{1/32}\big),$$

where a and b are strings such that $H_\ell = \sigma_X(a)\sigma_Z(b)$, and $\hat{H}_\ell$ is the observable applied by the special player upon receiving the query (XZ, a, b) in the energy test.

Moreover, the honest strategy succeeds in the test with probability 1.

Proof. We show that XZ-queries, X-queries, and Z-queries on the special player are all consistent with $\overline{(X, c, c+a)}$ and $\overline{(Z, c, c+b)}$ queries to the composite player. The analysis uses similar techniques to the analysis of the linearity test. First, let us analyze the case when the verifier chooses $W = X$. Let the POVM applied by the composite player be $\{\overline{M}^{\alpha\alpha'}_{c,c+a}\}$ and define marginalized operators

$$\overline{M}^{\alpha}_{c|c,c+a} = \sum_{\alpha'} \overline{M}^{\alpha\alpha'}_{c,c+a}.$$

Likewise, let the POVM applied by the special player be $\hat{P}_\ell^{\alpha\alpha'}$ and define marginalized operators for the special player:

$$\hat{H}_{a|\ell}^{\alpha} = \sum_{\alpha'} \hat{P}_\ell^{\alpha\alpha'}, \qquad \hat{H}_{b|\ell}^{\alpha'} = \sum_{\alpha} \hat{P}_\ell^{\alpha\alpha'}.$$

The observable $\hat{H}_\ell$ corresponding to the product of the special player's measurement outcomes is defined as

$$\hat{H}_\ell = \sum_{\alpha\alpha'} (-1)^{\alpha\cdot\alpha'} \hat{P}_\ell^{\alpha\alpha'}.$$

Recall that the Pauli braiding test (Theorem 3.3.3) guarantees the existence of operators $P^A(a,b)$ exactly satisfying the Pauli relations; let

$$\mathcal{X}(a) := P^A(s,0) \qquad \text{and} \qquad \mathcal{Z}(b) := P^A(0,b).$$

Item (a) of Theorem 3.3.3 guarantees that $\mathcal{X}(a)$ (resp. $\mathcal{Z}(b)$) is within $O(\varepsilon^{1/8})$ of $\hat{X}(a)$ (resp. $\hat{Z}(b)$), in the state-dependent distance d_ρ. Associated with the observable $\mathcal{X}(a)$ are the projectors $\mathcal{X}^\alpha(a), \alpha \in \{\pm 1\}$, and likewise $\mathcal{Z}^\beta(b)$ for $\mathcal{Z}(b)$.

The following relations follow from the assumption that the players succeed with probability $1-\varepsilon$ in the energy consistency test. We use the notation $\mathbf{E}_{\ell,a\sim H_\ell}$ to indicate that the index ℓ is chosen uniformly at random, and then the string a is chosen from the distribution of queries induced by the Hamiltonian term H_ℓ; in contrast to $\mathbf{E}_a$ which indicates a uniformly random string.

$$\mathbf{E}_{\ell,a\sim H_\ell} \mathbf{E}_c \, \mathrm{C}_\rho(\overline{M}^{\alpha}_{c|c,c+a}, \hat{X}^\alpha(c)) = 1 - O(\varepsilon), \tag{3.9}$$

$$\mathbf{E}_{\ell,a\sim H_\ell} \mathbf{E}_c \, \mathrm{C}_\rho(\overline{M}^{\alpha}_{c+a|c,c+a}, \hat{X}^\alpha(c+a)) = 1 - O(\varepsilon), \tag{3.10}$$

$$\mathbf{E}_{\ell,a\sim H_\ell} \mathbf{E}_c \, \mathrm{C}_\rho\Big(\hat{H}^{\alpha}_{a|\ell}, \sum_{\beta\cdot\beta'=\alpha} M^{\beta\beta'}_{c,c+a}\Big) = 1 - O(\varepsilon). \tag{3.11}$$

We use these relations to show that the special player's marginalized measurement $\hat{H}^{\alpha}_{a|\ell}$ is close to $\mathcal{X}^\alpha(a)$. We show this in two steps. First, we relate the special player's measurement $\hat{H}^{\alpha}_{a|\ell}$ to the composite player's measurement:

$$\begin{aligned}
\mathbf{E}_{\ell,a\sim H_\ell} \mathrm{C}_\rho\left(\hat{H}^{\alpha}_{a|\ell}, \mathcal{X}^\alpha(a)\right) &\geq \mathbf{E}_{\ell,a\sim H_\ell} \mathbf{E}_c \Big[\mathrm{C}_\rho\Big(\sum_{\beta\cdot\beta'=\alpha} \overline{M}^{\beta\beta'}_{c,c+\alpha}, \mathcal{X}^\alpha(a)\Big) \\
&\qquad - \mathrm{d}_\rho\Big(\hat{H}^{\alpha}_{a|\ell}, \sum_{\beta\cdot\beta'=\alpha} \overline{M}^{\beta\beta'}_{c,c+a}\Big)\Big] \\
&\geq \mathbf{E}_{\ell,a\sim H_\ell} \mathbf{E}_c \, \mathrm{C}_\rho\Big(\sum_{\beta\cdot\beta'=\alpha} \overline{M}^{\beta\beta'}_{c,c+a}, \mathcal{X}^\alpha(a)\Big) - O(\sqrt{\varepsilon}),
\end{aligned}$$

where the first inequality follows from Lemma 2.4.1 and the second from (2.4) and (3.11).

Next we relate M to a product of two measurements $\hat{X}$:

$$\begin{aligned}\mathbf{E}_{\ell,a\sim H_\ell}\,\mathrm{C}_\rho\left(\hat{H}^\alpha_{a|\ell},\mathcal{X}^\alpha(a)\right) &\geq \mathbf{E}_{\ell,a\sim H_\ell}\,\mathbf{E}_c\,\mathrm{C}_\rho\Big(\sum_{\beta\cdot\beta'=\alpha}\overline{M}^{\beta}_{c|c,c+a}\overline{M}^{\beta'}_{c+a|c,c+a},\mathcal{X}^\alpha(a)\Big)-O(\sqrt{\varepsilon})\\ &\geq \mathbf{E}_{\ell,a\sim H_\ell}\,\mathbf{E}_c\,\mathrm{C}_\rho\Big(\sum_{\beta\cdot\beta'=\alpha}\hat{X}^\beta(c)\hat{X}^{\beta'}(c+a)\mathcal{X}^\alpha(a)\Big)-O(\sqrt{\varepsilon}),\end{aligned}$$

as follows from (3.10), (3.9) and Lemmas 2.4.1 and (2.4). Finally, we use the Pauli braiding test to relate $\hat{X}$ to the exactly linear observable $\mathcal{X}$. Starting from the above and using Lemma 3.3.6 to switch $\hat{X}(c)$ to $\bar{X}(c)$,

$$\mathbf{E}_{\ell,a\sim H_\ell}\,\mathrm{C}_\rho\left(\hat{H}^\alpha_{a|\ell},\mathcal{X}^\alpha(a)\right)\geq \mathbf{E}_{\ell,a\sim H_\ell}\,\mathbf{E}_c\,\mathrm{C}_\rho\Big(\sum_{\beta\cdot\beta'=\alpha}\bar{X}^\beta(c)\hat{X}^{\beta'}(c+a),\mathcal{X}^\alpha(a)\Big)-O(\sqrt{\varepsilon}).$$

Next, we use Theorem 3.3.3 and Lemma 2.4.1 to sequentially exchange the remaining $\hat{X}$, then $\overline{X}$, to $\mathcal{X}$, to obtain

$$\mathbf{E}_{\ell,a\sim H_\ell}\,\mathrm{C}_\rho\left(\hat{H}^\alpha_{a|\ell},\mathcal{X}^\alpha(a)\right)\geq \mathbf{E}_{\ell,a\sim H_\ell}\,\mathbf{E}_c\,\mathrm{C}_\rho\Big(\sum_{\beta\cdot\beta'=\alpha}\mathcal{X}^\beta(c)\mathcal{X}^{\beta'}(c+a),\mathcal{X}^\alpha(a)\Big)-O(\varepsilon^{1/16}). \tag{3.12}$$

Finally, the product of the three $\mathcal{X}$ operators can be eliminated using the exact linearity relations. Performing an analogous analysis for the Z operators,

$$\mathbf{E}_{\ell,b\sim H_\ell}\,\mathrm{C}_\rho(\hat{H}^\beta_{b|\ell},\mathcal{Z}(b)^\beta)\geq 1-O(\varepsilon^{1/16}). \tag{3.13}$$

To put these results together it remains to apply the stabilizer property to these operators. While we cannot do this directly since a and b are not distributed uniformly, we can use the exact linearity to write $\mathcal{Z}(b)=\mathbf{E}_c\,\mathcal{Z}(b+c)\mathcal{Z}(c)$, and apply Lemma 3.3.6 to each term in the product:

$$\begin{aligned}\hat{H}_\ell|\psi\rangle &=^\ell \hat{H}_{a|\ell}\hat{H}_{b|\ell}|\psi\rangle\\ &\approx^\ell_{\varepsilon^{1/32}} \hat{H}_{a|\ell}\mathcal{Z}(b)|\psi\rangle && \text{by (3.13), Lemma 2.4.1, and (2.4)}\\ &=^\ell \mathbf{E}_c\,\hat{H}_{a|\ell}\mathcal{Z}(b+c)\mathcal{Z}(c)|\psi\rangle && \text{by exact linearity}\\ &\approx^\ell_{\varepsilon^{1/16}} \mathbf{E}_c\,\bar{Z}(c)\bar{Z}(b+c)\hat{H}_{a|\ell}|\psi\rangle && \text{by Theorem 3.3.3 and Lemma 3.3.6}\\ &\approx^\ell_{\varepsilon^{1/32}} \mathbf{E}_c\,\bar{Z}(c)\bar{Z}(b+c)\mathcal{X}(a)|\psi\rangle && \text{by (3.12) and Lemma 2.4.1}\\ &\approx^\ell_{\varepsilon^{1/16}} \mathbf{E}_c\,\mathcal{X}(a)\mathcal{Z}(b+c)\mathcal{Z}(c)|\psi\rangle && \text{by Theorem 3.3.3 and Lemma 3.3.6}\\ &=^\ell \mathcal{X}(a)\mathcal{Z}(b)|\psi\rangle && \text{by exact linearity.}\end{aligned}$$

□

3.4.5 Amplification

In this section we show how Theorem 3.4.4 can be used to obtain Corollary 3.1.2. The main idea consists in leveraging the fact that our protocol does not require locality of the Hamiltonian to first "brute-force" amplify the gap of the underlying instance of the local Hamiltonian problem to a constant, and then run the protocol on the amplified non-local instance. This is achieved by first shifting the Hamiltonian by the appropriate multiple of identity so that the energy in the yes-instance is less than or equal to 0. The gap is amplified by taking sufficiently many tensor product copies of the Hamiltonian, resulting in a nonlocal instance.

Lemma 3.4.7 (Gap amplification). *Let H be an n-qubit Hamiltonian with minimum energy $\lambda_{\min}(H) \geq 0$ and such that $\|H\| \leq 1$. Let $p(n), q(n)$ be polynomials such that $p(n) > q(n)$ for all n. Let*

$$H' = \mathrm{Id}^{\otimes a} - (\mathrm{Id} - (H - a^{-1}\,\mathrm{Id}))^{\otimes a}, \qquad \textit{where} \qquad a = \left(\frac{1}{q} - \frac{1}{p}\right)^{-1}.$$

Then H' is a (non-local) Hamiltonian over an $= O(np(n))$ qubits with $\|H'\| = O(1)$, such that if $\lambda_{\min}(H) \leq 1/p$, then $\lambda_{min}(H') \leq 1/2$, whereas if $\lambda_{\min}(H) \geq 1/q$, then $\lambda_{min}(H') \geq 1$.

Proof. The proof follows by observing that $\lambda_{\min}(H') = 1 - (1 - (\lambda_{min}(H) - a^{-1}))^a$, and $(1 \pm \delta)^k = 1 \pm k\delta + O(\delta^2)$ when $k\delta = O(1)$. □

Proof of Corollary 3.1.2. By applying the result of Theorem 3.4.4 to the Hamiltonian H' obtained from H as in Lemma 3.4.7, we obtain the statement of Corollary 3.1.2, except with $p_{\mathrm{c}} = p$ and $p_{\mathrm{s}} = q$ for some constants $0 < q < p < 1$. To match the constants in the statement of Corollary 3.1.2, we make the verifier automatically accept with probability $1 - p'$, and perform the test with probability p', for some $0 \leq p' \leq 1$. Then we get $p_{\mathrm{c}} = 1 - p' + p'p$ and $p_{\mathrm{s}} = 1 - p' + p'q$. If p' is chosen as $p' = \frac{1}{2(1+p-2q)}$, we get $p_{\mathrm{c}} = 1/2 + 2\eta_0$ and $p_{\mathrm{s}} = 1/2 + \eta_0$ as desired, with $\eta_0 = \frac{(p-q)}{2(1+p-2q)}$. □

3.5 Delegated Computation

It was noticed in [FH15] that an interactive proof system for the local Hamiltonian problem can also be used for delegated quantum computation with so-called *post-hoc* verification. The key idea is to use the Feynman-Kitaev construction to produce a Hamiltonian encoding the desired computation; measuring the ground energy of this Hamiltonian reveals whether the computation accepts or rejects. Following the same connection, we are able to give a post-hoc verifiable delegated computation scheme with a purely classical verifier and a constant number of players. The players only need the power of BQP. The scheme has a constant completeness-soundness gap independent of the size of the circuit to be computed, unlike the scheme of [FH15] and the classical scheme of [RUV13a], which both have inverse-polynomial gaps. However, unlike the scheme of [RUV13a] (and similarly to the one in [FH15]), our protocol is

not *blind*: the verifier must reveal the entire circuit to be computed to all the players before the verification process starts.

Theorem 3.5.1. *There exists an interactive proof system for BQP with seven quantum entangled players and one classical verifier, with one round of communication, in which the player sends $O(\mathrm{poly}(n))$-bit questions and receives $O(1)$-bit answers. The honest players only need the power of BQP.*

Proof sketch. For any poly-size quantum circuit C, we construct the history Hamiltonian H_C and announce to the seven players. In the honest case, the players produce the state

$$|\psi\rangle = \mathrm{ENC}\Big(\frac{1}{\sqrt{T}}\sum_{t=1}^{T}|t\rangle_{\mathrm{clock}} \otimes |\psi_t\rangle\Big),$$

where ENC is the encoding map of the 7-qubit code, t labels the clock states of the computation from 1 to T, and $|\psi_t\rangle$ is the state of the circuit C at step t. This state can be prepared with a BQP machine. The players are then separated; in the honest case, each player receives a share of the encoded state $|\psi\rangle$. The verifier plays the game of Theorem 3.4.4 with the players and accepts if and only if they succeed. □

Given a local Hamiltonian $H = \sum_{\ell=1}^{m} \alpha_\ell H_\ell$, where $\alpha_\ell \in [-1, 1]$ and each $H_\ell = \sigma_X(a_\ell)\sigma_Z(b_\ell)$. Let $p \in (0, 1)$ be a parameter of the protocol.
The verifier performs one of the following three tests at random, the first with probability $(1 - p)$ and the second and third with probability $p/2$ each.

1. (Pauli braiding test) Choose one of the r players uniformly at random to be the special player. The other players form the composite player. Simulate the Pauli braiding test with these two players, where the role of Alice is assigned to the special player and the role of Bob to the composite player.

2. (Energy test) Choose $\ell \in \{1, \ldots, m\}$ uniformly at random. Define an operator Q_ℓ acting on rn qubits by replacing each σ_X in H_ℓ with $X_{logical}$ on the r-qubit code state, and σ_Z by $Z_{logical}$. Send each player a query (XZ, a, b) representing the associated share of Q_ℓ. The players should each return two values in $\{-1, 1\}$. The verifier takes the product of all values received. If its sign disagrees with that of α_ℓ, he accepts. If they agree, he rejects with probability $|\alpha_\ell|$ and accepts otherwise.

3. (Energy consistency test) Choose one of the r players uniformly at random to be the special player. The other players form the composite player. Let $W \in \{X, Z\}$, each chosen with probability $1/2$. Also choose a, b according to the same distribution as in the energy test. The verifier performs one of the following tests, each chosen with the indicated probability.

   - With probability $1/2$, send the special player (XZ, a, b), and the composite player $\overline{(W, c, c + a)}$ if $W = X$ and $\overline{(W, c, c + b)}$ if $W = Z$, where $c \in \{0, 1\}^n$ is chosen uniformly at random. Accept if the special player's answer agrees with the product of the composite player's two answers.
   - With probability $1/4$, send the special player (W, c, d), and the composite player $\overline{(W, c, c + a)}$, where $c, d \in \{0, 1\}^n$ are chosen uniformly at random. Accept if the special player and composite player agree on the answer associated with c.
   - With probability $1/4$, send the special player $(W, c + a, d)$, and the composite player $\overline{(W, c, c + a)}$, where $c, d \in \{0, 1\}^n$ are chosen uniformly at random. Accept if the special player and composite player agree on the answer associated with $c + a$.

Figure 3-3: The Hamiltonian self-test

Chapter 4

Two-prover low degree test

In this chapter, we show that the maximum success probability of players sharing quantum entanglement in a two-player game with classical questions of logarithmic length and classical answers of constant length is NP-hard to approximate to within constant factors. As a corollary, the inclusion NEXP $\subseteq$ MIP*, first shown in [IV12] with three provers, holds with two provers only. The proof is based on a simpler, improved analysis of the low-degree test Raz and Safra (STOC'97) against two entangled provers.

4.1 Introduction

The class MIP* is the class of languages having multi-prover interactive proofs between a classical polynomial-time verifier and quantum provers who may share entanglement. Allowing the provers to use entanglement may affect both the completeness and soundness parameters of a proof system. As a result, the only trivial lower bound on MIP* is IP, since the verifier can ignore one of the provers, and there are no trivial upper bounds, as the size of entangled-prover strategies can be arbitrary.

The class MIP* was introduced in [CHTW04], where it is shown that entangled provers can in some cases have much more power than classical unbounded provers, leading to the collapse of certain proof systems based on XOR games. Nevertheless, a sequence of works established techniques to limit the power of entangled provers, eventually leading to a proof that MIP $\subseteq$ MIP* [IV12]. The result is a corollary of the inclusion NEXP $\subseteq$ MIP*, whose proof follows the same structure as Babai et al.'s celebrated proof that NEXP $\subseteq$ MIP. The main technical component of the proof is an analysis of the soundness of Babai et al.'s multilinearity test with entangled provers. The result was later refined in [Vid13], who obtained a scaled-down version that applies to multiplayer games specified in explicit (matrix) form: the main result of [Vid13] is that it is NP-hard to approximate the value of a three-player entangled games. The main technical component of the proof is an analysis of the soundness of the "plane-vs-point" low-degree test [RS97] with entangled provers.

A rather intriguing limitation of the results in [IV12, Vid13] is that they only apply to games, or interactive proof systems, with three or more entangled players, or

provers. Even though in any interaction the verifier in the proof systems considered only exchanges messages with two out of the three provers,[1] the technical analysis seems to crucially require that the joint Hilbert space supporting the provers' strategies can be decomposed in at least three tensor factors. This requirement is used at key steps in the analysis, including the quantum analogue of the "self-improvement lemma" that is key to control the accumulation of approximation errors in the inductive proofs of both the multilinearity and low-degree tests.

Even though this may at first seem like a purely technical limitation, it has been known at least since the work of Toner [Ton09] that this kind of "embedding" of a two-player game in a three-player game can effectively limit the players' ability to take advantage of their shared entanglement, in some cases drastically lowering their maximum success probability in the game. At a conceptual level this effect can be understood as a manifestation of the phenomenon of monogamy of entanglement. Whether this is a fundamental limitation, or whether the same constraints as imposed by monogamy can be simulated within two players only, remains unclear. While the first NP-hardness results for entangled game, which applied only to inverse-polynomial approximations, were established for three-player games [KKM+11], they were shortly thereafter extended to the case of games with two players [IKM09]. The games that underlie the constant-factor hardness results in [IV12, Vid13] do not need more than two players to be played: could it be that the two-prover entangled value of the game can be approximated in polynomial time, while the three-player entangled value is NP-hard?

We answer this question by showing that the same plane-vs-point low-degree test analyzed in [Vid13] remains sound even when it is played with two, instead of three, entangled provers. As a consequence, we obtain the first non-trivial hardness results for the class $\mathrm{MIP}^*(2,1)$ of two-prover one-round entangled proof systems.

Theorem 4.1.1. *The inclusion* $\mathrm{NEXP} \subseteq \mathrm{MIP}^*(2,1)$ *holds. Furthermore, it still holds when* $\mathrm{MIP}^*(2,1)$ *is restricted to one-round proof systems with constant answer size.*

Theorem 4.1.1 is obtained by scaling up an NP-hardness result for two-player entangled projection games,[2] see Theorem 4.4.1 and Corollary 4.4.2 in Section 4.4.

The main ingredient needed to obtain Theorem 4.1.1, and our main technical contribution, is a soundness analysis of the plane-vs-point low-degree test in the presence of two entangled provers. The analysis that we provide is both conceptually and technically simpler than the analysis in [Vid13]. Even though the present proof is not entirely self-contained, as it relies on elementary reductions from [Vid13], we present it in a modular way which, we hope, will make it more easily accessible, and more conveniently re-usable, than the proof in [Vid13]. In the following subsection we describe the low-degree test and give a high-level overview of our analysis.

[1] More precisely, all tests considered, including the low-degree test, take the form: (i) the verifier selects two provers at random, and calls them "Alice" and "Bob"; (ii) the verifier plays a two-prover game with Alice and Bob.

[2] The reduction proceeds in a standard way by using an implicitly defined instance of the 3-SAT problem as starting point; we omit the details.

4.1.1 The low-degree test

We recall the "plane-vs-point" low-degree test from [Vid13] in Figure 4-1. The test is essentially the same as the classical test from [RS97]. It asks one prover for the restriction of a low-degree m-variate polynomial g to a random two-dimensional subspace s of $\mathbb{F}_q^m$, where $\mathbb{F}_q$ is the finite field with q elements, q a prime power, and the other prover for the evaluation of g at a random $x \in s$; the prover's answers are checked for consistency.

Out of the two provers, chose one at random to be Alice and the other to be Bob.

1. Let d, m be integer and q a prime power given as input.
2. Select a random point $x \in \mathbb{F}_q^m$ and two random directions $y_1, y_2 \in \mathbb{F}_q^m$. If y_1 and y_2 are not linearly independent, accept; otherwise, let s be the plane spanned by the two lines parallel to y_1, y_2 passing through x.
3. Send s to Alice and x to Bob. Receive g, a specification of a degree-d polynomial restricted to s, from Alice, and $a \in \mathbb{F}_q$ from Bob.
4. Accept if and only if $g(x) = a$.

Figure 4-1: The (d, m, q)-low-degree test.

Since the test treats both provers symmetrically, for the purposes of the soundness analysis we may reduce to the case where the provers share a permutation-invariant state and use the same collection of measurement operators. The following states the result of our analysis of the test. It extends Theorem 3.1 in [Vid13] to the case of two provers.[3] In the theorem, we use the notation $\langle A, B\rangle_\psi$ for $\langle\Psi|A \otimes B|\Psi\rangle$.

Theorem 4.1.2. *There exists a $\delta = \mathrm{poly}(\varepsilon)$ and a constant $c > 0$ such that the following holds. Let $\varepsilon > 0$, m, d integers, and q a prime power such that $q \geq (dm/\varepsilon)^c$. For any strategy for the players using entangled state $|\Psi\rangle$ and projective measurements $\{A_s^r\}_r$ that succeeds in the (d, m, q)-low-degree test with probability at least $1 - \varepsilon$, there exists a POVM $\{S^g\}_g$, where g ranges over m-variate polynomials over $\mathbb{F}_q$ of total degree at most d, such that the following hold:*

1. *Approximate consistency with A:*

$$\mathop{\mathrm{E}}_s \sum_g \sum_{r \neq g|_s} \langle A_s^r, S^g\rangle_\psi \leq \delta \,,$$

where the expectation is over a random two-dimensional subspace s of $\mathbb{F}_q^m$, as chosen by the verifier in the test;

[3] The self-consistency condition is not explicitly stated in [Vid13] but (as we will show) it follows easily from the proof.

2. *Self-consistency:*

$$\sum_g \langle S^g, (\mathrm{Id} - S^g) \rangle_\psi \leq \delta \, .$$

The proof of Theorem 4.1.2 follows the same structure as the proof of Theorem 3.1 in [Vid13]. The proof is by induction on the number of variables m. The base case $m = 2$ is trivial, since there is a single subspace s, and the provers' associated POVM $\{A^r\}$ can directly play the role of $\{S^g\}$ in the theorem. Suppose then that the theorem is true for a value $(m-1)$ such that $m - 1 \geq 2$. To show that the theorem holds for m there are three main steps:

1. (Section 6.3 of [Vid13]) By the induction hypothesis, for every $(m-1)$-dimension hyperplanes s in $\mathbb{F}_q^m$ there is a POVM $\{Q_s^g\}_g$ with outcomes g in the set of degree-d polynomials on s, such that on average over the choice of a uniformly random s and $x \in s$ the POVM $\{Q_s^g\}$ is consistent with $\{A_x^a\}$.

2. (Section 6.4 of [Vid13]) Measurements $\{Q_s^g\}_g$ associated with k parallel subspaces $s_1, \ldots, s_k$ are inductively "pasted" together, for $k = 1, \ldots,$, to yield a combined measurement $\{Q_{(s_i)}^{(g_i)}\}$ that returns a k-tuple of degree-d polynomials g_i defined on s_i.

3. (Section 6.5 of [Vid13]) Finally, for k sufficiently large compared to d, the measurement $\{Q_{(s_i)}^{(g_i)}\}$ is consolidated into a single global measurement $\{S^g\}$ that satisfies the conclusion of the theorem for the m-variate case.

These three steps remain unchanged in the current proof. At only very few places in [Vid13] is the presence of three provers used; in most cases this is only a matter of convenience and is easily avoided. For completeness, in Section 4.5 we explicitly list those places and how the recourse to three provers can be avoided.

As already mentioned the critical point in the proof where three provers, or rather the existence of three tensor factors in the provers' Hilbert space, is used, is to control the error increase throughout the induction. As shown by the analysis, if the measurements $\{Q_s^g\}$ produced by the induction hypothesis are δ-consistent with $\{A_x^a\}$, then the resulting S^g will be $O(\delta^c)$-consistent with the same $\{A_x^a\}$, for some constant $c < 1$. For poly-logarithmic m such an increase is unmanageable. Thus a key step in the analysis consists in establishing a "self-improvement lemma", which resets the consistency error to some constant baseline at each step of the induction. This is called the "consolidation procedure" in [Vid13].

The main result of the consolidation procedure is stated as Proposition 5.8 in [Vid13]. The procedure shows that the consistency error sustained by any POVM, when measured against a structure called a "robust triple" in [Vid13], can be automatically improved.

Our main technical contribution is a simpler, self-contained proof of a variant of that proposition which applies to strategies with two provers only. Our variant is based on a simpler notion than the robust triples from [Vid13], that we call "global consistency". Throughout we assume familiarity with the notation and proof structure

from [Vid13], though we recall the most important notions in Section 4.2. In particular we formally define robust triples and global consistency, and show that the former notion implies the latter, so that our result can be directly used in lieu of Proposition 5.8 in the analysis of [Vid13]. In Section 4.3 we prove our replacement for Proposition 5.8, Proposition 4.3.1. The proof of (the scaled-down version of) Theorem 4.1.1 follows from the analysis of the test using similar reductions as in [Vid13]; we briefly explain how in Section 4.4.

4.2 Preliminaries

4.2.1 Notation

We use $\mathcal{H}$ to denote a finite-dimensional Hilbert space, and $\mathrm{L}(\mathcal{H})$ for the linear operators on $\mathcal{H}$. Subscripts $\mathcal{H}_A$, $\mathcal{H}_B$ indicate distinct spaces. For $|\Psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ and $A \in \mathrm{L}(\mathcal{H}_A)$, $B \in \mathrm{L}(\mathcal{H}_B)$ we write $\langle A, B\rangle_\psi = \langle \Psi | A \otimes B | \Psi \rangle$. Note that we do not conjugate A or B. Given two families of operators $\{A_x^a\}$ and $\{B_x^a\}$ on $\mathcal{H}_A$, where $x \in \mathcal{X}$ and $a \in \mathcal{A}$ range over finite sets, and $0 \leq \delta \leq 1$, we write $A_x^a \approx_\delta B_x^a$ for

$$\mathop{\mathrm{E}}_x \sum_a \langle (A_x^a - B_x^a)^2, \mathrm{Id} \rangle_\psi = O(\delta) .$$

The expectation over x will usually be taken with respect to the uniform distribution. The distinction between taking an expectation (over x) or a summation (over a) will always be clear from context.

4.2.2 Measurements

Throughout, we consider a bipartite state $|\Psi\rangle \in \mathcal{H} \otimes \mathcal{H}$ assumed to be invariant under permutation of the two registers. All operators we consider act on the finite-dimensional space $\mathcal{H}$.

Definition 4.2.1. A *sub-measurement* $\{M^a\}_a$ is a collection of positive semidefinite operators satisfying $M = \sum_a M^a \leq \mathrm{Id}$. We say that a sub-measurement is η-complete if

$$\langle M, \mathrm{Id} \rangle_\Psi \geq 1 - \eta ;$$

η is called the *completeness error*. If $M = \mathrm{Id}$ then we say that $\{M^a\}_a$ is a measurement, in which case the completeness error is zero.[4]

The following definition appears in [Vid13].

Definition 4.2.2. Let $\mathcal{X}$ and $\mathcal{A}$ be finite sets. Let $\{M_x^a\}_a$ be a family of sub-measurements indexed by $x \in \mathcal{X}$ and with outcomes $a \in \mathcal{A}$. For each x, let $M_x = \sum_a M_x^a$. We say that $\{M_x^a\}$ is

[4]The converse does not necessarily hold, as $|\Psi\rangle$ may not have full support.

- *ε-self-consistent* if

$$\mathop{\mathrm{E}}_{x} \sum_{a \neq a'} \langle M_x^a,\, M_x^{a'} \rangle_\psi \leq \varepsilon \;,$$

- *γ-projective* if

$$\mathop{\mathrm{E}}_{x} \langle M_x,\, (\mathrm{Id} - M_x) \rangle_\Psi \leq \gamma \;.$$

- Let $\{T^g\}$ be a sub-measurement with outcomes in the set of all functions $g : \mathcal{X} \to \mathcal{A}$. We say that $\{M_x^a\}$ and $\{T^g\}$ are *δ-consistent* if

$$\mathop{\mathrm{E}}_{x} \sum_{g,a:\, a \neq g(x)} \langle T^g,\, M_x^a \rangle_\psi \leq \delta \;.$$

We consider families of functions such that distinct functions have few points of intersection.

Definition 4.2.3. Let $\mathcal{X}$ and $\mathcal{A}$ be finite sets, $\mathcal{G}$ a set of functions from $\mathcal{X}$ to $\mathcal{A}$, and $0 \leq \kappa \leq 1$. We say that $(\mathcal{X}, \mathcal{A}, \mathcal{G})$ is κ-structured if for any two distinct $g, g' \in \mathcal{G}$,

$$\Pr_{x \in \mathcal{X}} \big(g(x) = g'(x) \big) \leq \kappa \;,$$

where the probability is taken under the uniform distribution on $\mathcal{X}$.

The following lemma states useful properties of consistency.

Lemma 4.2.4. *Let $(\mathcal{X}, \mathcal{A}, \mathcal{G})$ be κ-structured. Let $\{A_x^a\}_{a \in \mathcal{A}}$ be a family of measurements indexed by $x \in \mathcal{X}$ that is ε-self-consistent. Let $\{T^g\}_{g \in \mathcal{G}}$ be a sub-measurement that is δ-consistent with $\{A_x^a\}$. Then*

- *$\{T^g\}$ is δ'-self-consistent, for $\delta' = O(\sqrt{\varepsilon} + \sqrt{\delta} + \kappa)$;*
- *Let $T = \sum_g T^g$, and suppose $\{T^g\}$ is γ-projective. Then*

$$T A_x^a \approx_{\sqrt{\varepsilon}+\sqrt{\delta}+\gamma+\kappa} A_x^a T \;.$$

Proof. We sketch the proof. For the first item,

$$\begin{aligned}
\sum_{g \neq g'} \langle T^g, T^{g'} \rangle_\psi &= \mathop{\mathrm{E}}_{x} \sum_{a} \sum_{g \neq g'} \langle T^g,\, T^{g'} A_x^a \rangle_\psi \\
&\approx_{\sqrt{\delta}} \mathop{\mathrm{E}}_{x} \sum_{g \neq g'} \langle T^g,\, T^{g'} A_x^{g(x)} \rangle_\psi \\
&\approx_{\sqrt{\varepsilon}} \mathop{\mathrm{E}}_{x} \sum_{g \neq g'} \langle T^g A_x^{g(x)},\, T^{g'} \rangle_\psi \\
&\approx_{\sqrt{\delta}} \mathop{\mathrm{E}}_{x} \sum_{g \neq g'} \mathbf{1}_{g(x)=g'(x)} \langle T^g A_x^{g(x)},\, T^{g'} \rangle_\psi \\
&\approx_{\sqrt{\delta}} \mathop{\mathrm{E}}_{x} \sum_{g \neq g'} \mathbf{1}_{g(x)=g'(x)} \langle T^g,\, T^{g'} \rangle_\psi
\end{aligned}$$

$$\leq \kappa \,.$$

For the second item, it suffices to lower bound

$$\begin{aligned}
\mathop{\mathrm{E}}_x \sum_a \langle TA_x^a TA_x^a, \mathrm{Id}\rangle_\psi &\approx_{\sqrt{\varepsilon}} \mathop{\mathrm{E}}_x \sum_a \sum_g \langle TA_x^a T^g, A_x^a\rangle_\psi \\
&\approx_{\sqrt{\delta}} \mathop{\mathrm{E}}_x \sum_a \sum_g \langle TA_x^a T^g, A_x^{g(x)}\rangle_\psi \\
&\approx_{\sqrt{\delta}} \mathop{\mathrm{E}}_x \sum_{a,a'} \sum_g \langle TA_x^a T^g, A_x^{a'}\rangle_\psi \\
&= \langle T^2, \mathrm{Id}\rangle_\psi \,.
\end{aligned}$$

The claimed bound then follows by expanding $\mathrm{E}_x \sum_a (TA_x^a - A_x^a T)^2$ and regrouping terms. □

4.2.3 Global consistency

The analysis of the low-degree test amounts to arguing that a set of measurement operators which produce outcomes that are locally consistent can be combined into a single measurement which returns a global object consistent with each of the local measurements: it is possible to recombine local views. In [Vid13] the notion of local consistency used is called a "robust triple". For convenience we recall the definition.

Definition 4.2.5 (Definition 5.2 in [Vid13]). Let $G = (V, E)$ be a graph, S a finite set, $\mathcal{G} \subseteq \{g : V \to S\}$ a set of functions and for every $v \in V$, $\{A_v^a\}_{a\in S}$ a measurement with outcomes in S. Given $\delta > 0$ and $0 < \mu \leq 1$, we say that $(G, \{A_x^a\}, \mathcal{G})$ is a (δ, μ)-robust triple if:

1. (self-consistency) The family of measurements $\{A_v^a\}$ is δ-self-consistent;
2. (small intersection) $(V, S, \mathcal{G})$ is δ-structured;
3. (stability) For any sub-measurement $\{R^g\}_{g\in\mathcal{G}}$ it holds that

$$\mathop{\mathrm{E}}_{v\in V} \mathop{\mathrm{E}}_{v'\in N(v)} \sum_g \langle R^g, (A_v^{g(v)} - A_{v'}^{g(v')})^2\rangle_\psi \leq \delta \,,$$

   where $N(v)$ is the set of neighbors of v in G;
4. (expansion) G has mixing time $O(\mu^{-1})$. Precisely, if for any $v \in V$ we let $p_k(v)$ denote the distribution on V that results from starting a k-step random walk at v, then for any $\delta > 0$ and some $k = O(\log(1/\delta)\log(1/\mu))$ it holds that $\mathrm{E}_{v\in V} \|p_k(v) - |V|^{-1}\|_1 \leq \delta$.

We observe that the only way in which items 3. and 4. from the definition are used for the self-improvement results is through [Vid13, Claim 5.3], which states the following.

Claim 4.2.6 (Claim 5.3 in [Vid13]). *Suppose $(G, A, \mathcal{G})_\Psi$ is a (δ, μ)-robust triple. Then there exists a $\delta' = O\big(\delta^{1/2} \log^2(1/\delta) \log^2(1/\mu)\big)$ such that for any sub-measurement $\{R^g\}_{g \in \mathcal{G}}$,*

$$\sum_g \langle R^g, A^g - (A^g)^2 \rangle_\psi \leq \delta' , \tag{4.1}$$

where $A^g = \mathrm{E}_{v \in V} A_v^{g(v)}$.

It is more direct, and more general, to use condition (4.1) directly as part of the definition, as this allows us to set aside any notion of an expanding graph.

Definition 4.2.7. Let $(\mathcal{X}, \mathcal{A}, \mathcal{G})$ be κ-structured. Let $\{A_x^a\}_{a \in \mathcal{A}}$ be a family of measurements indexed by $x \in \mathcal{X}$ and with outcomes $a \in \mathcal{A}$. For $g \in \mathcal{G}$, let $A^g = \mathrm{E}_x A_x^{g(x)}$. Let $|\Psi\rangle$ be a permutation-invariant bipartite state. For $0 \leq \varepsilon, \delta \leq 1$ we say that $(\{A_x^a\}, \mathcal{G})$ is (ε, δ)-globally consistent on $|\Psi\rangle$ if:

1. $\kappa = O(\varepsilon)$;
2. The family $\{A_x^a\}$ is ε-self-consistent;
3. There exists a positive semidefinite operator Z such that

$$\forall g \in \mathcal{G},\ 0 \leq A^g - (A^g)^2 \leq Z, \qquad \text{and} \qquad \langle Z, \mathrm{Id} \rangle_\psi \leq \delta.$$

It is not hard to verify that condition 3. in the definition is equivalent to (4.1). This can be seen by writing the bound δ in the condition as the optimum of a semidefinite program, and taking the dual. This is done in a similar way to the analysis of the semidefinite program (4.2). The only difference is that the latter considers consistency when the state $|\Psi\rangle$ is maximally entangled. Formally, we have the following lemma.

Lemma 4.2.8. *Let $|\Psi\rangle \in \mathcal{H} \otimes \mathcal{H}$ be a state invariant under permutation of its two registers, such that the reduced density of $|\Psi\rangle$ on either register has full support. Let $\{A_i\}$ a family of positive semidefinite operators on $\mathcal{H}$ with $A_i \leq \mathrm{Id}$ for all i. Then the following primal and dual semidefinite program satisfy strong duality, and hence have the same optimum value:*

Primal SDP

$$\begin{aligned} \sup \quad & \sum_i \langle T_i, A_i \rangle_\psi \\ s.t. \quad & T_i \geq 0 \qquad \forall i\ , \\ & \sum_i T_i \leq \mathrm{Id}\ . \end{aligned}$$

Dual SDP

$$\begin{aligned} \inf \quad & \langle Z, \mathrm{Id} \rangle_\psi \\ s.t. \quad & Z \geq A_i \qquad \forall i\ , \\ & Z \geq 0\ . \end{aligned}$$

Proof. Both the primal and dual are strictly feasible, as can be seen by taking e.g. $T_i \propto \mathrm{Id}$ such that $\sum_i T_i = \mathrm{Id}/2$, and $Z = 2\,\mathrm{Id}$. □

Taking A_i in Lemma 4.2.8 to equal $A^g - (A^g)^2$, the primal value being less than δ' is equivalent to (4.1), while the dual value being less than δ' is equivalent to item 3. in Definition 4.2.7.

For later use we note that self-consistency of $\{A_x^a\}$ implies self-consistency of the operators A^g introduced in Definition 4.2.7, in the following sense.

Lemma 4.2.9. *Let $\{A_x^a\}$ be a family of measurements that is ε-self-consistent. Then for any sub-measurement $\{R^g\}$,*

$$\sum_g \langle A^g,\, R^g\rangle_\psi \approx_{\sqrt{\varepsilon}} \sum_g \langle \mathrm{Id},\, R^g A^g\rangle_\psi.$$

Proof. Write

$$\begin{aligned}
\sum_g \langle A^g,\, R^g\rangle_\psi &= \sum_g \mathop{\mathrm{E}}_x \langle A_x^{g(x)},\, R^g\rangle_\psi \\
&= \sum_{g,a} \mathop{\mathrm{E}}_x \langle A_x^{g(x)},\, R^g A_x^a\rangle_\psi \\
&\approx_{\sqrt{\varepsilon}} \sum_g \mathop{\mathrm{E}}_x \langle A_x^{g(x)},\, R^g A_x^{g(x)}\rangle_\psi \\
&\approx_{\sqrt{\varepsilon}} \sum_g \mathop{\mathrm{E}}_x \langle \mathrm{Id},\, R^g A_x^{g(x)}\rangle_\psi .
\end{aligned}$$

□

4.3 Self-improvement with two provers

The main result on self-improvement from [Vid13] is stated as Proposition 5.8 in that paper. Our main technical result, Proposition 4.3.1 below, improves upon Proposition 5.8 in the following respects:

- Proposition 4.3.1 allows to perform sel-improvement with two provers only;
- Proposition 4.3.1 only requires the notion of consistency introduced in Definition 4.2.7, which as argued in Section 4.2.3 is less restrictive than the notion of robust triple used in [Vid13];
- The proof of Proposition 4.3.1 is simpler and yields better parameters.

We state the proposition and give its proof. In Section 4.4 we show how the proposition is used to obtain the hardness results.

Proposition 4.3.1. *There exists universal constants $\varepsilon_0, \delta_0, t_0 > 0$ such that the following holds. Let $(\mathcal{X}, \mathcal{A}, \mathcal{G})$ be κ-structured. Let $\{A_x^a\}_{a\in\mathcal{A}}$ be a family of measurements indexed by $x \in \mathcal{X}$, and $|\Psi\rangle$ a bipartite permutation-invariant state. Suppose that the following conditions hold:*

1. $(\{A_x^a\}, \mathcal{G})$ *is* (ε, δ)*-globally consistent on* $|\Psi\rangle$*, for some* $0 \leq \varepsilon \leq \varepsilon_0$*,* $0 \leq \delta \leq \delta_0$*;*

2. *There exists a function* $t = t(\varepsilon', \delta')$ *and* $\varepsilon_0', \delta_0' > 0$ *such that for any* $0 \leq \varepsilon' \leq \varepsilon_0'$ *and* $0 \leq \delta' \leq \delta_0'$ *it holds that* $t(\varepsilon', \delta') \leq t_0$*, and such that the following holds. For any* (ε', δ') *and state* $|\Phi\rangle$ *such that* $(\{A_x^a\}, \mathcal{G})$ *is* (ε', δ')*-globally consistent on* $|\Phi\rangle$*, there exists a measurement* $\{Q^g\}_{g \in \mathcal{G}}$ *that is* $t(\varepsilon', \delta')$*-consistent with* $\{A_x^a\}$*.*

Then there exists a measurement $\{R^g\}_{g \in \mathcal{G}}$ *that is* δ'*-consistent with* $\{A_x^a\}$*, for some* $\delta' = O(\sqrt{r(\varepsilon, \delta)})$*, where* $r(\varepsilon, \delta)$ *is the function defined in Lemma 4.2.8.*

The key "improvement" provided by the proposition is that, while the function t is only assumed to be bounded by a fixed constant for sufficiently small values of the arguments, the proposition returns a measurement $\{R^g\}$ that has an explicit consistency δ' with $\{A_x^a\}$, where δ' is polynomial in ε and δ, irrespective of t (indeed t need not approach 0 as ε, δ approach 0).

We note that, in our language, [Vid13, Proposition 5.8] considers a family of globally consistent pairs $(\{A_{t,x}^a\}, \mathcal{G}_t)$, parametrized by some finite set $t \in T$, and makes both the assumptions and the conclusions of Proposition 4.3.1 in an averaged sense, for uniformly random $t \in T$. For simplicity we state and prove the proposition for $|T| = 1$. The case of general T is needed for the inductive application of the Proposition towards the proof of Theorem 4.1.2. We sketched the inductive step in the introduction. We refer to [Vid13] for details of the derivation of Theorem 4.1.2 from Proposition 4.3.1, which is identical to the derivation of [Vid13, Theorem 3.1] from [Vid13, Proposition 5.8], up to minor modifications that we review in Appendix 4.5.

The main step in the proof of the proposition is provided by the following lemma, which is analogous to [Vid13, Claim 5.4]. The semidefinite program considered in the proof of the lemma, and its analysis, are our main points of departure from the proof in [Vid13]. Indeed, the proof of an upper bound on the completeness error of the sub-measurement $\{S^g\}$ constructed in the proof of the lemma is the main point where the existence of a three-fold tensor product decomposition of the Hilbert space is most crucially used in [Vid13].

Lemma 4.3.2. *There exists a function* $r(\varepsilon, \delta) = O(\sqrt{\varepsilon} + \sqrt{\delta})$ *such that the following holds for all* $0 \leq \varepsilon, \delta, \eta \leq 1$*. Let* $(\mathcal{X}, \mathcal{A}, \mathcal{G})$ *be* κ*-structured. Let* $\{A_x^a\}_{a \in \mathcal{A}}$ *be a family of measurements indexed by* $x \in \mathcal{X}$*. Let* $|\Psi\rangle$ *be a permutation-invariant bipartite state and assume* $(\{A_x^a\}, \mathcal{G})$ *are* (ε, δ)*-globally consistent on* $|\Psi\rangle$*. Let* $\{Q^g\}_{g \in \mathcal{G}}$ *be a sub-measurement that is* η*-consistent with* $\{A_x^a\}$ *on* $|\Psi\rangle$*. Then there exists a sub-measurement* $\{S^g\}$ *that is* $r(\varepsilon, \delta)$*-consistent with* $\{A_x^a\}$ *and projective and has completeness error*

$$\langle \mathrm{Id} - S,\, \mathrm{Id} \rangle_\Psi \;\leq\; \langle \mathrm{Id} - Q,\, \mathrm{Id} \rangle_\Psi + \eta + r(\varepsilon, \delta)\,.$$

Proof. For $g \in \mathcal{G}$, let $A^g = \mathrm{E}_x A_x^{g(x)}$. Consider the following primal and dual semidefinite program, obtained from the semidefinite program in Lemma 4.2.8 by setting A_i to A^g and choosing $|\Psi\rangle$ to be the maximally entangled state: the primal becomes

$$\omega \;=\; \sup \quad \sum_g \mathrm{Tr}(T^g A^g) \tag{4.2}$$

$$\begin{aligned} \text{s.t.} \quad & T^g \geq 0 \qquad \forall g \in \mathcal{G} \,, \\ & \sum_g T^g \leq \mathrm{Id} \,, \end{aligned}$$

and the dual

$$\begin{aligned} \min \quad & \mathrm{Tr}(Z) \\ \text{s.t.} \quad & Z \geq A^g \qquad \forall g \in \mathcal{G} \,, \\ & Z \geq 0 \,. \end{aligned} \tag{4.3}$$

As shown in Lemma 4.2.8 both the primal and dual are strictly feasible, so that strong duality holds. Let $\{T^g\}$ be an optimal primal solution. Without loss of generality, $\sum_g T^g = \mathrm{Id}$, as any solution such that $(\mathrm{Id} - \sum_g T^g)A^{g'} \neq 0$ for any g' is clearly not optimal. The complementary slackness conditions imply

$$T^g Z \;=\; T^g A^g \qquad \forall g \in \mathcal{G} \,. \tag{4.4}$$

For each $g \in \mathcal{G}$ let

$$S^g = \mathop{\mathrm{E}}_x A_x^{g(x)} T^g A_x^{g(x)} \,.$$

Then $\{S^g\}$ is a sub-measurement. We show that S^g satisfies the desired consistency, projectivity and completeness properties.

(i) Consistency: We have that

$$\mathop{\mathrm{E}}_x \sum_g \sum_{a \neq g(x)} \langle S^g, A_x^a \rangle_\Psi = \sum_g \langle S^g, (\mathrm{Id} - A^g) \rangle_\Psi \,.$$

Using self-consistency of $\{A_x^a\}$,

$$\begin{aligned} \sum_g \langle S^g, \mathrm{Id} \rangle_\Psi &= \mathop{\mathrm{E}}_x \sum_g \langle A_x^{g(x)} T^g A_x^{g(x)}, \mathrm{Id} \rangle_\psi \\ &\approx_{\sqrt{\varepsilon}} \mathop{\mathrm{E}}_x \sum_g \langle T^g, A_x^{g(x)} \rangle_\psi \\ &= \sum_g \langle T^g, A^g \rangle_\psi \,. \end{aligned} \tag{4.5}$$

Similarly,

$$\begin{aligned} \sum_g \langle S^g, A^g \rangle_\Psi &= \mathop{\mathrm{E}}_x \sum_g \langle A_x^{g(x)} T^g A_x^{g(x)}, A^g \rangle_\psi \\ &\approx_{\sqrt{\varepsilon}} \mathop{\mathrm{E}}_x \sum_g \langle T^g, A_x^{g(x)} A^g A_x^{g(x)} \rangle_\psi \,. \end{aligned} \tag{4.6}$$

Using the Cauchy-Schwarz inequality,

$$\begin{aligned}\mathop{\mathrm{E}}_x \sum_g \langle T^g,\, \big(A^g - A_x^{g(x)}\big) A^g A_x^{g(x)} \rangle_\psi &\leq \Big(\mathop{\mathrm{E}}_x \sum_g \langle T^g,\, A_x^{g(x)} (A^g)^2 A_x^{g(x)} \rangle_\psi \Big)^{\frac{1}{2}} \\ &\quad \cdot \Big(\mathop{\mathrm{E}}_x \sum_g \langle T^g,\, \big(A^g - A_x^{g(x)}\big)^2 \rangle_\psi \Big)^{\frac{1}{2}} \\ &\leq \Big(\mathop{\mathrm{E}}_x \sum_g \langle T^g,\, \big(A^g - (A^g)^2\big) \rangle_\psi \Big)^{\frac{1}{2}} \\ &\leq \sqrt{\delta}\,, \end{aligned} \tag{4.7}$$

where the second inequality uses $A_x^{g(x)} (A^g)^2 A_x^{g(x)} \leq \mathrm{Id}$ for the first term, and expands the square and uses $(A_x^{g(x)})^2 \leq A_x^{g(x)}$ for the second term, and the last inequality follows from item 3. in the definition of globally consistent. Combined with (4.5) and (4.6), we have shown

$$\mathop{\mathrm{E}}_x \sum_g \sum_{a \neq g(x)} \langle S^g,\, A_x^a \rangle_\Psi \approx_{\sqrt{\delta}} \sum_g \langle T^g,\, (A^g - (A^g)^3) \rangle_\Psi\,. \tag{4.8}$$

Writing

$$\begin{aligned} A^g - (A^g)^3 &= A^g - (A^g)^2 + \sqrt{A^g} \big(A^g - (A^g)^2\big) \sqrt{A^g} \\ &\leq 2\big(A^g - (A^g)^2\big)\,, \end{aligned}$$

since all terms commute and $(A^g)^2 \leq A^g \leq \mathrm{Id}$, using item 3. in the definition of globally consistent the right-hand side of (4.8) is at most 2δ.
(ii) *Completeness:*

$$\begin{aligned} \sum_g \langle S^g,\, \mathrm{Id} \rangle_\psi &= \mathop{\mathrm{E}}_x \sum_g \langle A_x^{g(x)} T^g A_x^{g(x)},\, \mathrm{Id} \rangle_\psi \\ &\approx_{\sqrt{\varepsilon}} \mathop{\mathrm{E}}_x \sum_g \langle T^g, A_x^{g(x)} \rangle_\psi \\ &\approx_{\sqrt{\varepsilon}} \sum_g \langle T^g A^g,\, \mathrm{Id} \rangle_\psi \\ &= \sum_g \langle T^g Z,\, \mathrm{Id} \rangle_\psi \\ &= \langle Z,\, \mathrm{Id} \rangle_\psi\,, \end{aligned}$$

where the third line uses Lemma 4.2.9 and the penultimate equality follows from (4.4), and for the last we used $\sum_g T^g = \mathrm{Id}$. We establish a lower bound on this last expression by introducing $\{Q^g\}$:

$$\langle Q,\, \mathrm{Id} \rangle_\psi - \eta \leq \sum_g \langle Q^g,\, A^g \rangle_\psi$$

$$\leq \sum_g \langle Q^g,\, Z\rangle_\psi$$
$$\leq \langle \mathrm{Id},\, Z\rangle_\psi\ ,$$

where the second inequality uses the dual constraint (4.3), and the third uses $\sum_g Q^g \leq \mathrm{Id}$. It follows that

$$\sum_g \langle S^g,\, \mathrm{Id}\rangle_\psi \geq \langle Q,\, \mathrm{Id}\rangle_\psi - \eta - O\big(\sqrt{\varepsilon}\big).$$

(iii) Projectivity: By proceeding exactly as in (4.7), we can show

$$\begin{aligned}
\langle S,\, S\rangle_\psi &= \sum_g \mathop{\mathrm{E}}_x \langle A_x^{g(x)} T^g A_x^{g(x)},\, S\rangle_\psi \\
&\approx_{\sqrt{\varepsilon}+\sqrt{\delta}} \sum_g \mathop{\mathrm{E}}_x \langle A^g T^g A^g,\, S\rangle_\psi \\
&= \sum_{g,g'} \mathop{\mathrm{E}}_x \langle A^g T^g A^g,\, A_x^{g'(x)} T^{g'} A_x^{g'(x)}\rangle_\psi \\
&\approx_{\sqrt{\varepsilon}+\sqrt{\delta}} \sum_{g,g'} \mathop{\mathrm{E}}_x \langle A_x^{g(x)} T^g A_x^{g(x)},\, A_x^{g'(x)} T^{g'} A_x^{g'(x)}\rangle_\psi\ .
\end{aligned}$$

Using self-consistency of $\{A_x^a\}$, from the above we get

$$\begin{aligned}
\langle S,\, S\rangle_\psi &\approx_{\sqrt{\varepsilon}+\sqrt{\delta}} \sum_{g,g'} \mathop{\mathrm{E}}_x \langle T^g A_x^{g(x)},\, A_x^{g'(x)} T^{g'} A_x^{g'(x)}\rangle_\psi \\
&\approx_{\sqrt{\varepsilon}+\sqrt{\delta}} \sum_{g,g'} \langle T^g A^g,\, S^{g'}\rangle_\psi \\
&= \mathrm{Tr}_\Psi \langle Z,\, S\rangle_\psi\ ,
\end{aligned} \tag{4.9}$$

where the second line again uses similar arguments as (4.7) and the last line uses (4.4) and $\sum_g T^g = \mathrm{Id}$. Using the dual constraint (4.3), we deduce

$$\begin{aligned}
\langle S,\, S\rangle_\psi &\geq \sum_g \langle A^g,\, S^g\rangle_\psi - O(\sqrt{\varepsilon}+\sqrt{\delta}) \\
&\approx_{\sqrt{\varepsilon}+\sqrt{\delta}} \langle S, \mathrm{Id}\rangle_\psi\ ,
\end{aligned}$$

where the second line follows from consistency of $\{S^g\}$ and $\{A_x^a\}$ shown in item (i). □

Based on Lemma 4.3.2, we give the proof of Proposition 4.3.1.

Proof of Proposition 4.3.1. Let ε, δ be as in condition 1., and $\{Q^g\}$ be the measurement whose existence follows from condition 2. in the proposition, when $|\Phi\rangle = |\Psi\rangle$ and $\varepsilon', \delta' = \varepsilon, \delta$. By applying Lemma 4.2.8 to the state $|\Psi\rangle$ and measurements $\{A_x^a\}$ and $\{Q^g\}$ we obtain a sub-measurement $\{S^g\}$ that is $\eta = r(\varepsilon, \delta)$-projective and consistent with $\{A_x^a\}$. Among all sub-measurements that are η-projective and consistent

with $\{A_x^a\}$, let $\{T^g\}$ be one that minimizes the completeness error $\theta = \langle \mathrm{Id} - T, \mathrm{Id} \rangle$. Provided ε_0, δ_0 are small enough we may assume $\theta = t(\varepsilon, \delta) + r(\varepsilon, \delta) \leq 1/4$. To complete the proof we need to prove a better upper bound on θ. Towards this, introduce a state

$$|\Phi\rangle = \frac{|\tilde{\Phi}\rangle}{\||\tilde{\Phi}\rangle\|}, \qquad \text{where} \qquad |\tilde{\Phi}\rangle = (\mathrm{Id} - T) \otimes (\mathrm{Id} - T)|\Psi\rangle \ .$$

Then

$$\begin{aligned}
\big\||\tilde{\Phi}\rangle\big\|^2 &= \langle (\mathrm{Id} - T)^2, (\mathrm{Id} - T)^2 \rangle_\psi \\
&= \langle \mathrm{Id} - 2T + T^2, \mathrm{Id} - 2T + T^2 \rangle_\psi \\
&= 1 - 4\langle T, \mathrm{Id} \rangle_\psi + 4\langle T, T \rangle_\psi + 2\langle T^2, \mathrm{Id} \rangle_\psi - 4\langle T^2, T \rangle_\psi + \langle T^2, T^2 \rangle_\psi \\
&= 1 - 4\langle T, (\mathrm{Id} - T) \rangle_\psi + 2\langle T^2, (\mathrm{Id} - T) \rangle_\psi - \langle T^2, T(\mathrm{Id} - T) \rangle_\psi - \langle T^2, T \rangle_\psi \\
&\approx_{\sqrt{\eta}} 1 - \langle T, T^2 \rangle_\psi \\
&\approx_{\sqrt{\eta}} 1 - \langle T, \mathrm{Id} \rangle_\psi \ , \qquad (4.10)
\end{aligned}$$

where the last two approximation use the projectivity assumption on T.

Claim 4.3.3. *There are $\varepsilon' = O(\varepsilon + \sqrt{\eta})$ and $\delta' = O(\delta + \sqrt{\eta})$ such that $(\{A_x^a\}, \mathcal{G})$ is (ε', δ')-globally consistent on $|\Phi\rangle$.*

Proof. We verify the properties in Definition 4.2.7. Item 1. is automatic. For item 2., self-consistency of $\{A_x^a\}$ on $|\Phi\rangle$, write

$$\begin{aligned}
\mathop{\mathrm{E}}_x \sum_a \langle A_x^a, A_x^a \rangle_{\tilde{\Phi}} &= \mathop{\mathrm{E}}_x \sum_a \langle A_x^a(\mathrm{Id} - T) - T A_x^a(\mathrm{Id} - T), (\mathrm{Id} - T)A_x^a - (\mathrm{Id} - T)A_x^a T \rangle_\psi \\
&\approx_{\sqrt{\eta}} \mathop{\mathrm{E}}_x \sum_a \langle A_x^a, A_x^a \rangle_\psi - \langle T, A_x^a \rangle_\psi + \langle A_x^a(\mathrm{Id} - T), T \rangle_\psi \\
&\approx_{\sqrt{\eta}} 1 - \varepsilon - \langle T, \mathrm{Id} \rangle_\psi \ .
\end{aligned}$$

Together with (4.10), it follows that $\{A_x^a\}$ is ε'-self-consistent on $|\Phi\rangle$, for some $\varepsilon' = O(\varepsilon + \sqrt{\eta})$. For item 3. in the definition, let Z be such that $A^g - (A^g)^2 \leq Z$ for all $g \in \mathcal{G}$, and $\langle Z, \mathrm{Id} \rangle_\psi \leq \delta$. Then

$$\begin{aligned}
\langle Z, \mathrm{Id} \rangle_{\tilde{\Phi}} &\approx_{\sqrt{\eta}} \langle Z, (\mathrm{Id} - T) \rangle_\Psi \\
&\leq \delta \ ,
\end{aligned}$$

and the property follows using (4.10). □

Applying condition 2. in the proposition to $|\Phi\rangle$ and $(\{A_x^a\}, \mathcal{G})$ we obtain a measurement $\{Q^g\}$ that is $\eta' = t(\varepsilon', \delta')$-projective and consistent with $\{A_x^a\}$ on $|\Phi\rangle$. Define a sub-measurement $\{R^g\}$ by

$$R^g := T T^g T + (1 - T) Q^g (1 - T) \ .$$

The completeness of this measurement on $|\Psi\rangle$ is

$$\begin{aligned}\langle R,\,\mathrm{Id}\rangle_\Psi &= \langle T^3,\,\mathrm{Id}\rangle_\psi + \langle (1-T)^2,\,\mathrm{Id}\rangle_\psi \\ &\approx_{\sqrt{\eta}} 1\,, \end{aligned} \tag{4.11}$$

since

$$\langle T^3,\,\mathrm{Id}\rangle_\psi \approx_{\sqrt{\eta}} \langle T^2,\,\mathrm{Id}\rangle_\psi \approx_{\sqrt{\eta}} \langle T,\,\mathrm{Id}\rangle_\psi\,.$$

To evaluate consistency with $\{A_x^a\}$,

$$\begin{aligned}\mathop{\mathrm{E}}_x \sum_g \sum_{a\neq g(x)} \langle R^g, A_x^a\rangle_\Psi &= \mathop{\mathrm{E}}_x \sum_g \sum_{a\neq g(x)} \big(\langle TT^gT,\, A_x^a\rangle_\psi + \langle (1-T)Q^g(1-T),\, A_x^a\rangle_\psi\big) \\ &\approx_{\sqrt{\varepsilon}+\sqrt{\eta}+\kappa} \mathop{\mathrm{E}}_x \sum_g \sum_{a\neq g(x)} \big(\langle TT^g,\, TA_x^a\rangle_\psi + \langle (1-T)Q^g,\, (1-T)A_x^a\rangle_\psi\big) \\ &= O(\sqrt{\eta}) + O(\sqrt{\eta'})\big\||\tilde\Phi\rangle\big\|^2\,,\end{aligned}$$

where the second line uses the second item in Lemma 4.2.4 and the last $\varepsilon = O(\eta)$, given the definition of the function r. Using (4.11), if we complete $\{R^g\}$ into a measurement $\{\tilde R^g\}$ by adding an arbitrary term, the latter will have consistency $\delta'' = O(\sqrt{\eta}) + O(\sqrt{\eta'})\||\tilde\Phi\rangle\|^2$ with $\{A_x^a\}$. Applying Lemma 4.2.8 yields a sub-measurement $\{V^g\}$ that is $\eta = r(\varepsilon,\delta)$-projective and consistent with $\{A_x^a\}$, and for which

$$\langle (\mathrm{Id} - V),\,\mathrm{Id}\rangle_\psi \;=\; O(\sqrt{\eta}) + O(\sqrt{\eta'})\||\tilde\Phi\rangle\|^2.$$

Recall that by assumption, $\{T^g\}$ is the most complete measurement that is η-projective and consistent with A_x. Hence, $\langle (\mathrm{Id} - V), \mathrm{Id}\rangle \geq \langle (\mathrm{Id} - T), \mathrm{Id}\rangle$, so that

$$\theta \;\leq\; O(\sqrt{\eta}) + O(\sqrt{\eta'})(\theta + O(\sqrt{\eta})).$$

Provided ε, δ are small enough that $O(\sqrt{\eta'}) = O(\sqrt{t(\varepsilon',\delta')})$, with ε', δ' as in Claim 4.3.3, is at most $1/4$, as can be assumed from the assumed upper bound $t(\varepsilon',\delta') \leq t_0$ for $\varepsilon' \leq \varepsilon_0$ and $\delta' \leq \delta_0$ provided t_0 is a small enough universal constant, we have obtained $\theta = O(\sqrt{\eta}) = O(\sqrt{r(\varepsilon,\delta)})$, as claimed. □

4.4 NP-hardness for two-player entangled games

Based on the result of the analysis of the low-degree test stated in Theorem 4.1.2 and following the same sequence of reductions — composition of the low-degree test with itself, to reduce answer size, and combination with the 3-SAT test — as in [Vid13] we obtain the following analogue of [Vid13, Theorem 4.1], which establishes NP-hardness for games with poly(log log n)-bit answers.

Theorem 4.4.1. *There is an $\varepsilon > 0$ such that the following holds. Given a 2-player game G in explicit form, it is NP-hard to distinguish between $\omega(G) = 1$ and $\omega^*(G) \leq 1 - \varepsilon$. Furthermore, the problem is still NP-hard when restricting to games G of size*

n that are projection games for which questions and answers can be specified using $O(\log n)$ bits and $\mathrm{poly}(\log \log n)$ bits respectively.

In [Vid13] this result is improved to obtain hardness for games with constant-bit answers by reducing the 3-SAT test, on which the proof of Theorem 4.4.1 is based, to the three-player QUADEQ test for testing satisfiability of a system of quadratic equations in binary variables. This amounts to composing a PCP based on low-degree polynomials with the "exponential PCP" based on the three-query linearity test of [BLR93], and yields hardness for three-player games with binary answers. The same steps can be completed with two players only by using the technique of oracularization to transform the QUADEQ and linearity tests into two-player games. The idea of oracularization is that for every triple of questions (q_1, q_2, q_3) to be sent to the three players in the original test, the verifier sends the entire triple to a single player, Alice, and receives a triple of answers. The verifier also sends a randomly selected question from the triple to a second player, Bob. The verifier accepts if and only if Bob's answer is consistent with Alice's, and the triple of answers provided by Alice would have been accepted in the original test. For concreteness, we summarize the oracularized QUADEQ test in Figure 4-2. (Note that the third element in each of Alice's question and answer triples is redundant and can be eliminated.)

It is easy to see that honest strategies pass the oracularized QUADEQ test with probability 1. To establish soundness of the test, i.e to show an analogue of Lemma 3.5 of [Vid13], we can follow essentially the same steps as in the proof of that lemma. The key step of the proof is to argue that, due to the soundness of the linearity test against entangled provers, there exist measurements on each prover's space whose outcomes are linear functions that are consistent with the measurements applied in the test. For the oracularized test, we can perform this step using the soundness of the oracularized linearity test against entangled provers, which was analyzed in [NV17a]. The rest of the proof proceeds unchanged. As a result we obtain the following corollary, which establishes Theorem 4.1.1; it is completely analogous to [Vid13, Corollary 4.3], except that due to the oracularization, the two provers now have to provide answers of two bits each instead of one.

Corollary 4.4.2. *There is an $\varepsilon > 0$ such that the following holds. Given a two-player projection game G in explicit form in which answers from one player is restricted to 2 bits, and answers from the other player to a single bit, it is NP-hard to distinguish between $\omega(G) = 1$ and $\omega^*(G) \leq 1 - \varepsilon$.*

Using that the games G for which NP-hardness is shown in Corollary 4.4.2 are projection games, we may apply results on the parallel repetition of two-player entangled projection games [DSV15] to amplify the completeness and soundness parameters from 1 and $1 - \varepsilon$ to 1 and δ respectively, for any $\delta > 0$, by repeating the game $\mathrm{poly}(\varepsilon^{-1} \log \delta^{-1})$ times and incurring a corresponding multiplicative factor blow-up in the length of questions and answers in the game.

Out of the two provers, chose one at random to be Alice and the other to be Bob.

1. With probability 1/4 each, do the following:
   (a) Send label ℓ_1 to the two players and perform the $(n/2)$-bit (oracularized) linearity test.
   (b) Same with label ℓ_2.
   (c) Send labels (ℓ_1, ℓ_2) to the two players and perform the n-bit linearity test.
   (d) Same but perform the n^2-bit linearity test.
2. Select random $u, v \in \mathbb{F}_2^{n/2}$ and $i \in [3]$, and generate the three queries $q_1 = (\ell_1, u)$, $q_2 = (\ell_2, v)$, $q_3 = (\ell_1, \ell_2, (u, v))$. Send q_1, q_2 to Alice, receiving answers a_1, a_2, and let $a_3 = a_1 + a_2$. Send q_i to Bob, receiving answer b. Accept if $b = a_i$.
3. Select random $u, v \in \mathbb{F}_2^n$ and $i \in [3]$, and generate the three queries $q_1 = (\ell_1, \ell_2, u)$, $q_2 = (\ell_1, \ell_2, v)$, $q_3 = (\ell_1, \ell_2, u \otimes v)$. Send q_1, q_2 to Alice, receiving answers a_1, a_2 and let $a_3 = a_1 \cdot a_2$. Send q_i to Bob, receiving answer b. Accept if $b = a_i$.
4. Select a random vector $v \in \mathbb{F}_2^K$ and let $w = \sum_k w_k a^{(k)} \in \mathbb{F}_2^{n^2}$. Send (ℓ_1, ℓ_2, w) to a randomly chosen player and check that the answer $a = \sum_k w_k c^{(k)}$.

Figure 4-2: The two-prover QUADEQ test. See Section [Vid13, Section 3.4] for additional explanations regarding the notation.

4.5 Modified proofs from [Vid13]

As noted in the introduction, the principal modifications to the soundness analysis of the low-degree test in [Vid13] necessary to make it hold for two provers concern the self-improvement results of section 5. There are a few other steps of the proof of the main theorem in [Vid13] that seem to require a tripartite tensor product factorization of the Hilbert space to be carried out. In all cases this is easily avoided by simple modification of the proof. Although they remain very elementary, in this appendix we describe the only two other non-trivial modifications needed. The first is in the proof of [Vid13, Claim 6.10]. (We refer to the paper [Vid13] for context, including an explanation of the notation; the following discussion is meant for a reader already familiar with the proofs in [Vid13].)

Claim 4.5.1 (Claim 6.10 in [Vid13]). *The measurements* $\{Q_s^g\}_{g\in\mathcal{P}_d(s)}$ *satisfy*

$$\mathop{\mathrm{E}}_{s\in\mathcal{S}_{m-1}(\mathbb{F}_q^m)} \sum_{g\in\mathcal{P}_d(s)} \langle Q_s^g, (\mathrm{Id} - Q_s^g)\rangle_\Psi = O(\varepsilon^{c\ell}) \ .$$

Proof. The proof is the same as in [Vid13], except the third tensor factor is not needed — the second can be used for the same purpose:

$$\begin{aligned}
&\mathop{\mathrm{E}}_{s\in\mathcal{S}_{m-1}(\mathbb{F}_q^m)} \sum_{g,g'\in\mathcal{P}_d(s),g\neq g'} \langle Q_s^g, Q_s^{g'}\rangle_\Psi \\
&\quad\approx \mathop{\mathrm{E}}_{s\in\mathcal{S}_{m-1}(\mathbb{F}_q^m)} \mathop{\mathrm{E}}_{x\in S} \sum_{g,g'\in\mathcal{P}_d(s),g\neq g'} \langle Q_s^g, Q_s^{g'} A_x^{g(x)}\rangle_\psi + O(\varepsilon^{c\ell}) \\
&\quad\approx_{\varepsilon^{c\ell}} \mathop{\mathrm{E}}_{s\in\mathcal{S}_{m-1}(\mathbb{F}_q^m)} \mathop{\mathrm{E}}_{x\in S} \sum_{g,g'\in\mathcal{P}_d(s),g\neq g'} \langle Q_s^g A_x^{g(x)}, Q_s^{g'}\rangle_\psi + O(\varepsilon^{c\ell}) + O(\varepsilon) \\
&\quad\approx O(\varepsilon^{c\ell}) + O(\varepsilon) \ .
\end{aligned}$$

In the first line, we used the consistency between Q_s^g on the first prover and $A_x^{g(x)}$ on the second; in the second line, we used the self-consistency of A; and in the third, we used the consistency between $Q_s^{g'}$ on the second prover and $A_x^{g(x)}$ on the first prover. □

The second is in the proof of [Vid13, Claim 6.14]. Here again, the use of a third tensor factor can be avoided by a simple modification. Specifically, the last set of centered equations on p.1056 (right below (6.22)) should be replaced with

$$\begin{aligned}
\mathop{\mathrm{E}}_{(s_i)} \sum_{g,\deg(g)>d} \langle R_{(s_i)}^g, \mathrm{Id}\rangle_\Psi &\approx_{\varepsilon^{c\ell}} \mathop{\mathrm{E}}_{(s_i),z,\ell,\ell'\ni z} \sum_{g,\deg(g)>d} \sum_{\substack{h(\ell\cap s_i)=g(\ell\cap s_i)\\ h'(\ell'\cap s_i)=g(\ell'\cap s_i)}} \langle R_{(s_i)}^g, B_\ell^h B_{\ell'}^{h'}\rangle_\psi \\
&\approx_{\varepsilon^{c\ell}} \mathop{\mathrm{E}}_{(s_i),z,\ell,\ell'\ni z} \sum_{g,\deg(g)>d} \sum_{\substack{h(\ell\cap s_i)=g(\ell\cap s_i)\\ h'(\ell'\cap s_i)=g(\ell'\cap s_i)}} \langle R_{(s_i)}^g B_{\ell'}^{h'}, B_\ell^h\rangle_\psi
\end{aligned}$$

$$= O(\varepsilon^{d_c/2})$$

Chapter 5

Low-degree testing for quantum states

In this and the following chapter, we show that given an explicit description of a multiplayer game, with a classical verifier and a constant number of players, it is QMA-hard, under randomized reductions, to distinguish between the cases when the players have a strategy using entanglement that succeeds with probability 1 in the game, or when no such strategy succeeds with probability larger than $\frac{1}{2}$. This proves the "games quantum PCP conjecture" of Fitzsimons and the second author (ITCS'15), albeit under randomized reductions.

The core component in our reduction, described in this chapter, is a construction of a family of two-player games for testing n-qubit maximally entangled states. For any integer $n \geq 2$, we give such a game in which questions from the verifier are $O(\log n)$ bits long, and answers are $\text{poly}(\log \log n)$ bits long. We show that for any constant $\varepsilon \geq 0$, any strategy that succeeds with probability at least $1 - \varepsilon$ in the test must use a state that is within distance $\delta(\varepsilon) = O(\varepsilon^c)$ from a state that is locally equivalent to a maximally entangled state on n qubits, for some universal constant $c > 0$. The construction is based on the classical plane-vs-point test for multivariate low-degree polynomials of Raz and Safra (STOC'97). We extend the classical test to the quantum regime by executing independent copies of the test in the generalized Pauli X and Z bases over $\mathbb{F}_q$, where q is a sufficiently large prime power, and combine the two through a test for the Pauli twisted commutation relations. Our analysis makes essential us of the soundness of the Raz-Safra test against two entangled provers, shown in Chapter 4.

In the following chapter, our main complexity-theoretic result is obtained by combining this family of games with techniques from the classical PCP literature. More specifically, we use constructions of PCPs of proximity introduced by Ben-Sasson et al. (CCC'05), and crucially rely on a linear property of such PCPs. Another consequence of our results is a deterministic reduction from the games quantum PCP conjecture to a suitable formulation of the constraint satisfaction quantum PCP conjecture.

5.1 Introduction

The PCP theorem [ALM+98, AS98] makes a remarkable statement: any language that admits efficiently verifiable proofs of membership, i.e. any problem in NP, also admits proofs that can be verified by reading only a *constant* number of bits of the proof. Do similar encodings exist for problems that admit *quantum* proofs? Consider the local Hamiltonian problem. Is there a way to encode a witness for the minimal energy of a Hamiltonian in a way that the energy can be estimated to within inverse polynomial accuracy while accessing only a constant number of bits, or qubits, from the witness? The pursuit of this question, which, broadly speaking, asks for quantum extensions of the PCP theorem, has been one of the most fruitful and challenging problems animating quantum complexity theory in the past decade: it ties in to the theory of quantum error-correcting codes, has applications to quantum cryptography, and promises insights into the study of entanglement in ground states of local Hamiltonians [AAV13].

The question can be formalized in multiple ways. A first formulation, the "constraint satisfaction" variant of the quantum PCP (QPCP) conjecture [AALV09], asks for the complexity of constant-factor approximations to the minimal energy of a local Hamiltonian H, normalized so that $\|H\| = 1$. Despite considerable attention progress on the conjecture has been difficult [AE15, BH13, EH15].

More recently a second formulation has been put forward. The "multiplayer games" variant of the QPCP conjecture, introduced in [FV15], asks for the complexity of estimating, to within constant accuracy, the maximum success probability of provers (we use the terminology "provers" and "players" interchangeably) sharing entanglement in a multiplayer game, a quantity referred to as the *entangled value* of the game. The conjecture is a natural analogue of the "oracularized" formulation of the PCP theorem, which states that the maximum success probability of *classical* provers in a multiplayer game is NP-hard to approximate to within constant factors. (This can be thought of as a "scaled down" formulation of the equality MIP = NEXP [BFL91].)

In [Vid13], building on [IV12] it was shown that the approximation problem for the entangled value of a multiplayer game remains NP-hard, provided there are at least three provers. This was extended to games with two provers only in [NV17b] (this result appeared in Chapter 4, and will be used as a building block in the present chapter). In [FV15, Ji16a] it was shown that inverse-polynomial approximations are QMA-hard (provided there are at least five provers), a result that is akin to a "quantum Cook-Levin theorem for entangled games." These results motivate the following conjecture, first made in [FV15]:

Conjecture 5.1.1 (Games QPCP conjecture (informal)). *Suppose given as input an explicit description of a classical multiplayer game. Then it is* QMA*-hard to determine whether provers sharing quantum entanglement (of arbitrary dimension) have optimal success probability at least $\frac{2}{3}$ or at most $\frac{1}{3}$ in the game.*

We show that the conjecture holds, under randomized reductions.

Theorem 5.1.2 (Games QPCP under randomized reductions). *Suppose given as input an explicit description of a classical multiplayer game. Then it is* QMA*-hard, under randomized reductions, to determine whether provers sharing quantum entanglement (of arbitrary dimension) have optimal success probability at least* 1 *or at most* $\frac{1}{2}$ *in the game.*

Theorem 5.1.2 is stated and proved as Corollary 6.2.14 in Chapter 6. The choice of constant $\frac{1}{2}$ in Theorem 5.1.2 is arbitrary, as for the kind of games we consider soundness amplification can be performed efficiently in parallel [BVY17].

We explain the need for a randomized reduction. Informally, the reason is that we do not know of a strong enough QMA-hardness result for the local Hamiltonian problem to initiate our reduction. In fact, we give two alternate formulations of Theorem 5.1.2 that would also establish the same QMA-hardness result, under deterministic reductions, provided that either:

(i) it is QMA-hard to approximate the minimum energy of a local Hamiltonian in Y-free form (Definition 6.2.8) to within constant accuracy (this is a variant of the quantum PCP conjecture for local Hamiltonians), or

(ii) it is QMA hard to approximate the ground energy of (not necessarily local) frustration-free Hamiltonian whose every term is a tensor product of generalized Pauli τ_X or τ_Z observables.

Note that point (i) amounts to a deterministic reduction from Conjecture 5.1.2 to the constraint satisfaction quantum PCP conjecture, and establishes the first proven relation between the two conjectures (see [GKP16] for an incomparable result that relates stronger variants of both conjectures). Point (ii) is arguably a weaker assumption, as the gap is not required to be a constant and the terms of the Hamiltonian are not required to be local. However, due to the restriction that the Hamiltonian is frustration-free, it is currently not known whether the problem is QMA-hard (or even QMA_1-hard — though the frustration-free assumption can be relaxed to having exponentially small ground state energy).

Our results build on two main tools: a framework for protocols to test ground states, introduced in [FV15] and further developed in [Ji16a, NV17a], and a new proof of soundness of the classical low-degree test of Raz and Safra against two entangled provers [NV17b]. The main result that underlies the complexity-theoretic applications is a two-prover test for n-qudit maximally entangled states, where each qudit has dimension $q = p^t = \mathrm{poly}\log(n)$ for a prime p and integer t, that has inverse robustness independent of n (for all ε that are at least inverse polylogarithmic in n) and in which the verifier sends only $O(\log(n))$ bits to the provers, who reply with $O(\log\log n)$ bits each (Theorem 5.3.2). This is an exponential improvement over all previous results, and provides the first robust entanglement test with sub-linear communication. While the ability to "test" structured objects with sub-linear efficiency has become customary in classical computer science, we find it remarkable that the framework for such tests may be extended to test such a complex object as quantum entanglement.

We first describe this test in more detail, before expanding on the complexity-theoretic consequences.

Efficient, robust entanglement tests. The driving question behind our work is the following: "Is it possible to verify a quantum state using an amount of resources that scales sub-linearly in the number of qubits of the state?" We start with the "simplest" such state—the maximally entangled state. Results in self-testing have yielded increasingly efficient and robust tests for this state and other, more general families of highly entangled states. Here we loosely refer to the "efficiency" of a test as a measure of the total number of bits of communication involved in an execution of the test. The "robustness" of the test indicates how tightly success in the test characterizes the desired state: a test is $\delta(\varepsilon)$-robust if for all $\varepsilon \geq 0$, any strategy for the provers that succeeds with probability at least $1 - \varepsilon$ in the test must use an entangled state that is within distance $\delta(\varepsilon)$ from the tested state (see Definition 5.2.5). Using these measures, the best prior self-tests for a maximally entangled state of n qubits are a test with communication $O(\log n)$ and robustness $O(n^{5/2}\sqrt{\varepsilon})$ [CRSV17] and a test with communication $O(n)$ and robustness $O(\sqrt{\varepsilon})$ [NV17a]. Other recent results in this direction include [OV16, CN16, Col16, CS17].

Our test is the first to combine robustness $\delta(\varepsilon) = \text{poly}(\varepsilon)$ that is independent of n, and logarithmic communication. Achieving both simultaneously is crucial to applications: constant (in n) robustness allows us to achieve gap-preserving reductions; logarithmic communication allows us to achieve efficient reductions.

As in previous results, the test is designed to constrain successful provers to use observables satisfying suitable relations; a statement about the entangled state follows by using that the state is stabilized by (a subset of) these observables. In the case of the maximally entangled state, the observables are all n-fold tensor products of Pauli observables. For reasons to be discussed below we test for qudits of dimension $q = p^t$ a prime power of order $q = \text{poly}\log(n)$. This leads us to consider tensor products of single-qudit Pauli observables defined over the prime power field $\mathbb{F}_q$, which we denote using the symbol τ:

$$\tau_X(a) = \sum_{j \in \mathbb{F}_q} |j + a\rangle\langle j| \qquad \text{and} \qquad \tau_Z(b) = \sum_{j \in \mathbb{F}_q} \omega^{\text{tr}(bj)} |j\rangle\langle j| \,, \tag{5.1}$$

where $a, b \in \mathbb{F}_q$, $\omega = e^{\frac{2i\pi}{p}}$, addition and multiplication are over $\mathbb{F}_q$, and $\text{tr}(\cdot)$ denotes the trace of $\mathbb{F}_q$ over $\mathbb{F}_p$. The main difficulty we face is that there are $2 \cdot q^n$ such observables, $\tau_X(a) = \tau_X(a_1) \otimes \cdots \otimes \tau_X(a_n)$ and $\tau_Z(b) = \tau_Z(b_1) \otimes \cdots \otimes \tau_Z(b_n)$ for $a, b \in \mathbb{F}_q^n$, an exponentially larger number than any test with polylogarithmic communication gives us direct access to. It is then natural to consider a test that certifies observables $\tau_X(a)$ and $\tau_Z(b)$ for $a, b \in T \subseteq \mathbb{F}_q^n$, where $|T| = \text{poly}(n)$, and attempt to construct observables for all $a, b \in \mathbb{F}_q^n$ in an inductive fashion, as is done in e.g. [CRSV17], where T is the set of all strings of Hamming weight at most 2. Unfortunately, any naïve procedure will induce an error accumulation at each step of the induction, eventually resulting in a robustness parameter that depends polynomially on n (as is the case in [CRSV17]).

It is thus crucial to choose the set T carefully — informally, it seems natural to require that this set behave in a "pseudorandom" way. We take direct inspiration from the classical proof of the PCP theorem, and use a set T specified as the set of

all codewords of a suitably chosen Reed-Muller code; this is the reason for using a sufficiently large qudit dimension q. Our proof eventually reduces the analysis to the soundness of the entangled-prover classical low-degree test [NV17b]. We explain the test, and its analysis, in more detail in Section 5.1.1 below.

Testing ground states and a "gap preserving" reduction. We sketch how our test for entanglement is applied to obtain results on the complexity of multiplayer entangled games. In the classical case, the proof that the value of a multiplayer game is at least as hard to approximate as the maximum fraction of constraints simultaneously satisfiable in a local constraint satisfaction problem proceeds via the technique of oracularization: the verifier selects a constraint at random and asks one prover for an assignment to all variables in the constraint and the other for an assignment to a single one of the variables. Given the provers' answers, the verifier checks the natural satisfaction and consistency constraints. In the quantum case the analogous idea would require each prover to hold a copy of the ground state of a QMA-complete local Hamiltonian, and return qubits as requested by the verifier. This reduction does not work: it is not possible in general to check for "consistency" between the same qubit taken from two copies of an entangled state. In [FV15] the idea was introduced of encoding the ground state using an error-correcting code and distributing a share to each prover. Subsequent work [Ji16a] showed that this idea can be used to show QMA-hardness of inverse-polynomial approximations to the entangled value of a multiplayer game. Unfortunately the reduction in [Ji16a] is not "gap-preserving": a large promised energy gap in the starting instance of the local Hamiltonian problem does not lead to a large completeness-soundness gap in the resulting game. As a result, even assuming the "constraint satisfaction" QPCP does not lead to hardness for approximation factors larger than a fixed inverse polynomial. In [NV17a] we leveraged an entanglement test with constant robustness to achieve a gap-preserving reduction; unfortunately communication in the test is linear, resulting in a game with exponential size, so that no new complexity-theoretic consequence is obtained.

Armed with an exponentially more efficient entanglement test we are able to provide a much more effective reduction, yielding games of polynomial size from instances of the local Hamiltonian problem. The reduction follows similar lines as previous work, but with a new difficulty. Our entanglement test only certifies a specific family of observables: tensor products of generalized Pauli observables (5.1) over $\mathbb{F}_q$, for q a sufficiently large prime power. This requires us to initiate any direct reduction with a specific class of Hamiltonians, in so-called Y-free form (see Definition 6.2.8); informally, these are local Hamiltonians such that each local term is a tensor product of generalized τ_X and τ_Z observables. In the absence of general gap-preserving reductions between different variants of the local Hamiltonian problem (perturbation techniques [CM14] do not generally preserve the promise gap) we obtain a reduction to the hardness of constant-factor approximations to the ground energy of local Hamiltonian of this form only. Nevertheless, even though the entanglement test requires a qudit dimension that scales (poly-logarithmically) with n, we show that

any qubit Hamiltonian in Y-free form can be embedded in a Hamiltonian in Y-free form over qudits of dimension 2^t for any $t \geq 1$. As a result, we immediately obtain point (i) discussed earlier: that Conjecture 5.1.2 would follow from QMA-hardness of constant-factor approximations to local Hamiltonian whose every local term is a tensor product of τ_X and τ_Z Pauli observables (signed weights of up to poly-logarithmic size are allowed).

Composition and PCP. To obtain strong results we develop more elaborate reductions, with the aim of removing the assumption on *locality* of the Hamiltonian whose ground state energy is being tested. As our entanglement test has direct access only to local Pauli observables, it cannot be used to evaluate the expectation value of non-local observables (acting on more than a constant number of qudits). We get around this as follows. Say the verifier would like to estimate the expectation value of a nonlocal tensor product observable such as $\tau_X(b)$, for some $b \in \mathbb{F}_q^n$. The verifier asks each prover to measure all its qudits in the X basis, obtaining an outcome $a \in \mathbb{F}_q^n$, and report the value of the inner product $c = b \cdot a$. This provides the verifier with an estimate of the energy of $\tau_X(b)$. However, it remains to ensure that the outcome reported by the prover was obtained honestly, i.e. by measuring all qudits on which the observable acts, without having the ability to "read" all the single-qubit outcomes obtained. This sounds very similar to the kind of NP statements that PCPs are designed to allow efficient verification of, and indeed we employ classical PCP techniques, more specifically the notion of *PCP of proximity* (PCPP).

In order to verify that a prover honestly computed the inner product $c = b \cdot a$, the verifier asks it to provide PCPP of this fact. A PCPP for a language is a proof that a given input is in the language, which can be verified by making only a few queries to both the proof and the input. In our setting, the verifier asks each prover to compute a PCPP Π for the claim that the measurement outcome string a is in the language $L = \{x : b \cdot x = c\}$. This proof can be verified by making constantly-many queries to Π, together with constantly many queries to a. Both of these correspond to *local* measurements, either of the shared quantum state, or the proof string Π generated from the measurement outcomes, and can thus be certified using our entanglement test.

There are two subtleties that arise. First, a PCPP (viewed as a nonlocal game) that is classically sound need not be sound against entangled provers. To address this, we perform a further layer of composition, encoding the PCPP proof Π in a low-degree polynomial and querying this polynomial. Secondly, in our setting *completeness* does not automatically hold either. This is because each prover j only has access to one share of the shared state, which is a qudit-by-qudit encoding of the actual QMA witness. The prover can thus only supply bits from a proof Π_j computed from its share. As a result the usual method of transforming a PCP into a game, namely by querying multiple provers for locations in the proof and checking consistency between them, fails since even honest provers do not know each other's measurement outcomes and thus cannot answer consistently. To surmount this obstacle, we exploit the linearity of the error correcting code, together with a linear

PCPP construction from [BSGH+05], for which the proof Π is a linear function of the input a; the linearity holds as long as the language L is itself specified by a set of linear equations, i.e. $L = \{x : Ax = b\}$. The linearity of the PCPP allows the verifier to check consistency between one prover's answers and the appropriate linear combination of answers returned by the other provers.[1].

With this PCPP-based protocol for measuring nonlocal Pauli observables in place, the proof of Theorem 5.1.2 follows: starting with a QMA-hard instance of the local Hamiltonian problem with inverse-polynomial promise gap, we amplify the gap by taking a large tensor product, and then randomly sample a polynomial subset of the exponentially many terms in the tensor product. By the matrix Chernoff bound [AW02], with high probability this sampling preserves the promise gap, and the resulting nonlocal Hamiltonian can be tested using our protocol. (This random sampling is the source of the "randomized reductions" in Theorem 5.1.2.)

Finally, our PCPP-based protocol enables us to check not just one nonlocal term but also many terms at once, provided that they are all tensor products of Paulis in the same basis. This allows us to obtain a protocol that accommodates an inverse-polynomial promise gap for the ground energy, provided the Hamilton is frustration free (all of its terms are simultaneously satisfied in the ground state), and each of it terms can be expressed as a tensor product of generalized τ_X or τ_Z observables, acting on an arbitrary number of qudits (see Definition 6.2.16). This shows point (ii) discussed earlier.

5.1.1 Techniques

Our main result, a robust entanglement test with logarithmic communication, can be stated informally as follows. For a formal statement, we refer to Theorem 5.3.2 in Section 5.3.

Theorem. *Let n be an integer and $q = p^t$ a prime power such that $q = \Theta(\frac{\log^2 n}{\log\log n})$. Then there exists a two-prover test* Q-LOWDEG *in which the verifier sends questions of length* $\mathrm{poly}(\log n, \log q)$ *and receives answers of length* $O(\mathrm{poly}\log\log(n)\cdot\log q)$ *such that the following hold:*

1. (Completeness:) *There exists a strategy for the provers based on sharing an n-qudit maximally entangled state, with qudits of local dimension q, and making measurements in the eigenbasis of tensor products of generalized τ_X or τ_Z observables over $\mathbb{F}_q$;*
2. (Soundness:) *For any $\varepsilon \geq 0$, any strategy that is accepted with probability at least $1-\varepsilon$ in the test must use an entangled state that is (up to local isometries) within distance $\delta = \mathrm{poly}(\mathrm{poly}(p)\cdot\mathrm{poly}(\varepsilon))$ from an n-qudit maximally entangled state.*[2]

[1]We note that, just as in [BSGH+05], we require linearity of the PCP in order for it to interface with a linear error correcting code.

[2]Here and throughout we use the notation $f(X) = \mathrm{poly}(h(X)))$ as an abbreviation for "there exists a universal constant $c > 0$ such that $f(X) = O(h(X)^c)$ as $X \to 0$ (if $X = \varepsilon$) or as $X \to \infty$ (if $X = n$); in the theorem p, t and q are all allowed to be implicitly functions of n, but not ε.

A typical setting of parameters for the theorem is to choose p a constant, e.g. $p = 2$, $t = \Theta(\log \log n)$, and ε a small constant, which leads to constant soundness δ.

The test mentioned in the theorem has three components: (a) a low-degree test in the X basis; (b) a low-degree test in the Z basis; (c) an anti-commutation test relating the two bases. Both (a) and (b) are direct adaptations of the "plane-vs-point" low-degree test from [RS97]. The basis label, X or Z, asks the prover to measure its n qudits in the simultaneous eigenbasis of the observables $\tau_X(a)$ or $\tau_Z(b)$ defined in (5.1) respectively. The prover is then asked to encode the resulting outcome $a \in \mathbb{F}_q^n$ as a low-degree polynomial $g_a : \mathbb{F}_q^m \to \mathbb{F}_q$, where $m = O(\log n / \log \log n)$, and return either the evaluation of the polynomial at a randomly chosen point $x \in \mathbb{F}_q^m$, or its restriction to a randomly chosen two-dimensional subspace s of $\mathbb{F}_q^m$. Part (c) is designed to enforce the "twisted commutation" relations $\tau_X(a)\tau_Z(b) = \omega^{-\mathrm{tr}(ab)}\tau_Z(b)\tau_X(a)$ satisfied by these observables. Before explaining the test and its analysis in greater detail, we first review the main steps that go into showing soundness of the classical low-degree test.

Classical low-degree tests. The effectiveness of the classical low-degree test is based on the use of the following Reed-Muller encoding of an n-variable assignment $a = (a_1, \ldots, a_n) \in \{0,1\}^n$. First, integer values h and m are chosen so that $h^m \geq n$, and an injection $\pi : \{1, \ldots, n\} \to \{0, \ldots, h-1\}^m$ is fixed. Second, a finite field $\mathbb{F}_q$ is chosen such that $q \geq h$. Third, a function $g_a : \mathbb{F}_q^m \to \mathbb{F}_q$ is defined such that $g_a(\pi(i)) = a_i$ for all $i \in \{1, \ldots, n\}$, and g_a has degree at most h in each of its m variables; g_a can be obtained by straightforward polynomial interpolation. Finally, the encoding of a is defined as the concatenation of the evaluation table of g_a at every point $x \in \mathbb{F}_q^m$ with a table describing the restriction of g_a to every two-dimensional subspace $s \subseteq \mathbb{F}_q^m$. The encoding has roughly q^{3m} entries, and each entry has size $O(d^2 \log q)$, where $d = mh$ is the total degree of g_a. Choosing $h \approx \log n$ and $m \approx \log n / \log \log n$ yields an encoding of quasi-polynomial size, $n^{O(\log n)}$, as long as q is also polynomial in n.

When used for constructions of PCPs, the low-degree test provides an encoding that can be tested and evaluated while making only a small number of queries. This is achieved based on the following observations. First, the encoding can be checked by making only a constant number of queries: the test selects a pair (x, s) such that s is a uniformly random subspace and x a uniformly random point in s, and checks consistency between the corresponding entries of the encoding. Second, the evaluation of g_a at any point $z \in \mathbb{F}_q^m$ can be recovered by making $O(d)$ queries to the encoding in a way that each query is uniformly distributed: select a uniformly random line going through z, query $d+1$ points at random on the line, and interpolate to recover the value at z.

The analysis of the low-degree test described in the previous paragraph is not simple. The goal is to show that any table which passes the test with probability $1 - \varepsilon$ must be close to the encoding of a polynomial of the form g_a, for some $a \in \mathbb{F}_q^n$. The proof is constructive: it recovers a low-degree polynomial g_a through m successive steps of interpolation. The case $m = 2$ is immediate, since by definition the encoding

contains the restriction of g_a to any two-dimensional subspace. For general m, one selects $(d+1)$ parallel $(m-1)$-dimensional subspaces, applies the induction hypothesis to each, and interpolates to recover a m-variate polynomial defined over the whole space. The key difficulty in the analysis is to control the error: naïvely, it would, at best, double at each step, resulting in an unmanageable blow-up. The key innovation of the test, and its analysis, is a method to limit this blow-up by a procedure of "self-improvement".

Entanglement tests. Before moving on to our quantum low-degree test, it is useful to first recall the intuition behind our prior work [NV17a], which establishes a similar quantum analogue for the Hadamard encoding, which is based on the linearity test of Blum et al. [BLR93].

In the linearity test, the assignment $a \in \{0,1\}^n$ is encoded as the evaluation table of the function $f_a : \mathbb{F}_2^n \to \mathbb{F}_2$, $f_a(x) = x \cdot a$. Each entry of the encoding is a single bit, but there are 2^n entries, thus the table has exponential size. The linearity test makes three queries, x, y and $x+y$ for x, y uniformly distributed in $\mathbb{F}_2^n$, and verifies that $f_a(x) + f_a(y) = f_a(x+y)$. The soundness analysis of the test is based on Fourier analysis; no induction is needed.

To turn the linearity test into a test for entanglement we first re-interpret it using the language of representation theory. The additive structure of $\mathbb{F}_2^n$ makes it into an abelian group, whose irreducible representations are the 2^n characters $\chi_a(x) = (-1)^{a \cdot x}$. An arbitrary table $f : \mathbb{F}_2^n \to \mathbb{F}_2$ can also be seen as a mapping $g = (-1)^f$ from the additive group of $\mathbb{F}_2^n$ to the 1-dimensional unitary group, $U(\mathbb{C})$. A table f which is accepted in the linearity test with probability $1 - \varepsilon$ is an approximate representation of the group, in the sense that $\mathrm{E}_{x,y} |g(x)g(y) - g(x+y)|^2 = O(\varepsilon)$, where the expectation is uniform. Thus the analysis of the linearity test exactly amounts to showing that approximate representations of abelian groups are close to exact representations (i.e. the characters, which precisely correspond to the linear functions).

We can try to apply the same reasoning to entangled-prover strategies. Using matrix-valued Fourier analysis it is possible to show that a quantum strategy which succeeds with probability $1-\varepsilon$ in an X-basis linearity test (resp. an Z-basis linearity test) implies the existence of observables for the provers which satisfy approximate linearity conditions $X(a)X(b) \approx X(a+b)$ (resp. $Z(a)Z(b) \approx Z(a+b)$), where the approximation holds on average over uniform $a, b \in \mathbb{F}_2^n$ and is measured using the state-dependent norm that is standard in testing. These relations by themselves do not imply anything "quantum"; in particular they are satisfied by one-dimensional observables $X(a) = Z(a) = (-1)^{f(a)}$. To obtain a truly quantum test we are missing a constraint relating the two bases: the Pauli (anti)-commutation relation $X(a)Z(b) = (-1)^{a \cdot b} Z(b)X(a)$. Enforcing this relation would allow us to frame the family of unitaries $\{\pm X(a)Z(b),\, a, b \in \mathbb{F}_2^n\}$ as a representation of the Pauli group modulo complex phase (also known as the Weyl-Heisenberg group) and combine results on the stability of approximate representations [GH15] with information on the structure of irreducible representations of that group to conclude. This is what justi-

fies the inclusion of part (c), an anti-commutation test, which can be based on e.g. the Mermin-Peres Magic Square game [Ara02] to test for the desired anti-commutation relations.

A quantum low-degree test. The previous outline of an entanglement test based on the BLR linearity test is implemented in [NV17a]. The use of the linearity test has two main advantages: (i) when executed in a single basis, its analysis with two entangled provers follows a direct argument using Fourier analysis; (ii) combining the linearity test in the X and Z bases naturally gives access to two families of observables $X(a)$ and $Z(b)$ for the provers, that can be used to specify an approximate representation of the n-qubit Weyl-Heisenberg group as described above, with the (anti)-commutation test certifying all required pairwise group relations.

To reduce the communication required in the test, it is natural to turn to low-degree tests: as described above, the latter only require poly-logarithmic, instead of linear, communication. Due to the fact that the test has only a quasi-polynomial number of questions, however, a strategy for the provers only involves a quasi-polynomial number of observables: how can one show that all exponentially many (anti)-commutation relations hold, in principle, between observables defined on the prover's space, if the test itself only requires the existence of a tiny subset of these observables in order to be played?

This difficulty can be overcome as follows. From the classical analysis of the low-degree test, or rather its entanglement-resistant analogue [NV17b], it is possible to show that a strategy that succeeds in the X-basis (resp. Z-basis) low-degree test implies the existence of a family of observables $X(a)$ (resp. $Z(b)$), for $a \in \mathbb{F}_q^n$, that satisfy the commutation relations $X(a)X(b) = X(a+b)$ (resp. $Z(a)Z(b) = Z(a+b)$). Moreover, the use of an appropriate generalization of the Magic Square game over $\mathbb{Z}_2$, introduced in [CS17], to $\mathbb{Z}_s$, for any integer s, that allows us to test for the appropriate twisted commutation relation between any two observables that are actually queried in the test. The difficulty is to establish the right relations between observables $X(a)$ and $Z(b)$ that are not queried from the test, but whose existence follows from the independent application of the entangled-prover analysis of the low-degree test to the X- and Z- basis executions of the test.

Our solution proceeds in three steps. The first step consists in combining X and Z observables together into a single family of commuting observables. We do this by adjoining two ancilla systems for each prover, each initialized in a maximally entangled state local to the prover, and setting $\hat{X}(x) = X(x)_{\mathsf{A}} \otimes \tau_X(x)_{\mathsf{A}'} \otimes \mathrm{Id}_{\mathsf{A}''}$, where $\tau_X(x)_{\mathsf{A}'}$ denotes the n-qudit Pauli that the prover's $X(x)$ is supposed to implement, for x among the possible queries in the test. Defining $\hat{Z}(z)$ similarly, provided $\hat{X}(x)$ and $\hat{Z}(z)$ satisfy the (conjugate of) the twisted commutation relation satisfied by $\tau_X(x)$ and $\tau_Z(z)$ we have obtained a family of (approximately) commuting observables.

In the second step we use these commuting observables to define a strategy for the classical low-degree test, not over m-variate polynomials as the initial test requires, but over $2m$ variables, half of which are "X" variables, and half of which are "Z" variables. To construct such a strategy we have to define "points" and "subspace"

measurements from the $\hat{X}(x)$ and $\hat{Z}(z)$, using the information that the initial observables $X(x)$ and $Z(z)$ came from a strategy for the provers that independently succeeded, with good probability, in the classical low-degree test. Once this has been completed we apply the analysis of the classical low-degree test against two entangled provers to recover a single family of measurements $\{\hat{S}^g\}$ with outcomes in the set of low-degree polynomials g over $\mathbb{F}_q^{2m}$.

The last step consists in "pulling apart" the measurements obtained in the previous step to recover observables $\tilde{X}(x)$ and $\tilde{Z}(z)$, now defined for all $x, z \in \mathbb{F}_q^n$ (and not only the special subset used as queries in the test). Given the definition of $\hat{X}(x)$ from $X(x)$, it is natural to define $\tilde{X} = (\mathrm{Id}_{\mathsf{A}} \otimes \mathrm{Id}_{\mathsf{A}'} \otimes \tau_X(x)_{\mathsf{A}''}) \cdot \hat{X}(x)$, which has the effect of "undoing" the initial tensoring of $X(x)$ by a Pauli on A' (this uses that the ancillas $\mathsf{A}'\mathsf{A}''$ are initialized in a maximally entangled state). It remains to argue that the exponentially many operators thus constructed approximately satisfy the Pauli twisted commutation relations. Once this has been established the result follows as in our previous work [NV17a], as it can be shown directly that such operators must be close to operators exactly satisfying all Pauli relations, whose only joint eigenvalue-1 eigenstate is the maximally entangled state.

Pauli observables over a prime power field. To conclude this overview we briefly discuss some difficulties encountered while working with generalized Pauli observables over a prime power field. Had we restricted attention to prime fields the proof (and certainly the notation!) would have been somewhat simpler. The motivation for considering prime powers comes from the desire to allow embedding qubit Hamiltonians, which we can achieve if $q = 2^t$, but did not see how to implement for odd values of q. Over prime power fields, we are faced with two possible definitions of generalized Pauli observables: the "clock" and "shift" operators mod q, with eigenvalues that are q-th roots of unity, and the definition (5.1), with eigenvalues that are p-th roots of unity. The former are more common in the literature and offer the convenience of allowing to encode a projective measurement with outcomes in $\mathbb{F}_q$ into a single generalized observable. However, they are not well-suited for describing strategies in the low-degree test, since they are defined in terms of addition and multiplication over $\mathbb{Z}_q$, whereas in the low degree test, all operations are performed over $\mathbb{F}_q$. Hence, we opted for the second definition, using families of t such observables to encode a single measurement with outcomes in $\mathbb{F}_q \simeq \mathbb{F}_p^t$.

5.1.2 Further work

There are several open problems raised by our work. Firstly, it would be interesting to expand the range of Hamiltonians for which we are able to give constant-gap interactive proofs, with the goal of eventually reaching a QMA-complete family, and thus a proof of Conjecture 5.1.1 based on a deterministic reduction. Secondly, a different route towards the proof of the conjecture would consist in establishing QMA-hardness results for either of the two classes of Hamiltonians described in Definition 6.2.8 and Definition 6.2.16, for which we do already have a deterministic reduction to a game.

As further motivation, we note that, if such a QMA-hardness result were achieved by constructing a "history Hamiltonian" from a polynomial quantum circuit—as in all such hardness results known—then by an observation of Fitzsimons and Hajdušek [FH15], our results could be used to give an efficient delegation scheme for BQP in the "post-hoc" model. More broadly, the classical PCP theorem and MIP proof systems have become important tools in the design of delegated computation schemes (e.g. [KRR14, RRR16]), and we hope that similar applications may arise from the games variant of QPCP. Beyond the quantum games PCP conjecture, essentially resolved in this work, the complexity of the class MIP* of languages that have multi-prover interactive proof systems with entangled provers remains wildly open. Recent work of [Ji16c] introduces a "compression" technique, that allows him to obtain MIP* protocols for language in NEEXP (non-deterministic doubly-exponential time), albeit at the cost of an exponentially small completeness-soundness gap. Could our techniques be used to obtain the same result, for a constant gap? Such a result would provide an unconditional separation between MIP and MIP*.

In a different direction, it could be useful to extend our entanglement test to sub-constant error, in the same spirit as [AFY17, AFB17]. Currently, all self-testing results we are aware of only provide guarantees in a regime where the success probability is close to 1, which is arguably more challenging to demonstrate in experiments.

Organization. We start with important notation and general preliminaries in Section 5.2. The quantum low-degree test is stated in Section 5.3, and its soundness analysis is given in Section 5.4. In Section 6.1 we extend the test to allow testing arbitrary states encoded using a suitable error-correcting code. Finally, Section 6.2 applies the test to prove Theorem 5.1.2, together with the two variants discussed as items (i) and (ii) in the introduction.

5.2 Preliminaries

This section defines notation relevant to this chapter and Chapter 6.

5.2.1 Notation

We use $\mathcal{H}$ to denote a finite-dimensional Hilbert space, $\mathrm{L}(\mathcal{H})$ for the linear operators on $\mathcal{H}$, and $\mathrm{U}(\mathcal{H})$ the set of unitary operators. Subscripts $\mathcal{H}_\mathsf{A}$, $\mathcal{H}_\mathsf{B}$ indicate distinct spaces.

We use the notation $\mathrm{poly}(f(n))$ to denote $O(f^c(n))$ for some universal constant $c > 0$ (which may vary each time the notation is used). Similarly, we write $\mathrm{poly}^{-1}(f(n))$ to denote $\Omega(f^{-c}(n))$. All parameters used in this and the following chapter will generally be a function of a single parameter n, and asymptotic notation $O(\cdot)$, $\Omega(\cdot)$, etc., should be understood as $n \to \infty$.

5.2.2 Finite fields and polynomials

Throughout we use p to denote a prime and $q = p^t$ a prime power. We let $\mathbb{F}_q$ denote the finite field with q elements, and $\mathbb{Z}_p$ denote the cyclic group mod p. The additive group of $\mathbb{F}_p$ coincides with $\mathbb{Z}_p$, but this is no longer the case for $\mathbb{F}_q$. The finite field trace is denoted by $\mathrm{tr}(a)$; it is a map from $\mathbb{F}_q$ to the prime subfield $\mathbb{F}_p$, defined by $\mathrm{tr}(a) = \sum_{\ell=0}^{t-1} a^{p^\ell}$. The trace respects linear combinations with coefficients drawn from the prime subfield: $\mathrm{tr}(\alpha a + \beta b) = \alpha \mathrm{tr}(a) + \beta \mathrm{tr}(b)$ for $\alpha, \beta \in \mathbb{F}_p$. A useful alternative view of $\mathbb{F}_q$ is as a t-dimensional vector space over $\mathbb{F}_p$. Each element $e \in \mathbb{F}_q$ can be written as $e_1 b_1 + e_2 b_2 + \cdots + e_t b_t$, where $(b_1, \ldots, b_t)$ is a basis for $\mathbb{F}_q$ over $\mathbb{F}_p$ and the coefficients e_ℓ lie in the field of scalars $\mathbb{F}_p$. This representation of $\mathbb{F}_q$ is convenient for addition, since one can add the individual components e_ℓ separately, but in general, it is hard to do multiplication. However, if q is even or $q = p^t$ with both p and t odd there always exists a basis satisfying the property of *self-duality*, i.e.

$$\mathrm{tr}(b_i b_j) = \delta_{ij} \tag{5.2}$$

for all $i, j \in \{1, \ldots, t\}$ (see e.g. [MBG+13, Theorem 1.9]). This property allows to express $\mathrm{tr}(ef)$, for $e, f \in \mathbb{F}_q$, as the inner product, over $\mathbb{F}_p$, of their respective vector of components along the basis. As shown below, this property will make it convenient to express q-dimensional qudits as tensor products of p-dimensional qudits. For the remainder of the thesis we only consider choices of q such that $\mathbb{F}_q$ admits a self-dual basis over $\mathbb{F}_p$.

For integer d, m and a subspace $s \subset \mathbb{F}_q^m$ we let $\deg_d(s)$ denote the set of polynomials on s of total degree at most d (specified with respect to some fixed, implicit basis for s). We write $\omega = e^{\frac{2i\pi}{p}}$ for a fixed primitive p-th root of unity. Let

$$|\mathrm{EPR}_q\rangle = \frac{1}{\sqrt{q}} \sum_{i \in \mathbb{F}_q} |i\rangle \otimes |i\rangle \in \mathbb{C}^q \otimes \mathbb{C}^q \,. \tag{5.3}$$

Coordinates and polynomials. Let $n \geq 1$ be an integer, and h, m two integers such that $h^m \geq n$ and $h \leq q$. Throughout we fix an arbitrary injection $\pi : \{1, \ldots, n\} \to \{0, 1, \ldots, h-1\}^m \subseteq \mathbb{F}_q^m$, where n, h, m are integers such that $h^m \geq n$ that will be clear from context. For $x \in \mathbb{F}_q^m$ and $i \in \{1, \ldots, n\}$ define

$$x_{\pi(i)} = \prod_{j=1}^{m} \frac{\prod_{\substack{k=0 \\ k \neq \pi(i)_j}}^{h-1} (k - x_j)}{\prod_{\substack{k=0 \\ k \neq \pi(i)_j}}^{h-1} (k - \pi(i)_j)} \in \mathbb{F}_q \,,$$

and let $x_\pi = (x_{\pi(1)}, \ldots, x_{\pi(n)}) \in \mathbb{F}_q^n$. Note that for $x \in \{0, 1, \ldots, h-1\}^m$, $x_{\pi(i)} = 1$ if $x = \pi(i)$ and $x_{\pi(i)} = 0$ otherwise. By ranging over all possible values for x we obtain a subset of $\mathbb{F}_q^n$ of size q^m; we think of $x \mapsto x_\pi$ as a pseudo-random "coordinate expansion" map.

Let $g : \mathbb{F}_q^m \to \mathbb{F}_q$ be an m-variate polynomial of degree at most h in each coordi-

nate. Then by interpolation we can write

$$g(x) = \sum_{i=1}^{n} x_{\pi(i)} g(\pi(i)) = g \cdot x_\pi \ , \tag{5.4}$$

where we abuse notation and write g for the vector $(g(\pi(1)), \ldots, g(\pi(n))) \in \mathbb{F}_q^n$. Conversely, for any $a \in \mathbb{F}_q^n$ we let g_a be the m-variate polynomial of individual degree at most h over $\mathbb{F}_q$ defined by

$$g_a : \ x \in \mathbb{F}_q^m \mapsto \sum_i a_i x_{\pi(i)} \ = \ a \cdot x_\pi \ . \tag{5.5}$$

The map from $\mathbb{F}_q^n$ to $\mathbb{F}_q^{q^m}$ that maps a to the evaluation table of g_a is the m-variate Reed-Muller code of individual degree h. Note that $(g_a(\pi(1)), \ldots, g_a(\pi(n))) = a$.

We recall the Schwartz-Zippel lemma [Zip79, Sch80], which we will use repeatedly.

Lemma 5.2.1 (Schwartz-Zippel). *Let $d, m \geq 1$ be integers and r a non-zero polynomial in m variables of total degree at most d defined over the finite field $\mathbb{F}_q$. Then r has at most $d|\mathbb{F}_q|^{m-1}$ zeros.*

5.2.3 Pauli measurements and observables for qudits

To any projective measurement $\{M^a\}$ with outcomes $a \in \mathbb{Z}_p$ we can associate a generalized observable with eigenvalues that are p-th roots of unity: the unitary matrix $M = \sum_a \omega^a M^a$, where $\omega = e^{\frac{2i\pi}{p}}$. The generalized Pauli operators over $\mathbb{F}_p$ are a set of generalized observables indexed by a basis setting X or Z and an element a or b of $\mathbb{F}_p$, with eigenvalues that are p-th roots of unity. They are given by

$$\sigma_X(a) = \sum_{j \in \mathbb{F}_p} |j + a\rangle\langle j| \qquad \text{and} \qquad \sigma_Z(b) = \sum_{j \in \mathbb{F}_p} \omega^{bj} |j\rangle\langle j| \ , \tag{5.6}$$

where addition and multiplication are over $\mathbb{F}_p$. These observables obey the "twisted commutation" relations

$$\forall a, b \in \mathbb{F}_p, \qquad \sigma_X(a)\sigma_Z(b) \ = \ \omega^{-ab}\, \sigma_Z(b)\sigma_X(a) \ . \tag{5.7}$$

Similarly, over a field $\mathbb{F}_q$ we can define a set of generalized Pauli operators, indexed by a basis setting X or Z and an element of $\mathbb{F}_q$. There are different possible definitions for these operators. We choose them to have eigenvalues that are p-th roots of unity. For $a, b \in \mathbb{F}_q$ they are given by

$$\tau_X(a) = \sum_{j \in \mathbb{F}_q} |j + a\rangle\langle j| \qquad \text{and} \qquad \tau_Z(b) = \sum_{j \in \mathbb{F}_q} \omega^{\mathrm{tr}(bj)} |j\rangle\langle j| \ ,$$

where addition and multiplication are over $\mathbb{F}_q$. Powers of these observables obey the relation

$$\forall W \in \{X, Z\},\ \forall a \in \mathbb{F}_q,\ \forall b \in \mathbb{F}_p, \qquad (\tau_W(a))^b = \tau_W(ab) \ .$$

In particular, since $pa = 0$ for any $a \in \mathbb{F}_q$ we get that that $(\tau_W(a))^p = \mathrm{Id}$ for any $a \in \mathbb{F}_q$. The observables obey analogous "twisted commutation" relations to (5.7),

$$\forall a, b \in \mathbb{F}_q, \qquad \tau_X(a)\tau_Z(b) = \omega^{-\mathrm{tr}(ab)}\tau_Z(b)\tau_X(a) \; . \tag{5.8}$$

It is clear from the definition that all of the τ_X operators commute with each other, and similarly all the τ_Z operators with each other. Thus, it is meaningful to speak of a common eigenbasis for all τ_X operators, and a common eigenbasis for all τ_Z operators. The common eigenbasis for the τ_Z operators is the computational basis. To map this basis to the common eigenbasis of the τ_X operators, one can apply the Fourier transform

$$F = \frac{1}{\sqrt{q}} \sum_{j,k \in \mathbb{F}_q} \omega^{-\mathrm{tr}(jk)} |j\rangle\langle k| \; . \tag{5.9}$$

Explicitly, the eigenbases consist of the vectors $|e_W\rangle$ labeled by an element $e \in \mathbb{F}_q$ and $W \in \{X, Z\}$, given by

$$|e_X\rangle = \frac{1}{\sqrt{q}} \sum_j \omega^{-\mathrm{tr}(ej)} |j\rangle \; , \qquad |e_Z\rangle = |e\rangle \; .$$

We denote the POVM whose elements are projectors onto basis vectors of the eigenbasis associated with the observables τ_W by $\{\tau_W^e\}_e$. Then the observables $\tau_W(a)$ can be written as

$$\forall W \in \{X, Z\}, \forall a \in \mathbb{F}_q, \qquad \tau_W(a) = \sum_{e \in \mathbb{F}_q} \omega^{\mathrm{tr}(ae)} \tau_W^e \; .$$

For choices of q such that $\mathbb{F}_q$ admits a self-dual basis $(b_1, \ldots, b_t)$, we can decompose a q-dimensional qudit (a "quqit") as a tensor product of t p-dimensional qudits ("qupits"). Based on this decomposition, for $W \in \{X, Z\}$ and $\ell \in \{1, \ldots, t\}$ we define the W-basis Pauli operator acting on the ℓ-th qupit by

$$\forall a \in \mathbb{F}_p, \qquad \sigma_{W,\ell}(a) = \sum_{e_1, \ldots, e_t \in \mathbb{F}_p} \omega^{ae_\ell} \tau_W^{(e_1 b_1 + \cdots + e_t b_t)} = \tau_W(ab_\ell) \; . \tag{5.10}$$

It can be verified by direct computation that for every $\ell \in \{1, \ldots, t\}$, $\sigma_{X,\ell}$ and $\sigma_{Z,\ell}$ obey the Pauli twisted commutation relations (5.7), and that when $\ell \neq \ell' \in \{1, \ldots, t\}$, $\sigma_{X,\ell}$ and $\sigma_{Z,\ell'}$ commute. Both of these facts also follow from noting that the transformation F that maps $|e_Z\rangle$ to $|e_X\rangle$ decomposes as a tensor product over the qupits:

$$\begin{aligned} F &= \frac{1}{\sqrt{q}} \sum_{jk} \omega^{-\mathrm{tr}(jk)} |j\rangle\langle k| \\ &= \frac{1}{\sqrt{q}} \sum_{j_1, \ldots j_t, k_1, \ldots k_t} \omega^{-\mathrm{tr}(\sum_{\ell,\ell'} j_\ell k_{\ell'} b_\ell b_{\ell'})} |j_1\rangle\langle k_1| \otimes \cdots \otimes |j_t\rangle\langle k_t| \end{aligned}$$

$$
\begin{aligned}
&= \frac{1}{\sqrt{q}} \sum_{j_1,\ldots j_t,k_1,\ldots k_t} \omega^{-\sum_{\ell,\ell'} j_\ell k_{\ell'} \mathrm{tr}(b_\ell b_{\ell'})} |j_1\rangle\langle k_1| \otimes \cdots \otimes |j_t\rangle\langle k_t| \\
&= \frac{1}{\sqrt{q}} \sum_{j_1,\ldots j_t,k_1,\ldots k_t} \omega^{-\sum_{\ell} j_\ell k_\ell} |j_1\rangle\langle k_1| \otimes \cdots \otimes |j_t\rangle\langle k_t| \\
&= \bigotimes_{\ell=1}^{t} \Big(\frac{1}{\sqrt{p}} \sum_{j_\ell,k_\ell} \omega^{-j_\ell k_\ell} |j_\ell\rangle\langle k_\ell| \Big) ,
\end{aligned}
$$

where in going from the second to the third line we used the linearity of the trace and the fact that $j_\ell, k_{\ell'}$ are elements of the prime subfield $\mathbb{F}_p$. We will sometimes consider the case where $p = 2$, in which case the $\sigma_{W,\ell}$ behave as the standard Pauli spin matrices acting on t qubits, with the index ℓ labeling the qubit acted on. Also, it will be sometimes useful to allow the index a to range over all of $\mathbb{F}_q$ instead of just $\mathbb{F}_p$; extending (5.10) we define $\sigma_{W,\ell}(a)$ to be $\tau_W(ab_\ell)$ for any $a \in \mathbb{F}_q$.

For systems with many qudits, we will consider tensor products of the operators τ_W. Slightly abusing notation, for $W \in \{X, Z\}$ and $a \in \mathbb{F}_q^n$ we denote by $\tau_W(a)$ the tensor product $\tau_W(a_1) \otimes \ldots \otimes \tau_W(a_n)$. These obey the twisted commutation relations

$$
\forall a, b \in \mathbb{F}_q^n, \qquad \tau_X(a)\tau_Z(b) = \omega^{-\mathrm{tr}(a \cdot b)} \tau_Z(b)\tau_X(a) ,
$$

where $a \cdot b = \sum_{i=1}^n a_i b_i \in \mathbb{F}_q$. For $W \in \{X, Z\}$ and $e \in \mathbb{F}_q^n$ define the eigenstates

$$
|e_W\rangle = |(e_1)_W\rangle \otimes \ldots \otimes |(e_n)_W\rangle ,
$$

and associated rank-1 projectors τ_W^e.

State-dependent distance. For operators $A, B \in \mathrm{L}(\mathcal{H})$, where $\mathcal{H}$ is a finite-dimensional Hilbert space, and a vector $|\psi\rangle \in \mathcal{H} \otimes \mathcal{H}'$, where $\mathcal{H}'$ is another finite-dimensional Hilbert space, we write $A \approx_\delta B$ for $\|(A - B) \otimes \mathrm{Id}\, |\psi\rangle\|^2 = O(\delta)$. Note the state $|\psi\rangle$ and the space $\mathcal{H}'$ are usually kept implicit. We sometimes write the same with some free variables, e.g. $A_x^a \approx_\delta B_x^a$. By this we mean

$$
\mathop{\mathrm{E}}_x \sum_a \|(A_x^a - B_x^a) \otimes \mathrm{Id}\, |\psi\rangle\|^2 = O(\delta) .
$$

Variables appearing as subscript will most often be considered "inputs", and should be averaged; superscripts are considered "answers" and should be summed over. Which is which will always be clear from context, including the distribution on inputs.

For a family of POVM $\{A_x^a\}$ acting on $\mathcal{H}_A$, we will say that $\{A_x^a\}$ is δ-self-consistent if there exists a family of POVM $\{\boldsymbol{A}_x^a\}$ acting on $\mathcal{H}_B$ such that $A_x^a \otimes \mathrm{Id}_B \approx_\delta \mathrm{Id}_A \otimes \boldsymbol{A}_x^a$. Note that this definition relies on an implicit understanding of the space $\mathcal{H}_B$ and the operators $\{\boldsymbol{A}_x^a\}$, and we will only use the terminology when the space and operators are clear from context. The following lemma relates two measures of consistency, defined via observables or the underlying projective measurement.

Claim 5.2.2. *Let s be any integer, and let $\{A^a\}, \{B^b\}$ be projective measurements with outcomes $a, b \in \mathbb{Z}_s$. Let $A = \sum_a \omega_s^a A^a$ and $B = \sum_b \omega_s^b B^b$ where $\omega_s = \exp(2\pi i/s)$. Then for any state $|\psi\rangle$,*

$$\frac{1}{2}\Big(1 - \Re\big(\langle\psi|A \otimes B^\dagger|\psi\rangle\big)\Big) \leq \sum_{a\neq b} \big\|A^a \otimes B^b|\psi\rangle\big\|^2 \leq \frac{s^2}{2\pi^2}\Big(1 - \Re\big(\langle\psi|A \otimes B^\dagger|\psi\rangle\big)\Big) .$$

Proof. Expand

$$\big\|(A \otimes \mathrm{Id} - \mathrm{Id} \otimes B)|\psi\rangle\big\|^2 = \sum_{a\neq b} \big|\omega_s^a - \omega_s^b\big|^2 \big\|A^a \otimes B^b|\psi\rangle\big\|^2 ,$$

and use $\frac{2\pi}{s} \leq |\omega_s^a - \omega_s^b| \leq 2$ for all $a \neq b$. □

Claim 5.2.3. *Let s be an integer, $\delta \geq 0$, $|\psi\rangle \in \mathcal{H}$ a state and $B \in \mathrm{L}(\mathcal{H})$ a normal operator such that $\|(B^s - \mathrm{Id})|\psi\rangle\|^2 \leq \delta$. Then there exists a unitary U with the same eigenvectors as B such that $U^s = \mathrm{Id}$ and*

$$\big\|(B - U)|\psi\rangle\big\|^2 \leq 4\,\delta .$$

Proof. Let $\lambda = re^{2i\pi\theta}$ be any complex number, where $r \in \mathbb{R}_+$ and $\theta \in [-1/2, 1/2)$. Then

$$\begin{aligned} \big|re^{2i\pi\theta} - 1\big| &\geq \max\big(|r-1|,\, \big|e^{2i\pi\theta} - 1\big|\big) \\ &\geq \max\big(|r-1|,\, 4|\theta|\big) . \end{aligned} \tag{5.11}$$

Thus, by the triangle inequality,

$$\begin{aligned} \Big|\lambda - e^{\frac{2i\pi}{s}\lfloor s\theta\rfloor}\Big| &\leq |r-1| + \Big|e^{2i\pi\theta} - e^{\frac{2i\pi}{s}\lfloor s\theta\rfloor}\Big| \\ &\leq |r^s - 1| + 8\Big|\theta - \Big[\frac{1}{s}\lfloor s\theta\rfloor\Big]_1\Big| \\ &\leq \big|\lambda^s - 1\big| + \frac{2}{s}\big|\lambda^s - 1\big| , \end{aligned} \tag{5.12}$$

where in the second line we wrote $[x]_1$ for the representative of x mod 1 in $[-1/2, 1/2)$, and the last line follows from (5.11).

Write the eigendecomposition of $B = \sum_i \lambda_i \Pi_i$, where Π_i is a Hermitian projector and λ_i a complex number. We include zero eigenvalues, so that $\sum_i \Pi_i = \mathrm{Id}$. The assumption made in the claim can be written as

$$\|(B^s - \mathrm{Id})|\psi\rangle\|^2 = \Big\|\sum_i (\lambda_i^s - 1)\Pi_i|\psi\rangle\Big\|^2 = \sum_i |\lambda_i^s - 1|^2 \|\Pi_i|\psi\rangle\|^2 \leq \delta . \tag{5.13}$$

Let $\omega = e^{\frac{2\pi i}{s}}$. For each i, let ω^{a_i} be the closest s-th root of unity to λ_i. Define

$U = \sum_i \omega^{a_i} \Pi_i$. Then

$$\begin{aligned} \|(B-U)|\psi\rangle\|^2 &= \sum_i \left|\lambda_i - \omega^{a_i}\right|^2 \|\Pi_i|\psi\rangle\|^2 \\ &\leq \sum_i 4\left|\lambda_i^s - 1\right|^2 \|\Pi_i|\psi\rangle\|^2 \\ &\leq 4\,\delta\,, \end{aligned}$$

where the second line uses (5.12), and the last is by (5.13). □

5.2.4 Self-testing

We use the language of multi-player self-tests (we will often call the players "provers" as well).

Definition 5.2.4. Let $k \geq 1$ be an integer. A *k-partite strategy* $S = (|\psi\rangle, \mathcal{X}, \mathcal{A}, \mathcal{M})$ consists of finite question and answer sets $\mathcal{X} = X_1 \times \cdots \times X_k$ and $\mathcal{A} = A_1 \times \cdots \times A_k$ respectively, a k-partite quantum state $|\psi\rangle \in \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_k$, and for each $i \in \{1, \ldots, k\}$ a collection of measurement operators $\{M_x^a\}_{a \in A_i}$ on $\mathcal{H}_i$ and indexed by $x \in X_i$.[3] We say that the strategy is *partial* if it only specifies measurement operators for a subset of the possible questions, or if it does not specify a state $|\psi\rangle$.

We reproduce a standard definition in self-testing.

Definition 5.2.5. A *k-player self-test* with completeness c and robustness $\delta(\varepsilon)$ for a (partial) strategy $S = (|\Psi\rangle, \mathcal{X}, \mathcal{A}, \mathcal{M})$ is a distribution π on $\mathcal{X}$ and a family of coefficients $V(a_1, \ldots, a_k | x_1, \ldots, x_k) \in [0,1]$, for $(x_1, \ldots, x_k) \in \mathcal{X}$ and $(a_1, \ldots, a_k) \in \mathcal{A}$, such that the following hold:

- There exists a strategy $\hat{S}$ that extends the (partial) strategy S and succeeds in the test with probability at least c; formally,

$$\sum_{(x_1,\ldots,x_k)} \pi(x_1, \ldots, x_k) \sum_{a_1,\ldots,a_k} V(a_1, \ldots, a_k | x_1, \ldots, x_k) \, \langle\psi| \hat{M}_{x_1}^{a_1} \otimes \cdots \otimes \hat{M}_{x_k}^{a_k} |\psi\rangle \;\geq\; c\,.$$

- Any strategy with success at least $c - \varepsilon$ in the test must be $\delta(\varepsilon)$-close to the optimal strategy. Formally, for any strategy $\hat{S} = (|\hat{\psi}\rangle, \mathcal{X}, \mathcal{A}, \hat{\mathcal{M}})$ such that

$$\sum_{(x_1,\ldots,x_k)} \pi(x_1, \ldots, x_k) \sum_{a_1,\ldots,a_k} V(a_1, \ldots, a_k | x_1, \ldots, x_k) \, \langle\hat{\psi}| \hat{M}_{x_1}^{a_1} \otimes \cdots \otimes \hat{M}_{x_k}^{a_k} |\hat{\psi}\rangle \;\geq\; c - \varepsilon\,,$$

there exists a local isometry $\Phi = \Phi_1 \otimes \cdots \Phi_k$ and a state $|\text{AUX}\rangle$ such that

$$\left\| \Phi(|\hat{\psi}\rangle) - |\text{AUX}\rangle |\psi\rangle \right\| \;\leq\; \delta(\varepsilon)\,,$$

[3] Although this is left implicit in the notation, the measurement operators associated with different spaces need not be equal.

and

$$\sum_{x_1,\ldots,x_k} \pi(x_1,\ldots,x_k) \sum_{a_1,\ldots,a_k} \big\| \Phi\big(\hat{M}_{x_1}^{a_1} \otimes \cdots \otimes \hat{M}_{x_k}^{a_k} |\hat{\psi}\rangle\big) - |\mathrm{AUX}\rangle M_{x_1}^{a_1} \otimes \cdots \otimes M_{x_k}^{a_k} |\psi\rangle \big\| \leq \delta(\varepsilon) \,.$$

In case S only specifies a partial strategy, then the above expression is restricted to questions for which S is defined.

5.2.5 The commutation test

In designing self-tests, it is useful to have the ability to test commutation relations between pairs of observables applied by the provers. The following well-known test can be employed to certify that two observables commute:

Theorem 5.2.6. *Let s be an integer and $\varepsilon > 0$. There exists a two-player self-test $\mathrm{COM}(M, N)$ with completeness 1 and robustness $\delta(\varepsilon) = O(s\sqrt{\varepsilon})$, for the (partial) strategy S that uses commuting generalized observables M and N (with outcomes in $\mathbb{Z}_s$) for two special questions labelled 1 and 2, respectively. The test has 3 questions per player and answers either in $\mathbb{Z}_s$ (for questions 1 and 2) or $\mathbb{Z}_s^2$ (for question 3). Moreover, for any two commuting observables A and B, there exists a strategy in which the first player uses the observables M and N for questions 1 and 2, using a shared state $|\psi\rangle$ that is a maximally entangled state of appropriate dimension.*

The guarantees of the theorem are achieved by the following test, which is a simple instance of the idea of "oracularization" in multiprover interactive proofs. In the test, the verifier performs either of the following with equal probability $\frac{1}{2}$:

1. Send the first player a question q chosen uniformly from $\{1, 2\}$, and send the second player the question 3. Receive an answer $a \in \mathbb{Z}_s$ from the first player and $(b_1, b_2) \in \mathbb{Z}_s^2$ from the second player. Accept if $a = b_q$, and reject otherwise.
2. Perform the same as in item 1., but with the players interchanged.

The analysis of this test is standard; see, e.g. [CGJV17, Lemma 28].

5.2.6 The generalized Magic Square

In [CS17] a generalized version of the Magic Square game [Ara02] is introduced and shown to robustly self-test generalized observables satisfying twisted commutation relations over $\mathbb{Z}_s$, for any integer s.

Theorem 5.2.7 (Theorem 5.9 in [CS17]). *Let s be an integer and $\varepsilon > 0$. There exists a two-player self-test $\mathrm{MS}(X, Z)$, with completeness 1 and robustness $\delta(\varepsilon) = O(s^3\sqrt{\varepsilon})$, for the (partial) strategy S that uses observables σ_X and σ_Z on two special questions labeled X and Z respectively. The test has $O(1)$ questions per player (including two questions labeled X and Z) and answers in $\mathbb{Z}_s^2$. Furthermore, there is a strategy that succeeds with probability 1 using only σ_X, σ_Y and σ_Z observables on two s-dimensional qudits per player initialized in $|\psi\rangle = |\mathrm{EPR}_s\rangle \otimes |\mathrm{EPR}_s\rangle$.*

5.2.7 The classical low-degree test

A stepping stone in our analysis is an extension of the "classical low-degree test" from [Vid13] to the case of only two provers.

Theorem 5.2.8 (Theorem 2 in [NV17b] and Theorem 4.1.2 above). *Let $\varepsilon > 0$, m, d integers, and q a prime power such that $q \geq (dm/\varepsilon)^c$ for a universal constant $c \geq 1$. There is a two-prover test, called the* classical low-degree test C-LOWDEG(m, d, q), *in which queries to the provers are chosen among affine subspaces $s \subseteq \mathbb{F}_q^m$, and answers are polynomials r on s of total degree at most d, such that the following holds. For any strategy for the provers using entangled state $|\psi\rangle$ and projective measurements $\{M_s^r\}$ that succeeds with probability at least $1 - \varepsilon$ in the test there exists a POVM $\{S^g\}$, where g ranges over the polynomials on $\mathbb{F}_q^m$ of total degree at most d, and a $\delta = \mathrm{poly}(\varepsilon)$ such that the following hold:*

1. *Approximate consistency with M:*

$$\mathop{\mathrm{E}}_s \sum_g \sum_{r \neq g|_s} \langle \psi | M_s^r \otimes S^g | \psi \rangle \leq \delta,$$

2. *Self-consistency:*

$$\sum_g \langle \psi | S^g \otimes (\mathrm{Id} - S^g) | \psi \rangle \leq \delta.$$

We let π_{ld} denote the distribution on questions used by the verifier in the low-degree test from Theorem 5.2.8. This distribution is symmetric, and we slightly abuse notation by also writing π_{ld} for either marginal. We will use that the test from Theorem 5.2.8 that it satisfies the following properties:

(i) π_{ld} is a uniform mixture of the uniform distribution on pairs (s, w) such that s is an affine subspace of dimension 2 in $\mathbb{F}_q^m$ and $w \in s$ is a uniformly random point in s, and its permutation (w, s).

(ii) Whenever provers in the test are queried for a pair of subspaces (s, w), they are required to return a polynomial r defined on s and a value a in $\mathbb{F}_q$ such that $r(w) = a$.

Theorem 5.2.8 assumes that the strategy employed by the provers in the test is invariant under permutation of the two provers. It will be convenient to allow non-symmetric strategies as well.

Corollary 5.2.9. *Let m, d, q and ε be as in Theorem 5.2.8. Let $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ be a bipartite state, and $\{M_s^r\}$ and $\{\boldsymbol{M}_s^r\}$ be POVMs on $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively, such that the associated strategy for the provers succeeds in the test* C-LOWDEG(m, d, q) *from Theorem 5.2.8 with probability at least $1 - \varepsilon$. Then there exist POVMs $\{S^g\}$ and $\{\boldsymbol{S}^g\}$, where g ranges over the polynomials on $\mathbb{F}_q^m$ of total degree at most d, defined on $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively, and a $\delta = \mathrm{poly}(\varepsilon)$ such that the following relations hold, on average over $s \sim \pi_{\mathrm{ld}}$:*

$$\sum_g M_s^{g|_s} \otimes \boldsymbol{S}^g \approx_\delta \mathrm{Id}\,, \qquad \sum_g S^g \otimes \boldsymbol{M}_s^{g|_s} \approx_\delta \mathrm{Id}\,,$$

and

$$S^g \otimes \mathrm{Id} \approx_\delta \mathrm{Id} \otimes \boldsymbol{S}^g \ .$$

Proof. Extending A or B as needed, assume without loss of generality that $\mathcal{H}_\mathsf{A}$ and $\mathcal{H}_\mathsf{B}$ have the same dimension, and fix a canonical isomorphism between the two. Adjoin ancilla spaces $\mathcal{H}_{\mathsf{A}'}$ and $\mathcal{H}_{\mathsf{B}'}$, each isomorphic to $\mathbb{C}^2$. From an arbitrary strategy we can construct a symmetric one by letting

$$\hat{M}^r_s \ = \ M^r_s \otimes |0\rangle\langle 0|_{\mathsf{A}'} + \boldsymbol{M}^r_s \otimes |1\rangle\langle 1|_{\mathsf{A}'} \ ,$$

and

$$|\hat{\psi}\rangle \ = \ \frac{1}{\sqrt{2}}\big(|\psi\rangle_{\mathsf{AB}} \otimes |0\rangle_{\mathsf{A}'} \otimes |1\rangle_{\mathsf{B}'} + |\psi'\rangle_{\mathsf{AB}} \otimes |1\rangle_{\mathsf{A}'} \otimes |0\rangle_{\mathsf{B}'}\big) \ ,$$

where $|\psi'\rangle_{\mathsf{AB}}$ is obtained by swapping registers A and B in $|\psi\rangle_{\mathsf{AB}}$. Using that the test from Theorem 5.2.8 is symmetric, the success probability of this strategy is the same as that of the non-symmetric one. Applying Theorem 5.2.8 gives POVM $\{\hat{S}^g\}$ defined on AA' that are consistent with the $\{\hat{M}^r_s\}$, on the state $|\hat{\psi}\rangle$. It then suffices to define

$$S^g \ = \ \big(\mathrm{Id} \otimes \langle 0|_{\mathsf{A}'}\big)\, S^g \,\big(\mathrm{Id} \otimes |0\rangle_{\mathsf{A}'}\big) \ , \qquad \boldsymbol{S}^g \ = \ \big(\mathrm{Id} \otimes \langle 1|_{\mathsf{A}'}\big)\, S^g \,\big(\mathrm{Id} \otimes |1\rangle_{\mathsf{A}'}\big) \ .$$

□

The length of questions in the low-degree test C-LOWDEG(m, d, q) from Theorem 5.2.8 is $O(m \log q)$, which for a choice of $q = \mathrm{poly}\log(n)$ is logarithmic in n. However, answers have length $O(d^2 \log q)$, which is super-logarithmic. To achieve reduced answer length it is standard to compose the test with itself: any answer r from a prover is interpreted as an $n' = O(d^2 \log q)$-long string of bits, that can be encoded as a multilinear polynomial over $\mathbb{F}_q^{m'}$, for m' such that $2^{m'} \geq n'$. Questions in the composed test are a subspace $s \subseteq \mathbb{F}_q^m$, together with a subspace $s' \subseteq \mathbb{F}_q^{m'}$, and answers are the restriction to s' of the low-degree encoding of the polynomial r that the prover would answer to the question s. The analysis of the composition is standard, and we state the result as the following theorem.

Theorem 5.2.10. *Let $\varepsilon > 0$, m, d be integers, and q a prime power such that $q \geq (dm/\varepsilon)^c$ for a universal constant $c \geq 1$. Let $n' = O(d^2)$ be the answer length (in number of $\mathbb{F}_q$-symbols) in* C-LOWDEG(m, d, q)*, and $m' = \log(n') = O(\log\log n)$. There is a two-prover test, called the* composed classical low-degree test C-LOWDEG$^{(2)}(m, d, q)$*, in which queries to the provers are chosen among, either pairs of affine subspaces $(s, s') \subseteq \mathbb{F}_q^m \times \mathbb{F}_q^{m'}$, or points in $\mathbb{F}_q^m$, and answers are, either multilinear polynomials r' on s', or values $a \in \mathbb{F}_q$, such that the following holds. For any strategy specified by a shared state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ and measurement operators $\{M^{r'}_{s,s'}\}$ and $\{\boldsymbol{M}^{r'}_{s,s'}\}$ on $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively, such that the associated strategy succeeds in the test* C-LOWDEG$^{(2)}(m, d, q)$ *with probability at least $1 - \varepsilon$, there exist POVM $\{S^g\}$ and $\{\boldsymbol{S}^g\}$, where g ranges over the polynomials on $\mathbb{F}_q^m$ of total degree at most d, defined on $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively, and a $\delta = \mathrm{poly}(\varepsilon)$ such that the following relations hold,*

on average over $s \sim \pi_{\mathrm{Id}}$*:*

$$\sum_g \mathop{\mathrm{E}}_{s'} M_{s,s'}^{g_{|s,s'}} \otimes \boldsymbol{S}^g \approx_\delta \mathrm{Id}\,, \qquad \sum_g \mathop{\mathrm{E}}_{s'} S^g \otimes \boldsymbol{M}_{s,s'}^{g_{|s,s'}} \approx_\delta \mathrm{Id}\,,$$

where the expectation is over an s' *as sampled in the test (conditioned on* s*), and* $g_{|s,s'}$ *denotes the polynomial on* s' *obtained by restricting to* s' *the low-degree extension of the description of the restriction* $g_{|s}$ *of* g *to* s*. Furthermore,*

$$S^g \otimes \mathrm{Id} \approx_\delta \mathrm{Id} \otimes \boldsymbol{S}^g\,.$$

5.3 The quantum low-degree test

5.3.1 Description of the test

We denote our quantum low-degree test by Q-LOWDEG$^{(l)}$, for $l \in \{1,2\}$. Here l denotes the "level" of the test, before ($l = 1$) or after ($l = 2$) composition. In general we also write Q-LOWDEG for the "composed quantum low-degree test" Q-LOWDEG$^{(2)}$, which is the variant of the test with reduced answer size, and is the variant that will be used in our applications. The test is described in Figure 5-1. We show that the test is a self-test for the following class of Pauli strategies. To define the strategy, recall the definition of the POVM $\{\tau_W^a\}$ in Section 5.2.3, defined for each $W \in \{X, Z\}$. For $s \subset \mathbb{F}_q^m$ either a point or a 2-dimensional subspace, and r a polynomial defined on s, define

$$\tau_{W,s}^r = \sum_{a \in \mathbb{F}_q^n : (g_a)_{|s} = r} \tau_W^a\,, \tag{5.14}$$

where g_a is defined in (5.5). Finally, for reasons that will become clear later, it is convenient to introduce

$$\boldsymbol{\tau}_{X,s}^r = \tau_{X,s}^{-r} \qquad \text{and} \qquad \boldsymbol{\tau}_{Z,s}^r = \tau_{Z,s}^r\,. \tag{5.15}$$

Definition 5.3.1. Let p be a prime, $t \geq 1$ an integer, and $q = p^t$. The low-degree Pauli strategy S_{P} on n qudits of local dimension q is the strategy $(|\psi\rangle, \mathcal{X}, \mathcal{A}, \mathcal{M})$ where $|\psi\rangle = |\mathrm{EPR}_q\rangle^{\otimes n}$, $\mathcal{X} = \{X, Z\} \times (\mathcal{X}_1 \cup \mathcal{X}_2)$, where $\mathcal{X}_1 = \mathbb{F}_q^m$ and $\mathcal{X}_2$ is the set of all two-dimensional subspaces of $\mathbb{F}_q^m$, $\mathcal{A} = \mathcal{A}_1 \cup \mathcal{A}_2$, where $\mathcal{A}_1 = \mathbb{F}_q$ and $\mathcal{A}_2 = \deg_d(\mathbb{F}_q^2)$, and $\mathcal{M} = \mathcal{M}_1 \cup \mathcal{M}_2$, where $\mathcal{M}_1 = \{\tau_{W,w}^a\} \times \{\boldsymbol{\tau}_{W,w}^a\}$ and $\mathcal{M}_2 = \{\tau_{W,s}^r\} \times \{\boldsymbol{\tau}_{W,s}^r\}$, with $\tau_{W,w}^a$, $\tau_{W,s}^r$, and $\boldsymbol{\tau}_{W,w}^a$, $\boldsymbol{\tau}_{W,s}^r$ defined as in (5.14) and (5.15) respectively.

Theorem 5.3.2. *Let* $n \geq 1$ *be an integer. Let* h, m *be integer such that* $h^m \geq n$*, and let* $d = hm$*. Let* $q = p^t$ *be a prime power such that* $\mathbb{F}_q$ *admits a self-dual basis over* $\mathbb{F}_p$*. Then for any* $\varepsilon \geq 0$ *the test* Q-LOWDEG$^{(2)}(m, d, q)$ *is a 2-prover self-test for the low-degree Pauli strategy* S_P *on* n *qudits of local dimension* q *with completeness* 1 *and robustness* $\delta = \mathrm{poly}(\mathrm{poly}(p) \cdot \mathrm{poly}(\varepsilon) + \mathrm{poly}(d/q))$*. Moreover, the test has questions of length* $O(m \log q)$ *and answers of length* $O(\log^2(d) \log(q))$*.*

Test Q-LOWDEG$^{(l)}(m, d, q)$. m, d are integer, and $q = p^t$ is a prime power such that $\mathbb{F}_q$ admits a self-dual basis $(b_1, \ldots, b_t)$ over $\mathbb{F}_p$. $l \in \{1, 2\}$ is a parameter that indicates the level of the test.
The verifier performs the following with equal probability:

(a) Select $W \in \{X, Z\}$ uniformly at random and send W to both provers. If $l = 2$ execute the test C-LOWDEG$^{(2)}(m, d, q)$ from Theorem 5.2.10 with the provers. If $l = 1$ execute the test C-LOWDEG(m, d, q) from Theorem 5.2.8. Let r be the polynomial returned by the first prover, and r' by the second. If $W = X$, set $A = r$ and $\boldsymbol{A'} = -r'$. If $W = Z$, set $A = r$ and $\boldsymbol{A'} = r'$. Accept if and only if the pair of answers $(A, \boldsymbol{A'})$ would have been accepted in the classical test.

(b) Select $x, z \in \mathbb{F}_q^m$ and $u, u' \in \mathbb{F}_q$ uniformly at random, and let $a = \mathrm{tr}((ux_\pi) \cdot (u'z_\pi)) \in \mathbb{F}_p$.

- If $a = 0$, execute the self-test COM (see Theorem 5.2.6), replacing queries 1, 2, and 3 in the test by (X, x), (Z, z), and (x, z, uu') respectively, and in the case of queries 1 and 2, replacing the prover's answer $b \in \mathbb{F}_q$ by $\mathrm{tr}(ub)$ or $\mathrm{tr}(u'b) \in \mathbb{F}_p$, respectively, before making the same decision as the verifier in the test.
- If $a \neq 0$, execute the self-test MS (see Theorem 5.2.7) with the following modification: the question labeled X is replaced by the query (X, x) as in part (a), and the prover's answer $b \in \mathbb{F}_q$ is replaced by $\mathrm{tr}(ub) \in \mathbb{F}_p$; the question labeled Z is replaced by the query (Z, z) as in part (a), and the prover's answer $b \in \mathbb{F}_q$ is replaced by $a^{-1}\mathrm{tr}(u'b) \in \mathbb{F}_p$.

Figure 5-1: The quantum low-degree test. $l \in \{1, 2\}$ denotes the "level" of the test, before $(l = 1)$ or after $(l = 2)$ composition.

Completeness of the test is shown in Lemma 5.3.4 in Section 5.3.2. Soundness is shown in Lemma 5.4.1 in Section 5.4.

Remark 5.3.3. In a typical application of the test Q-LOWDEG$^{(2)}$, the parameters are chosen such that $m = \Theta(\frac{\log n}{\log\log n})$ and $h = \Theta(\log n)$, resulting in $d = \Theta(\frac{\log^2(n)}{\log\log n})$. Further, we chose p to be constant and $q = \Theta(\frac{\log^2(n)}{\log\log n})$ such that d/q is a small constant. This results in a question length that is $O(\log n)$ and an answer length that is poly$(\log\log n)$.

5.3.2 Completeness

The proof of the following lemma specifies the "honest" strategy that is expected of the provers in the quantum low-degree test.

Lemma 5.3.4 (Completeness). *For m, d, q as in Theorem 5.3.2 the strategy S_P introduced in Definition 5.3.1 can be extended to a strategy that succeeds with probability 1 in the test* Q-LOWDEG(m, d, q).

Proof. Let

$$|\psi_{\mathrm{EPR}}\rangle = \bigotimes_{j=1}^{n+1} |\mathrm{EPR}_q\rangle ,$$

where $|\mathrm{EPR}_q\rangle$ is defined in (5.3). We first describe a strategy for the players assuming questions in part (a) of the test come from C-LOWDEG, instead of the composed test C-LOWDEG$^{(2)}$. Once a strategy for the former has been defined it is straightforward to adapt it to a strategy for the latter; this only requires classical post-processing.

To define the strategy we use the generalized Pauli operators and projections defined in Section 5.2.3. When queried for a subspace $s \subseteq \mathbb{F}_p^m$ in a basis $W \in \{X, Z\}$, the prover measures the first n qudits using the projective measurement $\{\tau_W^a\}$ and returns the polynomial $(g_a)_{|s}$; this corresponds to the POVM described in (5.14).

To see that these measurements define a strategy which succeeds with probability 1 in part (a) of the test, note that the state $|\mathrm{EPR}_q\rangle$ is stabilized by $\tau_X(a) \otimes \tau_X(a)$ and $\tau_Z(b) \otimes \tau_Z(-b)$ for any $a, b \in \mathbb{F}_q$. Hence, if both provers measure the state $|\mathrm{EPR}_q\rangle$ in the X eigenbasis, and the first prover obtains an outcome $a \in \mathbb{F}_q$, the second prover will obtain the outcome $-a$; if they measure in the Z eigenbasis, they will both always obtain the same outcome. As a consequence, the following consistency relations hold for any s:

$$\begin{aligned} \sum_{r \in \deg_d(s)} \tau_{X,s}^r \otimes \tau_{X,s}^{-r} |\psi_{\mathrm{EPR}}\rangle &= |\psi_{\mathrm{EPR}}\rangle , \\ \sum_{r \in \deg_d(s)} \tau_{Z,s}^r \otimes \tau_{Z,s}^r |\psi_{\mathrm{EPR}}\rangle &= |\psi_{\mathrm{EPR}}\rangle . \end{aligned} \tag{5.16}$$

Thus whenever $W = X$ is selected in part (a) of the low-degree test the first prover's answers are consistent with the negation of the second prover's, as the verifier expects; in case $W = Z$ both provers' answers are consistent.

Using the notation introduced in (5.15), the consistency relations (5.16) become

$$\sum_q \tau^q_{W,s} \otimes \boldsymbol{\tau}^q_{W,s} |\psi_{\mathrm{EPR}}\rangle = |\psi_{\mathrm{EPR}}\rangle \ , \tag{5.17}$$

for any $W \in \{X, Z\}$.

To show completeness in part (b) of the test we introduce a family of generalized observables associated with the measurement performed by a prover in part (a) of the test when it is queried for a value at a single point $w \in \mathbb{F}_q^m$. The prover's answer in this case is a value in $\mathbb{F}_q$. To the provers' strategy for determining his answer we introduce a family of q observables over $\mathbb{F}_p$, indexed by $u \in \mathbb{F}_q$, each of which is associated with the value $\mathrm{tr}(ub) \in \mathbb{F}_p$, where $b \in \mathbb{F}_q$ is the answer obtained by the prover. We denote the corresponding for query (W, w) by $W_u(w_\pi)$:

$$\begin{aligned} W_u(w_\pi) &= \sum_{s \in \mathbb{F}_q^n} \omega^{\mathrm{tr}(g_s(w)u)} \, \tau^a_W \\ &= \sum_{s \in \mathbb{F}_q^n} \omega^{\mathrm{tr}(s \cdot (uw_\pi))} \, \tau^a_W \\ &= \tau_W(uw_\pi) \ . \end{aligned} \tag{5.18}$$

From this expression it is clear that for any $x, z \in \mathbb{F}_q^m$, $u, u' \in \mathbb{F}_q$, and $a = \mathrm{tr}((ux_\pi) \cdot (u' z_\pi))$,

$$X_u(x_\pi) Z_{u'}(a^{-1} z_\pi) = \omega^{-\mathrm{tr}(a^{-1}(ux_\pi)(u'z_\pi))} Z_{u'}(a^{-1} z_\pi) X_u(x_\pi) = \omega^{-1} Z_{u'}(a^{-1} z_\pi) X_u(x_\pi) \ .$$

Hence, the measurement operators corresponding to the questions labeled X and Z in part (b) of the test satisfy the required twisted commutation relation. It is then straightforward that each prover can implement a strategy that succeeds in part (b) of the test. In case the test COM is executed this is immediate; in case it is MS the provers may use the $(n+1)$-th qudit and a second pair of observables (X', Z') satisfying the same twisted commutation relation, so that (X, Z) and (X', Z') together form a strategy which succeeds with probability 1 in the test MS.

□

5.4 Soundness analysis

Lemma 5.4.1 (Soundness). *Let $n \geq 1$ be an integer and m, h, d, and $q = p^t$ as in Theorem 5.3.2. Let $\varepsilon \geq 0$. Suppose a strategy using state $|\psi\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$ and projective measurements $\{M^r_{W,s,s'}\}$ and $\{M^a_{W,w}\}$ succeeds in test* Q-LOWDEG(m, d) *with probability at least $1 - \varepsilon$. Then there is a $\delta = \mathrm{poly}(\mathrm{poly}(p) \cdot \mathrm{poly}(\varepsilon) + \mathrm{poly}(d/q))$, isometries $V_D : \mathcal{H}_D \to (\mathbb{C}^q)^{\otimes n}_{D''} \otimes \mathcal{H}_{D''}$ for $D \in \{A, B\}$, and a state $|\mathrm{AUX}\rangle \in \mathcal{H}_{A''} \otimes \mathcal{H}_{B''}$ such that*

$$\left\| V_A \otimes V_B |\psi\rangle - |\mathrm{EPR}_q\rangle^{\otimes n} |\mathrm{AUX}\rangle \right\|^2 \leq \delta \ ,$$

and for all $W \in \{X, Z\}$,

$$\mathop{\mathrm{E}}_{w\in\mathbb{F}_q^m} \sum_{a\in\mathbb{F}_q} \left\|(V_A \otimes V_B)(M^a_{W,w} \otimes \mathrm{Id})|\psi\rangle - (\tau^a_{W,w} \otimes \mathrm{Id})|\mathrm{EPR}_q\rangle^{\otimes n}|\mathrm{AUX}\rangle\right\|^2 \leq \delta\,.$$

Moreover, an analogous relation holds for the second prover's operators.

The outline for the proof of Lemma 5.4.1 is as follows:

1. In Section 5.4.1, we describe the conditions satisfied by any strategy that succeeds with high probability in the test.

2. In Section 5.4.2, we adjoin an ancilla to each of the provers' private registers, and define a set of approximately commuting "points" observables $\hat{X}_u(x_\pi)$ and $\hat{Z}_u(z_\pi)$, for each $u \in \mathbb{F}_q$, that act on the original shared state tensored with a maximally entangled state on the ancilla.

3. In Section 5.4.3, we construct a family of joint measurements $\{\hat{Q}^c_{x,z}\}$ indexed by a pair of values $x, z \in \mathbb{F}_q^m$ and with outcomes $c \in \mathbb{F}_q$, obtained as a common refinement of the $2q$ approximately commuting observables $\hat{X}_u(x_\pi)$ and $\hat{Z}_v(z_\pi)$, for all $u, v \in \mathbb{F}_q$, defined in the previous step. Joint measurability is proved by showing that the observables satisfy approximate linearity relations, in the sense of implying a successful strategy in the two-prover linearity test from [NV17a].

4. From these joint measurements we define a strategy for the test C-LOWDEG$(2m+2, d+1, q)$ over $\mathbb{F}_q^m \times \mathbb{F}_q^m \times \mathbb{F}_q^2$, denoted by $\{\hat{Q}^r_s\}$. Applying Theorem 5.2.10, we deduce a single low-degree measurement $\{\hat{S}^g\}$.

5. We argue that g must take the form $g(x, z, \alpha, \beta) = \alpha g_1(x) + \beta g_2(z)$ for low-degree polynomials $g_1, g_2 : \mathbb{F}_q^m \to \mathbb{F}_q$. This allows us to recover commuting low-degree measurements $\{\hat{S}^{g_1}_X\}$ and $\{\hat{S}^{g_2}_Z\}$.

6. In Section 5.4.4 we use the low-degree measurements obtained in the previous step to recover observables $\tilde{X}_\ell(x)$ and $\tilde{Z}_{\ell'}(z)$ defined for all points $x, z \in \mathbb{F}_p^n$ and indices $\ell \in \{1, \ldots, t\}$. By construction these operators exactly satisfy the same twisted commutation relations as the "honest" generalized observables $\tau_X(b_\ell x)$ and $\tau_Z(b_{\ell'} z)$ (recall that $\{b_1, \ldots, b_t\}$ is a self-dual basis of $\mathbb{F}_q$ over $\mathbb{F}_p$); moreover, we show that they are consistent with the provers' original observables $X_{b_\ell}, Z_{b_{\ell'}}$ at points of the form x_π, z_π.

7. Finally, in Section 5.4.5, we use that $\tilde{X}_\ell(x) \otimes \tilde{X}_\ell(x)$ and $\tilde{Z}_{\ell'}(z) \otimes \tilde{Z}_{\ell'}(z)$ approximately stabilize $|\psi\rangle$ to conclude that the provers' shared state is close to the target state $|\mathrm{EPR}_q\rangle^{\otimes n}$ (under the action of the appropriate isometry).

5.4.1 Arbitrary strategies in the test Q-LOWDEG

We start with the following preliminary claim, which establishes basic properties of successful strategies in the test Q-LOWDEG(m, d, q).

Claim 5.4.2. *Let $m, d, q = p^t$, ε, $|\psi\rangle$ and $\{M^r_{W,s,s'}\}$ be as in Lemma 5.4.1. There exists $\delta_M = \mathrm{poly}(p) \cdot \mathrm{poly}(\varepsilon)$ such that the following hold. For $W \in \{X, Z\}$ and $s \subseteq \mathbb{F}_q^m$ there exist projective measurements $\{M^r_{W,s}\}_{r \in \deg_d(s)}$ and $\{\boldsymbol{M}^r_{W,s}\}_{r \in \deg_d(s)}$ such that, on average over $s \sim \pi_{\mathrm{ld}}$,*

$$M^r_{W,s} \otimes \mathrm{Id} \approx_{\delta_M} \mathrm{Id} \otimes \boldsymbol{M}^r_{W,s} \,, \tag{5.19}$$

and moreover the $\{M^r_{W,s}\}_{r \in \deg_d(s)}$ and $\{\boldsymbol{M}^r_{W,s}\}_{r \in \deg_d(s)}$, together with the state $|\psi\rangle$, specify a strategy with success $1 - \varepsilon'$ in the test Q-LOWDEG$^{(1)}(m, d, q)$*, for some $\delta = \mathrm{poly}(p) \cdot \mathrm{poly}(\varepsilon)$.*

For $W \in \{X, Z\}$, $u \in \mathbb{F}_q$, and $w \in \mathbb{F}_q^m$ define[4]

$$W_u(w_\pi) = \sum_a \omega^{\mathrm{tr}(au)} M^a_{W,w} \,, \qquad \boldsymbol{W}_u(w_\pi) = \sum_a \omega^{\mathrm{tr}(au)} \boldsymbol{M}^a_{W,w} \,. \tag{5.20}$$

Then for fixed W and w, the q observables $\{W_u(w_\pi),\, u \in \mathbb{F}_q\}$ pairwise commute. For any $a \in \mathbb{F}_q$, we can write the POVM elements $M^a_{W,w}$ and $\boldsymbol{M}^a_{W,w}$ in terms of the observables $W_u(w_\pi)$ and $\boldsymbol{W}_u(w_\pi)$ as follows:[5]

$$M^a_{W,w} = \mathop{\mathrm{E}}_{u \in \mathbb{F}_q} \omega^{-\mathrm{tr}(au)} W_u(w_\pi) \,, \qquad \boldsymbol{M}^a_{W,w} = \mathop{\mathrm{E}}_{u \in \mathbb{F}_q} \omega^{-\mathrm{tr}(au)} \boldsymbol{W}_u(w_\pi) \,. \tag{5.21}$$

Moreover, on average over $w \in \mathbb{F}_q^m$ and for every $u \in \mathbb{F}_q$,

$$W_u(w_\pi) \otimes \mathrm{Id} \approx_{\delta_M} \mathrm{Id} \otimes \boldsymbol{W}_u(w_\pi) \,. \tag{5.22}$$

Finally,

$$X_u(x_\pi) Z_{u'}(z_\pi) \approx_{\delta_M} \omega^{\mathrm{tr}((ux_\pi) \cdot (u' z_\pi))} Z_{u'}(z_\pi) X_u(x_\pi) \,, \tag{5.23}$$

on average over uniformly random $x, z \in \mathbb{F}_q^m$ and $u, u' \in \mathbb{F}_p^t$.

Proof. For $s \subseteq \mathbb{F}_q^m$, $s' \subseteq \mathbb{F}_q^{m'}$ and $r \in \deg_d(s)$ let

$$\boldsymbol{M}^r_{X,s,s'} = M^{-r}_{X,s,s'} \qquad \text{and} \qquad \boldsymbol{M}^r_{Z,s,s'} = M^r_{Z,s} \,.$$

With this definition, (5.19) follows from the assumption that the provers' strategy succeeds with probability $1 - O(\varepsilon)$ in part (a) of the test Q-LOWDEG$^{(2)}$. Moreover, for any fixed choice of W and first part s of the question (s, s') in C-LOWDEG$^{(2)}(m, d, q)$, the induced strategy is a successful strategy in C-LOWDEG$^{(1)}(m', d', q)$, to which Theorem 5.2.8 can be applied. This defines the required POVM elements $\{M^r_{W,s}\}_{r \in \deg_d(s)}$ and $\{\boldsymbol{M}^r_{W,s}\}_{r \in \deg_d(s)}$.

Commutation of the $\{W_u(w_\pi),\, u \in \mathbb{F}_q\}$ follows since $\{M^a_{W,w}\}$ are projective measurements. Eq. (5.21) follows by expanding $W_u(w_\pi)$ using the definition.

Using that the distribution π_{ld} from the low-degree test places constant probability on subspaces of dimension 0, by Claim 5.2.2 the consistency conditions (5.19)

[4]The map $w \mapsto w_\pi$ from $\mathbb{F}_q^m$ to $\mathbb{F}_q^n$ is defined in Section 5.2.

[5]Note that here, and elsewhere, the superscript denotes the outcome of the measurement, not exponentiation.

imply (5.22).

Finally, using Theorems 5.2.6 and 5.2.7 success with probability at least $1-\varepsilon$ in part (b) of the test implies that the observables defined in (5.20) satisfy (5.23) for $\delta_M = O(p^3\sqrt{\varepsilon})$. □

5.4.2 Expanding the Hilbert space and defining commuting observables

From the initial strategy of the provers, satisfying the properties expressed in Claim 5.4.2, we define new observables on an extended Hilbert space that will be the main operators used in the proof.

Lemma 5.4.3. *Let $m, d, q = p^t$, ε, $|\psi\rangle$ and $\{M^r_{W,s}\}$ be as in Lemma 5.4.1, and $W_u(w_\pi)$ as in Claim 5.4.2. There exists a state*

$$|\hat{\psi}\rangle_{AA'A''BB'B''} \in \mathcal{H}_A \otimes (\mathbb{C}^q_{A'} \otimes \mathbb{C}^q_{A''})^{\otimes n} \otimes \mathcal{H}_B \otimes (\mathbb{C}^q_{B'} \otimes \mathbb{C}^q_{B''})^{\otimes n} ,$$

and for $W \in \{X, Z\}$, $s \subseteq \mathbb{F}_q^m$, $u \in \mathbb{F}_q$, and $w \in \mathbb{F}_q^m$ there are POVM $\{\hat{M}^r_{W,s}\}_{r\in \deg_d(s)}$, $\{\hat{\boldsymbol{M}}^r_{W,s}\}_{r\in \deg_d(s)}$ and observables $\hat{W}_u(w_\pi)$, $\hat{\boldsymbol{W}}_u(w_\pi)$ on $\mathcal{H}_A \otimes (\mathbb{C}^q_{A'})^{\otimes n}$ and $\mathcal{H}_B \otimes (\mathbb{C}^q_{B'})^{\otimes n}$ respectively,

$$\hat{W}_u(w_\pi) = W_u(w_\pi) \otimes \boldsymbol{\tau}_W(uw_\pi) , \qquad \hat{\boldsymbol{W}}_u(w_\pi) = \boldsymbol{W}_u(w_\pi) \otimes \tau_W(uw_\pi) , \tag{5.24}$$

such that the following hold for some $\delta_{\hat{M}} = \mathrm{poly}(\delta_M)$. On average over $(s, w) \sim \pi_{\mathrm{ld}}$ and for any $u \in \mathbb{F}_q$ and $W \in \{X, Z\}$,

$$\begin{aligned}
(\hat{M}^r_{W,s})_{AA'} \otimes \mathrm{Id} &\approx_{\delta_{\hat{M}}} \mathrm{Id} \otimes (\hat{\boldsymbol{M}}^r_{W,s})_{BA''} , \\
\hat{W}_u(w_\pi)_{AA'} \otimes \mathrm{Id} &\approx_{\delta_{\hat{M}}} \mathrm{Id} \otimes \hat{\boldsymbol{W}}_u(w_\pi)_{BA''} , \\
\sum_{r\in \deg_d(s)} (\hat{M}^r_{W,s})_{AA'} \otimes (\hat{\boldsymbol{W}}_u^{\mathrm{tr}(r(w)u)}(w_\pi))_{BA''} &\approx_{\delta_{\hat{M}}} \mathrm{Id} , \\
\sum_{r\in \deg_d(s)} (\hat{M}^r_{W,s})_{AA'} \otimes (\hat{\boldsymbol{M}}^{r(w)}_{W,w})_{BA''} &\approx_{\delta_{\hat{M}}} \mathrm{Id} ,
\end{aligned} \tag{5.25}$$

where

$$\hat{M}^a_{W,w} = \mathop{\mathrm{E}}_{u\in\mathbb{F}_q} \omega^{-\mathrm{tr}(au)} \hat{W}_u(w_\pi) , \qquad \hat{\boldsymbol{M}}^a_{W,w} = \mathop{\mathrm{E}}_{u\in\mathbb{F}_q} \omega^{-\mathrm{tr}(au)} \hat{\boldsymbol{W}}_u(w_\pi) . \tag{5.26}$$

Finally, on average over uniformly random $x, z \in \mathbb{F}_q^m$ and $u, u' \in \mathbb{F}_q$,

$$\hat{X}_u(x_\pi)\hat{Z}_{u'}(z_\pi) \approx_{\delta_{\hat{M}}} \hat{Z}_{u'}(z_\pi)\hat{X}_u(x_\pi) . \tag{5.27}$$

Proof. We first define the state $|\hat{\psi}\rangle$. For this we enlarge the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$ in two ways. First we assume that each prover has access to a sufficiently large number N of qubits initialized in the state $|0\rangle$. This allows us to apply Naimark's dilation

theorem to simulate a POVM measurement applied by the provers by a projective measurement, whenever it is convenient (we will always specify when we do so). Second, for each prover $D \in \{A, B\}$ we adjoin two ancilla registers $\mathsf{D'}, \mathsf{D''}$ initialized in state

$$|\psi_{\mathrm{EPR}}\rangle_{\mathsf{D'D''}} = |\mathrm{EPR}_q\rangle_{\mathsf{D'D''}}^{\otimes n} ,$$

where $|\mathrm{EPR}_q\rangle$ is defined in (5.3). The state of the enlarged system is

$$|\hat{\psi}\rangle_{\mathsf{AA'A''BB'B''}} = \left(|\psi\rangle \otimes |0\rangle^{\otimes 2N}\right)_{\mathsf{AB}} |\psi_{\mathrm{EPR}}\rangle_{\mathsf{A'A''}} |\psi_{\mathrm{EPR}}\rangle_{\mathsf{B'B''}} . \tag{5.28}$$

Next, for $W \in \{X, Z\}$, $s \subset \mathbb{F}_q^m$ and $r \in \deg_d(s')$ let

$$\hat{M}_{W,s}^r = \sum_{\substack{r',r'' \in \deg_d(s): \\ r'+r''=r}} M_{W,s}^{r'} \otimes \boldsymbol{\tau}_{W,s}^{r''} , \tag{5.29}$$

where $\{\tau_{W,s}^{r''}\}$ is the "honest" subspace measurement defined in (5.14). Define complementary measurements

$$\hat{\boldsymbol{M}}_{W,s}^r = \sum_{\substack{r',r'' \in \deg_d(s): \\ r'+r''=r}} \boldsymbol{M}_{W,s}^{r'} \otimes \tau_{W,s}^{r''} .$$

The following claim establishes (5.25).

Claim 5.4.4. *For $W \in \{X, Z\}$ the subspace measurements are self-consistent, and consistent with the point measurements: on average over $(s, w) \sim \pi_{\mathrm{ld}}$ and for any $u \in \mathbb{F}_q$,*

$$\begin{aligned}
\sum_{r \in \deg_d(s)} \left(\hat{M}_{W,s}^r\right)_{\mathsf{AA'}} \otimes \left(\hat{\boldsymbol{M}}_{W,s}^r\right)_{\mathsf{BA''}} &\approx_{\mathrm{poly}(\delta_M)} \mathrm{Id} , \\
\sum_{r \in \deg_d(s)} \left(\hat{M}_{W,s}^r\right)_{\mathsf{AA'}} \otimes \left(\hat{\boldsymbol{W}}_u^{\mathrm{tr}(r(w)u)}(w_\pi)\right)_{\mathsf{BA''}} &\approx_{\mathrm{poly}(\delta_M)} \mathrm{Id} , \\
\sum_{r \in \deg_d(s)} \left(\hat{M}_{W,s}^r\right)_{\mathsf{AA'}} \otimes \left(\hat{\boldsymbol{M}}_{W,w}^{r(w)}\right)_{\mathsf{BA''}} &\approx_{\delta_{\hat{M}}} \mathrm{Id} ,
\end{aligned}$$

and

$$\hat{W}_u(w_\pi)_{\mathsf{AA'}} \otimes \mathrm{Id} \approx_{\mathrm{poly}(\delta_M)} \mathrm{Id} \otimes \hat{\boldsymbol{W}}_u(w_\pi)_{\mathsf{BA''}} .$$

Proof. Note that $\{\hat{M}_{W,w}^a\}$ as defined in (5.26) is a well-defined projective measurement, given the definition of the $\{\hat{W}_u(w_\pi)\}$ in (5.24).

For the first identity, decompose $\hat{M}_{W,s}^r$ using the definition (5.29) and use self-consistency of $M_{W,s}^{r'}$, which is expressed in (5.19), and of $\tau_{W,s}^{r''}$, which follows since the ancilla introduced in (5.28) is maximally entangled on $\mathsf{A'A''}$.

For the second identity, decompose $\hat{M}_{W,s}^r$ and $\hat{W}_u^{\mathrm{tr}(ur(w))}(w_\pi)$ using the definition

to get

$$\begin{aligned}
&\sum_{r\in\deg_d(s)} \hat{M}^r_{W,s}\otimes \hat{\boldsymbol{W}}_u^{\mathrm{tr}(ur(w))}(w_\pi)\\
&\quad= \sum_{\substack{r',r'',a',a'':\\ \mathrm{tr}((r'+r'')(w)\cdot u)=(a'+a'')}} \left(M^{r'}_{W,s}\right)_{\mathsf{A}}\otimes\left(\boldsymbol{\tau}^{r''}_{W,s}\right)_{\mathsf{A}'}\otimes\left(\boldsymbol{W}_u^{a'}(w_\pi)\right)_{\mathsf{B}}\otimes\left(\tau_W^{a''}(uw_\pi)\right)_{\mathsf{A}''}\\
&\quad= \sum_{\substack{r',a':\\ \mathrm{tr}(r'(w)\cdot u)=a'}} \left(M^{r'}_{W,s}\right)_{\mathsf{A}}\otimes\left(\boldsymbol{W}_u^{a'}(w_\pi)\right)_{\mathsf{B}}\\
&\quad\approx_{\mathrm{poly}(\varepsilon)} \mathrm{Id}\ ,
\end{aligned}$$

where the second line uses consistency of $\boldsymbol{\tau}^{r''}_{W,s}$ with $\tau_W^{\mathrm{tr}(ur''(w))}(uw_\pi)$ (which follows from the analysis of the honest strategy given in the proof of Lemma 5.3.4), and the third follows from success of the provers' strategy in the low-degree test and the definition of $\boldsymbol{W}_u(w_\pi)$ in (5.20).

The third identity follows from the second and the definition (5.26).

Finally, the last relation follows from the first, specialized to $s = w$. Alternatively, combine consistency between W_{A} and $\boldsymbol{W}_{\mathsf{B}}$ (shown in (5.22)) and of $(\tau_W)_{\mathsf{A}'}$ and $(\boldsymbol{\tau}_W)_{\mathsf{A}''}$, which follows since the ancilla state is $|\psi_{\mathrm{EPR}}\rangle_{\mathsf{A}'\mathsf{A}''}$. □

The next claim establishes (5.27).

Claim 5.4.5. *On average over uniformly random $x, z \in \mathbb{F}_q^m$ and $u, u' \in \mathbb{F}_q$,*

$$\hat{X}_u(x_\pi)\hat{Z}_{u'}(z_\pi) \approx_{\mathrm{poly}(\delta_M)} \hat{Z}_{u'}(z_\pi)\hat{X}_u(x_\pi)\ .$$

Proof. Write

$$\begin{aligned}
\hat{X}_u(x_\pi)\hat{Z}_{u'}(z_\pi) &= X_u(x_\pi)Z_{u'}(z_\pi)\otimes\boldsymbol{\tau}_X(ux_\pi)\boldsymbol{\tau}_Z(u'z_\pi)\\
&= X_u(x_\pi)Z_{u'}(z_\pi)\otimes\tau_X(-ux_\pi)\tau_Z(u'z_\pi)\\
&\approx_{\delta_M} \left(\omega^{-\mathrm{tr}((ux_\pi)\cdot(u'z_\pi)}Z_{u'}(z_\pi)X_u(x_\pi)\right)\otimes\left(\omega^{\mathrm{tr}((ux_\pi)\cdot(u'z_\pi))}\tau_Z(u'z_\pi)\tau_X(-ux_\pi)\right)\\
&= Z_{u'}(z_\pi)X_u(x_\pi)\otimes\boldsymbol{\tau}_Z(u'z_\pi)\boldsymbol{\tau}_X(ux_\pi)\\
&= \hat{Z}_{u'}(z_\pi)\hat{X}_u(x_\pi)\ ,
\end{aligned}$$

where the approximation follows from (5.23) in Claim 5.4.2. □

□

5.4.3 Combining X and Z measurements

In this section we combine the approximately commuting observables $\hat{X}_u(x_\pi)$ and $\hat{Z}_u(z_\pi)$ constructed in the proof of Lemma 5.4.3 into a single POVM. We then show

that the POVM leads to a strategy for the classical low-degree test. Applying Theorem 5.2.8, we obtain a single POVM $\{\hat{S}^{g_1,g_2}\}_{g_1,g_2\in\deg_d(s)}$ which is simultaneously consistent with both families of observables, as shown in the following lemma.

Lemma 5.4.6. *Let $m, d, q = p^t$ be as in Lemma 5.4.1, and $|\hat{\psi}\rangle$, $\hat{W}_u(w_\pi)$, $\hat{\boldsymbol{W}}_u(w_\pi)$ and $\delta_{\hat{M}}$ as in Lemma 5.4.3. There exists projective measurements $\{\hat{S}^{g_1,g_2}_{AA'}\}$ and $\{\hat{\boldsymbol{S}}^{g_1,g_2}_{BA''}\}$ with outcomes in the set of pairs (g_1, g_2) of polynomials on $\mathbb{F}_q^m$ of total degree at most d each such that, on average over uniformly random $x, z \in \mathbb{F}_q^m$, and for all $u \in \mathbb{F}_q$,*

$$\sum_{g_1,g_2} \hat{S}^{g_1,g_2} \otimes \hat{\boldsymbol{X}}_u^{\mathrm{tr}(g_1(x)u)}(x_\pi) \approx_{\delta_S} \mathrm{Id}\,, \qquad \sum_{g_1,g_2} \hat{S}^{g_1,g_2} \otimes \hat{\boldsymbol{Z}}_u^{\mathrm{tr}(g_2(z)u)}(z_\pi) \approx_{\delta_S} \mathrm{Id}\,, \quad (5.30)$$

for some $\delta_S = \mathrm{poly}(p)\cdot\mathrm{poly}(\delta_{\hat{M}}) + \mathrm{poly}(d/q)$. Similar relations hold with $\hat{\boldsymbol{S}}$ and $\hat{X}$, $\hat{Z}$ instead of S and $\hat{\boldsymbol{X}}$, $\hat{\boldsymbol{Z}}$ respectively.

The proof of Lemma 5.4.6 proceeds in two steps. In the first step, for each pair $(u, v) \in \mathbb{F}_q^2$ we combine the approximately commuting observables $\hat{X}_u(x_\pi)$ and $\hat{Z}_v(z_\pi)$ into a single POVM $\{\hat{Q}^{a,b}_{xu,zv}\}$ that essentially measures in their joint eigenbasis. The following lemma shows how this can be done in general. (See [Gle10] for a similar claim that applies to arbitrary unitaries but is restricted to the Frobenius norm.)

Lemma 5.4.7. *Let $\eta > 0$, $|\psi\rangle \in \mathcal{H}\otimes\mathcal{H}'$, for finite-dimensional Hilbert spaces $\mathcal{H}, \mathcal{H}'$, and $W_j \in \mathrm{U}(\mathcal{H})$, $\boldsymbol{W}_j \in \mathrm{U}(\mathcal{H}')$, for $j = 1, \ldots, k$, be such that for all $j, \ell \in \{1, \ldots, k\}$, the powers $(W_j)^p = (\boldsymbol{W}_j)^p = \mathrm{Id}$, $\|(W_j \otimes \mathrm{Id} - \mathrm{Id}\otimes\boldsymbol{W}_j)|\psi\rangle\|^2 \leq \eta$, and $\|(W_jW_\ell - W_\ell W_j)\otimes \mathrm{Id}\,|\psi\rangle\|^2 \leq \eta$. Then there exists an $\eta' = \mathrm{poly}(p,k)\cdot\mathrm{poly}(\eta)$ and a POVM $\{Q^a\}_{a\in\mathbb{F}_p^k}$ such that*

$$Q^a \approx_{\eta'} \prod_j W_j^{a_j} \qquad \text{and} \qquad \forall j,\quad W_j \approx_{\eta'} \sum_a \omega^{a_j} Q^a\,,$$

where $W_j^{a_j}$ is the projector onto the eigenspace of W_j associated with the eigenvalue ω^{a_j}. Moreover, there exists a projective measurement $\{\boldsymbol{Q}^a\}_{a\in\mathbb{F}_p^k}$ satisfying analogous relations with respect to $\boldsymbol{W}_j$ and which is consistent with $\{Q^a\}$:

$$Q^a \otimes \mathrm{Id} \approx_{\eta'} \mathrm{Id}\otimes\boldsymbol{Q}^a\,.$$

Proof. Write the eigendecompositions

$$W_j = \sum_{a_j\in\mathbb{F}_p} \omega^{a_j} W^{a_j}\,, \qquad \boldsymbol{W}_j = \sum_{a_j\in\mathbb{F}_p} \omega^{a_j} \boldsymbol{W}^{a_j}\,,$$

where $\omega = e^{2i\pi/p}$. Using Claim 5.2.2 the consistency assumption on W_j implies that $\{W_j^{a_j}\}$ and $\{\boldsymbol{W}_j^{a_j}\}$ are also consistent projective measurements, with error $O(p^2\eta)$. We use the following general claim.

Claim 5.4.8. *Let $\{P^a\}$ and $\{Q^b\}$, and $\{\boldsymbol{P}^a\}$ and $\{\boldsymbol{Q}^b\}$, be projective measurements with outcomes $a, b \in \mathbb{F}_p$ for a prime p and such that $P^a\otimes\mathrm{Id} \approx_\eta \mathrm{Id}\otimes\boldsymbol{P}^a$ and $Q^b\otimes\mathrm{Id} \approx_\eta$*

$\mathrm{Id} \otimes \boldsymbol{Q}^b$ *for some* $\eta \geq 0$. *Let* $P = \sum_a \omega^a P^a$ *and* $Q = \sum_b \omega^b Q^b$. *Then*

$$\sum_{a,b} \left\| (P^a Q^b - Q^b P^a) \otimes \mathrm{Id} \, |\psi\rangle \right\|^2 \approx_{\mathrm{poly}(\eta)} O\Big(p^2 \left\| (PQ - QP) \otimes \mathrm{Id} \, |\psi\rangle \right\|^2 \Big) .$$

Proof. Expand

$$\begin{aligned}
&\langle\psi| (PQ - QP)(PQ - QP)^\dagger \otimes \mathrm{Id} \, |\psi\rangle \\
&\quad = 2 - \sum_{a,b,c,d} \omega^{a+b-(c+d)} \langle\psi| \big(P^a Q^b P^c Q^d + Q^a P^b Q^c P^d \big) \otimes \mathrm{Id} \, |\psi\rangle \\
&\quad \approx_{\mathrm{poly}(\eta)} 2 - \langle\psi| \Big(\sum_a \omega^a P^a \Big) \otimes \Big(\sum_{b,c,d} \omega^{b-(c+d)} \boldsymbol{Q}^d \boldsymbol{P}^c \boldsymbol{Q}^b \Big) |\psi\rangle \\
&\qquad\qquad - \langle\psi| \Big(\sum_a \omega^{-a} P^a \Big) \otimes \Big(\sum_{b,c,d} \omega^{-b+(c+d)} \boldsymbol{Q}^b \boldsymbol{P}^c \boldsymbol{Q}^d \Big) |\psi\rangle \, . \qquad (5.31)
\end{aligned}$$

Let $\delta = \frac{1}{2} \| (PQ - QP) \otimes \mathrm{Id} \, |\psi\rangle \|^2$. From (5.31) we get the consistency relation

$$\frac{1}{2} \sum_{a,b,c,d} \langle\psi| \big(\omega^{(a-c)+(b-d)} Q^d P^c Q^b + \omega^{(c-a)+(d-b)} Q^b P^c Q^d \big) \otimes \boldsymbol{P}^a |\psi\rangle \approx_{\mathrm{poly}(\eta)} 1 - O(\delta) \, .$$

We now repeat this argument, but replacing the observable Q with its power $(Q)^\alpha$ for $\alpha \in \mathbb{F}_p$ (not to be confused with the POVM element Q^a). Starting from $\| (P(Q)^\alpha - (Q)^\alpha P) \otimes \mathrm{Id} \, |\psi\rangle \|^2 = O(p\delta)$ for any $\alpha \in \mathbb{F}_p$ gives

$$\frac{1}{2} \sum_{a,b,c,d} \langle\psi| \big(\omega^{(a-c)+\alpha(b-d)} Q^d P^c Q^b + \omega^{(c-a)+\alpha(d-b)} Q^b P^c Q^d \big) \otimes \boldsymbol{P}^a |\psi\rangle \approx_{\mathrm{poly}(\eta)} 1 - O(p\delta) \, .$$

Averaging the relations over all $\alpha \in \mathbb{F}_p$ and using that $(b-d)\mathbb{F}_p = \mathbb{F}_p$ if $b - d \neq 0$ and $\{0\}$ otherwise yields

$$\frac{1}{2} \sum_{a,b,c} \langle\psi| \big(\omega^{a-c} + \omega^{c-a} \big) Q^b P^a Q^b \otimes \boldsymbol{P}^a |\psi\rangle \approx_{\mathrm{poly}(\eta)} 1 - O(p^2\delta) \, .$$

Using $|\omega^{a-c} + \omega^{c-a}| \leq 2 - \Omega(1/p)$ for $a \neq c$ proves the claim. □

We define the POVM elements $\{Q^a\}$ as

$$Q^a \;=\; W_k^{a_k} \cdots W_1^{a_1} \cdots W_k^{a_k} \, ,$$

and define $\{\boldsymbol{Q}^a\}$ analogously. The two relations in the lemma then follow from the definition, the fact that $\{W_j^{a_j}\}$ are projections, and Claim 5.4.8; similarly, consistency of $\{Q^a\}$ follows. □

Lemma 5.4.7 allows us to combine any pair of approximately commuting observables $\hat{X}_u(x_\pi)$ and $\hat{Z}_v(z_\pi)$ into a single POVM $\{\hat{Q}^{a,b}_{xu,zv}\}$, with outcomes $(a, b) \in \mathbb{F}_p^2$, that simultaneously refines both observables. In the following lemma we show that all

$\{\hat{Q}^{a,b}_{xu,zv}\}$, for $u, v \in \mathbb{F}_q$, can be pieced together into a single POVM $\{\hat{Q}^{a,b}_{xz}\}$ with outcomes $(a, b) \in \mathbb{F}_q^2$ which simultaneously refines all $2q$ observables $\hat{X}_u(x_\pi)$ and $\hat{Z}_v(z_\pi)$. Note that this is not trivial because we wish to avoid any dependence on q when combining the $2q$ approximately commuting observables. To achieve this, we rely on the linearity test from [NV17a].

Lemma 5.4.9. *For every $x, z \in \mathbb{F}_q^m$ there are projective measurements $\{\hat{Q}^{a,b}_{xz}\}_{a,b\in\mathbb{F}_q^2}$ and $\{\hat{\boldsymbol{Q}}^{a,b}_{xz}\}_{a,b\in\mathbb{F}_q^2}$ defined on AA′ and BA″ respectively such that the following hold, for some $\delta_Q = \mathrm{poly}(p) \cdot \mathrm{poly}(\delta_{\hat{M}})$:*

1. *The $\hat{Q}_{xz}$ are consistent with the $\hat{\boldsymbol{Q}}_{xz}$:*

$$\sum_{a,b} \left(\hat{Q}^{a,b}_{xz}\right)_{AA'} \otimes \left(\hat{\boldsymbol{Q}}^{a,b}_{xz}\right)_{BA''} \approx_{\delta_Q} \mathrm{Id} \,,$$

   on average over uniformly random $x, z \in \mathbb{F}_q^m$.

2. *The $\hat{Q}_{xz\alpha\beta}$ are consistent with $\hat{\boldsymbol{M}}_{X,x}$ and $\hat{\boldsymbol{M}}_{Z,z}$:*

$$\sum_{a,b} \left(\hat{Q}^{a,b}_{xz}\right)_{AA'} \otimes \left(\hat{\boldsymbol{M}}^{a}_{X,x}\hat{\boldsymbol{M}}^{b}_{Z,z}\right)_{BA''} \approx_{\delta_Q} \mathrm{Id} \,,$$

   on average over uniformly random $x, z \in \mathbb{F}_q^m$.

Proof. For every $x, z \in \mathbb{F}_q^m$ and $u, v \in \mathbb{F}_q$ we let $\{\hat{Q}^{a,b}_{xu,zv}\}_{a,b\in\mathbb{F}_p}$ and $\{\hat{\boldsymbol{Q}}^{a,b}_{xu,zv}\}_{a,b\in\mathbb{F}_p}$ be the projective measurements guaranteed by Lemma 5.4.7 when the observables P and Q are chosen as $\hat{X}_u(x_\pi)$ and $\hat{Z}_v(z_\pi)$ respectively; the assumptions of the lemma are satisfied by (5.25) and (5.27). We also define, for $c \in \mathbb{F}_p$,

$$\hat{Q}^{c}_{xu,zv} = \sum_{a,b:\, a+b=c} \hat{Q}^{a,b}_{xu,zv} \,, \tag{5.32}$$

and similarly define associated measurements $\{\hat{\boldsymbol{Q}}^{c}_{xu,zv}\}_{c\in\mathbb{F}_p}$. In the following claim we identify $\mathbb{F}_q$ with the vector space $\mathbb{F}_p^t$ to interpret this family of measurements as a strategy in the linearity test over $\mathbb{F}_p^{2t}$, with the queries specified by $(u, v) \in \mathbb{F}_p^{2t}$ and the answers $c \in \mathbb{F}_p$.

Claim 5.4.10. *On average over $x, z \in \mathbb{F}_q^m$ the family of projective measurements $\{\hat{Q}^{c}_{xu,zv}\}_{c\in\mathbb{F}_p}$, indexed by $(u, v) \in \mathbb{F}_p^{2t}$, together with $\{\hat{\boldsymbol{Q}}^{c}_{xu,zv}\}_{c\in\mathbb{F}_p}$, induces a strategy with success probability at least $1 - \mathrm{poly}(\delta_{\hat{M}})$ in the two-prover linearity test from [NV17a, Section 3].*

Proof. Consistency between $\hat{Q}^{c}_{xu,zv}$ and $\hat{\boldsymbol{Q}}^{c}_{xu,zv}$ is clear by the definition and Lemma 5.4.7. We need to verify (approximate) linearity. First note that from the definition of the observables $\hat{W}_u$ in (5.24), using that the underlying measurements are projective it follows that for $W \in \{X, Z\}$ the family of observables $\{\hat{W}_u(w_\pi)\}_{u\in\mathbb{F}_p^t}$ is linear, in the sense that for any $u, u' \in \mathbb{F}_p^t$, $\hat{W}_u(w_\pi)\hat{W}_{u'}(w_\pi) = \hat{W}_{u+u'}(w_\pi)$, where $u + u'$ is addition

as elements of the vector space $\mathbb{F}_p^t$. Using Lemma 5.4.7 it follows that $\{\hat{Q}^c_{xu,zv}\}$ is approximately linear in both u and v, i.e.

$$\mathop{\mathrm{E}}_{u,u',v,v'} \sum_{c,c'} \hat{Q}^c_{xu,zv}\hat{Q}^{c'}_{xu',zv'} \otimes \hat{\boldsymbol{Q}}^{c+c'}_{x(u+u'),z(v+v')} \approx_{\mathrm{poly}(p,\delta_{\hat{M}})} \mathrm{Id} \ .$$

Linearity for $\{\hat{Q}^c_{xu,zv}\}$ then follows directly from the definition (5.32). □

Applying [NV17a, Theorem 10] for every x, z we find a single POVM $\{\hat{Q}^{a,b}_{x,z}\}_{a,b\in\mathbb{F}_q^2}$ such that, on expectation over $u, v \in \mathbb{F}_p^t$, $\hat{Q}^e_{xu,zv} \approx \sum_{a,b:\,\mathrm{tr}(a\cdot u+b\cdot v)=e} \hat{Q}^{a,b}_{x,z}$.[6] Similarly, there exists a $\{\hat{\boldsymbol{Q}}^{a,b}_{x,z}\}_{a,b\in\mathbb{F}_q^2}$ that is consistent with $\{\hat{Q}^{a,b}_{x,z}\}_{a,b\in\mathbb{F}_q^2}$. The first item in the lemma now follows immediately from the consistency guarantees of the linearity test.

For the second item, note that from Lemma 5.4.7 and the guarantees of the linearity test, it follows that $\hat{Q}^{(a,b)}_{x,z}$ is approximately consistent with a randomly chosen product of $\hat{\boldsymbol{X}}_{\boldsymbol{u}}$ and $\hat{\boldsymbol{Z}}_{\boldsymbol{v}}$ POVM elements.

$$\begin{aligned}
\mathrm{Id} &\approx_{\delta'_{\hat{M}}} \mathop{\mathrm{E}}_{u,v} \sum_{(a,b)} (\hat{Q}^{a,b}_{x,z})_{\mathsf{AA'}} \otimes \Big(\sum_{c,d:\mathrm{tr}(au+bv)=c+d} \hat{\boldsymbol{X}}^c_u(x_\pi)\hat{\boldsymbol{Z}}^d_v(z_\pi) \Big)_{\mathsf{BA''}} \\
&= \mathop{\mathrm{E}}_{u,v} \sum_{(a,b)} (\hat{Q}^{a,b}_{x,z})_{\mathsf{AA'}} \otimes \Big(\sum_{a',b':\mathrm{tr}(au+bv)=\mathrm{tr}(a'u+b'v)} \hat{\boldsymbol{M}}^{a'}_{X,x}\hat{\boldsymbol{M}}^{b'}_{Z,z} \Big)_{\mathsf{BA''}} \\
&= \sum_{(a,b)} (\hat{Q}^{a,b}_{x,z})_{\mathsf{AA'}} \otimes \Big(\mathop{\mathrm{E}}_{u,v} \sum_{a',b'} 1_{\mathrm{tr}(au+bv)=\mathrm{tr}(a'u+b'v)} \hat{\boldsymbol{M}}^{a'}_{X,x}\hat{\boldsymbol{M}}^{b'}_{Z,z} \Big)_{\mathsf{BA''}} \\
&= \sum_{(a,b)} (\hat{Q}^{a,b}_{x,z})_{\mathsf{AA'}} \otimes \Big(\hat{\boldsymbol{M}}^{a}_{X,x}\hat{\boldsymbol{M}}^{b}_{Z,z} + \frac{1}{p}(\mathrm{Id} - \hat{\boldsymbol{M}}^{a}_{X,x}\hat{\boldsymbol{M}}^{b}_{Z,z}) \Big)_{\mathsf{BA''}} \\
&= \frac{1}{p}\mathrm{Id} + \Big(1 - \frac{1}{p}\Big) \sum_{(a,b)} (\hat{Q}^{a,b}_{x,z})_{\mathsf{AA'}} \otimes \Big(\hat{\boldsymbol{M}}^{a}_{X,x}\hat{\boldsymbol{M}}^{b}_{Z,z} \Big)_{\mathsf{BA''}} ,
\end{aligned}$$

where in the second to last equation we used the fact that any two distinct linear functions from $\mathbb{F}_p^{2t}$ to $\mathbb{F}_p$ agree with probability $1/p$. Moving the term proportional to Id to the left hand side, we obtain

$$\mathrm{Id} \approx_{O(\delta'_{\hat{M}})} \sum_{a,b} (\hat{Q}^{a,b}_{x,z})_{\mathsf{AA'}} \otimes \Big(\hat{\boldsymbol{M}}^{a}_{X,x}\hat{\boldsymbol{M}}^{b}_{Z,z} \Big)_{\mathsf{BA''}} ,$$

which is the desired consistency expression. □

For a subsequent application of the low-degree test it is more convenient to have a POVM which takes values $c \in \mathbb{F}_q$, rather than $(a, b) \in \mathbb{F}_q^2$. In order not to lose information, the following lemma re-arranges $\hat{Q}^{a,b}_{xz}$ into a family of POVMs $\{\hat{Q}^c_{xz\alpha\beta} = \sum_{a,b:\,\alpha a+\beta b=c} \hat{Q}^{a,b}_{xz}\}$, and shows that this family obeys similar consistency properties.

[6] The results in [NV17a, Theorem 10] apply to the analysis of the linearity test over $\mathbb{F}_2^{2t}$, i.e. the case $p = 2$ here. The same proof extends with, minor modifications, to the case of arbitrary prime p. We omit the details.

Lemma 5.4.11. *For every $\alpha, \beta \in \mathbb{F}_q$ and $x, z \in \mathbb{F}_q^m$ there are projective measurements $\{\hat{Q}^c_{xz\alpha\beta}\}_{c\in\mathbb{F}_q}$ and $\{\hat{\boldsymbol{Q}}^c_{xz\alpha\beta}\}_{c\in\mathbb{F}_q}$ defined on AA' and BA'' respectively such that the following hold, for δ_Q as in Lemma 5.4.9:*

1. *The $\hat{Q}_{xz\alpha\beta}$ are consistent with the $\hat{\boldsymbol{Q}}_{xz\alpha\beta}$:*

$$\sum_c \left(\hat{Q}^c_{xz\alpha\beta}\right)_{AA'} \otimes \left(\hat{\boldsymbol{Q}}^c_{xz\alpha\beta}\right)_{BA''} \approx_{\delta_Q} \mathrm{Id} \,,$$

   on average over uniformly random $\alpha, \beta \in \mathbb{F}_q$ and $x, z \in \mathbb{F}_q^m$.

2. *The $\hat{Q}_{xz\alpha\beta}$ are consistent with $\hat{\boldsymbol{M}}_{X,x}$ and $\hat{\boldsymbol{M}}_{Z,z}$:*

$$\sum_c \left(\hat{Q}^c_{xz\alpha\beta}\right)_{AA'} \otimes \Big(\sum_{\substack{a,a':\\ \alpha a+\beta a'=c}} \hat{\boldsymbol{M}}^a_{X,x} \hat{\boldsymbol{M}}^{a'}_{Z,z} \Big)_{BA''} \approx_{\delta_Q} \mathrm{Id} \,,$$

   on average over uniformly random $\alpha, \beta \in \mathbb{F}_q$ and $x, z \in \mathbb{F}_q^m$.

Proof. Let $\hat{Q}^{a,b}_{x,z}$ and $\hat{\boldsymbol{Q}}^{a,b}_{x,z}$ be the families of POVMs guaranteed by Lemma 5.4.9. We "collapse" the $\hat{Q}$ (and analogously, the $\hat{\boldsymbol{Q}}$) into a family of measurements with outcomes in $\mathbb{F}_q$ by defining, for every $\alpha, \beta \in \mathbb{F}_q$, $x, z \in \mathbb{F}_q^m$ and $c \in \mathbb{F}_q$,

$$\hat{Q}^c_{xz\alpha\beta} = \sum_{a,b:\, \alpha a+\beta b=c} \hat{Q}^{a,b}_{x,z} \,. \tag{5.33}$$

With this definition, both items in the claim follows from the definition (5.33) and corresponding items of Lemma 5.4.9.

□

The next step in the proof of Lemma 5.4.6 is to use the family of measurements $\{\hat{Q}^c_{xz\alpha\beta}\}$ to devise a strategy for the provers in the classical $(2m+2)$-variable degree-$(d+1)$ test. Towards this the following claim establishes the existence of appropriate subspace measurements.

Claim 5.4.12. *For every dimension-2 subspace $s \subseteq \mathbb{F}_q^{2m+2}$ there exists a POVM $\{\hat{Q}^r_s\}_r$, with outcomes $r \in \deg_{d+1}(s)$, such that, on average over a uniformly random s and $(x, z, \alpha, \beta) \in s$,*

$$\sum_{r,c:\, r(x,z,\alpha,\beta)\neq c} \langle\psi|\hat{Q}^r_s \otimes \hat{\boldsymbol{Q}}^c_{xz\alpha\beta}|\psi\rangle = \mathrm{poly}(\delta_Q) + O\big(d/q\big) \,.$$

Likewise, there exists $\{\hat{\boldsymbol{Q}}^r_s\}$ that are consistent with $\{\hat{Q}^c_{xz\alpha\beta}\}$, on average.

Proof. The argument is entirely symmetric between $\hat{Q}$ and $\hat{\boldsymbol{Q}}$. We give the construction for $\hat{Q}$.

Let $s \subset \mathbb{F}_q^{2m+2}$ be a two-dimensional linear subspace spanned by two vectors $y_1 = (x_1, z_1, \alpha_1, \beta_1), y_2 = (x_2, z_2, \alpha_2, \beta_2) \in \mathbb{F}_q^{2m+2}$. Let $s', s'' \subset \mathbb{F}_q^m$ be the (at most)

two-dimensional subspaces spanned by $\{x_1, x_2\}$ and $\{z_1, z_2\}$ respectively. Any point (λ, μ) in the subspace s corresponds to a point in the full space

$$\#(\lambda, \mu) = (\lambda x_1 + \mu x_2, \lambda z_1 + \mu z_2, \lambda \alpha_1 + \mu \alpha_2, \lambda \beta_1 + \mu \beta_2).$$

Let $g(x, y, \alpha, \beta) = \alpha p(x) + \beta q(y)$ be a $2m + 2$-variate polynomial. Its restriction r to the subspace s takes the values

$$r(\lambda, \mu) = g(\#(\lambda, \mu)) = (\lambda \alpha_1 + \mu \alpha_2) p(\lambda x_1 + \mu x_2) + (\lambda \beta_1 + \mu \beta_2) q(\lambda z_1 + \mu z_2).$$

From this expression, we see that r can be evaluated if we have access to the restrictions of p to s' and q to s'', respectively. We will now construct a measurement that, given s', s'' as input, jointly measures p and q in a manner that is consistent with the joint points measurement $\{\hat{Q}^{a,b}_{xz}\}$ guaranteed by Lemma 5.4.9. Define

$$T^{p,q}_{s',s''} = \hat{M}^p_{X,s'} \hat{M}^q_{Z,s''} \hat{M}^p_{X,s'}. \tag{5.34}$$

The collection $\{T^{p,q}_{s',s''}\}_{p,q}$ forms a valid POVM. Its inconsistency with $\hat{Q}^{a,b}_{xz}$ is:

$$\begin{aligned}
&\mathop{\mathrm{E}}_{s',s''} \mathop{\mathrm{E}}_{x \in s', z \in s''} \sum_{\substack{a,b,p,q: \\ (a,b) \neq (f(x),q(z))}} \langle \psi | T^{p,q}_{s',s''} \otimes \hat{\boldsymbol{Q}}^{a,b}_{xz} | \psi \rangle \\
&= \mathop{\mathrm{E}}_{s',s''} \mathop{\mathrm{E}}_{x \in s', z \in s''} \sum_{\substack{a,b,p,q: \\ (a,b) \neq (p(x),q(z))}} \langle \psi | \hat{M}^p_{X,s'} \hat{M}^q_{Z,s''} \hat{M}^p_{X,s'} \otimes \hat{\boldsymbol{Q}}^{a,b}_{xz} | \psi \rangle \\
&= 1 - \mathop{\mathrm{E}}_{s',s''} \sum_{p,q} \mathop{\mathrm{E}}_{x \in s', z \in s''} \langle \psi | \hat{M}^p_{X,s'} \hat{M}^q_{Z,s''} \hat{M}^p_{X,s'} \otimes \hat{\boldsymbol{Q}}^{p(x),q(z)}_{xz} | \psi \rangle \\
&\leq 1 - \mathop{\mathrm{E}}_{s',s''} \sum_{p,q,p'} \mathop{\mathrm{E}}_{x \in s', z \in s''} \langle \psi | \hat{M}^p_{X,s'} \hat{M}^q_{Z,s''} \hat{M}^{p'}_{X,s'} \otimes \hat{\boldsymbol{Q}}^{p(x),q(z)}_{xz} | \psi \rangle + \mathrm{poly}(\delta_Q) + O(d/q) \\
&= 1 - \mathop{\mathrm{E}}_{s',s''} \sum_{p,q} \mathop{\mathrm{E}}_{x \in s', z \in s''} \langle \psi | \hat{M}^p_{X,s'} \hat{M}^q_{Z,s''} \otimes \hat{\boldsymbol{Q}}^{p(x),q(z)}_{xz} | \psi \rangle + \mathrm{poly}(\delta_Q) + O(d/q) \\
&= \mathop{\mathrm{E}}_{s',s''} \sum_{p,q} \sum_{(a,b) \neq (p(x),q(z))} \mathop{\mathrm{E}}_{x \in s', z \in s''} \langle \psi | \hat{M}^p_{X,s'} \hat{M}^q_{Z,s''} \otimes \hat{\boldsymbol{Q}}^{a,b}_{xz} | \psi \rangle + \mathrm{poly}(\delta_Q) + O(d/q) \\
&= \mathrm{poly}(\delta_Q) + O(d/q) \,.
\end{aligned} \tag{5.35}$$

Here, in the first equation we used (5.34). In the third equation we used item 2. of Lemma 5.4.11 to bound the error terms where $p'(x) \neq p(x)$ by $\mathrm{poly}(\delta_Q)$, and used Lemma 5.2.1 to bound the probability that $p(x) = p'(x)$ on a randomly chosen x for distinct polynomials p, p' by $O(d/q)$. Finally, in the sixth equation, we again used item 2. of Lemma 5.4.11.

Finally, we will use this to construct a joint subspace measurement $\{\hat{Q}^r_s\}_r$:

$$\hat{Q}^r_s = \sum_{p,q: r = (\lambda \alpha_1 + \mu \alpha_2) p(\lambda x_1 + \mu x_2) + (\lambda \beta_1 + \mu \beta_2) q(\lambda z_1 + \mu z_2)} T^{p,q}_{s',s''} \,. \tag{5.36}$$

The consistency of $\hat{Q}^r_s$ with the re-arranged points measurement $\hat{Q}^c_{xz\alpha\beta}$ now follows directly from (5.36) together with the consistency of $T^{p,q}_{s',s''}$ with $\hat{Q}^{a,b}_{xz}$ established in (5.35). □

Claim 5.4.12 shows that the families of measurements $\{\hat{Q}^r_s\}_r$ and $\{\hat{Q}^c_{xz\alpha\beta}\}$ induce a strategy with success probability $1-\varepsilon'$ in the classical low-degree test, for some $\varepsilon' = \text{poly}(p)\cdot\text{poly}(\delta_{\hat{M}}) + O(d/q)$ (to obtain this error bound, recall that $\delta_Q = \text{poly}(p)\cdot\text{poly}(\delta_{\hat{M}})$). This allows us to apply Theorem 5.2.8 and conclude the proof of Lemma 5.4.6.

Proof of Lemma 5.4.6. The proof is symmetric under exchanging $\hat{S}, \hat{X}, \hat{Z}$ with $\hat{\boldsymbol{S}}, \hat{\boldsymbol{X}}, \hat{\boldsymbol{Z}}$, so we only present one direction. Claim 5.4.12 establishes the existence of a strategy $\{\hat{Q}^r_s, \hat{\boldsymbol{Q}}^r_s\}$ which succeeds with probability $1-\varepsilon'$, for some $\varepsilon' = \text{poly}(t)\cdot\text{poly}(\delta_{\hat{M}}) + O(d/q)$, in the classical low-degree test for $m' = 2m+2$ and $d' = d+1$. Increasing the error artificially by replacing $O(d/q)$ with $md/q^{1/c}$ if needed, the assumption $q \geq (dm/\varepsilon')^c$ from Theorem 5.2.8 is satisfied. The theorem yields a POVM $\{\hat{S}^g\}$ with outcomes in the set of polynomials $g : \mathbb{F}_q^{2m+2} \to \mathbb{F}_q$ of degree at most $d+1$ that is self-consistent and consistent with the $\{\hat{Q}^r_s\}$ and the family of POVM $\{\hat{Q}^c_{xz\alpha\beta}\}$ defined in Lemma 5.4.11. Moreover, applying Naimark's dilation theorem (taking advantage of the assumption that the state $|\hat{\psi}\rangle$ defined in (5.28), by definition, contains sufficiently many ancilla $|0\rangle$ qubits), we can assume without loss of generality that $\{\hat{S}^g\}$ is a projective measurement.

In general there is no a priori guarantee that g takes the form $g = \alpha g_1 + \beta g_2$ for g_1 (resp. g_2) a degree-d polynomial in x (resp. z) only. Let $\mathcal{G}$ denote the latter set of polynomials. We first show that the probability of obtaining an outcome g that does not fall within the set $\mathcal{G}'$ of $(2m+2)$-variate polynomials that are linear in α and β is small. Using consistency of $\{\hat{S}^g\}$ with the $\{\hat{Q}^c_{xz\alpha\beta}\}$, which follows from item 1. in Theorem 5.2.8,

$$\begin{aligned}\sum_{g\notin\mathcal{G}'} \hat{S}^g &\approx_{\text{poly}(\varepsilon')} \sum_{g\notin\mathcal{G}'} \mathop{\mathrm{E}}_{(x,z,\alpha,\beta)\in\mathbb{F}_q^{2m+2}} \hat{S}^g \otimes \hat{\boldsymbol{Q}}^{g(x,z,\alpha,\beta)}_{xz\alpha\beta} \\ &\approx_{\text{poly}(\delta_Q)} \sum_{g\notin\mathcal{G}'}\sum_{a,b} \mathop{\mathrm{E}}_{x,z}\Big(\mathop{\mathrm{E}}_{\alpha,\beta} 1_{\alpha a+\beta b=g(x,z,\alpha,\beta)}\Big)\hat{S}^g \otimes \hat{\boldsymbol{M}}^a_{X,x}\hat{\boldsymbol{M}}^b_{Z,z}\,, \end{aligned} \tag{5.37}$$

where the second approximation follows from item 2. in Lemma 5.4.11. If g contains a term of degree higher than 1 in α or β the expectation inside the brackets in (5.37) is at most $O(d/q)$. This bounds the contribution of outcomes $g \notin \mathcal{G}'$. Next we show that outcomes in $\mathcal{G}'\backslash\mathcal{G}$ are unlikely, i.e. that g_1 should depend solely on x and g_2 solely on z. (Note that either polynomial has degree at most d, since g itself has degree at most $d+1$.) Towards this, starting from (5.37), write

$$\begin{aligned}\sum_{g=\alpha g_1+\beta g_2\in\mathcal{G}'} \hat{S}^g &\approx_{\text{poly}(\varepsilon',\delta_Q)} \sum_{g=\alpha g_1+\beta g_2} \hat{S}^g \otimes \mathop{\mathrm{E}}_z \sum_b \Big(\sum_a \mathop{\mathrm{E}}_x 1_{a=g_1(x,z)}1_{b=g_2(x,z)}\hat{\boldsymbol{M}}^a_{X,x}\Big)\hat{\boldsymbol{M}}^b_{Z,z} \\ &\approx_{\text{poly}(\delta_Q)} \sum_{g=\alpha g_1+\beta g_2} \hat{S}^g \otimes \mathop{\mathrm{E}}_z \sum_b\sum_a \mathop{\mathrm{E}}_x 1_{a=g_1(x,z)}1_{b=g_2(x,z)}\hat{\boldsymbol{Q}}^{a,b}_{x,z}\end{aligned}$$

$$\leq \sum_{g=\alpha g_1+\beta g_2} \hat{S}^g \otimes \mathop{\mathrm{E}}_z \sum_b \mathop{\mathrm{E}}_x 1_{b=g_2(x,z)} \Big(\sum_a \hat{\boldsymbol{Q}}^{a,b}_{x,z} \Big)$$
$$\approx_{\mathrm{poly}(\delta_Q)} \sum_{g=\alpha g_1+\beta g_2} \hat{S}^g \otimes \mathop{\mathrm{E}}_z \sum_b \Big(\mathop{\mathrm{E}}_x 1_{b=g_2(x,z)} \Big) \hat{\boldsymbol{M}}^b_{Z,z} \ ,$$

where the inequality removes the first indicator by using positivity. If $g_2(x,z)$ depended on x, the indicator $1_{b=g_2(x,z)}$ appearing within the expression inside the brackets would have probability at most $O(d/q)$ to be satisfied, for a random choice of b and z, on average over x. Thus outcomes $g = \alpha g_1 + \beta g_2$ for which g_2 depends on x have small probability; similarly for z. The relation (5.30) then follows directly from the above, Claim 5.4.4, and the second item in Lemma 5.4.11. □

5.4.4 Generalized X and Z observables

In this section we complete the last main step of the proof. For $W \in \{X, Z\}$, $w \in \mathbb{F}_q^m$ and $u \in \mathbb{F}_q$ let $W_u(w_\pi)$ be the observable defined in Claim 5.4.2, and $\hat{W}_u(w_\pi)$ defined in Lemma 5.4.3. For convenience we consider a "basis" for these sets of observables, as u ranges over $\mathbb{F}_p^t$, by defining

$$\forall \ell \in \{1, \ldots, t\} \ , \qquad W_\ell(w_\pi) = W_{b_\ell}(w_\pi) \qquad \text{and} \qquad \hat{W}_\ell(w_\pi) = \hat{W}_{b_\ell}(w_\pi) \ , \quad (5.38)$$

where $\{b_1, \ldots, b_t\}$ is a self-dual basis for $\mathbb{F}_q$ over $\mathbb{F}_p$. The corresponding "true" Paulis $\sigma_{W,\ell}(w_\pi)$ were defined in (5.10). Similarly define $\boldsymbol{W}_\ell(w_\pi)$ and $\hat{\boldsymbol{W}}_\ell(w_\pi)$. In this section we use these observables to construct a family of observables $\tilde{W}_\ell(a)$, for $a \in \mathbb{F}_q^n$, which satisfy appropriate self-consistency and twisted commutation relations, as expressed in the following lemma.

Lemma 5.4.13. *Let $m, d, q = p^t$ be as in Lemma 5.4.1, $|\hat{\psi}\rangle$ as in Lemma 5.4.3, $W_\ell(w_\pi)$ and $\boldsymbol{W}_\ell(w_\pi)$, $\hat{W}_\ell(w_\pi)$ and $\hat{\boldsymbol{W}}_\ell(w_\pi)$ as in* (5.38)*, and $\{\hat{S}^{g_1,g_2}\}$, $\{\hat{\boldsymbol{S}}^{g_1,g_2}\}$, and δ_S as in Lemma 5.4.6.*

For every $a \in \mathbb{F}_q^n$ and $\ell \in \{1, \ldots, t\}$ there are observables $\tilde{X}_\ell(a)$ acting on AA'A'' and $\tilde{\boldsymbol{X}}_\ell(a)$ acting on BB'B'', and for every $b \in \mathbb{F}_q^n$ and $\ell' \in \{1, \ldots, t\}$ observables $\tilde{Z}_{\ell'}(b)$ acting on AA'A'' and $\tilde{\boldsymbol{Z}}_\ell(b)$ acting on BB'B'', such that the following properties hold for some $\delta_W = \mathrm{poly}(\delta_S) + \mathrm{poly}(d/q)$:

1. *The families of observables $\{\tilde{X}_\ell(a), \tilde{Z}_{\ell'}(b),\ a, b \in \mathbb{F}_q^n,\ \ell, \ell' \in \{1, \ldots, t\}\}$ and $\{\tilde{\boldsymbol{X}}_\ell(a), \tilde{\boldsymbol{Z}}_{\ell'}(b),\ a, b, \in \mathbb{F}_q^n,\ \ell, \ell' \in \{1, \ldots, t\}\}$ exactly satisfy the same algebraic relations as the Pauli observables $\sigma_{W,\ell}$ over $\mathbb{F}_q$ defined in* (5.10)*;*

2. *On average over $x, z \in \mathbb{F}_q^m$, and for all $\ell, \ell' \in \{1, \ldots, t\}$,*

$$\tilde{X}^e_\ell(x_\pi) \approx_{\delta_W} X^e_\ell(x_\pi) \qquad \text{and} \qquad \tilde{Z}^e_{\ell'}(z_\pi) \approx_{\delta_W} Z^e_{\ell'}(z_\pi) \ ,$$

and the analogous relations between $\tilde{\boldsymbol{X}}_\ell, \tilde{\boldsymbol{Z}}_{\ell'}$ and $\boldsymbol{X}_\ell, \boldsymbol{Z}_{\ell'}$ hold;

3. *The $\tilde{X}_\ell(a)$, $\tilde{Z}_{\ell'}(b)$ are approximately consistent with the $\tilde{\boldsymbol{X}}_\ell(a)$, $\tilde{\boldsymbol{Z}}_{\ell'}(b)$: in expectation over $a, b \in \mathbb{F}_q^n$,*

$$\sum_{e\in\mathbb{F}_p} \tilde{X}_\ell^e(a) \otimes \tilde{\boldsymbol{X}}_\ell^e(a) \approx_{\delta_W} \mathrm{Id} \,, \qquad \sum_{e\in\mathbb{F}_p} \tilde{Z}_{\ell'}^e(b) \otimes \tilde{\boldsymbol{Z}}_{\ell'}^e(b) \approx_{\delta_W} \mathrm{Id} \,.$$

Proof. For any $a, b \in \mathbb{F}_q^n$ and $\ell \in \{1, \ldots, t\}$ define

$$\begin{aligned}
\tilde{X}_\ell(a)_{\mathsf{AA'A''}} &= \Big(\sum_{g_1,g_2} \omega^{\mathrm{tr}(b_\ell(g_1\cdot a))}\, \hat{S}^{g_1,g_2}_{\mathsf{AA'}}\Big) \otimes \sigma_{X,\ell}(a)^\dagger_{\mathsf{A''}} \,, \\
\tilde{Z}_\ell(b)_{\mathsf{AA'A''}} &= \Big(\sum_{g_1,g_2} \omega^{\mathrm{tr}(b_\ell(g_2\cdot b))}\, \hat{S}^{g_1,g_2}_{\mathsf{AA'}}\Big) \otimes \sigma_{Z,\ell}(b)^\dagger_{\mathsf{A''}} \,, \\
\tilde{\boldsymbol{X}}_\ell(a)_{\mathsf{BB'B''}} &= \Big(\sum_{g_1,g_2} \omega^{\mathrm{tr}(b_\ell(g_1\cdot a))}\, \hat{\boldsymbol{S}}^{g_1,g_2}_{\mathsf{BB'}}\Big) \otimes \boldsymbol{\sigma}_{X,\ell}(a)^\dagger_{\mathsf{B''}} \,, \\
\tilde{\boldsymbol{Z}}_\ell(b)_{\mathsf{BB'B''}} &= \Big(\sum_{g_1,g_2} \omega^{\mathrm{tr}(b_\ell(g_2\cdot b))}\, \hat{\boldsymbol{S}}^{g_1,g_2}_{\mathsf{BB'}}\Big) \otimes \boldsymbol{\sigma}_{Z,\ell}(b)^\dagger_{\mathsf{B''}} \,,
\end{aligned} \tag{5.39}$$

where $\hat{\boldsymbol{S}}^{g_1,g_2}_{\mathsf{BB'}}$ is defined as $\hat{\boldsymbol{S}}^{g_1,g_2}_{\mathsf{BA'}}$, with the role of the register $\mathsf{A'}$ replaced by $\mathsf{B'}$ (note the two are isomorphic). From Lemma 5.4.6 we know that $\{\hat{S}^{g_1,g_2}\}$ is a projective measurement. In particular the first component of each of the observables defined in (5.39) commute; hence the first item in the lemma follows from the fact that $\sigma_{X,\ell}(a)$ and $\sigma_{Z,\ell}(b)$ themselves satisfy the required Pauli relations.

Next we verify the second item. We give the proof for the X observables; the arguments for $Z, \boldsymbol{X}, \boldsymbol{Z}$ are similar. Using the definition (5.39), on average over $x \in \mathbb{F}_q^m$,

$$\begin{aligned}
\tilde{X}^a_\ell(x_\pi) &= \sum_{b,c\in\mathbb{F}_p:\, b-c=a} \Big(\sum_{g_1,g_2:\, \mathrm{tr}(b_\ell g_1(x))=b} \hat{S}^{g_1,g_2}_{\mathsf{AA'}}\Big) \otimes \sigma^c_{X,\ell}(x_\pi)_{\mathsf{A''}} \\
&\approx_{\mathrm{poly}(\delta_S)} \sum_{b,c\in\mathbb{F}_p:\, b-c=a} \hat{X}^b_\ell(x_\pi)_{\mathsf{AA'}} \otimes \sigma^c_{X,\ell}(x_\pi)_{\mathsf{A''}} \\
&= \sum_{b',b'',c\in\mathbb{F}_p:\, b'+b''-c=a} X^{b'}_\ell(x_\pi)_{\mathsf{A}} \otimes \boldsymbol{\sigma}^{b''}_{X,\ell}(x_\pi)_{\mathsf{A'}} \otimes \sigma^c_{X,\ell}(x_\pi)_{\mathsf{A''}} \\
&= X^a_\ell(x_\pi),
\end{aligned}$$

where the second line follows from (5.30) in Lemma 5.4.6 and the definition (5.38), the third uses the definition (5.24) of $\hat{X}$ from Claim 5.4.2, and the last uses the fact that $|\hat{\psi}\rangle$ defined in Lemma 5.4.3 is an EPR pair on $\mathsf{A'A''}$ together with (5.17) to set $b'' = c$ (so the equality holds in the state-dependent distance).

Finally we show the third item in the lemma. We show consistency for $\tilde{X}$; consistency for $\tilde{Z}$ is similar For ease of notation we write g for g_1 and omit the outcome

g_2, which in this argument is always summed over. Using the definition (5.39),

$$\begin{aligned}
&\sum_e \tilde{X}^e_\ell(a)_{\mathsf{AA'A''}} \otimes \tilde{\boldsymbol{X}}^e_\ell(a)_{\mathsf{BB'B''}} \\
&\quad= \sum_{\substack{g,c,g',c':\\ \mathrm{tr}(b_\ell(g\cdot a))-c=\mathrm{tr}(b_\ell(g'\cdot a))-c'}} \hat{S}^g_{\mathsf{AA'}} \otimes \sigma^c_{X,\ell}(a)_{\mathsf{A''}} \otimes \hat{\boldsymbol{S}}^{g'}_{\mathsf{BB'}} \otimes \boldsymbol{\sigma}^{c'}_{X,\ell}(a)^\dagger_{\mathsf{B''}} \\
&\quad\approx_{\mathrm{poly}(\delta_S)} \mathop{\mathrm{E}}_{x\in\mathbb{F}_q^m} \sum_{\substack{g,c,g',c':\\ \mathrm{tr}(b_\ell((g-g')\cdot a))=c-c'}} \hat{S}^g_{\mathsf{AA'}} \otimes \sigma^c_{X,\ell}(a)_{\mathsf{A''}} \otimes \hat{\boldsymbol{S}}^{g'}_{\mathsf{BB'}} \otimes \boldsymbol{\sigma}^{c'}_{X,\ell}(a)_{\mathsf{B''}} \\
&\qquad\cdot \Big(\sum_{\substack{r+s=g(x)\\ r'+s'=g'(x)}} (M^r_{X,x})_{\mathsf{A}} \otimes (\tau^s_{X,x})_{\mathsf{A'}} \otimes (\boldsymbol{M}^{r'}_{X,x})_{\mathsf{B}} \otimes (\tau^{s'}_{X,x})_{\mathsf{B'}} \Big) ,
\end{aligned} \tag{5.40}$$

where the approximation uses (5.30), (5.25), and (5.24) and (5.21). Using consistency of M with $\boldsymbol{M}$, as shown in Claim 5.4.2, additionally imposes the constraint that $r = r'$, i.e. $(g - g')(x) = s - s'$. Now, recall that $\sigma^c_{X,\ell}(a)_{\mathsf{A''}}$ is implemented by measuring all n qudits of register $\mathsf{A''}$ in the X basis, obtaining an outcome $h \in \mathbb{F}_q^n$, and reporting $c = \mathrm{tr}(b_\ell(h \cdot a))$ as the outcome. Similarly, $(\tau^s_{X,x})_{\mathsf{A''}}$ is implemented by measuring all n qudits of register $\mathsf{A''}$ in the X basis, obtaining an outcome $h \in \mathbb{F}_q^n$, and reporting $s = h(x) = h \cdot x_\pi$ as the outcome. Moreover, as the registers $\mathsf{A'A''}$ and $\mathsf{B'B''}$ are in EPR states, we can apply the exact consistency relations (5.17) between Pauli measurements. This lets us rewrite (5.40) as

$$\begin{aligned}
&\approx_{\mathrm{poly}(\delta_M)} \mathop{\mathrm{E}}_{x\in\mathbb{F}_q^m} \sum_{\substack{g,h,g',h':\\ \mathrm{tr}(b_\ell(g-g')\cdot a)=\mathrm{tr}(b_\ell(h-h')\cdot a)\\ (g-g')(x)=(h-h')(x)}} \sum_{r=(g-h)(x)} \Big[\hat{S}^g_{\mathsf{AA'}}(M^r_{X,x})_{\mathsf{A}} \otimes \hat{\boldsymbol{S}}^{g'}_{\mathsf{BB'}}(\boldsymbol{M}^r_{X,x})_{\mathsf{B}} \\
&\qquad\qquad \otimes (\tau^h_X)_{\mathsf{A''}} \otimes (\boldsymbol{\tau}^{h'}_X)_{\mathsf{B''}} \Big] \\
&= \mathop{\mathrm{E}}_{x\in\mathbb{F}_q^m} \sum_{\substack{g,h,g',h':\\ \mathrm{tr}(b_\ell(g-g')\cdot a)=\mathrm{tr}(b_\ell(h-h')\cdot a)\\ (g-g')(x)=(h-h')(x)}} \sum_{\substack{r=g(x)\\ r'=g'(x)}} \Big[\hat{S}^g_{\mathsf{AA'}}(\hat{M}^r_{X,x})_{\mathsf{AA'}} \otimes \hat{\boldsymbol{S}}^{g'}_{\mathsf{BB'}}(\hat{\boldsymbol{M}}^{r'}_{X,x})_{\mathsf{BB'}} \\
&\qquad\qquad \otimes (\tau^h_X)_{\mathsf{A''}} \otimes (\boldsymbol{\tau}^{h'}_X)_{\mathsf{B''}} \Big] \\
&\approx_{\mathrm{poly}(\delta_S)} \mathop{\mathrm{E}}_{x\in\mathbb{F}_q^m} \sum_{\substack{g,h,g',h':\\ \mathrm{tr}(b_\ell(g-g')\cdot a)=\mathrm{tr}(b_\ell(h-h')\cdot a)\\ (g-g')(x)=(h-h')(x)}} \hat{S}^g_{\mathsf{AA'}} \otimes \hat{\boldsymbol{S}}^{g'}_{\mathsf{BB'}} \otimes (\tau^h_X)_{\mathsf{A''}} \otimes (\boldsymbol{\tau}^{h'}_X)_{\mathsf{B''}} ,
\end{aligned} \tag{5.41}$$

where the second line uses the definition of $\hat{M}$, and for the last approximation we removed the constraint on r using (5.30). If $g - g' \neq h - h'$ then by Lemma 5.2.1 the condition $(g - g')(x) = (h - h')(x)$ holds at a random point $x \in \mathbb{F}_q^m$ with probability at most $O(d/q)$. If $g - g' = h - h'$ the constraint $\mathrm{tr}(b_\ell(g - g') \cdot a) = \mathrm{tr}(b_\ell(h - h') \cdot a)$ is superfluous. Hence, under the expectation, we can replace the constraints in the

summation in (5.41) by the constraint $(g-g')(x) = (h-h')(x)$, incurring an error of $O(d/q)$:

$$
\begin{aligned}
&\approx_{\mathrm{poly}(d/q)} \mathop{\mathrm{E}}_{x\in\mathbb{F}_q^m} \sum_{\substack{g,g',s,s':\\ (g-g')(x)=(s-s')}} \hat{S}^{g}_{\mathsf{AA'}} \otimes \hat{\boldsymbol{S}}^{g'}_{\mathsf{BB'}} \otimes (\tau^{s}_{X,x})_{\mathsf{A''}} \otimes (\boldsymbol{\tau}^{s'}_{X,x})_{\mathsf{B''}} \\
&\approx_{\delta_S} \mathop{\mathrm{E}}_{x\in\mathbb{F}_q^m} \sum_{\substack{e,e',s,s':\\ e-e'=s-s'}} (\hat{M}^{e}_{X,x})_{\mathsf{AA'}} \otimes (\hat{\boldsymbol{M}}^{e'}_{X,x})_{\mathsf{BB'}} \otimes (\tau^{s}_{X,x})_{\mathsf{A''}} \otimes (\boldsymbol{\tau}^{s'}_{X,x})_{\mathsf{B''}} \\
&= \mathop{\mathrm{E}}_{x\in\mathbb{F}_q^m} \sum_{\substack{e,e',f,f',s,s':\\ e+f-(e'+f')=s-s'}} (M^{e}_{X,x})_{\mathsf{A}} \otimes (\boldsymbol{M}^{e'}_{X,x})_{\mathsf{B}} \otimes (\boldsymbol{\tau}^{f}_{X,x})_{\mathsf{A'}} \otimes (\tau^{s}_{X,x})_{\mathsf{A''}} \otimes (\boldsymbol{\tau}^{f'}_{X,x})_{\mathsf{B'}} \otimes (\boldsymbol{\tau}^{s'}_{X,x})_{\mathsf{B''}} \\
&= \mathop{\mathrm{E}}_{x\in\mathbb{F}_q^m} \sum_{e} (M^{e}_{X,x})_{A} \otimes (M^{e}_{X,x})_{B} \\
&\approx_{\delta_M} \mathrm{Id} \,,
\end{aligned}
$$

where the second line is by (5.30), the third by the definition of $\hat{M}$ (Lemma 5.4.3), the fourth by consistency of τ on the EPR state, and the last is by self-consistency of M (Claim 5.4.2). □

5.4.5 Proof of Lemma 5.4.1

We conclude the proof of Lemma 5.4.1. Lemma 5.4.13 shows that whenever there exists a strategy for the provers that succeeds in the test Q-LOWDEG(m,d,q) with probability at least $1-\varepsilon$, for some ε small enough with respect to d/q so that the quantity δ_W in the lemma is a small constant, there exist operators $\tilde{X}_\ell(a)$ and $\tilde{Z}_\ell(b)$, for $a,b \in \mathbb{F}_q^n$, acting on the extended local spaces AA'A" and BB'B" respectively, that exactly satisfy the group relations of the generalized Pauli group (also known as the finite Heisenberg group).

Using these relations it is fairly straightforward to construct isometries V_A, V_B acting on each prover's space such that V_A maps $\tilde{W}_\ell(a)_{\mathsf{AA'A''}}$ to $\mathrm{Id}_{\mathsf{AA'}} \otimes \sigma_{W,\ell}(a)_{\mathsf{A''}}$ for $W \in \{X,Z\}$, $\ell \in \{1,\ldots,t\}$, and $a \in \mathbb{F}_q^n$, and likewise for V_B. The definition of V_A and V_B is analogous, so we drop the subscript. To explicitly define V, let U be a unitary such that $U\sigma_{W,\ell}(a)^\dagger U^\dagger = \sigma_{W,\ell}(a)$ for all $a \in \mathbb{F}_q^n$, $\ell \in \{1,\ldots,t\}$ and $W \in \{X,Z\}$; such a U can be explicitly defined through its expansion in the Pauli basis. Define

$$
V = \sum_{g_1 g_2} \hat{S}^{g_1,g_2}_{\mathsf{AA'}} \otimes U\tau_X(g_2)\tau_Z(g_1) \,,
$$

where in the notation $\tau_W(g)$ we interpret g as the corresponding vector of coefficients in $\mathbb{F}_q^n$. To see that this accomplishes the desired map, using that $\{\hat{S}^{g_1 g_2}\}$ is projective, evaluate

$$
V\tilde{X}_\ell(a)_{\mathsf{AA'A''}}V^\dagger = \sum_{g_1,g_2} \omega^{\mathrm{tr}(b_\ell(g_1\cdot a))} \hat{S}^{g_1,g_2}_{\mathsf{AA'}} \otimes U\tau_X(g_2)\tau_Z(g_1)\sigma_{X,\ell}(a)^\dagger \tau_Z(g_1)^\dagger \tau_X(g_2)^\dagger U^\dagger
$$

$$
\begin{aligned}
&= \sum_{g_1,g_2} \omega^{\mathrm{tr}(b_\ell(g_1\cdot a))} \hat{S}^{g_1,g_2}_{\mathsf{AA'}} \otimes U\tau_X(g_2)\tau_Z(g_1)\tau_X(b_\ell a)^\dagger \tau_Z(g_1)^\dagger \tau_X(g_2)^\dagger U^\dagger \\
&= \sum_{g_1,g_2} \hat{S}^{g_1,g_2}_{\mathsf{AA'}} \otimes U\tau_X(ab_\ell)^\dagger U^\dagger \\
&= \sum_{g_1,g_2} \hat{S}^{g_1,g_2}_{\mathsf{AA'}} \otimes U\sigma_{X,\ell}(a)^\dagger U^\dagger \\
&= \mathrm{Id} \otimes \sigma_{X,\ell}(a) \ .
\end{aligned}
$$

A similar calculation can be done for Z.

The combination of all isometries considered in the analysis might have increased the local dimension by a large amount. However, using the outcome consistency between $\tilde{X}_\ell(a)$ and $X_\ell(a)$ (item 3. in Lemma 5.4.13), we know that the state $|\hat{\psi}\rangle$ satisfies

$$
\mathop{\mathrm{E}}_{\ell\in\{1,\ldots,t\}} \mathop{\mathrm{E}}_{a\in\mathbb{F}_q^n} \sum_e \langle\hat{\psi}|\tilde{X}^e_\ell(a) \otimes \tilde{\boldsymbol{X}}^e_\ell(a)|\hat{\psi}\rangle \geq 1 - O(\delta_W) \ , \tag{5.42}
$$

and an analogous property also holds for the $\tilde{Z}_\ell(b)$. Let $H_W = \mathrm{E}_\ell \mathrm{E}_a \sum_e \sigma_{W,\ell}(a)^e \otimes \boldsymbol{\sigma}_{W,\ell}(a)^e$ for $W \in \{X, Z\}$, and $|\psi'\rangle = V_A \otimes V_B|\hat{\psi}\rangle$. In this notation, we can rewrite (5.42) as

$$
\langle\psi'|H_W|\psi'\rangle \geq 1 - O(\delta_W) \ , \tag{5.43}
$$

for $W \in \{X, Z\}$. By construction, the operators H_W are Hermitian with $0 \leq H_W \leq \mathrm{Id}$, and $H_X H_Z = H_Z H_X$. Hence, $H = H_X H_Z$ is Hermitian and $0 \leq H \leq \mathrm{Id}$. An application of the Cauchy-Schwarz inequality to (5.43) yields

$$
\langle\psi'|H|\psi'\rangle \geq 1 - O(\sqrt{\delta_W}) \ . \tag{5.44}
$$

Moreover, a direct calculation reveals that in fact $H = |\psi_{\mathrm{EPR}}\rangle\langle\psi_{\mathrm{EPR}}|$. First, we evaluate H_W:

$$
\begin{aligned}
H_W &= \mathop{\mathrm{E}}_a \mathop{\mathrm{E}}_\ell \sum_e \sigma^e_{W,\ell}(a) \otimes \boldsymbol{\sigma}^e_{W,\ell}(a) \\
&= \mathop{\mathrm{E}}_a \mathop{\mathrm{E}}_\ell \sum_{h,h':\mathrm{tr}(b_\ell h\cdot a)=\mathrm{tr}(b_\ell h'\cdot a)} \tau^h_W \otimes \boldsymbol{\tau}^{h'}_W \\
&= \mathop{\mathrm{E}}_a \mathop{\mathrm{E}}_\ell \sum_{h,h'} \omega^{\mathrm{tr}(b_\ell a\cdot(h-h'))} \tau^h_W \otimes \boldsymbol{\tau}^{h'}_W \\
&= \mathop{\mathrm{E}}_a \mathop{\mathrm{E}}_\ell \sigma_{W,\ell}(a) \otimes \boldsymbol{\sigma}_{W,\ell}(a)^\dagger \\
&= \mathop{\mathrm{E}}_\ell \Big(\mathop{\mathrm{E}}_{a\in\mathbb{F}_q} (\sigma_{W,\ell}(a) \otimes \boldsymbol{\sigma}^\dagger_{W,\ell}(a)) \Big)^{\otimes n} \ , \\
&= \mathop{\mathrm{E}}_\ell \Big(\mathop{\mathrm{E}}_{a\in\mathbb{F}_q} (\tau_W(ab_\ell) \otimes \boldsymbol{\tau}^\dagger_W(ab_\ell)) \Big)^{\otimes n} \ , \\
&= \Big(\mathop{\mathrm{E}}_{a\in\mathbb{F}_q} (\tau_W(a) \otimes \boldsymbol{\tau}^\dagger_W(a)) \Big)^{\otimes n} \ ,
\end{aligned}
$$

where in going to the last line, we did a change of variables on the variable a, to absorb the factor of b_ℓ. Now, we evaluate H:

$$\begin{aligned}
H &= H_X H_Z \\
&= \Big(\mathop{\mathrm{E}}_{a,b\in\mathbb{F}_q} \tau_X(a)\tau_Z(b) \otimes \boldsymbol{\tau}_X^\dagger(a)\boldsymbol{\tau}_Z^\dagger(b) \Big)^{\otimes n} \\
&= \Big(\mathop{\mathrm{E}}_{a,b\in\mathbb{F}_q} \tau_X(a)\tau_Z(b) \otimes \tau_X(a)\tau_Z(-b) \Big)^{\otimes n} \\
&= \Big(\mathop{\mathrm{E}}_{a,b\in\mathbb{F}_q} \sum_{i,j} \omega^{\mathrm{tr}(ib)} |i+a\rangle\langle i| \otimes \omega^{-\mathrm{tr}(jb)} |j+a\rangle\langle j| \Big)^{\otimes n} \\
&= \Big(\mathop{\mathrm{E}}_{a\in\mathbb{F}_q} \sum_{i} |i+a\rangle\langle i| \otimes |i+a\rangle\langle i| \Big)^{\otimes n} \\
&= |\psi_{\mathrm{EPR}}\rangle\langle\psi_{\mathrm{EPR}}| \,,
\end{aligned}$$

where in going from the fourth to the fifth line, we have used the fact that the summation over b vanishes unless $j = i$, and for the last we use that $\mathrm{E}_{a\in\mathbb{F}_q} |i+a\rangle|i+a\rangle = q^{-1/2}|\psi_{\mathrm{EPR}}\rangle$ for any $i \in \mathbb{F}_q$. Hence, from (5.44) we conclude that

$$\big\| \langle\psi_{\mathrm{EPR}}|\psi'\rangle \big\|^2 \geq 1 - O(\sqrt{\delta_W}) \,.$$

This completes the proof of Lemma 5.4.1.

Chapter 6

A quantum entangled games PCP

In this chapter, we complete the proof of the quantum games PCP theorem. We show how to leverage the test for EPR pairs developed in the previous to design a test for ground states of Hamiltonians. The reader is encouraged to consult Section 5.1 for a high-level overview of the proof.

6.1 A test for codewords

In this section we show that the low-degree test Q-LOWDEG can be combined with any weakly self-dual quantum CSS code $\mathcal{C}$ defined over $\mathbb{F}_q$ to obtain a self-test for states in the n-fold tensor product of the codespace, as well as certain tensor products of generalized Pauli observables on the codespace (including all single-qudit Pauli observables). The test uses as many provers as the dimension of the code.

6.1.1 CSS codes

We consider weakly self-dual *Calderbank-Shor-Steane (CSS) codes* [CS96, Ste96]. Let C be a classical $[k, k']$ linear error-correcting code over $\mathbb{F}_q$, for a prime power q: C is specified by a generator matrix $G \in \mathbb{F}_q^{k \times k'}$ and a parity check matrix $K \in \mathbb{F}_q^{(k-k') \times k}$ such that $C = \mathrm{Im}(G) = \ker(K)$. We say that C is weakly self-dual if the dual code $C^\perp$, with generator matrix K^T, is such that $C \subseteq C^\perp$; equivalently, $G^T G = 0$. To any such code C we associate a subspace $\mathcal{C}$ of $(\mathbb{C}^q)^{\otimes k}$ that is the simultaneous $+1$ eigenspace of a set of stabilizers $\{S_{W,j}\}_{W \in \{X,Z\}, j \in \{1,\ldots,k'\}}$ such that $S_{W,j}$ is a tensor product of Pauli W observables over $\mathbb{F}_q$ in the locations indicated by the j-th column of the generator matrix G, i.e.

$$S_{W,j} = \tau_W(G_{1j}) \otimes \tau_W(G_{2j}) \otimes \ldots \otimes \tau_W(G_{kj}),$$

where G_{ij} is the (i, j)-th entry of G. The condition that $G^T G = 0$ implies that all the $S_{W,j}$ commute, so that $\mathcal{C}$ is well-defined. We refer to [Got99, KKKS06] for more background on the theory of stabilizer codes over qudits.

Example 6.1.1 (EPR code)**.** A simple example of a weakly self-dual 2-qudit code

with dimension 1 is the "EPR code" (our terminology) with generator matrix $G = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ in case $q = 2$, and $G = \begin{pmatrix} 1 \\ \sqrt{-1} \bmod q \end{pmatrix}$ for $q \equiv 1 \bmod 4$. The associated code subspace $\mathcal{C}$ has dimension 1, and it is spanned by a maximally entangled state of two qudits.

Example 6.1.2 (Quadratic residue code). The 7-qudit code is a weakly self-dual CSS code that has $k = 7$, $k' = 3$, and encodes one qudit over $\mathbb{F}_q$ for any prime power $q = p^e$ such that p is a quadratic residue modulo 7. For example $p = 2$ is a quadratic residue modulo 7. See Theorem 40 in [KKKS06] for a more general construction.

6.1.2 The CODE-CHECK test

Let n be an integer and C a weakly self-dual $[k, k']$ linear code. Let $\mathcal{C}$ be the associated CSS code, as described in Section 6.1.1.[1] The test CODE-CHECK(C, n) is summarized in Figure 6-1. The test builds on the (composed) low-degree test described in Figure 3-3. Recall the following properties of the honest strategy for the provers in the test (see Section 5.3.2):

- In the first part of the test, each prover is sent a query of the form (W, s, s'), where $W \in \{X, Z\}$ designates a choice of basis and s, s' are the specification of a pair of subspaces. The honest prover measures each of his n qudits in the basis W, obtaining a string $a \in \mathbb{F}_q^n$. From a, the prover computes the degree-d polynomial g_a specified in (5.5), and returns the restriction of the (suitably encoded) bivariate polynomial $(g_a)_{|s}$ to the subspace s'.
- In the second part of the test, the prover is sent a query of the form (W_1, W_2), where $W_1, W_2 \in \{X, Z, Y\}^n$ are commuting n-qudit observables. The honest prover jointly measures W_1 and W_2 and returns the pair of outcomes obtained.

We now describe the test CODE-CHECK(C, n). In the test, the verifier splits the k provers into two groups. One prover, indexed by $t \in \{1, \ldots, k\}$, is chosen at random and called the "special prover". The remaining $(k-1)$ provers are jointly called "composite prover". In general a prover is not told whether it is the special prover, or a composite prover. In the test the verifier simulates queries from the two-prover low-degree test for the special and composite provers using the following scheme.

Definition 6.1.3 (Composite queries and answers). Let $G \in \mathbb{F}_q^{k \times k'}$ be the generator matrix for a $[k, k']$ weakly self-dual code C. Let Q be a query in the test Q-LOWDEG.

1. The composite query associated with Q, denoted $\boldsymbol{Q}$, is obtained by sending each prover forming the composite prover the query Q.

2. Given answers $(A_j)_{j \neq t}$ from the $(k-1)$ provers forming the composite prover, the composite answer $\boldsymbol{A}$ is obtained by selecting a uniformly random vector v in the

[1] All results in this and the next section can be obtained by restricting attention to the 7-qubit code described in Example 6.1.2.

column span of G such that $v_t = 1$, and computing the sum $\boldsymbol{A} = -\sum_{j \neq t} v_j A_j$.
[2]

This definition is consistent with the notation $\boldsymbol{M}$ used in Q-LOWDEG; in both cases, the answers obtained from the composite prover (in the case of the two-player test, the second prover) are multiplied by the appropriate entry of the generator matrix of a code. The test Q-LOWDEG differs only insofar as the EPR state is not a CSS code state, so the X and Z stabilizers are not identical. Moreover, in both cases, for honest strategies, the special and composite prover obtain the same outcome when given the same query. This fact is formalized in the following lemma.

Lemma 6.1.4. *Let $\ell \geq 1$ be an integer and $f : \mathbb{F}_q^n \to \mathbb{F}_q^\ell$ a linear function. Suppose that k provers share a (nk)-qudit state $|\Psi\rangle$ that is a valid qudit-by-qudit encoding of an n-qudit state $|\psi\rangle$ according to a k-qudit self-dual CSS code $\mathcal{C}$. Let $W \in \{X, Z\}^n$ and suppose that for each $j \in \{1, \ldots, k\}$, the j-th prover measures the i-qudit of its share of the state in the basis W_i, for each $i \in \{1, \ldots, n\}$, to obtain an assignment $a_j \in \mathbb{F}_q^n$, and returns the value $y_j = f(a_j) \in \mathbb{F}_q^\ell$. Then for any index $t \in \{1, \ldots, k\}$ for the special prover, and vector $v \in \mathbb{F}_q^k$ chosen as in item 2. in Definition 6.1.3, the special prover's answer y_t and the composite prover's answer $\boldsymbol{y} = -\sum_{j \neq t} v_j y_j$ are equal with certainty.*

Before giving the proof, we note that the functions computed in the low-degree test, i.e. polynomials g_a as in (5.5), evaluated on points or restricted to subspaces, are linear functions of a of the form considered in the lemma.

Proof. It follows from the definition of v and the stabilizer property of the code that

$$\sum_j v_j a_j = 0 \,.$$

Write the linear function f as $f(a) = Ka$, for $K \in \mathbb{F}_q^{\ell \times n}$. Then, a simple calculation shows that

$$\boldsymbol{y} = -\sum_{j \neq t} v_j \, f(a_j) = -\sum_{j \neq t} v_j \, (K a_j) = K\Big(-\sum_{j \neq t} v_j \, a_j \Big) = Ka = y \,.$$

□

6.1.3 Analysis of the CODE-CHECK self-test

We first show completeness of the test CODE-CHECK.

[2]The specific way in which this summation is performed depends on the form of the query Q. In general each A_i is expected to be either a low-degree polynomial, or of a pair of values in $\mathbb{F}_q$. In both cases, there is a natural way to add up the answers in order to obtain an answer $\boldsymbol{A}$ that is formatted as the prover's answer in the low-degree test.

Test CODE-CHECK(C, n): Given is the generator matrix G for a $[k, k']$ weakly self-dual linear code C over $\mathbb{F}_q$, as described in Section 6.1.1, and n an integer. Let $d = \lceil \log n \rceil \cdot \lceil \frac{\log n}{\log \log n} \rceil$ and $m = \lceil \frac{\log(n)}{\log \log(n)} \rceil$.

(a) The verifier selects one of the k provers at random and assigns it the label of "special prover". All remaining provers are given the label of "composite prover". (The provers are not told how they are labeled.) Let $t \in \{1, \ldots, k\}$ be the index of the special prover.

(b) The verifier executes the verifier for the test Q-LOWDEG$^{(2)}(m, d, q)$ to generate a pair of queries (Q, Q') for the two provers in that test. The verifier sends the query Q to the special prover, and distributes the query $\boldsymbol{Q'}$ to the composite prover. He receives answers A and $\boldsymbol{A'}$ respectively.

(c) The verifier accepts if and only if $(A, \boldsymbol{A'})$ is a pair of valid answers to queries (Q, Q') in the low-degree test.

Figure 6-1: The procedure CODE-CHECK(C, n) verifies that k provers share an entangled state which lies in the n-fold tensor product of the code $\mathcal{C}$, defined over k qudits each of dimension q.

Lemma 6.1.5. *Let C be a $[k, k']$ weakly self-dual linear code over $\mathbb{F}_q$, and n an integer. Let $\mathcal{C}$ be the associated CSS code, as described in Section 6.1.1. Then for any (nk)-qubit state $|\Psi\rangle \in \mathcal{C}^{\otimes n}$ there exists a strategy for the k provers based on sharing $|\Psi\rangle$ and measuring tensor products of Pauli observables, such that the strategy is accepted with probability 1 in the test* CODE-CHECK(C, n).

Proof. Fix $|\Psi\rangle \in \mathcal{C}^{\otimes n}$. The strategy for the provers is simple: each prover directly applies the honest strategy in the test Q-LOWDEG$^{(2)}$, as described in Section 5.3.2.

It remains to verify that the answers $(A, \boldsymbol{A'})$ computed by the verifier in step (c) of the test CODE-CHECK are valid answers to (Q, Q') in Q-LOWDEG$^{(2)}$. Fix a choice of codeword v as made by the verifier in the computation of the composite query $\boldsymbol{Q'}$ at step (b) of CODE-CHECK (see Definition 6.1.3). We make the following observations on the joint measurement performed by the provers that constitute the composite prover. Consider first queries of the form $Q' = (W, s, s')$. Upon receipt of such a query, the i-th prover that constitutes the composite prover measures each of its n qudits using the projective measurement τ_W to obtain outcomes $a'_i = (a'_{i,1}, \ldots, a'_{i,n})$, from which it computes a low-degree polynomial $g_{a'_i}$ as in (5.5). Since $a' \mapsto g_{a'}$ is a linear function, the answer $\boldsymbol{A'}$ computed by the verifier is the restriction to s' of the (suitably encoded) bivariate polynomial $(g_{a'})_{|s}$, where $a' = \sum_{i \neq t} v_i a'_i$ is the outcome of an imaginary joint measurement performed by the composite prover using the measurement $\boldsymbol{\tau}_W^{a'} = \sum_{a'_i : \sum_{i \neq t} v_i a'_i = a'} \otimes_{i \neq t} \tau_W^{a'_i}$. The situation in case the query Q' is taken from the second part of the low-degree test is similar.

To conclude we show that for any choice of codeword v made by the verifier,

the provers' strategy, conditioned on v, is isometric to the honest strategy for the low-degree test, as defined in the proof of Lemma 5.3.4.

To see this, observe that by definition, for a fixed v, the operators $X \otimes \boldsymbol{X}$ and $Z \otimes \boldsymbol{Z}$ stabilize each group of k qudits of $|\Psi\rangle$, where $X = \tau_X(1)$, $\boldsymbol{X} = \otimes_{i \neq t} \tau_X(v_i)$, and $Z = \tau_Z(2)$, $\boldsymbol{Z} = \otimes_{i \neq t} \tau_Z(v_i)$; indeed this is because v defines both an X and a Z stabilizer for $\mathcal{C}$. Moreover, $\boldsymbol{X}$ and $\boldsymbol{Z}$ satisfy the same twisted commutation relation as $\boldsymbol{\tau}_X$ and $\boldsymbol{\tau}_Z$; this is because $v_t = 1$ and $v \cdot v = 0$ by weak self-duality. Thus there exists a local isometry acting jointly on all provers forming the composite prover, which maps $\boldsymbol{X} \mapsto \boldsymbol{\tau}_X$ and $\boldsymbol{Z} \mapsto \boldsymbol{\tau}_Z$. The image of $|\Psi\rangle$ under this isometry is stabilized by $\tau_X \otimes \boldsymbol{\tau}_X$ and $\tau_Z \otimes \boldsymbol{\tau}_Z$, hence must be the state $|\mathrm{EPR}_q\rangle$. Lemma 5.3.4 then lets us conclude that the above-defined strategy succeeds with probability 1 in the test.

□

The next theorem shows soundness of the test CODE-CHECK.

Theorem 6.1.6. *Let n, k, k' be integer. Let $q = p^t$ be a prime power such that $\mathbb{F}_q$ admits a self-dual basis over $\mathbb{F}_p$. Let C be a $[k, k']$ weakly self-dual linear code over $\mathbb{F}_q$, and $\mathcal{C}$ the associated CSS code. Let m, d be as in Figure 6-1. Suppose a strategy using state $|\Psi\rangle \in \otimes_{i=1}^{k} \mathcal{H}_i$ and projective measurements $\{M^a_{W,w}\}$ for the special prover succeeds in test* CODE-CHECK(C, n) *with probability at least $1 - \varepsilon$, for some $\varepsilon \geq 0$. Then there is a $\delta_C = \max(\mathrm{poly}(p) \cdot \mathrm{poly}(\varepsilon), \mathrm{poly}(q^{-1}))$ and isometries $V_i : \mathcal{H}_i \to (\mathbb{C}^q)^{\otimes n} \otimes \mathcal{H}'_i$ for $i \in \{1, \ldots, t\}$, and states $|\psi\rangle \in \mathcal{C}$ and $|\mathrm{AUX}\rangle \in \otimes_i \mathcal{H}'_i$ such that*

$$\left\| (\otimes_i V_i) |\Psi\rangle - |\psi\rangle |\mathrm{AUX}\rangle \right\|^2 \leq \delta_C \,,$$

and for all $W \in \{X, Z\}$,

$$\mathop{\mathrm{E}}_{w \in \mathbb{F}_q^m} \sum_{a \in \mathbb{F}_q} \left\| (\otimes_i V_i)(M^a_{W,w} \otimes \mathrm{Id}) |\Psi\rangle - (\tau^a_{W,w} \otimes \mathrm{Id}) |\psi\rangle |\mathrm{AUX}\rangle \right\|^2 \leq \delta_C \,.$$

Proof. Fix a strategy for the k provers in the test that is accepted with probability at least $1 - \varepsilon$. Fix any $t \in \{1, \ldots, k\}$. By combining the $(k-1)$ strategies employed by provers $\{1, \ldots, k\} \backslash \{t\}$, when they play the role of the composite prover, into a single strategy, we obtain a two-prover strategy for the test Q-LOWDEG$^{(2)}(m, d, q)$ that has success probability at least $1 - \varepsilon$. Applying Theorem 5.3.2 shows the self-testing claim for the observables applied by prover t, when designated as the special prover. The same applies for all $t \in \{1, \ldots, k\}$, proving the theorem. □

Remark 6.1.7. We record here the bit complexity of the protocol CODE-CHECK. The test invokes the composed quantum low-degree test Q-LOWDEG$^{(2)}(m, d, q)$ with $m = \lceil \frac{\log n}{\log \log n} \rceil$ and $d = \Theta(\frac{\log^2 n}{\log \log n})$. Hence, the number of bits in the verifier's questions scales as $O(\frac{\log n}{\log \log n} \log q)$, and the number of bits in the provers' responses scales as $O((\log \log n)^2 \log q)$, so the overall bit complexity is $O(\frac{\log n}{\log \log n} \log q)$.

6.2 Energy tests

In the previous section we gave a test that enforces that the provers' shared state is close to a valid code state of an error-correcting code. In this section, we show how to further test any property of the encoded state that can be expressed in terms of a local Hamiltonian of the appropriate form. We achieve this by using interactive protocols to "command" the provers to measure a subset of the terms of a given Hamiltonian, perform a computation on the measurement outcomes, and return the result. We introduce the required tools from the classical PCP literature in Section 6.2.1, and adapt them to our setting in Section 6.2.2 and Section 6.2.3. In Section 6.2.4 we give a protocol to estimate the ground energy of a (not necessarily local) Hamiltonian up to constant precision, provided that the terms of the Hamiltonian have a certain form. As a consequence, we show that is QMA-hard to approximate the maximum success probability of a nonlocal game (i.e. one-round MIP* protocol) with logarithmic communication, either conditionally on the constraint satisfaction quantum PCP conjecture (Corollary 6.2.13), or unconditionally, but under randomized reductions (Corollary 6.2.14). In Section 6.2.5 we use similar tools to give a protocol to estimate the ground energy of a class of (not necessarily local) frustration-free Hamiltonians up to inverse polynomial accuracy.

As a note on terminology, in previous sections, we introduced "tests" for states with certain properties, such as of being a valid codestate. In this section we provide tests for states that encode the answer to a computational problem (in particular, variants of the local Hamiltonian problem). To formulate these tests we use the language of interactive proofs, and often refer to a test for a property as an MIP* protocol for the corresponding computational problem. The notions of a test, a nonlocal game, and a one-round MIP* protocol are roughly synonymous, and their meaning should always be clear from context.

6.2.1 Classical PCPs for linear functions

The codeword test introduced in Section 6.1 gives the verifier the ability to query a prover for a location in the low-degree encoding of the string of outcomes obtained by the prover when measuring all its qudits in the Pauli X or Z basis. For our applications, we would like to have the ability to command the provers to compute more general functions of their measurement outcomes. For example, upon obtaining an outcome $a \in \mathbb{F}_q^n$, we may want to ask the prover to compute the inner product $a \cdot b$ with a given string $b \in \mathbb{F}_q^n$ (that may not necessarily correspond to an entry in the low-degree encoding of a), agreed on in advance between the prover and the verifier. One approach to doing this is to use the sum-check protocol of [LFKN92], but this requires a logarithmic number of rounds of interaction, resulting in a polylogarithmic number of bits of communication. To achieve a protocol with logarithmic communication we rely on the following classical PCP construction, that can be extracted from [BSGH+05].

Theorem 6.2.1. *Let $p = 2$, $n, t \geq 1$ integer such that $t = \Theta(\log \log n)$, and $q = 2^t$. For any $a, b \in \mathbb{F}_q^n$, there exists a proof $\Pi_{a,b} \in \mathbb{F}_q^{n'}$, with $n' = O(\mathrm{poly}(n))$, each of*

whose bits is an $\mathbb{F}_q$-linear function of a, such that the following holds. There exists an efficient test $\text{LIN}(b)$ *that uses $O(\log n)$ random bits and reads a total of $O(1)$ bits from $\Pi_{a,b}$ and from the evaluation table of the low-degree extension g_a of a, as well as a value $c \in \mathbb{F}_q$, with the following properties:*

1. *Completeness: If $b \cdot a = c$ the test accepts with certainty.*
2. *Soundness: If $b \cdot a \neq c$, for any claimed proof Π, the test rejects with constant probability.*

Proof. We use the language of "PCPs of proximity" from [BSGH+05]. A PCP of proximity (PCPP) consists of an algorithm V to verify that a given input $a \in \{0,1\}^n$ (called the *assignment*) satisfies a *property* specified by a poly-sized Boolean circuit. The verifier V is given access to a and to an auxiliary proof string Φ of polynomial length, but is only allowed to query a small (e.g. constant) number of bits of a and Φ. The completeness and soundness requirements on the verifier are that whenever a satisfies the property (the YES case), there exists a proof Φ_a that convinces the verifier V to accept with certainty, and when a is (δn) far in Hamming distance from any string a' satisfying the property (the NO case), then for all proofs Φ, the verifier V rejects with at least constant probability. The parameter δ is called the *proximity parameter* of the PCPP.

From [BSGH+05, Theorem 3.3], with the parameter t appearing in that theorem[3] chosen to be a constant greater than 3, and for a proximity parameter $\delta = \Theta(1/t)$, there exists a PCPP for properties encoded by circuits of size $O(n)$, consisting of a proof Π and verifier V that uses $O(\log^{2/t} n)$ random bits, reads $O(t) = O(1)$ bits of the proof and assignment, and in the NO case rejects with probability $\Omega(1/t)$. Moreover, from the discussion in Section 8.4 of [BSGH+05] it follows that if the property can be expressed as an AND of linear constraints (i.e. of the form $b \cdot a = c$ over $\mathbb{F}_2$), then the bits of the proof string Φ are $\mathbb{F}_2$-linear functions of the assignment, and the checks performed by the verifier V are $\mathbb{F}_2$-linear constraints on Φ.

Ideally, we would like to directly apply this PCPP to check that the string $a \in \mathbb{F}_q^n$, interpreted as a bit string in $\{0,1\}^{nt}$, satisfies the condition $b \cdot a = c$, which is a linear condition over $\mathbb{F}_q$. To do this, we need to address two issues. First, the result of [BSGH+05] applies to $\mathbb{F}_2$-linear conditions, and the proof string $\tilde{\Pi}$ is an $\mathbb{F}_2$-linear function of the input, whereas the present theorem requires linearity over $\mathbb{F}_q$. We resolve this by noting that the $\mathbb{F}_q$-linear condition $b \cdot a = c$ can be expressed as a conjunction of $\mathbb{F}_2$-linear conditions $\text{tr}[(b \cdot a)\chi_i] = \text{tr}[c\chi_i]$ for every element χ_i of a self-dual basis for $\mathbb{F}_q$ over $\mathbb{F}_2$. Moreover, any $\mathbb{F}_2$-linear function $f : \mathbb{F}_2^{tn} \to \mathbb{F}_2$ can be expressed a function $f : \mathbb{F}_q^n \to \mathbb{F}_2$ of the form $\text{tr}[u \cdot a]$ for some $u \in \mathbb{F}_q^n$, and hence can be extended to an $\mathbb{F}_q$-linear function $\underline{f} : \mathbb{F}_q^n \to \mathbb{F}_q$ given by $\underline{f} = u \cdot a$. Applying this extension to each bit of Φ, we can construct a proof $\Pi_{a,b} \in \mathbb{F}_q^{\text{poly}(n)}$, such that each entry of $\Pi_{a,b}$ is an $\mathbb{F}_q$-linear function of a, and from which the PCPP verifier can recover the original proof Φ by taking the trace of each entry. Since $\tilde{\Pi}$ could

[3]Not to be confused with our parameter t, which controls the field size!

be verified by querying a constant number of bits, Π can be verified by querying a constant number of $\mathbb{F}_q$-valued entries.

The second issue concerns the soundness of the proof system. The statement of the present theorem requires soundness to hold against all non-satisfying a, not just those that satisfy the promise of the PCPP. Thus, instead of applying the PCPP directly to a, we apply it to the evaluation table of the low-degree encoding g_a of the assignment, which has length $O(n \log n)$. The condition $b \cdot a = c$ can be expressed as a linear condition on the evaluation table of g_a. Moreover, if $b \cdot a \neq c$, then the encoding g_a differs from the encoding $g_{a'}$ of any a' such that $b \cdot a' = c$ on at least a constant fraction of positions. (This follows from the Schwartz-Zippel lemma: if $a \neq a'$, then $g_a - g_{a'}$ is a nonzero polynomial and hence by Lemma 5.2.1, it cannot be 0 on more than $d/|\mathbb{F}_q|$ fraction of the points.) Hence, the soundness promise holds on the encoded input g_a. Finally, to check that the part of the proof that corresponds to g_a is a valid low-degree encoding, the verifier executes a standard low-degree test (such as the PCP version of the test C-LOWDEG); this can be done using a constant number of additional queries to the evaluation table of g_a (provided restrictions to lines and planes are included). □

6.2.2 A test for non-local Pauli observables

Theorem 6.2.1 specifies a test certifying that $a \cdot b = c$, given $O(1)$ queries to a proof $\Pi_{a,b}$ whose bits are $\mathbb{F}_q$-linear functions of a. Based on this test, in Figure 6-2 we give a multiprover protocol $\text{SUM}(C, W, b)$ in which the verifier commands one of k provers (supposedly) sharing an encoding of a state $|\psi\rangle$ according to C to measure their share of the state in a specified basis (X or Z) to obtain an assignment a, and report the value $a \cdot b$. The verifier checks that this value was computed correctly by using the test $\text{LIN}(b)$ from Theorem 6.2.1, together with the guarantees of the low-degree test. The test $\text{LIN}(b)$ requires a constant number of queries to both g_a and $\Pi_{a,b}$. In order to aggregate these queries, the verifier first asks the provers to encode $\Pi_{a,b}$ as a low-degree polynomial h; to query a constant number of entries of $\Pi_{a,b}$ the verifier then asks for the restriction $h|_s$ of h to a curve s that goes through all points to be queried. However, the number of bits required to specify the restriction $h|_s$ is, for our choice of parameters, polylogarithmic in n. To get around this we apply composition, in a similar way to the composed low degree test (Theorem 5.2.10). For concreteness, we explicitly state how to do this, following the variable substitution technique in [Vid13, Section 3.1.2], which appeared earlier in [DFK+11, Section 4.4].

Definition 6.2.2. Define the substitution map

$$\#_d : \mathbb{F}_q \to \mathbb{F}_q^{\mu(d)} , \quad \#(x) = (x, x^2, x^4, \ldots, x^d) , \tag{6.1}$$

where $\mu(d) = 2\lceil \log(d+1) \rceil$.

Under this map, any univariate degree-d polynomial $f(x)$ can be viewed as a degree $\delta(d) = O(\log d)$, $\mu(d)$-variate polynomial $f(\#x)$, by formally identifying powers of x with products of the substituted variables. Thus, instead of querying for the

restriction $h|_s$, we view this restriction itself as a multivariate polynomial over $\mathbb{F}_q^{\mu(d)}$, and query the restriction of that polynomial to a curve over $\mathbb{F}_q^{\mu(d)}$. This can be described in logarithmically fewer bits. The precise form of the queries we make to the prover is specified in Figure 6-2.

Before stating the completeness and soundness properties of the test $\text{SUM}(C, W, b)$, we state the strategy followed by the honest prover.

Definition 6.2.3. In the game $\text{SUM}(C, W, b = \{b_1, \ldots, b_k\})$, the honest strategy is defined as follows:

- State: the provers share a state $|\Psi\rangle$ which is a qubit-by-qubit encoding of a state $|\psi\rangle \in (\mathbb{C}^q)^{\otimes n}$ using the CSS code $\mathcal{C}$ derived from the self-dual classical code C.

- Measurements: each prover performs a measurement of each of its qudits in the basis W, to obtain as outcome a string $a \in \mathbb{F}_q^n$. Using a, the prover determines a polynomial $g_a : \mathbb{F}_q^m \to \mathbb{F}_q$. In addition, the prover may be sent a vector $b_j \in \mathbb{F}_q^n$. If this is the case, the prover replies with $c = a \cdot b_j \in \mathbb{F}_q$. In addition, it computes a polynomial $h_a : \mathbb{F}_q^{m'} \to \mathbb{F}_q$ that is a low-degree extension $h_a = g_{\Pi_{a,b_j}}$ for the PCPP proof Π_{a,b_j} that verifies $c = a \cdot b_j$, as described in Theorem 6.2.1. Finally, the prover is sent a pair (s, s'). Here s (resp. s') may be: a question from the tests $\text{Q-LOWDEG}^{(2)}$ (resp. $\text{C-LOWDEG}^{(2)}$), or, in part (c) of the test, a single point in $\mathbb{F}_q^m$ (resp. $\mathbb{F}_q^{m'}$), or a specification of a curve of constant degree in $\mathbb{F}_q^m$ (resp. $\mathbb{F}_q^{m'}$) together with a point or a curve in the space $\mathbb{F}_q^{\mu(d)}$ (resp. $\mathbb{F}_q^{\mu(d')}$). The honest prover responds with the appropriate restriction of g_a (resp. h_a), composed with the variable substitution map whenever appropriate.

Theorem 6.2.4. *Let C be a $[k, k']$ weakly self-dual linear code. Let n be an integer, and d, m, q integer such that $q = 2^t$ and $d, m, \log q$ are polynomially bounded in n. Let $\varepsilon \geq d/q$. Let $b_1, \ldots, b_k \in \mathbb{F}_q^n$. The procedure $\text{SUM}(C, W, \{b_1, \ldots, b_k\})$ is a 1-round, k-prover interactive protocol with the following completeness and soundness properties.*

1. Completeness: *If the provers follow the strategy introduced in Definition 6.2.3, they pass the test with certainty.*

2. Soundness: *Suppose that a strategy for the provers is accepted with probability at least $1 - \varepsilon$ in $\text{SUM}(C, W, \{b_1, \ldots, b_k\})$. Suppose further that the restriction of the strategy to questions formatted as in $\text{Q-LOWDEG}^{(2)}(m, d, q)$ succeeds in that test with probability at least $1 - \varepsilon$. Then there is a $\delta = \text{poly}(\varepsilon, \delta_C)$, where δ_C is as specified in Theorem 6.1.6, such that the following holds. There exists an encoded state $|\Psi\rangle \in (\mathbb{C}^q)^{\otimes nk}$ such that the value returned by the verifier in step (d) of the protocol has expectation that is within δ of $\langle\Psi| \otimes_{i=1}^k \tau_W(b_i)|\Psi\rangle$.*

Remark 6.2.5. The number of bits communicated to a prover in SUM is at most the number of bits needed in the (composed) low-degree test, plus the number of bits needed to specify a constant-degree curve over $\mathbb{F}_q^n$. By Theorem 5.3.2, both are at most $O(m \log q) = O(\frac{\log n}{\log \log n} \log q)$. The number of bits in the provers' answers is at most

Test SUM$(C, W, b = \{b_1, \ldots, b_k\})$:
The verifier sends the basis label W to all provers. In the test, the verifier sends pairs of questions, generally formatted as in the test Q-LOWDEG$^{(2)}(m, d, q)$ and C-LOWDEG$^{(2)}(m', d, q)$. We write the first question as s, and the second as s'. Note that, as in Q-LOWDEG(m, d, q), s (resp. s') itself can consist of a point in $\mathbb{F}_q^m$ (resp. $\mathbb{F}_q^{m'}$), or a pair (s_1, s_2) (resp. s_1', s_2') of subspaces.

(a) Send the special prover a question $s = (s_1, s_2)$ distributed as in Q-LOWDEG$^{(2)}(m, d, q)$ (conditioned on the basis choice W having been made). Receive a polynomial $r \in \deg_d(s_2)$. Send the composite prover the composite query $(\boldsymbol{b_{t'}, (s, s')})$ consisting of the vector $b_{t'}$ as well as a question (s, s'), where s' is distributed as in C-LOWDEG$^{(2)}(m', d, q)$. Receive the composite answer $\boldsymbol{(r', r'')}$. Reject if $r \neq \boldsymbol{r'}$.

(b) Send b_t, where t is the index of the special prover, to both provers. Execute the tests Q-LOWDEG$^{(2)}(m, d, q)$ and C-LOWDEG$^{(2)}(m', d, q)$ in parallel. Accept if and only if the provers' answers pass both tests.

(c) Send $b_{t'}$ to both provers. Simulate the test LIN$(b_{t'})$ from Theorem 6.2.1 to obtain a tuple $(x_1, \ldots, x_\ell, i_1, \ldots, i_{\ell'})$ of queries, where $x_i \in \mathbb{F}_q^m$ are queries to g_a and i_j are indices of bits to be queried in the PCPP proof $\Pi_{a,b}$. Let s_1 be a constant-degree curve in $\mathbb{F}_q^m$ that goes through all the x_i, i.e. a constant-degree polynomial $s_1 : \mathbb{F}_q \to \mathbb{F}_q^m$ whose image contains each point x_i, and likewise s_1' a constant-degree curve in $\mathbb{F}_q^{m'}$ that goes through all $\pi(i_j)$. Moreover, let s_2 be a constant-degree curve in $\mathbb{F}_q^{\mu(d)}$ that goes through all of the points $\#(s_1^{-1}(x_i))$, and let s_2' be a constant-degree curve in $\mathbb{F}_q^{\mu(d')}$ that goes through all of the points $\#((s_1')^{-1}(\pi(i_{ij})))$, where $\#$ and $\mu(\cdot)$ are as in Definition 6.2.2. Perform one of the following tests with probability $\frac{1}{2}$ each.

(i) Choose uniformly random points y on s_1 and y' on s_1'. Send (y, y') to the special prover and $\boldsymbol{((s, \#y), (s', \#y'))}$ to the composite prover. Receive answers $(\alpha, \beta) \in \mathbb{F}_q^2$ and $\boldsymbol{(\gamma, \delta)} \in \mathbb{F}_q^2$, respectively. If $\alpha = \gamma$ and $\beta = \boldsymbol{\delta}$, then accept, else reject.

...

Figure 6-2: Procedure SUM(C, W, b), where C is a self-dual CSS code, $W \in \{X, Z\}$ a basis label, and $b = \{b_1, \ldots, b_k\}$, where each $b_j \in \mathbb{F}_q^n$.

(c) (ii) Send $((s_1, s_2), (s'_1, s'_2))$ to the special prover, and two points $(\boldsymbol{z}, \boldsymbol{z'})$ to the composite prover, where z is uniformly random in s_2 and z' is uniformly random in s'_2. Receive from the special prover a pair of polynomials (r, r'), where r is $\mu(d)$-variate and r' is $\mu(d')$-variate, and from the composite prover a pair of values $(\boldsymbol{\alpha}, \boldsymbol{\beta}) \in \mathbb{F}_q^2$. If the answers are consistent on points z, z' (i.e. $r(z) = \boldsymbol{\alpha}$ and $r'(z') = \boldsymbol{\beta}$) and if the entries of Π and g decoded from the answers r and r' on s and s' would be accepted in the test LIN(b), then accept, else reject.

(d) For $j \in \{1, \ldots, k\}$, send the j-th prover the vector b_j and a query $((s_1, s_2), (s'_1, s'_2))$ chosen as in part (c). Receive from each prover a value $c_j \in \mathbb{F}_q$, as well as a pair of polynomials (r_j, r'_j). If for each prover j, the entries of Π and g decoded from r_j and r'_j would be accepted in the test LIN(b_j), then return $\omega^{\mathrm{tr}[\sum_{j=1}^k c_j]}$.

Figure 6-2: Procedure SUM(C, W, b), where C is a self-dual CSS code, $W \in \{X, Z\}$ a basis label, and $b = \{b_1, \ldots, b_k\}$, where each $b_j \in \mathbb{F}_q^n$ (continued).

the maximum of the number of bits needed in the (composed) low-degree test, and the the number of bits needed to specify a degree-$\delta(d) = O(\log d)$ polynomial restricted to a constant-degree curve. By Theorem 5.3.2, the former is at most $O(\log^2(d) \log(q))$, while the latter is at most $O(\log(d) \log(q))$.

Proof. Completeness follows from the definition of the honest strategy, Lemma 6.1.4 and the completeness of LIN(b) as described in Theorem 6.2.1.

We show soundness. A strategy for a prover in the test SUM(C, W, b) consists of a family of measurements $\{M^{r,r'}_{b,s,s'}\}$ used in response to questions of the form (s, s'). As the subscripts indicate, these measurements depend on the vector b received by the prover. In addition, part (a) of the test involves cross-checking these measurements with a strategy for the quantum low-degree test Q-LOWDEG$^{(2)}(m, d, q)$, in which the players are *not* told b. The strategy used for this test is described by measurements $\{N^r_s\}$, which do not depend on b.

We show the soundness of the test in two steps. First, we note that success in parts (a) and (b) of SUM$(C, W, \{b_1, \ldots, b_k\})$ implies that the measurements used by the players are close to product form:

$$M^{rr'}_{b,s,s'} \approx_{\mathrm{poly}(\varepsilon)} A^r_{b,s} B^{r'}_{b,s'},$$

where $A^r_{b,s} = \mathrm{E}_{s'} \sum_{r'} M^{rr'}_{b,ss'}$ and $B^{r'}_{b,s'} = \mathrm{E}_s \sum_r M^{rr'}_{b,ss'}$ are the measurements obtained by marginalizing the joint measurements $M^{r''}_{b,ss'}$. This follows from a standard "orac-

ularization" analysis, similar to the one in the proof of Theorem 5.2.6.

From success in part (a) of the test it follows that the measurements $A^r_{b,s}$ must be poly(ε)-close to the measurements N^r_s used in the test Q-LOWDEG$^{(2)}(m,d,q)$. By applying Theorem 6.1.6 to the strategy N^r_s, which is independent of b, this implies that, after applying a suitable isometry,

$$A^r_{b,s} \approx_{\mathrm{poly}(\varepsilon,\delta_C)} \tau^r_{W,s} = \sum_{a:\,(g_a)_{|s}=r} \tau^a_W \ ,$$

where $\tau^r_{W,s}$ is the measurement used in the honest strategy for Q-LOWDEG$^{(2)}(m,d,q)$ as defined in Definition 5.3.1. Moreover, this implies that the shared state is poly(ε,δ_C)-close, under the isometry, to some encoded state $|\Psi\rangle$.

Moreover, success in part (b) of the test implies that the measurements $\{B^{r'}_{b,s'}\}$ must constitute a good strategy for the classical low-degree test C-LOWDEG$^{(2)}(m',d,q)$ (in which the players *are* informed of b and j). This implies that there exists a measurement $\{B^h_b\}$ with outcomes h that are m'-variate degree-d polynomials over $\mathbb{F}_q$, such that

$$B^{r'}_{b,s'} \approx \sum_{h:h|_{s'}=r'} B^h_b \ .$$

Finally, from part (c), we conclude that the set of outcomes (g,h) that are such that the string $\Pi \in \mathbb{F}_q^{n'}$ for which h is the low-degree extension, together with g, are not accepted by the PCPP verifier, must have low probability of being obtained when performing the corresponding measurement. Hence, by the soundness of the PCPP from Theorem 6.2.1, it follows that, for each prover j, the polynomial g obtained by this prover encodes an assignment a_j which satisfies $b_j \cdot a_j = c_j$ with high probability. This implies that the expectation value of the output $\omega^{\mathrm{tr}[\sum_j c_j]}$ computed by the verifier in part (d) is close to the expectation value of the Pauli observable $\otimes_{i=1}^k \tau_W(b_i)$, as desired. □

6.2.3 Evaluating multiple-basis operators

Building on the test SUM, we design a test EVAL that can measure operators which are tensor products of both X- and Z-basis Paulis. In anticipation of our application to testing Hamiltonians, we describe EVAL as taking as input a distribution over logical operators to be measured. The process of translating these logical operators into physical operators to be measured by each prover is bundled into the test.

The procedure EVAL$_\xi(C,\pi,\overline{x},\overline{z})$ is described in Figure 6-3. It takes as input a $[k,k']$ weakly self-dual linear code C, a distribution[4] π over $\{S \subseteq \{1,\ldots,n\}\} \times \mathbb{F}_q^n \times \{\pm 1\}$, and strings $\overline{x},\overline{z} \in \mathbb{F}_q^k$ such that the operators $\overline{X} = \tau_X(\overline{x})$ and $\overline{Z} = \tau_Z(\overline{z})$ are respectively logical τ_X and τ_Z operators for the CSS code $\mathcal{C}$ associated with C. To

[4]There should be no confusion between π and the coordinate expansion map π used in previous sections.

Test $\text{EVAL}_\xi(C, \pi, \overline{x}, \overline{z})$: Given is a distribution π over $\{S \subseteq \{1, \ldots, n\}\} \times \mathbb{F}_q^n \times \{\pm 1\}$, a $[k, k']$ weakly self-dual linear code C, $\overline{x}, \overline{z} \in \mathbb{F}_q^k$ such that $\overline{X} = \tau_X(\overline{x})$ and $\overline{Z} = \tau_Z(\overline{z})$ are τ_X and τ_Z logical operators for $\mathcal{C}$ respectively, and a parameter $0 \leq \xi \leq 1$.
The verifier samples $(S, u, \epsilon) \sim \pi$. The verifier performs one of the following two tests, the first with probability $(1 - \xi)$, and the second with probability ξ:

(a) (Test) Let u_S and $u_{\overline{S}}$ be the substrings of u indexed by S and $\overline{S}$ respectively.

(i) Do either of the following, with probability 1/2 each:

1. Send either S, $\overline{S}$, $\emptyset$ or $\{1, \ldots, n\}$ to all provers, with probability 1/4 each. Execute the test CODE-CHECK(C, n).
2. Do as in 1., except the sets sent to the special and composite provers are complemented ($S, \overline{S}$ or $\emptyset, \overline{\emptyset}$), and so is the choice of basis W in CODE-CHECK(C, n).

(ii) Send S to the special prover, and either $\emptyset$ or $\overline{\emptyset}$ to the composite prover. Choose a random vector $v \in \mathbb{F}_q^k$ in the column span of G, as in Definition 6.1.3. Execute the test SUM$(C, X, \{v_1 s, v_2 s, \ldots, v_k s\})$ on query string $s = u_{\overline{S}}$ (case $\emptyset$) or $s = u_S$ (case $\overline{\emptyset}$). Reject if the test SUM rejects, or if the returned value is not 1.

(b) (Eval) Let u_S and $u_{\overline{S}}$ be the substrings of u indexed by S and $\overline{S}$ respectively. For $i \in \{1, \ldots, k\}$ let u_i be the string with substrings $u_{S,i} = \overline{x}_i u_S$ indexed on S and $u_{\overline{S},i} = \overline{z}_i u_{\overline{S}}$ indexed on $\overline{S}$. Send all provers the set S. Execute part (d) of SUM$(C, X, \{u_1, \ldots u_k\})$ with all the provers. Let E be the returned value. Return $\epsilon \cdot E$.

Figure 6-3: Procedure EVAL$(C, \pi, \overline{x}, \overline{z})$ to evaluate the expectation of a set of Pauli operators, chosen according to distribution π, on an encoded state.

any triple (S, u, ε) in the support of π we associate a qudit Pauli operator

$$h_S(u) = \otimes_{i \in S} \tau_X(u_i) \otimes_{i \in \overline{S}} \tau_Z(u_i) \,. \tag{6.2}$$

The procedure is divided into a "test" and an "eval" part. The relative weight given to each part is governed by the parameter $0 \leq \xi \leq 1$. The goal of the testing part is to ensure that the provers' answers in the evaluation part are distributed according to a distribution that can be obtained by performing Pauli measurements on the encoding of a fixed n-qudit state $|\psi\rangle$ using the CSS code $\mathcal{C}$ associated with C, where the Pauli τ_X and τ_Z are encoded using $\overline{X}$ and $\overline{Z}$ respectively. The test is formulated using the notion of "special" and "composite" prover introduced in Section 6.1.2; recall the scheme for distributing queries to the composite prover specified in Definition 6.1.3.

Lemma 6.2.6. *Let C be a $[k, k']$ weakly self-dual linear code and $\overline{X} = \tau_X(\overline{x})$, $\overline{Z} = \tau_Z(\overline{z})$ logical τ_X and τ_Z operators for the associated CSS code $\mathcal{C}$ respectively. Let n be an integer and π a distribution over $\{S \subseteq \{1, \ldots, n\}\} \times \mathbb{F}_q^n \times \{\pm 1\}$, and let ξ be a real number between 0 and 1. Then the procedure $\text{EVAL}_\xi(C, \pi, \overline{x}, \overline{z})$ has the following properties:*

- (Completeness) *For any state $|\psi\rangle \in (\mathbb{C}^q)^{\otimes n}$ there is a strategy for the provers that is accepted with probability 1 in part (a) of the test, and such that the value returned by the verifier in part (b), conditioned on the choice of (S, u, ϵ), has expectation $\epsilon \cdot \Re(\langle\psi|h_S(u)|\psi\rangle)$, where $h_S(u)$ is defined in (6.2).*

- (Soundness) *Suppose a strategy for the provers is accepted with probability at least $1 - \varepsilon$ in each of the "test" rounds of the procedure $\text{EVAL}_\xi(C, \pi, \overline{x}, \overline{z})$. Then there exists a state $|\psi\rangle \in (\mathbb{C}^q)^{\otimes n}$ such that, on expectation over $(S, u, \epsilon) \sim \pi$, the value returned by the verifier in step (b) of the protocol, conditioned on the choice of (S, u, ϵ), has expectation that is within $\text{poly}(\varepsilon, \delta_C)$ of $\epsilon \cdot \Re(\langle\psi|h_S(u)|\psi\rangle)$, where δ_C is as specified in Theorem 6.1.6.*

Remark 6.2.7. The amount of bits communicated to any prover in the procedure EVAL is at most the number of bits necessary to communicate an element sampled from π (which scales as the logarithm of the support size of π) plus the maximum of the number of bits communicated in either the SUM or CODE-CHECK tests. It follows from Remark 6.2.5 that the former requires $O(m \log q) = O(\frac{\log n}{\log \log n} \log q)$ bits, and from Remark 6.1.7 that the latter similarly requires $O(\frac{\log n}{\log \log n} \log q)$ bits.

Proof. We first show the completeness property. Let $|\psi\rangle \in (\mathbb{C}^q)^{\otimes n}$ and $|\Psi\rangle \in (\mathbb{C}^q)^{\otimes nk}$ a qudit-by-qudit encoding of $|\psi\rangle$ according to $\mathcal{C}$. The strategy for the provers uses $|\Psi\rangle$ as a shared state. When a prover is sent a set S, it immediately applies an F gate (5.9) to all qudits in S. If sent a query from the test CODE-CHECK, it applies the honest strategy for the test, as described in Lemma 6.1.5. If asked to execute the protocol $\text{SUM}(C, X, \{s_1, \ldots, s_k\})$, on a query string $s_j \in \mathbb{F}_q^n$, it measures all its qubits in the X basis to obtain a string $a \in \mathbb{F}_q^n$ and then executes the protocol honestly, following the strategy specified in Definition 6.2.3.

We verify that this strategy succeeds in each of the sub-tests of part (a) with probability 1. For (i) this is a direct consequence of success in CODE-CHECK and the fact that the code is self-dual; application of F merely exchanges the role of the X and Z bases for all provers. For (ii) this follows from the completeness property in Theorem 6.2.4.

Regarding soundness, assume that a strategy for the provers succeeds with probability at least $1 - \varepsilon$ in each of the sub-tests executed in part (a). Using (i)1., by Theorem 6.1.6, for each S the associated strategy is isometric to a δ_S-extension of a Pauli $\mathcal{C}$-codeword strategy, where $\mathrm{E}_{S\sim\pi}\, \delta_S = \delta_C(\varepsilon, q)$, as stated in the theorem. Note that in general the implied isometry depends on the choice of S. For the remainder of the proof, assume that a prover applies observable $\tau_{S,W}(w)$ when sent a query of the form (W, w), after having been told the set S. Using the symmetry in the tests we may also assume that $\tau_{S,X}(w) = \tau_{\overline{S},Z}(w)$ for all w and S.

Next consider part (ii). Since the composite prover is not sent the set S, the value $\boldsymbol{c}$ it claims also does not depend on S. Since the only way for the test SUM to return 1 in part (d) of the test is for the values $\boldsymbol{c}$ and c to have identical trace, from the previous analysis it follows that we may assume that the value $c = a \cdot s$ returned by the special prover is obtained from the outcome obtained by a measurement of the composite prover in the eigenbasis of $\tau_{\emptyset,X}$ (case $s = u_S$) or $\tau_{\emptyset,Z}$ (case $s = u_{\overline{S}}$).

As a result, the distribution of claimed values obtained in part (b) of the test is close to what would be obtained if all provers were to perform a measurement in the eigenbasis of $\tau_{\emptyset,X}$ for the qudits in S, and $\tau_{\emptyset,Z}$ for the qudits in $\overline{S}$. By definition of the strings $u_{S,i}$ and $u_{\overline{S},i}$ that are actually sent to prover i, the resulting physical observable implements the logical n-qudit observable $h_S(u)$, as desired. □

6.2.4 Efficient energy test for local Hamiltonians

We show how to use the EVAL test to estimate the energy of a Hamiltonian up to constant accuracy, provided that the terms of the Hamiltonian are (not necessarily local) Pauli operators of a particular form, which we call Y-free. From this, we deduce two results in the direction of the quantum games PCP conjecture: we show QMA-hardness of approximating the maximum success probability of a nonlocal game with logarithmic communication, either conditionally, assuming the Local Hamiltonian problem is QMA-complete for a constant-error approximation (Corollary 6.2.13), or unconditionally, under randomized reductions (Corollary 6.2.14).

Definition 6.2.8. Let n be an integer and q a prime power. We say that a Hamiltonian H on $(\mathbb{C}^q)^{\otimes n}$ is a Hamiltonian in Y-free form if H can be expressed as

$$H = \mathop{\mathrm{E}}_{S\subseteq\{1,\ldots,n\},u\in\mathbb{F}_q^n} \frac{\alpha_{S,u}}{2}\left(h_S(u) + h_S(u)^\dagger\right), \tag{6.3}$$

where each term $h_S(u)$ is a Pauli operator of the form described in (6.2), the weights $\alpha_{S,u} \in \mathbb{R}$ are such that $|\alpha_{S,u}| \leq 1$ for all (S, u), and the expectation is taken according to a distribution π with polynomial-size support.

The term Y-free refers to the fact that there are no Pauli Y operators (i.e. products of X and Z acting on the same qudit) in any of the terms. As motivation for considering this class of Hamiltonians, we remark that in the case of $q = 2$, i.e. for qubits, our definition of Y-free Hamiltonians includes the generalized XZ model of [CM14].[5] In that reference, it was shown that the local Hamiltonian problem for the XZ model is QMA-complete, for an inverse-polynomial promise gap. The class of Y-free Hamiltonians is considerably more general as it imposes no limits on the locality of the terms in the Hamiltonian, and accommodates qudits of dimension up to $\text{poly}(\log n)$.

The following lemma shows that it is possible to embed qubit Hamiltonians of the XZ model into qudit Y-free Hamiltonians with local dimension $q = 2^t$ for any t. This will be useful since the low-degree test requires fields of large enough size.

Lemma 6.2.9. *Given any Hamiltonian H in the XZ model over qubits, and $q = 2^t$, there exists a Hamiltonian H' in Y-free form over qudits of dimension q with the same spectrum (up to multiplicity) as H.*

Proof. Recall from Section 5.2.3 that when $q = 2^t$ for any t, the field $\mathbb{F}_q$ admits a self-dual basis over $\mathbb{F}_2$, and a qudit of dimension q decomposes as a tensor product of t qubits. Moreover, qubit Pauli operators $\{\sigma_{W,\ell}\}_{\ell \in \{1,\ldots,t\}}$ acting on a single "sub-qubit" can be recovered from the qudit Paulis by the formula

$$\sigma_{W,\ell} = \tau_W(b_\ell), \tag{6.4}$$

where $\{b_1, \ldots, b_t\}$ is a self-dual basis for $\mathbb{F}_q$ over $\mathbb{F}_2$. Extending this to multiple qudits, we can view a system of n qudits of dimension $q = 2^t$ each as a collection of tn qubits of dimension 2 each. Let us index these qubits by pairs (i, ℓ), where $i \in \{1, \ldots, n\}$ labels a qudit, and $\ell \in \{1, \ldots, t\}$ labels a sub-qubit of the ith qudit. Then, given a qubit Hamiltonian H over n qubits, we construct the desired H' by, for each qubit X or Z Pauli term in H acting on qubits i, j, including the corresponding Pauli term acting on qubits $(i, 1)$ and $(j, 1)$. By (6.4) this can be implemented by a generalized Pauli τ_X or τ_Z acting on qudits i and j, and hence H' is in Y-free form. Moreover, H' decomposes as a tensor product $H \otimes \text{Id}$ of H acting on qubits $(1, 1), (2, 1), \ldots, (n, 1)$, and Id acting on the remaining qubits. Hence H' has the same spectrum (up to multiplicity) as H. □

Given a Hamiltonian H in Y-free form provided as input, we describe a test whose maximum success probability is linearly related to the minimum energy of the Hamiltonian. The test requires the honest provers to share an encoding of a minimum-energy eigenstate of H according to a quantum code $\mathcal{C}$, and relies on the procedure EVAL described in Figure 6-3 to estimate the energy of the encoded state under H. The energy test is described in Figure 6-4, and its guarantees are stated in Theorem 6.2.10 below.

[5] Called the XY model in their convention; to convert to ours it suffices to relabel the Pauli Y and Z operators.

Test $\text{ENERGY}_\xi(C, H)$: Given as input is a Hamiltonian in Y-free form, specified by real coefficients $\{\alpha_{S,u}\}$ as in (6.3), a $[k, k']$ weakly self-dual linear code C such that the associated CSS code $\mathcal{C}$ encodes at least one logical qubit, and a parameter $0 \leq \xi \leq 1$.

1. Let $\overline{x}, \overline{z} \in \mathbb{F}_q^n$ be such that $\tau_X(a\overline{x})$ and $\tau_Z(b\overline{z})$ are logical $\tau_X(a)$ and $\tau_Z(b)$ operators for the code $\mathcal{C}$, respectively.

2. Let π be the distribution over $\{S \subseteq \{1, \ldots, n\}\} \times \mathbb{F}_q^n \times \{\pm 1\}$ that is obtained by sampling (S, u) uniformly, and returning $(S, u, \text{sign}(\alpha_{S,u}))$ with probability $|\alpha_{S,u}|$, and a symbol "$\perp$" with probability $1 - |\alpha_{S,u}|$.

3. Execute $\text{EVAL}_\xi(C, \pi, \overline{x}, \overline{z})$. If the element sampled from π is $\perp$, then automatically accept in case part (a) of the test is executed, and reject in case part (b) is executed. Otherwise, if the test returns ACCEPT or REJECT, then accept or reject accordingly. Finally, if the test returns a value e such that $\Re(e) \in [-1, 1]$, then accept with probability $\frac{1}{2}(1 - \Re(e))$.

Figure 6-4: Test $\text{ENERGY}_\xi(C, H)$ for the ground state of a Hamiltonian H in Y-freeform.

Theorem 6.2.10. *Let H be a Hamiltonian in Y-free form, C a weakly self-dual linear code, and $0 \leq \eta \leq 2$.*

- (Completeness) *If $\lambda_{\min}(H) \leq -1 + \eta$, there is a strategy for the provers such that for any $0 \leq \xi \leq 1$ the test $\text{ENERGY}_\xi(C, H)$ accepts with probability at least $1 - \frac{1}{2}\eta\xi$.*

- (Soundness) *If there exists a strategy with probability of success in the test $\text{ENERGY}_\xi(C, H)$ at least $1-\varepsilon$, then $\lambda_{\min}(H) \leq -1+\eta'$ for $\eta' = \frac{2\varepsilon}{\xi} + \text{poly}(\frac{\varepsilon}{1-\xi}, \delta_C(\frac{\varepsilon}{1-\xi}))$, where δ_C is as specified in Theorem 6.1.6.*

We show the completeness and soundness properties claimed in Theorem 6.2.10 in two separate lemma.

Lemma 6.2.11 (Completeness). *Let H be a Hamiltonian in Y-free form such that H has an eigenstate $|\psi\rangle$ with associated eigenvalue $\lambda \in [-1, 1]$, and $0 \leq \xi \leq 1$. Then for any weakly self-dual linear code C there is a strategy for the provers, based on sharing an encoding of the state $|\psi\rangle$ according to $\mathcal{C}$, whose success probability in the test $\text{ENERGY}_\xi(C, H)$ is $(1 - \xi) + \frac{\xi}{2}(1 - \lambda)$.*

Proof. Let $|\psi\rangle \in (\mathbb{C}^q)^{\otimes n}$ be as in the lemma, and $|\Psi\rangle \in (\mathbb{C}^q)^{\otimes kn}$ a qudit-by-qudit encoding of $|\psi\rangle$ under the code C, where each individual qudit is encoded according to the logical operators $\overline{x}$, $\overline{z}$ used by the verifier in the test ENERGY. When sent a query by the verifier, each prover applies the honest strategy in the test CODE-CHECK,

as specified in Lemma 6.1.5. By definition this strategy succeeds with probability 1 in part (a) of EVAL.

Regarding part (b), it follows from the definition of the distribution π and the completeness property of the procedure EVAL stated in Lemma 6.2.6 that the probability of accepting in the third step of the procedure ENERGY, conditioned on part (b) of EVAL being executed by the verifier, is precisely $\frac{1}{2}(1 - \langle\psi|H|\psi\rangle)$. □

Lemma 6.2.12 (Soundness). *Let H be a Hamiltonian in Y-free form, $0 \leq \xi \leq 1$ and C a weakly self-dual linear code. Suppose there exists a strategy for the provers whose success probability in the test $\text{ENERGY}_\xi(C, H)$ is $1 - \varepsilon$, for some $\varepsilon \leq \xi$. Then H has an eigenvector with energy at most $-1 + \frac{2\varepsilon}{\xi} + \text{poly}(\frac{\varepsilon}{1-\xi}, \delta_C)$.*

Proof. By definition of the test ENERGY_ξ, the provers' strategy must succeed with probability at least $1 - \frac{\varepsilon}{1-\xi} = 1 - \varepsilon'$ in part (a) of EVAL_ξ. Applying Lemma 6.2.6, it follows that the value returned by the verifier in part (b) of the test is a random variable whose expectation is within $\text{poly}(\varepsilon', \delta_C)$ of $\frac{1}{2}(1 - \langle\psi|H|\psi\rangle)$, for some state $|\psi\rangle$. Thus letting $\lambda = \langle\psi|H|\psi\rangle$ and p_a, p_b the provers' success probability in parts (a) and (b) of the test respectively we have

$$p_{\text{success}} = \frac{(1-\xi)}{2} p_a + \xi p_b \,,$$

thus $p_{\text{success}} \geq 1 - \varepsilon$ implies that $\xi p_b \geq \xi - \varepsilon$. Using that $p_b \leq \frac{1}{2}(1 - \lambda + \text{poly}(\varepsilon', \delta_C))$ yields

$$\lambda \leq -1 + \frac{2\varepsilon}{\xi} + \text{poly}(\varepsilon', \delta_C) \,,$$

giving the conclusion of the lemma. □

Corollary 6.2.13. *Assume the Local Hamiltonian problem for qubit Hamiltonians in the XZ model with promise gap $b - a = \Omega(1)$ is* QMA*-complete. Then, there is a one-round, 7-prover* MIP* *protocol for the class* QMA *with $O(\log(n))$-bits of communication and constant completeness-soundness gap.*

Proof. First, note that by the hardness assumption made in the corollary and Lemma 6.2.9, it follows that estimating the ground energy of qudit Hamiltonians with local dimension 2^t in Y-free form with $\Omega(1)$ promise gap is QMA-hard for any choice of t. Thus, to establish the conclusion, it suffices to show that there exists an MIP* protocol with the desired parameters for this variant of the Local Hamiltonian Problem.

Let a Hamiltonian in Y-free form be given, scaled such that the energy threshold in the YES case is $-1+\eta$, and in the NO case is $-1+\eta'$ with $\eta' - \eta = \Omega(1)$. Furthermore, let $q = 2^t$ where $t = \Theta(\log\log(n))$, and let C be the quadratic residue code from Example 6.1.2, which has $k = 7$. Using Theorem 6.2.10, the test $\text{ENERGY}_\xi(C, H)$ succeeds with probability $p_{\text{YES}} \geq 1 - \frac{\eta\xi}{2}$ in the YES case, and in the NO case with probability $p_{\text{NO}} \leq 1 - \varepsilon$ for ε such that

$$\frac{2\varepsilon}{\xi} + \text{poly}\left(\frac{\varepsilon}{1-\xi}, \delta_C\right) = \eta' \,, \tag{6.5}$$

where $\delta_C = \max(\text{poly}(\frac{\varepsilon}{1-\xi}), \text{poly}(q^{-1}))$. Denote the difference between these two probabilities by Δ; it is given by

$$\begin{aligned}\Delta &= p_{\text{YES}} - p_{\text{NO}} \\ &\geq \varepsilon - \frac{\eta\xi}{2} \\ &= \frac{\xi}{2}(\eta' - \eta) - \frac{\xi}{2}\,\text{poly}(\frac{\varepsilon}{1-\xi}, \delta_C)\,. \end{aligned} \tag{6.6}$$

For Δ to be positive it suffices to ensure that the quantity $\text{poly}(\frac{\varepsilon}{1-\xi}, \delta_C)$ is less than, say, $\frac{1}{2}(\eta' - \eta)$, which is a constant. Given the definition of δ_C and our choice of $q \sim n^{\log n}$, this can be ensured for some constant ε, ξ depending only on $\frac{1}{2}(\eta' - \eta)$. This results in a constant Δ. Therefore, the energy test $\text{ENERGY}_\xi(C, H)$ constitutes a MIP* protocol for QMA with a constant completeness-soundness gap. Regarding the communication cost, by plugging $q = O(\log \log n)$ into the bounds for the test EVAL given in Remark 6.2.7, we find that the test $\text{ENERGY}_\xi(C, H)$ requires $O(\log n)$ bits communication. □

Without making any assumptions, we can show a QMA-hardness result under randomized reductions.

Corollary 6.2.14. *It is* QMA*-hard under poly-time randomized Karp reductions to determine whether the maximum acceptance probability of a one-round* MIP* *protocol with logarithmic communication is at least* 1 *or at most* $\frac{1}{2}$.

The idea for the proof of Corollary 6.2.14 is to start with a QMA-hard instance of the Local Hamiltonian problem, with inverse-polynomial promise gap, and amplify this gap by taking a tensor power of the Hamiltonian. Expanding the tensor powers results in a Hamiltonian that is an average of exponentially many terms. We then apply the Ahlswede-Winter matrix Chernoff bound to randomly sub-sample a set of terms from the amplified Hamiltonian, yielding a Hamiltonian with polynomially many terms whose ground state energy can be tested using the ENERGY test.

Lemma 6.2.15 (Gap amplification, Lemma 26 of [NV17a] and Lemma 3.4.7 above)**.** *Let H be an n-qudit Hamiltonian with minimum energy $\lambda_{\min}(H) \geq 0$ and such that $\|H\| \leq 1$. Let $p(n), q(n)$ be polynomials such that $p(n) > q(n)$ for all n. Let*

$$H' = \text{Id}^{\otimes a} - (\text{Id} - (H - a^{-1}\,\text{Id}))^{\otimes a}, \qquad \textit{where} \qquad a = \left(\frac{1}{q} - \frac{1}{p}\right)^{-1}.$$

Then H' is a (non-local) Hamiltonian over $an = O(np(n))$ qudits with norm $\|H'\| = O(1)$ and with each term having norm $O(1)$, such that if $\lambda_{\min}(H) \leq 1/p$, then $\lambda_{min}(H') \leq 1/2$, whereas if $\lambda_{\min}(H) \geq 1/q$, then $\lambda_{min}(H') \geq 1$.

Proof of Corollary 6.2.14. We start by recalling that the Local Hamiltonian problem is QMA-complete for qubit Hamiltonians in the XZ model, up to inverse-polynomial promise gap [CM14]. Let

$$H = \mathop{\text{E}}_{j \in \{1,\ldots,\ell\}} H_j$$

be a given Hamiltonian on n qubits from the XZ model (also allowing terms that are multiples of the identity), with $\ell = \text{poly}(n)$ local terms H_j, normalized such that $0 \leq H \leq \text{Id}$. As can be seen from Definition 6.2.8, this Hamiltonian can be equivalently viewed as a Hamiltonian in Y-free form acting on qubits. We aim to give a protocol that distinguishes between the cases $\lambda_{\min}(H) \leq 1/p$ (YES) or $\lambda_{\min}(H) \geq 1/q$ (NO), where $0 \leq 1/p < 1/q \leq 1$ and p and q are polynomial functions of n. By applying Lemma 6.2.15 to H and scaling down the resulting Hamiltonian, we obtain a new Hamiltonian

$$H' = c\left(\text{Id}^{\otimes a} - (\text{Id} - (H - a^{-1}\,\text{Id}))^{\otimes a}\right)$$

acting on $an = \text{poly}(n)$ qudits with norm $\|H'\| = 1$ and all of whose terms have norms bounded by 1, such that $\lambda_{\min}(H') \leq c/2$ in the YES case and $\lambda_{\min}(H') \geq c$ in the NO case, for some constant $0 < c < 1$. For our purposes, it will be useful to express H' as an average

$$H' = \mathop{\mathrm{E}}_{J \in \{1,\ldots \ell'\}} H'_J\,,$$

where each term H'_J is of the form $c\,\text{Id}^{\otimes a} - \alpha_J h_{S_J}(u_J)$ for some Pauli operator $h_{S_J}(u_J)$ and weight $\alpha_J \in [-1, 1]$. The number of terms in this decomposition is $\ell' = (\ell + 1)^a$, which is exponential in n. This means that executing the test $\text{ENERGY}(C, H')$ would require $\text{poly}(n)$ bits of communication with the verifier, just to specify a single term in the Hamiltonian. To avoid this problem, we use randomness to sample a subset of the terms. First, rescale H' so that all of the terms are positive and have norm at most 1:

$$H'' = \mathop{\mathrm{E}}_{J \in \{1,\ldots,\ell'\}} H''_J\,, \qquad H''_J = \frac{1}{2}\left(H'_J + \text{Id} - c\right)\,.$$

This rescaled Hamiltonian satisfies $\lambda_{\min}(H'') = \frac{1}{2}(1 - c + \lambda_{\min}(H')) \geq \frac{1}{2}(1 - c)$. Now, let H''' be a Hamiltonian obtained by uniformly sampling m terms at random from H'', where m is a parameter to be chosen. By the matrix Chernoff Bound [AW02, Theorem 19], for any $\varepsilon \in [0, 1/2]$,

$$\Pr[\lambda_{\min}(H''') \notin [(1-\varepsilon)\lambda_{\min}(H''), (1+\varepsilon)\lambda_{\min}(H'')]] \leq 2 \cdot \exp\left(an \ln 2 - m\frac{\varepsilon^2 \lambda_{\min}(H'')}{2 \ln 2}\right).$$

In particular, taking $\varepsilon \leq c/(4 - 2c)$ and $m = \text{poly}(n)$, we obtain that, with probability exponentially close to 1, in the YES case $\lambda_{\min}(H''') \leq c_1$ and in the NO case $\lambda_{\min}(H''') \geq c_2$ where $c_2 - c_1 \geq c/8$. Moreover, H''' is a Y-free Hamiltonian with polynomially many terms. Hence, by the same arguments as in the proof of Corollary 6.2.13, there exists a 7-prover MIP^* protocol with $O(\log(n))$-bit messages and constant completeness-soundness gap to estimate the ground energy of H''' up to precision $c/16$, and hence to solve the Local Hamiltonian problem for H. □

6.2.5 Energy test for frustration-free Hamiltonians with small gap

In this section we show how the procedure SUM can be used in a different scenario than the one considered in the previous section: the case of an n-qubit Hamiltonian that is either frustration-free, or has ground state energy that is at most an inverse polynomial in n. The tests described in this section are more restrictive than those considered in the previous section, but they have the advantage of not relying on a randomized reduction. They apply to the following form of "linear XZ Hamiltonian".

Definition 6.2.16. A n-qudit Hamiltonian H, where each qudit has dimension a prime power q, is in *linear XZ form* if it can be written as

$$H = \mathop{\mathrm{E}}_{W\in\{X,Z\},j\in\{1,\ldots,\ell\}} \Pi_{W,j} \ ,$$

where the expectation is taken under the uniform distribution, and for each $W \in \{X, Z\}$ and $j \in \{1, \ldots, \ell\}$ the term $\Pi_{W,j}$ is a projector that is diagonal in the basis W (for each qubit), and such that the nullspace of $\Pi_{W,j}$ can be described by a collection of $t_{W,j}$ linear equations $\{s_{W,j,i} \cdot a = b_{W,j,i}, i \in \{1, \ldots, t_{W,j}\}\}$ over $\mathbb{F}_q$, where here $a = (a_1, \ldots, a_n) \in \mathbb{F}_q^n$ specifies a basis state $|a\rangle_W$ in basis W for the n qudits, and $s_{W,j,1}, \ldots, s_{W,j,t_j} \in \mathbb{F}_q^n$ and $b_{W,j,i} \in \mathbb{F}_q$ are coefficients of linear equations.

Note that a special case of the definition is one in which some of the $\Pi_{W,j}$ have rank 1, since any fixed element $a \in \mathbb{F}_q^n$ can be uniquely specified by a system of n linear equations.

A Hamiltonian H in linear XZ form is specified by the collection of equations $\{(s_{W,j,i}, b_{W,j,i}), W \in \{X, Z\}, j \in \{1, \ldots, \ell\}, i \in \{1, \ldots, t_j\}$. We will be interested in the problem of deciding whether H has ground state energy 0, or at least some inverse polynomial in n, $\gamma(n)$. Replacing each $\Pi_{W,j}$ in H by an average of $t_{W,j}$ terms, each associated with a single equation $(s_{W,j,i}, b_{W,j,i})$, preserves the distinction between these two cases, up to a polynomial multiplicative scaling in γ. Therefore, for the remainder of this section we assume that $t_{W,j} = 1$ for all W, j, and write $(s_{W,j}, b_{W,j})$ for $(s_{W,j,1}, b_{W,j,1})$.

The main result of this section is an interactive protocol for deciding between the cases where a Hamiltonian H in linear XZ form is frustration free, or has energy at least some inverse polynomial in n. The main ingredients for the protocol are the low-degree test from Theorem 5.3.2 and the test SUM. As for the case of the Y-free Hamiltonians considered in Section 6.2.4, it would be straightforward to extend the results of this section to Hamiltonians as in Definition 6.2.16, but allowing a polynomial number of possible basis choices for the n qudits, chosen among $\{X, Z\}^n$, instead of only X^n and Z^n. For simplicity, we focus on the case of two bases only.

We state the main result of this section.

Theorem 6.2.17. *Let n be an integer, $q = p^t$ a prime power such that $q = \Theta(\mathrm{poly}\log n)$, and $\gamma(n) = \Omega(\mathrm{poly}^{-1}(n))$. There exists a universal constant $\varepsilon_0 > 0$ and $N = O(\mathrm{poly}(n))$ such that the following holds. For any n-qudit Hamiltonian H in linear XZ form,*

Test $\mathrm{XZ}_N(H)$: Given as input is a n-qudit Hamiltonian in linear XZ form, where each qudit is of dimension a prime power q, and an integer N. Let C be a $[k, k']$ weakly self-dual linear code over $\mathbb{F}_q$, known to all parties, such that C encodes at least one qudit. The verifier performs one of the following, with probability $1/2$ each:

1. Select a basis $W \in \{X, Z\}$ uniformly at random. Select an equation (s, b) as described in the proof of Theorem 6.2.17 (this depends on the parameter N). Choose $\overline{w} \in \mathbb{F}_q^k$ to be a random vector such that $\tau_W(\overline{w})$ is a logical operator for $\mathcal{C}$, and execute the test $\textsc{sum}(C, W, \{\overline{w}_1 s, \overline{w}_2 s, \ldots, \overline{w}_k s\})$ with the provers. Reject if the protocol rejects, or if the linear combination $\sum_{i=1}^{k} c_k$ of the claimed values is not equal to E. Else, accept.

2. Execute test $\textsc{code-check}(C, n')$ with the provers, where $n' = Nn$ is as in the proof of Theorem 6.2.17.

Figure 6-5: Test $\mathrm{XZ}_N(H)$ for the ground state energy of a Hamiltonian H in linear XZ form.

- *If H has ground state energy 0, then there is a strategy for the provers that is accepted in the test $\mathrm{XZ}_N(H)$ with probability 1.*

- *If H has ground state energy at least $\gamma(n)$, then no strategy for the provers is accepted with probability more than $1 - \varepsilon_0$ in the test $\mathrm{XZ}_N(H)$.*

By basing the test on the code from Example 6.1.2, the test can be executed with 7 provers and a total amount of communication between the verifier and the provers that is $O(\log n)$.

Proof. We start by amplifying the promise gap by taking a tensor product of N copies of H, for $N = \lceil \delta \gamma^{-1}(n) \rceil$, for some $0 < \delta \leq 1$ to be determined. For any $W \in \{X, Z\}$ and $j \in \{1, \ldots, \ell\}$ let $\tilde{\Pi}_{W,j} = \mathrm{Id} - \Pi_{W,j}$. Define

$$\begin{aligned} H' &= \mathrm{Id} - (\mathrm{Id} - H)^{\otimes N} \\ &= \mathrm{Id} - (\mathop{\mathrm{E}}_{(W,j)} (\mathrm{Id} - \Pi_{W,j}))^{\otimes N} \\ &= \mathrm{Id} - \mathop{\mathrm{E}}_{W_1, j_1, \ldots, W_N, j_N} \tilde{\Pi}_{W_1, j_1} \otimes \ldots \otimes \tilde{\Pi}_{W_N, j_N} \,, \end{aligned} \tag{6.7}$$

where all expectation are uniform over the appropriate sets. Then $H' \geq 0$. If H is frustration-free then H' is frustration-free as well. If H has ground energy at least γ, then H' has ground energy at least $1 - e^{-\delta} \geq \delta/2$. Note that H' is again a Hamiltonian in linear XZ form such that H' acts on $n' = Nn$ qudits.

For any $\mathbf{W} = (W_1, \ldots, W_N)$ and $\mathbf{j} = (j_1, \ldots, j_N)$ let $\tilde{\Pi}^X_{\mathbf{W},\mathbf{j}} = \otimes_{i=1}^N \tilde{\Pi}^X_{W_i, j_i}$, where $\tilde{\Pi}^X_{W,j} = \tilde{\Pi}_{W,j}$ if $W = X$ and $\tilde{\Pi}^X_{W,j} = \mathrm{Id}$ otherwise. Define $\tilde{\Pi}^Z_{\mathbf{W},\mathbf{j}}$ similarly. From (6.7),

we get

$$H' = \mathrm{Id} - \mathop{\mathrm{E}}_{\mathbf{W},\mathbf{j}} \tilde{\Pi}^X_{\mathbf{W},\mathbf{j}} \tilde{\Pi}^Z_{\mathbf{W},\mathbf{j}} \,. \tag{6.8}$$

We use the following claim:

Claim 6.2.18. *Let A, B be two positive semidefinite operators such that $A, B \leq \mathrm{Id}$ and $AB = BA$. Then*

$$\mathrm{Id} - AB \leq \big(\mathrm{Id} - A\big) + \big(\mathrm{Id} - B\big) \,.$$

Proof. Note that since B commutes with A, it must also commute with the positive square root of A. Hence $AB = A^{1/2} B A^{1/2} \geq 0$. Likewise, $(\mathrm{Id} - A)$ commutes with $(\mathrm{Id} - B)$, so $(\mathrm{Id} - A)(\mathrm{Id} - B) \geq 0$. □

Starting from (6.8) and applying Claim 6.2.18,

$$H' \leq 2 \mathop{\mathrm{E}}_{W \in \{X,Z\}} \Big(\mathrm{Id} - \mathop{\mathrm{E}}_{\mathbf{W},\mathbf{j}} \tilde{\Pi}^W_{\mathbf{W},\mathbf{j}} \Big) \,. \tag{6.9}$$

For $W \in \{X, Z\}$ let $H'_W = \mathrm{Id} - \mathrm{E}_{\mathbf{W},\mathbf{j}} \tilde{\Pi}^W_{\mathbf{W},\mathbf{j}}$. If H' has ground energy zero, then both H'_Z and H'_X have ground energy zero as well. If H' has ground energy at least $\delta/2$, then for any vector $|\psi\rangle$, either $\langle\psi|H'_X|\psi\rangle \geq \delta/4$ or $\langle\psi|H'_Z|\psi\rangle \geq \delta/4$.

The goal of the test $\mathrm{XZ}_N(H)$ described in Figure 6-5 is to distinguish between these two cases. To complete the description of the test we specify how the linear equation (s, b) considered in item 1. of the test is obtained. First form the set $S = \{(s_\ell, b_\ell),\ 1 \leq \ell \leq t\}$ that is the union of all equations which specify the $+1$ eigenspace of each individual $\tilde{\Pi}_{W_i,j_i}$ such that $W_i = W$. Using the notation from Definition 6.2.16 we have $|S| = t = \sum_{i=1}^N 1_{W_i=W} t_{W,j_i}$, which is polynomial in n. Then (s, b) is obtained by sampling $(\delta/8)$-biased random variables $(y_1, \ldots, y_t) \in \mathbb{F}_q^t$ and setting $s = \sum_\ell y_\ell s_\ell$ and $b = \sum_\ell y_\ell b_\ell$. We refer to e.g. [AMN98] for a construction of such random variables using $\mathrm{poly}\log(t, q, \delta^{-1})$ random bits; note that this use of δ-biased random variables is analogous to their use in the classical exponential PCP for QUADEQ. Thus the amount of communication required to specify s to a prover is $\mathrm{poly}\log(t, q, \delta^{-1}) = \mathrm{poly}\log\log(n)$.

We show that the test $\mathrm{XZ}_N(H)$ satisfies the requirements of the theorem. We first argue completeness, and then soundness.

Claim 6.2.19 (Completeness)**.** *Suppose that H has ground energy 0. Then there is a strategy for the provers that is accepted with probability 1 in the test $\mathrm{XZ}_N(H)$.*

Proof. Let $|\psi\rangle$ be a ground state of H. Let C be the linear code used by the verifier. Consider the strategy for test CODE-CHECK(C, n') described in Lemma 6.1.5, where the encoded state is the n'-qudit state $|\psi\rangle^{\otimes N}$. From the lemma it follows that the strategy succeeds with probability 1 in item 2. of the test $\mathrm{XZ}_N(H)$.

It remains to describe the behavior of the provers when elected to perform the test SUM in item 1. of $\mathrm{XZ}_N(H)$. The prover j first measures its share of each qudit

in the basis W, obtaining outcomes $a_j \in \mathbb{F}_q^{n'}$. The prover then executes the honest behavior in test $\text{SUM}(C, W, \{\overline{w}_1 s, \ldots, \overline{w}_k s\})$, with the claimed value being $c_j = \overline{w}_j s \cdot a_j$. Moreover, since $|\psi\rangle$ is a ground state of H, the condition $\sum_j c_j = s \cdot \sum_j \overline{w}_j a_j = b$ is satisfied with certainty. Hence, the honest strategy is accepted with probability 1. □

The next claim shows soundness of the protocol.

Claim 6.2.20 (Soundness). *Suppose that H has ground energy at least γ. Then any strategy for the provers in the test $\text{XZ}_N(H)$ is accepted with probability at most $1-\delta_s$, for some $\delta_s = \max(\text{poly}(\delta), \text{poly}(q^{-1}))$.*

Proof. Fix a strategy for the provers that has success probability at least $1-\varepsilon$ in the test, for some $\varepsilon > 0$. This consists of a state $|\Psi\rangle$ and measurement operators $\{M_s^q\}$ for the special prover. The strategy must succeed with probability at least $1-2\varepsilon$ in item 2. of test $\text{XZ}_N(H)$. Applying Theorem 6.1.6, it follows that there exists a state $|\psi\rangle \in (\mathbb{C}^p)^{\otimes n'}$ such that, up to local isometries, $|\Psi\rangle$ is within distance δ_C of a valid $n'k$-qudit encoding of some state $|\psi\rangle$ according to the code C; under the same isometry, each prover's measurement upon query (W, w) is δ_C-close to an application of the observable $\tau_W(w_\pi)$ on the prover's share of the encoding. Up to an increase of δ_C in the error we assume for the remainder of the proof that all provers apply the honest strategy when given queries distributed as in the test CODE-CHECK.

We now analyze item 1. of test $\text{XZ}_N(H)$. By assumption, the honest strategy, based on state $|\psi\rangle$, succeeds with probability at least $1 - O(\delta_C)$ in this part of the test (we can assume $\delta_C \geq \varepsilon$ without loss of generality). Since H has ground energy at least γ, by (6.9) either $\langle\psi|H'_X|\psi\rangle \geq \delta/4$, or $\langle\psi|H'_Z|\psi\rangle \geq \delta/4$. Assume the former. This means that whenever each of the n' qudits of $|\psi\rangle$ is measured in the X basis, the probability that the outcome string a is such that a satisfies all linear equations $s_\ell \cdot a = b_\ell$, $\ell \in \{1, \ldots, t\}$, considered by the verifier, when the basis is chosen to be $W = X$, is at most $1 - \delta/4$. By definition of the equation (s, b), the probability (which now includes the verifier's coin tosses in selecting (s, b)) that $s \cdot a = b$ is at most $1 - \delta/8$. It follows from the soundness part of Theorem 6.2.4 that the provers must be rejected with probability $\text{poly}(\delta) - O(\delta_C)$. This gives a contradiction for any ε small enough such that $O(\delta_C) \ll \text{poly}(\delta)$. □

To conclude the proof of the theorem, we choose the constant δ to be sufficiently small so that δ_s in Claim 6.2.20 is a positive constant. □

Appendix A

The Parallel-Repeated Magic Square Game is Rigid

We show that the n-round parallel repetition of the Magic Square game of Mermin and Peres is rigid, in the sense that for any entangled strategy succeeding with probability $1 - \varepsilon$, the players' shared state is $O(\text{poly}(n\varepsilon))$-close to $2n$ EPR pairs under a local isometry. Furthermore, we show that, under local isometry, the players' measurements in said entangled strategy must be $O(\text{poly}(n\varepsilon))$-close to the "ideal" strategy when acting on the shared state.

A.1 Introduction

Nonlocal games have long been a fundamental topic in both complexity theory, especially the study of multiprover interactive proof systems, PCPs, and hardness of approximation, and in quantum information, starting from Bell's pioneering work in the 1960s. In both the quantum and the classical setting, games can be viewed as *tests* whereby a referee verifies that provers possess a certain resource: e.g., a satisfying assignment to a 3SAT formula. In the classical setting, due to a simple convexity argument, the optimal strategy of the provers in any game can always be described by a deterministic function returning an answer for every possible question the verifier can ask. However, in the quantum setting, provers have access to a much richer class of strategies: they are allowed to perform local measurements on their share of a shared entangled quantum state. This added power is both a blessing and a curse: it opens the door to quantum nonlocal games that test for uniquely quantum resources, such as a particular entangled state. However, it also makes it much harder to demonstrate the soundness of these tests against dishonest quantum provers.

The first indication of the power of nonlocal games to test quantum states was celebrated the result of Bell [Bel64], which showed that for a certain two-player nonlocal game, two players sharing a single pair of entangled qubits (an EPR pair) between them can win with substantially higher probability than they could by following the best classical strategy. In Bell's original game, the messages between the players and the referee were real numbers, but soon afteward, Clauser, Horne, Shimony, and

Holt [CHSH69] discovered a game (called the CHSH game) with similar properties, but with messages consisting of just one bit. The CHSH game is a test for the "quantumness" of a system, with good *soundness*: that is, the probability of a non-quantum system fooling the test is at most 3/4. However, the test lacks the property of so-called *perfect completeness*: as shown by Tsirelson [Cir80a], even the optimal quantum strategy succeeds with probability at most $(2+\sqrt{2})/4 \approx 0.854$. To remedy this drawback, Mermin [Mer90] and independently Peres [Per90] independently introduced the *Magic Square game*: a two-player game with two-bit inputs and outputs, and for which the best classical strategy succeeds with probability 8/9, but there exists a quantum strategy using only two shared EPR pairs succeeding with probability 1.

Later, Mayers and Yao [MY98] realized that the CHSH game could be used not only to test for "quantumness," but to test for a *specific* quantum state: namely, the EPR pair. Such a test is often called a "self-test." Mayers and Yao showed that in any optimal quantum strategy for CHSH, the players' shared state is equivalent under a local isometry[1] to an EPR pair. This result was not *robust* in that required the CHSH correlations to hold *exactly*: however, several subsequent works [MMMO06b, MYS12b, MS12] were able to achieve a robust self-test based on a game of Mayers and Yao, and later the CHSH game, for a single EPR pair. That is, they showed that for any strategy that wins CHSH with probability $\geq p_{\max} - \varepsilon$, there exists an isometry V mapping the players' state $|\psi\rangle$ to a state $|\phi\rangle$ which is $O(\sqrt{\varepsilon})$-close to the EPR pair state in 2-norm. Moreover, they showed that the *measurements* applied by the players must also be close to the measurements used in the ideal strategy, as measured in a state-dependent distance: for instance, if X is the operator applied by player 1 when asked to measure a Pauli X, then under the same isometry V, $\|V(X|\psi\rangle) - \sigma_X|\phi\rangle\| \leq O(\sqrt{\varepsilon})$, where σ_X is the Pauli X-matrix. Such a result is called a *rigidity* result, because it shows that any strategy that is close to optimal must have the same structure as the ideal strategy. We refer to the bound that appears in the right-hand side of the norm inequalities (here $\sqrt{\varepsilon}$) as the *robustness* of the test. These results have been extended by many authors [YN13, BP15, WCY+14, PVN14, BNS+15] to various families of few-qubit and few-qudit states; in particular, Wu et al. [WBMS16b] showed rigidity for Mermin and Peres's Magic Square game, demonstrating that it serves as robust self-test for a single EPR pair.

In recent years, self-testing has found applications to quantum cryptography (QKD, device independent QKD, and randomness expansion), as well as to multiprover quantum interactive proof systems (the complexity class MIP*) [RUV13b]. However, these applications all rely on testing *multi-qubit* states, whereas known robust self-testing results are directly applicable only to states of a few qubits. A natural strategy to obtain a multi-qubit test is to *repeat* the single-qubit tests, either in series (i.e. over many rounds) or in parallel (i.e. in one round)—for instance, the work of Reichardt, Unger, and Vazirani [RUV13b] uses a serially repeated CHSH test,

[1] Since either player could apply a local unitary to their half of the state and their measurements, without affecting their winning probability, equivalence under local isometry is the best one could hope for.

and McKague [McK15b] gives a parallel self-test based on CHSH. The lack of perfect completeness considerably complicates the analysis of these tests, since one cannot demand that the players win *every* repetition of the test—rather, one has to check whether the fraction of successful repetitions is above a certain threshold.

In this appendix, we circumvent these issues by studying the n-round parallel repetition of the Magic Square game. We achieve a proof of rigidity, showing that if the players win with probability $1 - \varepsilon$, their state is $O(\text{poly}(n\varepsilon))$-close to $2n$ EPR pairs, under a local isometry. This is an exponential improvement in error dependence over the strictly parallel self-testing result of [McK15b], which has error depedence $O(\exp(n)\,\text{poly}(\varepsilon))$ [2], and is the previous best known result for rigidity of strictly parallel repeated non-local games (McKague's result is stated for the parallel repeated CHSH game with a threshold test, rather than the parallel repeated Magic Square game). We note that McKague's result has $O(\log(n))$-bit questions, whereas our game has $O(n)$-bit questions and answers, but additionally robustly certifies all n-qubit measurement operators. This means that our result is a strictly parallel test, that can be used to "force" untrusted provers to apply all n-qubit Pauli operators faithfully (in expectation), which is a new feature that we believe will be valuable in the context of complexity applications.

As a fundamental building block for our result, we make use of the rigidity of a single round of the Magic Square game, which was established in [WBMS16b]. A key observation of our work is that, by leveraging a "global consistency check" which occurs naturally within the parallel repeated Magic Square game, we can establish approximate commutation between the different copies (or "rounds") of the game in the parallel repeated test. This then allows us to extend the single round analysis of [WBMS16b], to a full n-round set of approximate anti-commutation relations for the provers measurements, which is expressed in Theorem A.4.1. A second important technical tool in our proof is a theorem (Theorem A.4.2) which, given operators on the players' state that approximately satisfy the algebraic relations of single-qubit Pauli matrices, constructs an isometry that maps the players' "approximate Paulis" close to exact Pauli operators acting on a $2n$-qubit space. The proof of Theorem A.4.2 relies on an isometry inspired by the works of McKague [McK10, McK16a], but is designed to take the guarantees produced by Theorem A.4.1 and conclude closeness of the players "approximate Paulis" to exact Pauli operators in expectation, where all $2n$-qubit Pauli operators are handled simultaneously, with polynomial error dependence.

Very recently, we became aware of two independent works achieving related results in this area. The first is an unpublished paper of Chao, Reichardt, Sutherland, and Vidick [CRSV16], which proves a theorem similar to our Theorem A.4.2. The second is a paper by Coladangelo [Col16], which proves a self-testing result for the parallel repeated Magic Square game that is similar our own, albeit with slightly different polynomial factors. Furthermore, the robustness analysis of the results in [Col16] makes use of the same key theorem of [CRSV16], which is, in turn, similar to our

[2] Note that, by repeating the test in section 4 of [McK15b] a polynomial number of times, one can achieve a self-test for n EPR pairs with polynomial error dependence. However, the test given in section 4 is not a strictly parallel test, and does not robustly certify n-qubit measurement operators, as our result does.

own Theorem A.4.2. The theorem of [CRSV16] (and consequently the robustness result of Coladangelo) achieve a robustness of $n^{3/2}\sqrt{\varepsilon}$ for for all single-qubit operators (i.e., to achieve constant robustness, ε must scale as $1/n^3$). On the other hand, our Theorem A.4.2 achieves a robustness of $n\varepsilon^{1/4}$ (i.e. $\varepsilon \sim 1/n^4$) , but for operators acting on *all* $2n$ qubits simultaneously. It is natural to ask whether one can prove a single result which combines the strengths of these two different error dependencies. We expect that this is possible, but leave it for future work.

A.2 Preliminaries

We use the standard quantum formalism of states and measurements. An *observable* is a Hermitian operator whose eigenvalues are ± 1, and encodes a two-outcome projective measurement (the POVM elements of the two outcomes are the projections on to the $+1$ and -1 eigenspaces). Throughout this appendix, we make use of the Pauli matrices. These are 2×2 Hermitian matrices defined by

$$\sigma_X := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_Z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \sigma_Y := \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}.$$

They satisfy the anticommutation relation

$$XZ = -ZX.$$

To represent n-qubit tensor products of Paulis, we use the notation $\sigma_X(\mathbf{a})$ where $\mathbf{a} \in \{0,1\}^n$. This is defined to be the operator $\otimes_{i=1}^n (\sigma_{X,i})^{a_i}$ that applies σ_X to the ith qubit if $a_i = 1$, and the identity otherwise. We will also often consider the *sequential* product of many operators, denoted by $\prod_{i=1}^n S_i$. This means the product taken from left to right in the order from 1 to n, i.e. $S_1 S_2 \dots S_n$. Likewise, by $\prod_{i=n}^1 S_i$ we mean $S_n S_{n-1} \dots S_2 S_1$.

A.3 The Magic Square game

In this section we introduce the nonlocal game analyzed in this work: the n-round parallel repeated Magic Square game. We also introduce notation to describe entangled strategies for the game and state some simple properties they satisfy.

The parallel repeated Magic Square game is played between players (which we will refer to as Alice and Bob), and a verifier. First, let us define the single-round Magic Square game, originally introduced by Mermin [Mer90] and Peres [Per90]. The rules of the game are described in Fig. A-1. Any entangled strategy for this game is described by a shared quantum state $|\psi\rangle_{AB}$ and projectors $P_r^{a_0,a_1}$ for Alice and $Q_c^{b_0,b_1}$ for Bob. It can be seen that the game can be won with certainty for the following

The magic square game is a one-round, two-player game, played as follows

1. The verifier sends Alice a question $r \in \{0,1,2\}$ and Bob a question $c \in \{0,1,2\}$.
2. Alice sends the verifier a response $(a_0, a_1) \in \{0,1\}^2$, and Bob sends a response $(b_0, b_1) \in \{0,1\}^2$.
3. Let $a_2 := a_0 \oplus a_1$ and $b_2 := 1 \oplus b_0 \oplus b_1$. Then Alice and Bob win the game if $a_c = b_r$ and lose otherwise.

Figure A-1: The magic square game

strategy:

$$
\begin{aligned}
|\psi\rangle &= \frac{1}{2} \sum_{i,j \in \{0,1\}} |ij\rangle_A \otimes |ij\rangle_B \\
P_0^{a_0,a_1} &= \frac{1}{4}(I + (-1)^{a_0} Z)_{A1} \otimes (I + (-1)^{a_1} Z)_{A2} \otimes I_B \\
P_1^{a_0,a_1} &= \frac{1}{4}(I + (-1)^{a_1} X)_{A1} \otimes (I + (-1)^{a_0} X)_{A2} \otimes I_B \\
Q_0^{b_0,b_1} &= \frac{1}{4} I_A \otimes (I + (-1)^{b_0} Z)_{B1} \otimes (I + (-1)^{b_1} X)_{B2} \\
Q_1^{b_0,b_1} &= \frac{1}{4} I_A \otimes (I + (-1)^{b_1} X)_{B1} \otimes (I + (-1)^{b_0} Z)_{B2}
\end{aligned}
$$

This strategy is represented pictorially in Fig. A-2, where each row contains a set of simultaneously-measurable observables that give Alice's answers, and likewise each column for Bob.

ZI	IZ	ZZ
IX	XI	XX
-ZX	-XZ	YY

Figure A-2: The ideal strategy for a single round of magic square. Alice and Bob share the state $|\mathrm{EPR}\rangle^{\otimes 2}$.

The game we study in this appendix is the n-fold parallel repetition of the above game.

Definition A.3.1. The n-fold parallel repeated Magic Square game is a game with two players, Alice and Bob, and one verifier. The player sends Alice a vector $\mathbf{r} \in \{0,1,2\}^n$ and Bob a vector $\mathbf{c} \in \{0,1,2\}^n$, where each coordinate of $\mathbf{r}$ and $\mathbf{c}$ is chosen uniformly at random. Alice responds with two n-bit strings $\mathbf{a}_0, \mathbf{a}_1$, and Bob with two n-bit strings $\mathbf{b}_0, \mathbf{b}_1$. The players win if for every $k \in [n]$, the kth components of Alice

and Bob's answers $a_{0,k}, a_{1,k}, b_{0,k}, b_{1,k}$ satisfy the win conditions of the Magic Square game with input r_k and c_k.

Throughout this appendix we will refer to the non-local entangled strategy applied by the players according to the following definitions:

Definition A.3.2. Let $\{P_{\mathbf{r}}^{\mathbf{a}_0,\mathbf{a}_1}\}_{\mathbf{a}_0,\mathbf{a}_1}$ denote the set of orthogonal projectors describing Alice's measurement when she receives input $\mathbf{r}$.

Likewise, let $\{Q_{\mathbf{c}}^{\mathbf{b}_0,\mathbf{b}_1}\}_{\mathbf{b}_0,\mathbf{b}_1}$ denote the set of orthogonal projectors describing Bob's measurement when he receives input $\mathbf{c}$.

Definition A.3.3. Define $\mathbf{a}_2 \equiv \mathbf{a}_0 + \mathbf{a}_1 \pmod 2$ an $\mathbf{b}_2 \equiv \mathbf{b}_0 + \mathbf{b}_1 + \mathbf{1} \pmod 2$.

Definition A.3.4. Define the column-$\mathbf{c}$ output observables for Alice as $A_{\mathbf{r},\mathbf{p}}^{\mathbf{c}} \equiv \sum_{\mathbf{a}_0,\mathbf{a}_1} (-1)^{\mathbf{a}_\mathbf{c}\cdot\mathbf{p}} P_{\mathbf{r}}^{\mathbf{a}_0,\mathbf{a}_1}$.

Where $a_{\mathbf{c}}$ is defined to be the n dimensional vector whose i^{th} component is defined by $(a_{\mathbf{c}})_i \equiv (\mathbf{a}_{\mathbf{c}_i})_i$.

Similarly, define the row-$\mathbf{r}$ observables for Bob as $B_{\mathbf{c},\mathbf{q}}^{\mathbf{r}} \equiv \sum_{\mathbf{b}_0,\mathbf{b}_1} (-1)^{\mathbf{b}_\mathbf{r}\cdot\mathbf{q}} Q_{\mathbf{c}}^{\mathbf{b}_0,\mathbf{b}_1}$.

Remark A.3.5. By definition, it follows that $A_{\mathbf{r},\mathbf{p}}^{\mathbf{c}} = A_{\mathbf{r},\mathbf{p}}^{\mathbf{c}'}$ if $\mathbf{c}$ and $\mathbf{c}'$ differ only on rounds where the coordinate of $\mathbf{p}$ is 0, and likewise for B and $\mathbf{r}$.

The win conditions for magic square:

Fact A.3.6. *Suppose Alice and Bob win the magic square game with probability* $\geq 1 - \varepsilon$. *Then it holds that*

$$\forall \mathbf{p}, \quad \mathbf{E}_{\mathbf{r},\mathbf{c}} \langle\psi| A_{\mathbf{r},\mathbf{p}}^{\mathbf{c}} B_{\mathbf{c},\mathbf{p}}^{\mathbf{r}} |\psi\rangle \geq 1 - \varepsilon. \tag{A.1}$$

In Remark A.3.5, we noted that we can freely change the output column for Alice (resp. row for Bob) on the "ignored" rounds. In the following lemma, we show that we can also change the *input* row (resp. column), up to an $O(\varepsilon)$ error, provided that the strategy is ε close to optimal.

Lemma A.3.7. *Suppose Alice and Bob have an* ε*-optimal strategy. Then,* $\forall i, r, \mathbf{c}$,

$$\left|1 - \mathbf{E}_{\mathbf{r},\mathbf{r}':r'_i=r_i=r} \langle\psi| A_{\mathbf{r},\mathbf{e}_i}^{\mathbf{c}} \cdot A_{\mathbf{r}',\mathbf{e}_i}^{\mathbf{c}} |\psi\rangle\right| \leq 36\varepsilon$$

Proof. To start we define an extended state

$$|\sigma\rangle \equiv |\psi\rangle \otimes \frac{1}{\sqrt{3^{-(n-1)}}} \sum_{\mathbf{r}_{-i}} |\mathbf{r}_{-i}\rangle \otimes \frac{1}{\sqrt{3^{-(n-1)}}} \sum_{\mathbf{r}'_{-i}} |\mathbf{r}'_{-i}\rangle \otimes \frac{1}{\sqrt{3^{-(n-1)}}} \sum_{\mathbf{s}_{-i}} |\mathbf{s}_{-i}\rangle$$

as well as extended operators:

$$T \equiv \sum_{\mathbf{r}_{-i}} A_{\mathbf{r},\mathbf{e}_i}^{\mathbf{c}} \otimes |\mathbf{r}_{-i}\rangle\langle\mathbf{r}_{-i}| \otimes I \otimes I = \sum_{\mathbf{r}_{-i}} \sum_{\mathbf{s}_{-i}} A_{\mathbf{r},\mathbf{e}_i}^{c_i \cup \mathbf{s}_{-i}} \otimes |\mathbf{r}_{-i}\rangle\langle\mathbf{r}_{-i}| \otimes I \otimes |\mathbf{s}_{-i}\rangle\langle\mathbf{s}_{-i}|$$

Note that, by Remark A.3.5, these two definitions are equivalent because $A^{\mathbf{c}}_{\mathbf{r},\cdot\mathbf{e}_i}$ is identically equal to $A^{c_i\cup\mathbf{s}_{-i}}_{\mathbf{r},\mathbf{e}_i}$ by definition, regardless of the value of $\mathbf{s}_{-i}$. Further define

$$T' \equiv \sum_{\mathbf{r}'_{-i}} A^{\mathbf{c}}_{\mathbf{r}',\mathbf{e}_i} \otimes I \otimes |\mathbf{r}'_{-i}\rangle\langle\mathbf{r}'_{-i}| \otimes I = \sum_{\mathbf{r}'_{-i}}\sum_{\mathbf{s}_{-i}} A^{c_i\cup\mathbf{s}_{-i}}_{\mathbf{r}',\mathbf{e}_i} \otimes I \otimes |\mathbf{r}'_{-i}\rangle\langle\mathbf{r}'_{-i}| \otimes |\mathbf{s}_{-i}\rangle\langle\mathbf{s}_{-i}|,$$

as well as

$$\begin{aligned}
S &\equiv \sum_{\mathbf{r}_{-i}}\sum_{\mathbf{s}_{-i}} B^{r_i\cup\mathbf{r}_{-i}}_{\mathbf{c}_i\cup s_{-i},\mathbf{e}_i} \otimes |\mathbf{r}_{-i}\rangle\langle\mathbf{r}_{-i}| \otimes I \otimes |\mathbf{s}_{-i}\rangle\langle\mathbf{s}_{-i}| \\
&= \sum_{\mathbf{r}_{-i}}\sum_{\mathbf{s}_{-i}} B^{r_i\cup\mathbf{r}_{-i}}_{\mathbf{c}_i\cup s_{-i},\mathbf{e}_i} \otimes |\mathbf{r}_{-i}\rangle\langle\mathbf{r}_{-i}| \otimes \sum_{\mathbf{r}'_{-i}} |\mathbf{r}'_{-i}\rangle\langle\mathbf{r}'_{-i}| \otimes |\mathbf{s}_{-i}\rangle\langle\mathbf{s}_{-i}| \\
&= \sum_{\mathbf{r}'_{-i}}\sum_{\mathbf{s}_{-i}} B^{r'_i\cup\mathbf{r}'_{-i}}_{\mathbf{c}_i\cup s_{-i},\mathbf{e}_i} \otimes \sum_{\mathbf{r}_{-i}} |\mathbf{r}_{-i}\rangle\langle\mathbf{r}_{-i}| \otimes |\mathbf{r}'_{-i}\rangle\langle\mathbf{r}'_{-i}| \otimes |\mathbf{s}_{-i}\rangle\langle\mathbf{s}_{-i}| \\
&= \sum_{\mathbf{r}'_{-i}}\sum_{\mathbf{s}_{-i}} B^{r_i\cup\mathbf{r}'_{-i}}_{\mathbf{c}_i\cup s_{-i},\mathbf{e}_i} \otimes I \otimes |\mathbf{r}'_{-i}\rangle\langle\mathbf{r}'_{-i}| \otimes |\mathbf{s}_{-i}\rangle\langle\mathbf{s}_{-i}|,
\end{aligned}$$

where, to conclude equivalence of the different versions of the last definition, we are using Remark A.3.5 as well as the fact that $r_i = r'_i = r$, some fixed value. Now, note that:

$$\begin{aligned}
\langle\sigma|T\cdot S|\sigma\rangle = &\left(\langle\psi| \otimes \frac{1}{\sqrt{3^{-(n-1)}}}\sum_{\mathbf{r}_{-i}}\langle\mathbf{r}_{-i}| \otimes \frac{1}{\sqrt{3^{-(n-1)}}}\sum_{\mathbf{r}'_{-i}}\langle\mathbf{r}'_{-i}| \otimes \frac{1}{\sqrt{3^{-(n-1)}}}\sum_{\mathbf{s}_{-i}}\langle\mathbf{s}_{-i}|\right) \\
&\times \left(\sum_{\mathbf{r}_{-i}}\sum_{\mathbf{s}_{-i}} A^{c_i\cup\mathbf{s}_{-i}}_{\mathbf{r},\mathbf{e}_i} \otimes |\mathbf{r}_{-i}\rangle\langle\mathbf{r}_{-i}| \otimes I \otimes |\mathbf{s}_{-i}\rangle\langle\mathbf{s}_{-i}|\right) \\
&\times \left(\sum_{\mathbf{r}_{-i}}\sum_{\mathbf{s}_{-i}} B^{r_i\cup\mathbf{r}_{-i}}_{\mathbf{c}_i\cup s_{-i},\mathbf{e}_i} \otimes |\mathbf{r}_{-i}\rangle\langle\mathbf{r}_{-i}| \otimes I \otimes |\mathbf{s}_{-i}\rangle\langle\mathbf{s}_{-i}|\right) \\
&\times \left(|\psi\rangle \otimes \frac{1}{\sqrt{3^{-(n-1)}}}\sum_{\mathbf{r}_{-i}} |\mathbf{r}_{-i}\rangle \otimes \frac{1}{\sqrt{3^{-(n-1)}}}\sum_{\mathbf{r}'_{-i}} |\mathbf{r}'_{-i}\rangle \otimes \frac{1}{\sqrt{3^{-(n-1)}}}\sum_{\mathbf{s}_{-i}} |\mathbf{s}_{-i}\rangle\right) \\
= &\frac{1}{3^{-2(n-1)}}\sum_{\mathbf{r}_{-i},\mathbf{s}_{-i}} \langle\psi|A^{c_i\cup\mathbf{s}_{-i}}_{\mathbf{r},\mathbf{e}_i} B^{r_i\cup\mathbf{r}_{-i}}_{\mathbf{c}_i\cup s_{-i},\mathbf{e}_i}|\psi\rangle \cdot \left(\frac{1}{\sqrt{3^{-(n-1)}}}\sum_{\mathbf{r}'_{-i}}\langle\mathbf{r}'_{-i}|\right) \\
&\times \left(\frac{1}{\sqrt{3^{-(n-1)}}}\sum_{\mathbf{r}'_{-i}} |\mathbf{r}'_{-i}\rangle\right) \\
= &\frac{1}{3^{-2(n-1)}}\sum_{\mathbf{r}_{-i},\mathbf{s}_{-i}} \langle\psi|A^{c_i\cup\mathbf{s}_{-i}}_{\mathbf{r},\mathbf{e}_i} B^{r_i\cup\mathbf{r}_{-i}}_{\mathbf{c}_i\cup s_{-i},\mathbf{e}_i}|\psi\rangle
\end{aligned}$$

$$= \mathbf{E}_{\mathbf{r}_{-i},\mathbf{s}_{-i}} \langle\psi| A^{c_i \cup \mathbf{s}_{-i}}_{\mathbf{r},\mathbf{e}_i} B^{r_i \cup \mathbf{r}_{-i}}_{\mathbf{c}_i \cup s_{-i},\mathbf{e}_i} |\psi\rangle$$
$$\geq 1 - 9\varepsilon,$$

where the last line follows by Fact A.3.6. Similarly,

$$\begin{aligned}
\langle\sigma|T' \cdot S|\sigma\rangle = &\left(\langle\psi| \otimes \frac{1}{\sqrt{3^{-(n-1)}}} \sum_{\mathbf{r}_{-i}} \langle \mathbf{r}_{-i}| \otimes \frac{1}{\sqrt{3^{-(n-1)}}} \sum_{\mathbf{r}'_{-i}} \langle \mathbf{r}'_{-i}| \otimes \frac{1}{\sqrt{3^{-(n-1)}}} \sum_{\mathbf{s}_{-i}} \langle \mathbf{s}_{-i}| \right) \\
&\times \left(\sum_{\mathbf{r}'_{-i}} \sum_{\mathbf{s}_{-i}} A^{c_i \cup \mathbf{s}_{-i}}_{\mathbf{r}',\mathbf{e}_i} \otimes I \otimes |\mathbf{r}'_{-i}\rangle\langle \mathbf{r}'_{-i}| \otimes |\mathbf{s}_{-i}\rangle\langle \mathbf{s}_{-i}| \right) \\
&\times \left(\sum_{\mathbf{r}'_{-i}} \sum_{\mathbf{s}_{-i}} B^{r_i \cup \mathbf{r}'_{-i}}_{\mathbf{c}_i \cup s_{-i},\mathbf{e}_i} \otimes I \otimes |\mathbf{r}'_{-i}\rangle\langle \mathbf{r}'_{-i}| \otimes |\mathbf{s}_{-i}\rangle\langle \mathbf{s}_{-i}| \right) \\
&\times \left(|\psi\rangle \otimes \frac{1}{\sqrt{3^{-(n-1)}}} \sum_{\mathbf{r}_{-i}} |\mathbf{r}_{-i}\rangle \otimes \frac{1}{\sqrt{3^{-(n-1)}}} \sum_{\mathbf{r}'_{-i}} |\mathbf{r}'_{-i}\rangle \otimes \frac{1}{\sqrt{3^{-(n-1)}}} \sum_{\mathbf{s}_{-i}} |\mathbf{s}_{-i}\rangle \right) \\
= &\frac{1}{3^{-2(n-1)}} \sum_{\mathbf{r}'_{-i},\mathbf{s}_{-i}} \langle\psi| A^{c_i \cup \mathbf{s}_{-i}}_{\mathbf{r}',\mathbf{e}_i} B^{r_i \cup \mathbf{r}'_{-i}}_{\mathbf{c}_i \cup s_{-i},\mathbf{e}_i} |\psi\rangle \cdot \left(\frac{1}{\sqrt{3^{-(n-1)}}} \sum_{\mathbf{r}_{-i}} \langle \mathbf{r}_{-i}| \right) \\
&\times \left(\frac{1}{\sqrt{3^{-(n-1)}}} \sum_{\mathbf{r}_{-i}} |\mathbf{r}_{-i}\rangle \right) \\
= &\frac{1}{3^{-2(n-1)}} \sum_{\mathbf{r}'_{-i},\mathbf{s}_{-i}} \langle\psi| A^{c_i \cup \mathbf{s}_{-i}}_{\mathbf{r}',\mathbf{e}_i} B^{r_i \cup \mathbf{r}'_{-i}}_{\mathbf{c}_i \cup s_{-i},\mathbf{e}_i} |\psi\rangle \\
= &\mathbf{E}_{\mathbf{r}'_{-i},\mathbf{s}_{-i}} \langle\psi| A^{c_i \cup \mathbf{s}_{-i}}_{\mathbf{r}',\mathbf{e}_i} B^{r_i \cup \mathbf{r}'_{-i}}_{\mathbf{c}_i \cup s_{-i},\mathbf{e}_i} |\psi\rangle \\
\geq &1 - 9\varepsilon,
\end{aligned}$$

where the last line again follows by Fact A.3.6. It follows by Lemma A.6.5, that

$$\langle\sigma|T \cdot T'|\sigma\rangle \geq 1 - 36\varepsilon.$$

The same inner product can be alternately evaluated as follows:

$$\begin{aligned}
\langle\sigma|T \cdot T'|\sigma\rangle = &\left(\langle\psi| \otimes \frac{1}{\sqrt{3^{-(n-1)}}} \sum_{\mathbf{r}_{-i}} \langle \mathbf{r}_{-i}| \otimes \frac{1}{\sqrt{3^{-(n-1)}}} \sum_{\mathbf{r}'_{-i}} \langle \mathbf{r}'_{-i}| \otimes \frac{1}{\sqrt{3^{-(n-1)}}} \sum_{\mathbf{s}_{-i}} \langle \mathbf{s}_{-i}| \right) \\
&\times \left(\sum_{\mathbf{r}_{-i}} A^{\mathbf{c}}_{\mathbf{r},\mathbf{e}_i} \otimes |\mathbf{r}_{-i}\rangle\langle \mathbf{r}_{-i}| \otimes I \otimes I \right) \left(\sum_{\mathbf{r}'_{-i}} A^{\mathbf{c}}_{\mathbf{r}',\mathbf{e}_i} \otimes I \otimes |\mathbf{r}'_{-i}\rangle\langle \mathbf{r}'_{-i}| \otimes I \right)
\end{aligned}$$

$$\times \left(|\psi\rangle \otimes \frac{1}{\sqrt{3^{-(n-1)}}} \sum_{\mathbf{r}_{-i}} |\mathbf{r}_{-i}\rangle \otimes \frac{1}{\sqrt{3^{-(n-1)}}} \sum_{\mathbf{r}'_{-i}} |\mathbf{r}'_{-i}\rangle \otimes \frac{1}{\sqrt{3^{-(n-1)}}} \sum_{\mathbf{s}_{-i}} |\mathbf{s}_{-i}\rangle \right)$$

$$= \frac{1}{3^{-2(n-1)}} \sum_{\mathbf{r}_{-i},\mathbf{r}'_{-i}} \langle\psi| A^{\mathbf{c}}_{\mathbf{r},\mathbf{e}_i} A^{\mathbf{c}}_{\mathbf{r}',\mathbf{e}_i} |\psi\rangle = \mathbf{E}_{\mathbf{r}_{-i},\mathbf{r}'_{-i}::r'_i=r_i=r} \langle\psi| A^{\mathbf{c}}_{\mathbf{r},\mathbf{e}_i} A^{\mathbf{c}}_{\mathbf{r}',\mathbf{e}_i} |\psi\rangle.$$

So, we have,

$$\left|1 - \mathbf{E}_{\mathbf{r},\mathbf{r}':r'_i=r_i=r} \langle\psi| A^{\mathbf{c}}_{\mathbf{r},\mathbf{e}_i} \cdot A^{\mathbf{c}}_{\mathbf{r}',\mathbf{e}_i} |\psi\rangle\right| = |1 - \langle\sigma|T \cdot T'|\sigma\rangle| \leq 36\varepsilon$$

□

A.4 Results

In this section, we state and prove our technical results on the structure of strategies for the parallel repeated Magic Square game. We first give an overview of the proof and then fill in the technical details.

A.4.1 Overview

Our result has two main technical components. The first is a theorem that, given a near-optimal strategy, shows how to construct observables on each players' Hilbert space that approximately satisfy a set of pairwise commutation and anticommutation relations.

Theorem A.4.1. *Suppose that two players Alice and Bob have an entangled strategy for the n-round parallel repeated Magic Square game, which wins with probability at least $1 - \varepsilon$. Then, if we adjoin an ancilla register to Alice's space in the appropriate state $|ancilla\rangle_A$ (and similarly for Bob in the appropriate state $|ancilla\rangle_B$), there exist observables $\tilde{A}^c_{r,k}$ indexed by $r, c \in \{0,1,2\}$ and $k \in [n]$ acting on Alice's space such that*

$$\begin{aligned} &\forall k, r, c, r', c', \qquad d_{\psi'}(\tilde{A}^c_{r,k}\tilde{A}^{c'}_{r',k}, (-1)^{f(r,r',c,c')}\tilde{A}^{c'}_{r',k}\tilde{A}^c_{r,k}) &&\leq O(\sqrt{\varepsilon}) \\ &\forall k \neq k', r, c, r', c', \qquad d_{\psi'}(\tilde{A}^c_{r,k}\tilde{A}^{c'}_{r',k'}, \tilde{A}^{c'}_{r',k'}\tilde{A}^c_{r,k}) &&\leq O(\sqrt{\varepsilon}). \end{aligned} \tag{A.2}$$

where $|\psi'\rangle = |\psi\rangle \otimes |ancilla\rangle_A \otimes |ancilla\rangle_B$ denotes the state together with the ancilla registers, and $f(r,r',c,c') = 1$ if $r \neq r'$ and $c \neq c'$, and 0 otherwise.

Likewise, there exist observables $\tilde{B}^c_{r,k}$ on Bob's space such that

$$\begin{aligned} &\forall k, r, c, r', c', \qquad d_{\psi'}(\tilde{B}^r_{c,k}\tilde{B}^{r'}_{c',k}, (-1)^{f(r,r',c,c')}\tilde{B}^{r'}_{c',k}\tilde{B}^r_{c,k}) &&\leq O(\sqrt{\varepsilon}) \\ &\forall k \neq k', r, c, r', c', \qquad d_{\psi'}(\tilde{B}^r_{c,k}\tilde{B}^{r'}_{c',k'}, \tilde{B}^{r'}_{c',k'}\tilde{B}^r_{c,k}) &&\leq O(\sqrt{\varepsilon}). \end{aligned} \tag{A.3}$$

Moreover, the following consistency relations hold in expectation:

$$\forall \mathbf{c}, \mathbf{p}, \quad \mathbf{E}_{\mathbf{r}}\, d_{\psi'}(A^{\mathbf{c}}_{\mathbf{r},\mathbf{p}} \otimes I_{ancilla}, \prod_{k=1}^{n} (\tilde{A}^{c_k}_{r_k,k})^{p_k})^2 \leq O(n\sqrt{\varepsilon}) \tag{A.4}$$

$$\forall \mathbf{r}, \mathbf{p}, \quad \mathbf{E}_{\mathbf{c}}\, d_{\psi'}(B^{\mathbf{r}}_{\mathbf{c},\mathbf{p}} \otimes I_{ancilla}, \prod_{k=1}^{n} (\tilde{B}^{r_k}_{c_k,k})^{p_k})^2 \leq O(n\sqrt{\varepsilon}) \tag{A.5}$$

Proof of Theorem A.4.1. The single-round phase relations in Equations (A.2) and (A.3) follow from Lemma A.4.6. The commutation relations between rounds follow from Lemma A.4.7. The consistency relations (Equations (A.4) and (A.5)) follow from Lemma A.4.11. □

Having constructed these observables, we use them to build an isometry that "extracts" a $2n$-qubit state out of the shared state of Alice and Bob. This isometry is *local*: it does not create any entanglement between Alice and Bob. Moreover, it maps the measurements in the players' strategy to $2n$-qubit measurements that are close to the ideal strategy.

Theorem A.4.2. *Suppose that two players share an entangled state in a Hilbert space $\mathcal{H}$ and operators $\tilde{A}^c_{r,k}, \tilde{B}^r_{c,k}$ satisfying Equations* (A.2) *and* (A.3)*. Then there exists an isometry $V : \mathcal{H} \to \mathcal{H} \otimes \mathbb{C}^{2n} \otimes \mathbb{C}^{2n} \otimes \mathbb{C}^{2n} \otimes \mathbb{C}^{2n}$, and for every $\mathbf{s}, \mathbf{t} \in \{0,1\}^{2n}$, there exists an operator $W^A{}_{\mathbf{s},\mathbf{t}}$ on Alice's space, and for every $\mathbf{u}, \mathbf{v} \in \{0,1\}^{2n}$ there exists an operator $W^B{}_{\mathbf{u},\mathbf{v}}$ on Bob's space, such that*

$$\forall \mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d}, \qquad \left|\langle\phi|\sigma^A_X(\mathbf{s})\sigma^A_Z(\mathbf{t})\sigma^B_X(\mathbf{u})\sigma^B_Z(\mathbf{v})|\phi\rangle - \langle\psi|W^A{}_{\mathbf{s},\mathbf{t}} W^B{}_{\mathbf{u},\mathbf{v}}|\psi\rangle\right| \leq O(n^2\sqrt{\varepsilon}), \tag{A.6}$$

where $|\phi\rangle = V(|\psi\rangle)$, σ^A_X, σ^A_Z are Pauli operators acting on the second output register of V, and σ^B_X, σ^B_Z are Pauli operators acting on the fourth output register of V.

The proof of this theorem is deferred to Section A.4.3. As a corollary, we show that the output state of the isometry has high overlap with the state $|\mathrm{EPR}\rangle^{\otimes 2n}$ consisting of $2n$ EPR pairs shared between Alice and Bob.

Corollary A.4.3. *Suppose that two players have an entangled strategy for the n-round parallel repeated Magic Square game, which wins with probability at least $1-\varepsilon$. Then, letting $|\phi\rangle = V(|\psi\rangle)$ as in Theorem A.4.2,*

$$\langle\phi||\mathrm{EPR}\rangle\langle\mathrm{EPR}|^{\otimes 2n} \otimes I_{junk}|\phi\rangle \geq 1 - O(n^2\sqrt{\varepsilon}),$$

whwere the identity operator I_{juk} acts on the first, third, and fifth register of the isometry output.

Proof. This follows from Lemma A.4.18 and Lemma A.4.15. □

A.4.2 Single-round observables

Definition A.4.4. Let $k \in [n]$ be the index of a round, and denote the single round observables associated with that round by $A^c_{r,k} := A^{\mathbf{c}}_{\mathbf{r},\mathbf{e}_k}$ and $B^r_{c,k} := B^{\mathbf{r}}_{\mathbf{c},\mathbf{e}_k}$, where $\mathbf{c}$ and $\mathbf{r}$ are any vectors whose kth coordinates are r and c respectively, and $\mathbf{e}_k$ is the vector with a 1 in the kth position and 0s elsewhere.

Definition A.4.5. For each round k, define the state

$$|\text{ancilla}_k\rangle_k := \frac{1}{\sqrt{3^{n-1}}} \sum_{\mathbf{r}_{-k} \in \{0,1,2\}^{n-1}} |\mathbf{r}_{-k}\rangle.$$

Define the dilated state

$$|\psi'\rangle := |\psi\rangle \otimes |\text{ancilla}_1\rangle_1^A \otimes \ldots \otimes |\text{ancilla}_n\rangle_n^A \otimes |\text{ancilla}_1\rangle_1^B \otimes \ldots \otimes |\text{ancilla}_n\rangle_n^B$$

and define dilated observables on Alice's side

$$\begin{aligned}\tilde{A}^c_{r,k} &:= \sum_{\mathbf{r}_{-k}} \sum_{\mathbf{a}_0,\mathbf{a}_1} (-1)^{(\mathbf{a}_c)_k} P^{\mathbf{a}_0,\mathbf{a}_1}_{\mathbf{r}} \otimes I_1 \otimes \ldots \otimes I_{k-1} \otimes |\mathbf{r}_{-k}\rangle\langle\mathbf{r}_{-k}| \otimes I_{k+1} \ldots \otimes I_n \\ &= \sum_{\mathbf{r}_{-k}} A^{\mathbf{c}}_{\mathbf{s},\mathbf{e}_k} \otimes I_1 \otimes \ldots \otimes I_{k-1} \otimes |\mathbf{r}_{-k}\rangle\langle\mathbf{r}_{-k}| \otimes I_{k+1} \ldots \otimes I_n\end{aligned}$$

Where $\mathbf{c}$ in the last line can be any $\mathbf{c}$ satisfying $\mathbf{c}_k = c$, and wherever we write a sum over $\mathbf{r}_{-k}$ it is implicit that r_k is fixed to be $r_k = r$.

Observe that the operators $\tilde{A}^c_{r,k}$ are true observables, i.e. they are Hermitian and square to I. Moreover, $\tilde{A}^c_{r,k}$ simulates the two-outcome POVM whose elements are given by $M^{a_c} := \mathbf{E}_{\mathbf{r}_{-k}} P^{a_c}_{\mathbf{r},k}$.

Similarly, define dilated observables on Bob's side

$$\begin{aligned}\tilde{B}^r_{c,k} &:= \sum_{\mathbf{c}_{-k}} \sum_{\mathbf{b}_0,\mathbf{b}_1} (-1)^{(\mathbf{b}_r)_k} Q^{\mathbf{b}_0,\mathbf{b}_1}_{\mathbf{c}} \otimes I_1 \otimes \ldots \otimes I_{k-1} \otimes |\mathbf{r}_{-k}\rangle\langle\mathbf{r}_{-k}| \otimes I_{k+1} \ldots \otimes I_n \\ &= \sum_{\mathbf{c}_{-k}} B^{\mathbf{r}}_{\mathbf{c},\mathbf{e}_k} \otimes I_1 \otimes \ldots \otimes I_{k-1} \otimes |\mathbf{r}_{-k}\rangle\langle\mathbf{r}_{-k}| \otimes I_{k+1} \ldots \otimes I_n\end{aligned}$$

Where $\mathbf{r}$ in the last line can be any $\mathbf{r}$ satisfying $\mathbf{r}_k = r$, and wherever we write a sum over $\mathbf{c}_{-k}$ it is implicit that c_k is fixed to be $c_k = c$.

Observe that the operators $\tilde{B}^r_{c,k}$ are true observables, i.e. they are Hermitian and square to I. Moreover, $\tilde{B}^r_{c,k}$ simulates the two-outcome POVM whose elements are given by $M^{b_c} := \mathbf{E}_{\mathbf{c}_{-k}} P^{b_r}_{\mathbf{c},k}$.

Lemma A.4.6. *For all k, r, r', c, c', it holds that*

$$\|(\tilde{A}^c_{r,k}\tilde{A}^{c'}_{r',k} - (-1)^{f(r,r',c,c')}\tilde{A}^{c'}_{r',k}\tilde{A}^c_{r,k})|\psi'\rangle\| \leq O(\sqrt{\varepsilon}).$$

The analogous statement also holds for Bob operators.

Proof. Follows from single round analysis. See Appendix A.7. Replacing the operators A_r^c in that analysis with $\tilde{A}_{r,k}^c$, and replacing B_c^r in that analysis with $\tilde{B}_{c,k}^r$ one may observe that the analysis in Appendix A.7 still holds. □

Lemma A.4.7. *For all $k \neq k', r, r', c, c'$, it holds that*

$$\|(\tilde{A}_{r,k}^c \tilde{A}_{r',k'}^{c'} - \tilde{A}_{r',k'}^{c'} \tilde{A}_{r,k}^c)|\psi'\rangle\| \leq O(\sqrt{\varepsilon}).$$

The analogous statement also holds for Bob operators.

Proof. Let $\mathbf{c}$ be any choice of columns such that $c_k = c, c_{k'} = c'$.

Recall that by equation (A.1) we have that

$$\forall \mathbf{p}, \quad \mathbf{E}_{\mathbf{r},\mathbf{c}} \langle\psi| A_{\mathbf{r},\mathbf{p}}^{\mathbf{c}} B_{\mathbf{c},\mathbf{p}}^{\mathbf{r}} |\psi\rangle \geq 1 - \varepsilon. \tag{A.7}$$

Setting $\mathbf{p} = \mathbf{e}_k$ gives that, for all fixed values of r_k and c_k,

$$\forall k, \quad \mathbf{E}_{\mathbf{r}_{-k},\mathbf{c}_{-k}} \langle\psi| A_{\mathbf{r},\mathbf{e}_k}^{\mathbf{c}} B_{\mathbf{c},\mathbf{e}_k}^{\mathbf{r}} |\psi\rangle \geq 1 - 9\varepsilon. \tag{A.8}$$

So,

$$\forall k, \quad \mathbf{E}_{\mathbf{r}_{-k},\mathbf{c}_{-k}} d_\psi \left(A_{\mathbf{r},\mathbf{e}_k}^{\mathbf{c}} B_{\mathbf{c},\mathbf{e}_k}^{\mathbf{r}}\right)^2 \leq 18\varepsilon \tag{A.9}$$

Further, recall that $A_{\mathbf{r},\mathbf{e}_k}^{\mathbf{c}} = A_{\mathbf{r},\mathbf{e}_k}^{\mathbf{c}'}$ as long as the kth coordinate of $\mathbf{c}$ and $\mathbf{c}'$ agree. Denote by $\mathbf{E}_{\mathbf{c}|k,k'}$ the uniform distribution over choices of column vector $\mathbf{c}$ such that $c_k = c$ and $c_{k'} = c'$. Then

$$d_\psi(\tilde{A}_{r,k}^c \tilde{A}_{r',k'}^{c'}, \tilde{A}_{r'k'}^{c'}, \tilde{A}_{r,k}^c) = \mathbf{E}_{\mathbf{c}|k,k'} d_{\psi'}\Big(\sum_{\mathbf{r}_{-k}} \sum_{\mathbf{r}'_{-k'}} A_{\mathbf{r},\mathbf{e}_k}^{\mathbf{c}} A_{\mathbf{r}',\mathbf{e}_{k'}}^{\mathbf{c}} \otimes |\mathbf{r}_{-k}, \mathbf{r}'_{-k'}\rangle\langle\mathbf{r}_{-k}, \mathbf{r}'_{-k'}|_{k,k'},$$
$$\sum_{\mathbf{r}_{-k}} \sum_{\mathbf{r}'_{-k'}} A_{\mathbf{r}',\mathbf{e}_{k'}}^{\mathbf{c}} A_{\mathbf{r},\mathbf{e}_k}^{\mathbf{c}} \otimes |\mathbf{r}_{-k}, \mathbf{r}'_{-k'}\rangle\langle\mathbf{r}_{-k}, \mathbf{r}'_{-k'}|_{k,k'}\Big).$$

Note that the column vector $\mathbf{c}$ is common to both A operators. Also, as a convention, wherever there is a sum or expectation over $\mathbf{r}_{-k}$ or $\mathbf{r}'_{-k'}$ in this proof, it is implicit that the values of r_k and $r'_{k'}$ are fixed to be $r_k = r$ and $r'_{k'} = r'$. Now, we apply Lemma A.6.2 to move the leftmost A operator to Bob.

$$d_\psi(\dots) \leq \mathbf{E}_{\mathbf{c}|k,k'} \Big[d_{\psi'}\Big(\sum_{\mathbf{r}_{-k}} \sum_{\mathbf{r}'_{-k'}} A_{\mathbf{c},\mathbf{e}_k}^{\mathbf{r}} B_{\mathbf{c},\mathbf{e}_{k'}}^{\mathbf{r}'} \otimes |\mathbf{r}_{-k}, \mathbf{r}'_{-k'}\rangle\langle\mathbf{r}_{-k}, \mathbf{r}'_{-k'}|_{k,k'},$$
$$\sum_{\mathbf{r}_{-k}} \sum_{\mathbf{r}'_{-k'}} A_{\mathbf{r}',\mathbf{e}_{k'}}^{\mathbf{c}} A_{\mathbf{r},\mathbf{e}_k}^{\mathbf{c}} \otimes |\mathbf{r}_{-k}, \mathbf{r}'_{-k'}\rangle\langle\mathbf{r}_{-k}, \mathbf{r}'_{-k'}|_{k,k'}\Big) +$$
$$d_{\psi'}\Big(\sum_{\mathbf{r}_{-k}} A_{\mathbf{r},\mathbf{e}_k}^{\mathbf{c}} \otimes |\mathbf{r}_{-k}\rangle\langle\mathbf{r}_{-k}| \otimes I_{k'} \sum_{\mathbf{r}'_{-k'}} A_{\mathbf{r}',\mathbf{e}_{k'}}^{\mathbf{c}} \otimes I_k \otimes |\mathbf{r}'_{-k'}\rangle\langle\mathbf{r}'_{-k'}|,$$
$$\sum_{\mathbf{r}_{-k}} A_{\mathbf{r},\mathbf{e}_k}^{\mathbf{c}} \otimes |\mathbf{r}_{-k}\rangle\langle\mathbf{r}_{-k}| \otimes I_{k'} \sum_{\mathbf{r}'_{-k'}} B_{\mathbf{c},\mathbf{e}_{k'}}^{\mathbf{r}'} \otimes I_k \otimes |\mathbf{r}'_{-k'}\rangle\langle\mathbf{r}'_{-k'}|\Big)\Big]$$

Note that $\| \sum_{\mathbf{r}_{-k}} A^{\mathbf{c}}_{\mathbf{r},\mathbf{e}_k} \otimes |\mathbf{r}_{-k}\rangle\langle\mathbf{r}_{-k}| \otimes I_{k'} \| \leq 1$. Hence, applying Lemma A.6.3 and Lemma A.6.4, we get

$$\leq \mathbf{E}_{\mathbf{c}|k,k'} \Big[d_{\psi'} \Big(\sum_{\mathbf{r}_{-k}} \sum_{\mathbf{r}'_{-k'}} A^{\mathbf{r}}_{\mathbf{c},\mathbf{e}_k} B^{\mathbf{r}'}_{\mathbf{c},\mathbf{e}_{k'}} \otimes |\mathbf{r}_{-k}, \mathbf{r}'_{-k'}\rangle\langle\mathbf{r}_{-k}, \mathbf{r}'_{-k'}|_{k,k'},$$
$$\sum_{\mathbf{r}_{-k}} \sum_{\mathbf{r}'_{-k'}} A^{\mathbf{c}}_{\mathbf{r}',\mathbf{e}_{k'}} A^{\mathbf{c}}_{\mathbf{r},\mathbf{e}_k} \otimes |\mathbf{r}_{-k}, \mathbf{r}'_{-k'}\rangle\langle\mathbf{r}_{-k}, \mathbf{r}'_{-k'}|_{k,k'} \Big) +$$
$$\mathbf{E}_{\mathbf{r}'_{-k'}} d_{\psi}(A^{\mathbf{c}}_{\mathbf{r}',\mathbf{e}_{k'}}, B^{\mathbf{r}'}_{\mathbf{c},\mathbf{e}_{k'}}) \Big]$$

By performing the same steps on the other A operator, we obtain

$$\leq \mathbf{E}_{\mathbf{c}|k,k'} \Big[d_{\psi'} \Big(\sum_{\mathbf{r}_{-k}} \sum_{\mathbf{r}'_{-k'}} B^{\mathbf{r}'}_{\mathbf{c},\mathbf{e}_{k'}} B^{\mathbf{r}}_{\mathbf{c},\mathbf{e}_k} \otimes |\mathbf{r}_{-k}, \mathbf{r}'_{-k'}\rangle\langle\mathbf{r}_{-k}, \mathbf{r}'_{-k'}|_{k,k'},$$
$$\sum_{\mathbf{r}_{-k}} \sum_{\mathbf{r}'_{-k'}} A^{\mathbf{c}}_{\mathbf{r}',\mathbf{e}_{k'}} A^{\mathbf{c}}_{\mathbf{r},\mathbf{e}_k} \otimes |\mathbf{r}_{-k}, \mathbf{r}'_{-k'}\rangle\langle\mathbf{r}_{-k}, \mathbf{r}'_{-k'}|_{k,k'} \Big) +$$
$$\mathbf{E}_{\mathbf{r}_{-k}} d_{\psi}(A^{\mathbf{c}}_{\mathbf{r},\mathbf{e}_k}, B^{\mathbf{r}}_{\mathbf{c},\mathbf{e}_k}) + \mathbf{E}_{\mathbf{r}'_{-k'}} d_{\psi}(A^{\mathbf{c}}_{\mathbf{r}',\mathbf{e}_{k'}}, B^{\mathbf{r}'}_{\mathbf{c},\mathbf{e}_{k'}}) \Big]$$

Now the B operators can be commuted exactly since they share the same input $\mathbf{c}$.

$$\leq \mathbf{E}_{\mathbf{c}|k,k'} \Big[d_{\psi'} \Big(\sum_{\mathbf{r}_{-k}} \sum_{\mathbf{r}'_{-k'}} B^{\mathbf{r}}_{\mathbf{c},\mathbf{e}_k} B^{\mathbf{r}'}_{\mathbf{c},\mathbf{e}_{k'}} \otimes |\mathbf{r}_{-k}, \mathbf{r}'_{-k'}\rangle\langle\mathbf{r}_{-k}, \mathbf{r}'_{-k'}|_{k,k'},$$
$$\sum_{\mathbf{r}_{-k}} \sum_{\mathbf{r}'_{-k'}} A^{\mathbf{c}}_{\mathbf{r}',\mathbf{e}_{k'}} A^{\mathbf{c}}_{\mathbf{r},\mathbf{e}_k} \otimes |\mathbf{r}_{-k}, \mathbf{r}'_{-k'}\rangle\langle\mathbf{r}_{-k}, \mathbf{r}'_{-k'}|_{k,k'} \Big) +$$
$$\mathbf{E}_{\mathbf{r}_{-k}} d_{\psi}(A^{\mathbf{c}}_{\mathbf{r},\mathbf{e}_k}, B^{\mathbf{r}}_{\mathbf{c},\mathbf{e}_k}) + \mathbf{E}_{\mathbf{r}'_{-k'}} d_{\psi}(A^{\mathbf{c}}_{\mathbf{r}',\mathbf{e}_{k'}}, B^{\mathbf{r}'}_{\mathbf{c},\mathbf{e}_{k'}}) \Big]$$

We move the Bs back to Alice by reversing the previous steps, again using Lemmas A.6.2, A.6.3, and A.6.4

$$\leq \mathbf{E}_{\mathbf{c}|k,k'} \Big[d_{\psi'} \Big(\sum_{\mathbf{r}_{-k}} \sum_{\mathbf{r}'_{-k'}} A^{\mathbf{c}}_{\mathbf{r}',\mathbf{e}_{k'}} A^{\mathbf{c}}_{\mathbf{r},\mathbf{e}_k} \otimes |\mathbf{r}_{-k}, \mathbf{r}'_{-k'}\rangle\langle\mathbf{r}_{-k}, \mathbf{r}'_{-k'}|_{k,k'},$$
$$\sum_{\mathbf{r}_{-k}} \sum_{\mathbf{r}'_{-k'}} A^{\mathbf{c}}_{\mathbf{r}',\mathbf{e}_{k'}} A^{\mathbf{c}}_{\mathbf{r},\mathbf{e}_k} \otimes |\mathbf{r}_{-k}, \mathbf{r}'_{-k'}\rangle\langle\mathbf{r}_{-k}, \mathbf{r}'_{-k'}|_{k,k'} \Big) +$$
$$2\,\mathbf{E}_{\mathbf{r}_{-k}} d_{\psi}(A^{\mathbf{c}}_{\mathbf{r},\mathbf{e}_k}, B^{\mathbf{r}}_{\mathbf{c},\mathbf{e}_k}) + 2\,\mathbf{E}_{\mathbf{r}'_{-k'}} d_{\psi}(A^{\mathbf{c}}_{\mathbf{r}',\mathbf{e}_{k'}}, B^{\mathbf{r}'}_{\mathbf{c},\mathbf{e}_{k'}}) \Big]$$
$$= \mathbf{E}_{\mathbf{c}|k,k'} (2\,\mathbf{E}_{vr_{-k}} d_{\psi}(A^{\mathbf{c}}_{\mathbf{r},\mathbf{e}_k}, B^{\mathbf{r}}_{\mathbf{c},\mathbf{e}_k}) + 2\,\mathbf{E}_{\mathbf{r}'_{-k'}} d_{\psi}(A^{\mathbf{c}}_{\mathbf{r}',\mathbf{e}_{k'}}, B^{\mathbf{r}'}_{\mathbf{c},\mathbf{e}_{k'}}))$$

Finally, we bound this by (A.9). Note that (A.9) is stated with $\mathbf{E}_{\mathbf{r}_{-k},\mathbf{c}_{-k}}$, but this implies the same statement with $\mathbf{E}_{\mathbf{c}|k,k'}\,\mathbf{E}_{\mathbf{r}_{-k}}$ with an additional constant factor of 3. Similarly for $\mathbf{E}_{\mathbf{c}|k,k'}\,\mathbf{E}_{\mathbf{r}_{-k'}}$. So, continuing our computation:

$$\leq 4 \cdot 3 \cdot 3\sqrt{2\varepsilon} = 36\sqrt{2\varepsilon}.$$

□

Lemma A.4.8.

$$\forall r, c, k, \quad d_{\psi'}\left(\tilde{A}^c_{r,k}, \tilde{B}^r_{c,k}\right) \leq O(\sqrt{\varepsilon})$$

Proof. In the argument below, let $\mathbf{r}$ be the row vectors agreeing with r on index k and $\mathbf{r}_{-k}$ on the remaining indices; likewise for $\mathbf{c}$ (note that $\mathbf{r}_{-k}$ is stored in Alice's register and and $\mathbf{c}_{-k}$ in Bob's). The main trick is to use the freedom of choice of $\mathbf{c}$ on Alice's operators to pick $\mathbf{c}$ agreeing with Bob's ancilla register $\mathbf{c}_{-k}$.

$$d_{\psi'}(\tilde{A}^c_{r,k}, \tilde{B}^r_{c,k})^2 = \| \frac{1}{3^{n-1}} \sum_{\mathbf{r}_{-k},\mathbf{c}_{-k}} A^{\mathbf{c}}_{\mathbf{r},\mathbf{e}_k} |\psi\rangle_{AB} \otimes |\mathbf{r}_{-k}\rangle^A_k \otimes |\mathbf{c}_{-k}\rangle^B_k - \frac{1}{3^{n-1}} \sum_{\mathbf{r}_{-k},\mathbf{c}_{-k}} B^{\mathbf{r}}_{\mathbf{c},\mathbf{e}_k} |\psi\rangle_{AB} \otimes |\mathbf{r}_{-k}\rangle^A_k \otimes |\mathbf{c}_{-k}\rangle^B_k \|^2$$

By Lemma A.6.4 with $i = (\mathbf{r}_{-k}, \mathbf{c}_{-k})$,

$$= \mathbf{E}_{\mathbf{r}_{-k},\mathbf{c}_{-k}}\, d_{\psi'}(A^{\mathbf{c}}_{\mathbf{r},k}, B^{\mathbf{r}}_{\mathbf{c},k})^2$$

This is bounded by the probability that round k of the test succeeds with inputs r and c

$$\leq O(\varepsilon).$$

□

Lemma A.4.9. *For all* $\mathbf{r}, \mathbf{c}, \mathbf{p}$ *and for all* $i \in [n]$,

$$\left|\langle\psi'|\left[(\prod_{k=n}^{i+1}(\tilde{B}^{r_k}_{c_k,k})^{p_k})A^{\mathbf{c}}_{\mathbf{r},\mathbf{p}}(\prod_{k=1}^{i}(\tilde{A}^{c_k}_{r_k,k})^{p_k}) - (\prod_{k=n}^{i}(\tilde{B}^{r_k}_{c_k,k})^{p_k})A^{\mathbf{c}}_{\mathbf{r},\mathbf{p}}(\prod_{k=1}^{i-1}(\tilde{A}^{c_k}_{r_k,k})^{p_k})\right]|\psi'\rangle\right| \leq O(\sqrt{\varepsilon}).$$

Proof. Fixing $\mathbf{r}, \mathbf{c}, \mathbf{p}$, and fixing $i \in [n]$ we have

$$\left|\langle\psi'|\left[(\prod_{k=n}^{i+1}(\tilde{B}^{r_k}_{c_k,k})^{p_k})A^{\mathbf{c}}_{\mathbf{r},\mathbf{p}}(\prod_{k=1}^{i}(\tilde{A}^{c_k}_{r_k,k})^{p_k}) - (\prod_{k=n}^{i}(\tilde{B}^{r_k}_{c_k,k})^{p_k})A^{\mathbf{c}}_{\mathbf{r},\mathbf{p}}(\prod_{k=1}^{i-1}(\tilde{A}^{c_k}_{r_k,k})^{p_k})\right]|\psi'\rangle\right|$$
$$= \left|\langle\psi'|(\prod_{k=n}^{i+1}(\tilde{B}^{r_k}_{c_k,k})^{p_k})A^{\mathbf{c}}_{\mathbf{r},\mathbf{p}}(\prod_{k=1}^{i-1}(\tilde{A}^{c_k}_{r_k,k})^{p_k})(\tilde{B}^{r_i}_{c_i,i})^{p_i}|\psi'\rangle\right.$$

$$
\begin{aligned}
&+ \langle\psi'|(\prod_{k=n}^{i+1}(\tilde{B}_{c_k,k}^{r_k})^{p_k})A_{\mathbf{r},\mathbf{p}}^{\mathbf{c}}(\prod_{k=1}^{i-1}(\tilde{A}_{r_k,k}^{c_k})^{p_k})\left((\tilde{A}_{c_i,i}^{r_i})^{p_i} - (\tilde{B}_{c_i,i}^{r_i})^{p_i}\right)|\psi'\rangle \\
&-\langle\psi'|(\prod_{k=n}^{i}(\tilde{B}_{c_k,k}^{r_k})^{p_k})A_{\mathbf{r},\mathbf{p}}^{\mathbf{c}}(\prod_{k=1}^{i-1}(\tilde{A}_{r_k,k}^{c_k})^{p_k})|\psi'\rangle\Big| \\
\leq &\Big|\langle\psi'|(\prod_{k=n}^{i+1}(\tilde{B}_{c_k,k}^{r_k})^{p_k})A_{\mathbf{r},\mathbf{p}}^{\mathbf{c}}(\prod_{k=1}^{i-1}(\tilde{A}_{r_k,k}^{c_k})^{p_k})(\tilde{B}_{c_i,i}^{r_i})^{p_i}|\psi'\rangle \\
&- \langle\psi'|(\prod_{k=n}^{i}(\tilde{B}_{c_k,k}^{r_k})^{p_k})A_{\mathbf{r},\mathbf{p}}^{\mathbf{c}}(\prod_{k=1}^{i-1}(\tilde{A}_{r_k,k}^{c_k})^{p_k})|\psi'\rangle\Big| \\
&+ \left|\langle\psi'|(\prod_{k=n}^{i+1}(\tilde{B}_{c_k,k}^{r_k})^{p_k})A_{\mathbf{r},\mathbf{p}}^{\mathbf{c}}(\prod_{k=1}^{i-1}(\tilde{A}_{r_k,k}^{c_k})^{p_k})\left((\tilde{A}_{c_i,i}^{r_i})^{p_i} - (\tilde{B}_{c_i,i}^{r_i})^{p_i}\right)|\psi'\rangle\right| \\
\leq &\Big|\langle\psi'|(\prod_{k=n}^{i+1}(\tilde{B}_{c_k,k}^{r_k})^{p_k})(\tilde{B}_{c_i,i}^{r_i})^{p_i}A_{\mathbf{r},\mathbf{p}}^{\mathbf{c}}(\prod_{k=1}^{i-1}(\tilde{A}_{r_k,k}^{c_k})^{p_k})|\psi'\rangle \\
&- \langle\psi'|(\prod_{k=n}^{i}(\tilde{B}_{c_k,k}^{r_k})^{p_k})A_{\mathbf{r},\mathbf{p}}^{\mathbf{c}}(\prod_{k=1}^{i-1}(\tilde{A}_{r_k,k}^{c_k})^{p_k})|\psi'\rangle\Big| + d_{\psi'}((\tilde{A}_{r_i,i}^{c_i})^{p_i},(\tilde{B}_{c_i,i}^{r_i})^{p_i}) \\
\leq &\, 0 + O(\sqrt{\varepsilon}) = O(\sqrt{\varepsilon}).
\end{aligned}
$$

Here the last inequality uses Lemma A.4.8, and the second to last inequality uses that $\tilde{B}_{c_i,i}^{r_i}$ commutes with all Alice operators, and that $(\prod_{k=n}^{i+1}(\tilde{B}_{c_k,k}^{r_k})^{p_k})A_{\mathbf{r},\mathbf{p}}^{\mathbf{c}}(\prod_{k=1}^{i-1}(\tilde{A}_{r_k,k}^{c_k})^{p_k})$ is a unitary, so that

$$
\begin{aligned}
&\left|\langle\psi'|(\prod_{k=n}^{i+1}(\tilde{B}_{c_k,k}^{r_k})^{p_k})A_{\mathbf{r},\mathbf{p}}^{\mathbf{c}}(\prod_{k=1}^{i-1}(\tilde{A}_{r_k,k}^{c_k})^{p_k})\left((\tilde{A}_{c_i,i}^{r_i})^{p_i} - (\tilde{B}_{c_i,i}^{r_i})^{p_i}\right)|\psi'\rangle\right| \\
&\quad\leq \|\left((\tilde{A}_{c_i,i}^{r_i})^{p_i} - (\tilde{B}_{c_i,i}^{r_i})^{p_i}\right)|\psi'\rangle\| \\
&\quad= d_{\psi'}((\tilde{A}_{r_i,i}^{c_i})^{p_i},(\tilde{B}_{c_i,i}^{r_i})^{p_i}).
\end{aligned}
$$

□

Lemma A.4.10.

$$
\begin{aligned}
\Big|\mathbf{E}_{\mathbf{r}}\Big(&\langle\psi'|(\prod_{k=n}^{i+2}(\tilde{B}_{c_k,k}^{r_k})^{p_k})(\prod_{k=n}^{i+1}A_{\mathbf{r},p_k\cdot\mathbf{e}_k}^{\mathbf{c}}\otimes I)(\tilde{A}_{r_{i+1},i+1}^{c_{i+1}})^{p_{i+1}}|\psi'\rangle \\
&- \langle\psi'|(\prod_{k=n}^{i+1}(\tilde{B}_{c_k,k}^{r_k})^{p_k})(\prod_{k=n}^{i}A_{\mathbf{r},p_k\cdot\mathbf{e}_k}^{\mathbf{c}}\otimes I)(\tilde{A}_{r_i,i}^{c_i})^{p_i}|\psi'\rangle\Big)\Big| \leq O(\sqrt{\varepsilon}) \qquad \text{(A.10)}
\end{aligned}
$$

and

$$
\mathbf{E}_{\mathbf{r}}\left(1 - \langle\psi'|A_{\mathbf{r},p_n\cdot\mathbf{e}_n}^{\mathbf{c}}(\tilde{A}_{r_n,n}^{c_n})^{p_n}|\psi'\rangle\right) \leq O(\sqrt{\varepsilon}) \qquad \text{(A.11)}
$$

Proof. We start by proving Equation A.10. Let us denote the LHS of this equation by Δ. Then we have

$$
\begin{aligned}
\Delta = \Big| \mathbf{E}_{\mathbf{r}} \Big(& \langle\psi'| \Big(\prod_{k=n}^{i+2} (\tilde{B}^{r_k}_{c_k,k})^{p_k}\Big)\Big(\prod_{k=n}^{i+1} A^{\mathbf{c}}_{\mathbf{r},p_k\cdot\mathbf{e}_k} \otimes I\Big)(\tilde{A}^{c_{i+1}}_{r_{i+1},i+1})^{p_{i+1}}|\psi'\rangle \\
& - \langle\psi'| \Big(\prod_{k=n}^{i+1} (\tilde{B}^{r_k}_{c_k,k})^{p_k}\Big)\Big(\prod_{k=n}^{i} A^{\mathbf{c}}_{\mathbf{r},p_k\cdot\mathbf{e}_k} \otimes I\Big)(\tilde{A}^{c_i}_{r_i,i})^{p_i}|\psi'\rangle \Big)\Big| \\
= \Big| \mathbf{E}_{\mathbf{r}} \Big(& \langle\psi'| \Big(\prod_{k=n}^{i+2} (\tilde{B}^{r_k}_{c_k,k})^{p_k}\Big)\Big(\prod_{k=n}^{i+1} A^{\mathbf{c}}_{\mathbf{r},p_k\cdot\mathbf{e}_k} \otimes I\Big)(\tilde{A}^{c_{i+1}}_{r_{i+1},i+1})^{p_{i+1}}|\psi'\rangle \\
& - \langle\psi'| \Big(\prod_{k=n}^{i+2} \tilde{B}^{r_k}_{c_k,k}\Big)\Big(\prod_{k=n}^{i+1} A^{\mathbf{c}}_{\mathbf{r},p_k\cdot\mathbf{e}_k} \otimes I\Big)(\tilde{B}^{r_{i+1}}_{c_{i+1},i+1})^{p_{i+1}}|\psi'\rangle \\
& + \langle\psi'| \Big(\prod_{k=n}^{i+2} (\tilde{B}^{r_k}_{c_k,k})^{p_k}\Big)\Big(\prod_{k=n}^{i+1} A^{\mathbf{c}}_{\mathbf{r},p_k\cdot\mathbf{e}_k} \otimes I\Big)(\tilde{B}^{r_{i+1}}_{c_{i+1},i+1})^{p_{i+1}}|\psi'\rangle \\
& - \langle\psi'| \Big(\prod_{k=n}^{i+1} (\tilde{B}^{r_k}_{c_k,k})^{p_k}\Big)\Big(\prod_{k=n}^{i} A^{\mathbf{c}}_{\mathbf{r},p_k\cdot\mathbf{e}_k} \otimes I\Big)(\tilde{A}^{c_i}_{r_i,i})^{p_i}|\psi'\rangle \Big)\Big| \\
\leq \Big| \mathbf{E}_{\mathbf{r}} \Big(& \langle\psi'| \Big(\prod_{k=n}^{i+2} (\tilde{B}^{r_k}_{c_k,k})^{p_k}\Big)\Big(\prod_{k=n}^{i+1} A^{\mathbf{c}}_{\mathbf{r},p_k\cdot\mathbf{e}_k} \otimes I\Big)(\tilde{A}^{c_{i+1}}_{r_{i+1},i+1})^{p_{i+1}}|\psi'\rangle \\
& - \langle\psi'| \Big(\prod_{k=n}^{i+2} (\tilde{B}^{r_k}_{c_k,k})^{p_k}\Big)\Big(\prod_{k=n}^{i+1} A^{\mathbf{c}}_{\mathbf{r},p_k\cdot\mathbf{e}_k} \otimes I\Big)(\tilde{B}^{r_{i+1}}_{c_{i+1},i+1})^{p_I i+1}|\psi'\rangle \Big)\Big| \\
& + \Big| \mathbf{E}_{\mathbf{r}} \Big(\langle\psi'| \Big(\prod_{k=n}^{i+2} (\tilde{B}^{r_k}_{c_k,k})^{p_k}\Big)\Big(\prod_{k=n}^{i+1} A^{\mathbf{c}}_{\mathbf{r},p_k\cdot\mathbf{e}_k} \otimes I\Big)(\tilde{B}^{r_{i+1}}_{c_{i+1},i+1})^{i+1}|\psi'\rangle \\
& - \langle\psi'| \Big(\prod_{k=n}^{i+1} (\tilde{B}^{r_k}_{c_k,k})^{p_k}\Big)\Big(\prod_{k=n}^{i} A^{\mathbf{c}}_{\mathbf{r},p_k\cdot\mathbf{e}_k} \otimes I\Big)(\tilde{A}^{c_i}_{r_i,i})^{p_i}|\psi'\rangle \Big)\Big| \\
\leq \Big| \mathbf{E}_{\mathbf{r}} & \Big(d_{\psi'}(\tilde{A}^{c_{i+1}}_{r_{i+1},i+1}, \tilde{B}^{r_{i+1}}_{c_{i+1},i+1}) \Big)\Big| \\
& + \Big| \mathbf{E}_{\mathbf{r}} \Big(\langle\psi'| \Big(\prod_{k=n}^{i+1} (\tilde{B}^{r_k}_{c_k,k})^{p_k}\Big)\Big(\prod_{k=n}^{i+1} A^{\mathbf{c}}_{\mathbf{r},p_k\cdot\mathbf{e}_k} \otimes I\Big)|\psi'\rangle \\
& - \langle\psi'| \Big(\prod_{k=n}^{i+1} (\tilde{B}^{r_k}_{c_k,k})^{p_k}\Big)\Big(\prod_{k=n}^{i+1} A^{\mathbf{c}}_{\mathbf{r},p_k\cdot\mathbf{e}_k} \otimes I\Big) \cdot A^{\mathbf{c}}_{\mathbf{r},p_i\cdot\mathbf{e}_i} \otimes I \cdot (\tilde{A}^{c_i}_{r_i,i})^{p_i}|\psi'\rangle \Big)\Big| \\
\leq \Big| \mathbf{E}_{\mathbf{r}} & \Big(d_{\psi'}(\tilde{A}^{c_{i+1}}_{r_{i+1},i+1}, \tilde{B}^{r_{i+1}}_{c_{i+1},i+1}) \Big)\Big| + \Big| \mathbf{E}_{\mathbf{r}} \Big(d_{\psi'}(I, (A^{\mathbf{c}}_{\mathbf{r},p_i\cdot\mathbf{e}_i} \otimes I) \cdot (\tilde{A}^{c_i}_{r_i,i})^{p_i}) \Big)\Big| .
\end{aligned}
$$

Above, the second to last inequality uses the fact that

$$
\|\langle\psi'| \Big(\prod_{k=n}^{i+2} (\tilde{B}^{r_k}_{c_k,k})^{p_k}\Big)\Big(\prod_{k=n}^{i+1} A^{\mathbf{c}}_{\mathbf{r},p_k\cdot\mathbf{e}_k} \otimes I\Big)\| = 1,
$$

and the third inequality uses that fact that

$$\|\langle\psi'|(\prod_{k=n}^{i+1}\tilde{B}_{c_k,k}^{r_k})^{p_k}(\prod_{k=n}^{i+1}A_{\mathbf{r},p_k\cdot\mathbf{e}_k}^{\mathbf{c}}\otimes I)\| = 1.$$

Now, applying Lemma A.4.8, we have

$$\begin{aligned}\Delta &\leq \mathbf{E}_{\mathbf{r}}\left(d_{\psi'}(\tilde{A}_{r_{i+1},i+1}^{c_{i+1}},\tilde{B}_{c_{i+1},i+1}^{r_{i+1}})\right)+\mathbf{E}_{\mathbf{r}}\left(d_{\psi'}(I,(A_{\mathbf{r},p_i\cdot\mathbf{e}_i}^{\mathbf{c}}\otimes I)\cdot(\tilde{A}_{r_i,i}^{c_i})^{p_i})\right)\\ &\leq O(\sqrt{\varepsilon})+\mathbf{E}_{\mathbf{r}}\left(d_{\psi'}(I,(A_{\mathbf{r},p_i\cdot\mathbf{e}_i}^{\mathbf{c}}\otimes I)\cdot(\tilde{A}_{r_i,i}^{c_i})^{p_i})\right). \qquad \text{(A.12)}\end{aligned}$$

We bound the second term on the RHS of (A.12). The term vanishes when $p_i = 0$ so we consider the case where $p_i = 1$ only.

$$\begin{aligned}\mathbf{E}_{\mathbf{r}}(\dots) &= \mathbf{E}_{\mathbf{r}}\left(\||\psi'\rangle-(A_{\mathbf{r},p_i\cdot\mathbf{e}_i}^{\mathbf{c}}\otimes I)\cdot\tilde{A}_{r_i,i}^{c_i}|\psi'\rangle\|^2\right)\\ &= \mathbf{E}_{\mathbf{r}}\left[2-2\langle\psi'|(A_{\mathbf{r},p_i\cdot\mathbf{e}_i}^{\mathbf{c}}\otimes I)\cdot\tilde{A}_{r_i,i}^{c_i}|\psi'\rangle\right]\\ &= \mathbf{E}_{\mathbf{r}}\Bigg[2-2\Bigg(\langle\psi|\otimes\frac{1}{\sqrt{3^{n-1}}}\sum_{\mathbf{r}_{-k}\in\{0,1,2\}^{n-1}}\langle\mathbf{r}_{-k}|\Bigg)\\ &\qquad\times(A_{\mathbf{r},p_i\cdot\mathbf{e}_i}^{\mathbf{c}}\otimes I)\\ &\qquad\times\Bigg(\sum_{\mathbf{r}':r'_i=r_i}A_{\mathbf{r}',\mathbf{e}_i}^{\mathbf{c}}\otimes|\mathbf{r}'_{-i}\rangle\langle\mathbf{r}'_{-i}|\Bigg)\times\dots\\ &\qquad\times\Bigg(|\psi\rangle\otimes\frac{1}{\sqrt{3^{n-1}}}\sum_{\mathbf{r}_{-k}\in\{0,1,2\}^{n-1}}|\mathbf{r}_{-k}\rangle\Bigg)\Bigg]\\ &= \mathbf{E}_{\mathbf{r}}\left(2-2\cdot\frac{1}{3^{n-1}}\sum_{\mathbf{r}':r'_i=r_i}\langle\psi|A_{\mathbf{r},p_i\cdot\mathbf{e}_i}^{\mathbf{c}}\cdot A_{\mathbf{r}',\mathbf{e}_i}^{\mathbf{c}}|\psi\rangle\cdot\langle\mathbf{r}'_{-i}||\mathbf{r}'_{-i}\rangle\langle\mathbf{r}'_{-i}||\mathbf{r}'_{-i}\rangle\right)\\ &= \mathbf{E}_{\mathbf{r}}\left(2-2\cdot\mathbf{E}_{\mathbf{r}':r'_i=r_i}\langle\psi|A_{\mathbf{r},p_i\cdot\mathbf{e}_i}^{\mathbf{c}}\cdot A_{\mathbf{r}',\mathbf{e}_i}^{\mathbf{c}}|\psi\rangle\right)\\ &= 2\left(1-\mathbf{E}_{\mathbf{r},\mathbf{r}':r'_i=r_i}\langle\psi|A_{\mathbf{r},p_i\cdot\mathbf{e}_i}^{\mathbf{c}}\cdot A_{\mathbf{r}',\mathbf{e}_i}^{\mathbf{c}}|\psi\rangle\right)\\ &\leq 2\cdot 3\cdot 36\varepsilon, \qquad \text{(A.13)}\end{aligned}$$

where the last inequality follows from Lemma A.3.7. Furthermore, by Jensen's inequality it follows that:

$$\mathbf{E}_{\mathbf{r}}\left(d_{\psi'}(I,(A_{\mathbf{r},p_i\cdot\mathbf{e}_i}^{\mathbf{c}}\otimes I)\cdot\tilde{A}_{r_i,i}^{c_i})\right)\leq\sqrt{\mathbf{E}_{\mathbf{r}}\left(d_{\psi'}(I,(A_{\mathbf{r},p_i\cdot\mathbf{e}_i}^{\mathbf{c}}\otimes I)\cdot\tilde{A}_{r_i,i}^{c_i})^2\right)}\leq O(\sqrt{\varepsilon}).$$

Now, resuming the calculation in equation (A.12), we have that

$$\Delta \leq O(\sqrt{\varepsilon}) + \mathbf{E}_{\mathbf{r}} \left(d_{\psi'}(I, (A^{\mathbf{c}}_{\mathbf{r},p_i \cdot \mathbf{e}_i} \otimes I) \cdot (\tilde{A}^{c_i}_{r_i,i})^{p_i}) \right) \leq O(\sqrt{\varepsilon}).$$

Finally, to obtain Equation A.11, note that, since Equation A.13 is valid for every i, it follows by the same calculation, with $i = n$, that:

$$\left| \mathbf{E}_{\mathbf{r}} \left(1 - \langle \psi' | A^{\mathbf{c}}_{\mathbf{r},p_n \cdot \mathbf{e}_n} (\tilde{A}^{c_n}_{r_n,n})^{p_n} | \psi' \rangle \right) \right| \leq O(\varepsilon) \leq O(\sqrt{\varepsilon})$$

□

Lemma A.4.11.

$$\forall \mathbf{c}, \mathbf{p}, \quad \mathbf{E}_{\mathbf{r}}\, d_{\psi'} \left(A^{\mathbf{c}}_{\mathbf{r},\mathbf{p}} \otimes I, \prod_{k=1}^{n} (\tilde{A}^{c_k}_{r_k,k})^{p_k} \right)^2 \leq O(n\sqrt{\varepsilon})$$

The analogous statement also holds for Bob operators

Proof. For simplicity of notation, throughout this proof, we will denote $A^{\mathbf{c}}_{\mathbf{r}} \otimes I$ simply by $A^{\mathbf{c}}_{\mathbf{r}}$. Start by noting that we have the following exact property:

$$A^{\mathbf{c}}_{\mathbf{r},\mathbf{p}} A^{\mathbf{c}}_{\mathbf{r},\mathbf{p}'} = A^{\mathbf{c}}_{\mathbf{r},\mathbf{p}+\mathbf{p}'}.$$

As a consequence, we may decompose each observable $A^{\mathbf{c}}_{\mathbf{r},\mathbf{p}}$ into a product of *single-round* observables

$$A^{\mathbf{c}}_{\mathbf{r},\mathbf{p}} = A^{\mathbf{c}}_{\mathbf{r},p_1} \ldots A^{\mathbf{c}}_{\mathbf{r},p_k}.$$

So, fixing any value of $\mathbf{c}$, and $\mathbf{p}$, we have

$$\begin{aligned}
&\mathbf{E}_{\mathbf{r}}\, d_{\psi'} \left(A^{\mathbf{c}}_{\mathbf{r},\mathbf{p}}, \prod_{k=1}^{n} (\tilde{A}^{c_k}_{r_k,k})^{p_k} \right)^2 \\
&= \mathbf{E}_{\mathbf{r}} \left(\langle \psi' | A^{\mathbf{c}\dagger}_{\mathbf{r},\mathbf{p}} A^{\mathbf{c}}_{\mathbf{r},\mathbf{p}} | \psi' \rangle + \langle \psi' | (\prod_{k=1}^{n} (\tilde{A}^{c_k}_{r_k,k})^{p_k})^\dagger (\prod_{k=1}^{n} (\tilde{A}^{c_k}_{r_k,k})^{p_k}) | \psi' \rangle \right. \\
&\left. - \langle \psi' | A^{\mathbf{c}\dagger}_{\mathbf{r},\mathbf{p}} (\prod_{k=1}^{n} (\tilde{A}^{c_k}_{r_k,k})^{p_k}) | \psi' \rangle - \langle \psi' | (\prod_{k=1}^{n} (\tilde{A}^{c_k}_{r_k,k})^{p_k})^\dagger A^{\mathbf{c}}_{\mathbf{r},\mathbf{p}} | \psi' \rangle \right) \\
&= 2\, \mathbf{E}_{\mathbf{r}} \left(1 - \langle \psi' | A^{\mathbf{c}}_{\mathbf{r},\mathbf{p}} (\prod_{k=1}^{n} (\tilde{A}^{c_k}_{r_k,k})^{p_k}) | \psi' \rangle \right),
\end{aligned}$$

where, in the second equality we are using the fact that $A^{\mathbf{c}}_{\mathbf{r},\mathbf{p}}$ is Hermitian to get that

$$\langle \psi' | A^{\mathbf{c}}_{\mathbf{r},\mathbf{p}} (\prod_{k=1}^{n} (\tilde{A}^{c_k}_{r_k,k})^{p_k}) | \psi' \rangle = \langle \psi' | A^{\mathbf{c}\dagger}_{\mathbf{r},\mathbf{p}} (\prod_{k=1}^{n} (\tilde{A}^{c_k}_{r_k,k})^{p_k}) | \psi' \rangle = \langle \psi' | (\prod_{k=1}^{n} (\tilde{A}^{c_k}_{r_k,k})^{p_k})^\dagger A^{\mathbf{c}}_{\mathbf{r},\mathbf{p}} | \psi' \rangle.$$

Continuing, we have

$$
\begin{aligned}
&\mathbf{E}_{\mathbf{r}}\, d_{\psi'}\left(A^{\mathbf{c}}_{\mathbf{r},\mathbf{p}}, \prod_{k=1}^{n}(\tilde{A}^{c_k}_{r_k,k})^{p_k}\right)^2 \\
&\quad = 2\,\mathbf{E}_{\mathbf{r}}\left(1 - \langle\psi'|A^{\mathbf{c}}_{\mathbf{r},\mathbf{p}}(\prod_{k=1}^{n}(\tilde{A}^{c_k}_{r_k,k})^{p_k})|\psi'\rangle\right) \\
&\quad = 2\,\mathbf{E}_{\mathbf{r}}\left(1 - \langle\psi'|(\prod_{k=n}^{2}(\tilde{B}^{r_k}_{c_k,k})^{p_k})A^{\mathbf{c}}_{\mathbf{r},\mathbf{p}}(\tilde{A}^{c_1}_{r_1,1})^{p_1}|\psi'\rangle\right. \\
&\qquad - \sum_{i=n}^{1}\left(\langle\psi'|(\prod_{k=n}^{i+1}(\tilde{B}^{r_k}_{c_k,k})^{p_k})A^{\mathbf{c}}_{\mathbf{r},\mathbf{p}}(\prod_{k=1}^{i}(\tilde{A}^{c_k}_{r_k,k})^{p_k})|\psi'\rangle\right. \\
&\qquad \left.\left. -\langle\psi'|(\prod_{k=n}^{i}(\tilde{B}^{r_k}_{c_k,k})^{p_k})A^{\mathbf{c}}_{\mathbf{r},\mathbf{p}}(\prod_{k=1}^{i-1}(\tilde{A}^{c_k}_{r_k,k})^{p_k})|\psi'\rangle\right)\right) \\
&\quad \le 2\,\mathbf{E}_{\mathbf{r}}\left(1 - \langle\psi'|(\prod_{k=n}^{2}(\tilde{B}^{r_k}_{c_k,k})^{p_k})A^{\mathbf{c}}_{\mathbf{r},\mathbf{p}}(\tilde{A}^{c_1}_{r_1,1})^{p_1}|\psi'\rangle\right) \\
&\qquad + \sum_{i=n}^{1} 2\,\mathbf{E}_{\mathbf{r}}\left(\left|\langle\psi'|(\prod_{k=n}^{i+1}(\tilde{B}^{r_k}_{c_k,k})^{p_k})A^{\mathbf{c}}_{\mathbf{r},\mathbf{p}}(\prod_{k=1}^{i}(\tilde{A}^{c_k}_{r_k,k})^{p_k})|\psi'\rangle\right.\right. \\
&\qquad \left.\left. -\langle\psi'|(\prod_{k=n}^{i}(\tilde{B}^{r_k}_{c_k,k})^{p_k})A^{\mathbf{c}}_{\mathbf{r},\mathbf{p}}(\prod_{k=1}^{i-1}(\tilde{A}^{c_k}_{r_k,k})^{p_k})|\psi'\rangle\right|\right).
\end{aligned}
$$

We now apply Lemma A.4.9 inside the expectation:

$$
\begin{aligned}
&\le 2\,\mathbf{E}_{\mathbf{r}}\left(1 - \langle\psi'|(\prod_{k=n}^{2}(\tilde{B}^{r_k}_{c_k,k})^{p_k})A^{\mathbf{c}}_{\mathbf{r},\mathbf{p}}(\tilde{A}^{c_1}_{r_1,1})^{p_1}|\psi'\rangle\right) + \sum_{i=1}^{n} 2\cdot O(\sqrt{\varepsilon}) \\
&= 2\,\mathbf{E}_{\mathbf{r}}\left(1 - \langle\psi'|(\prod_{k=n}^{2}(\tilde{B}^{r_k}_{c_k,k})^{p_k})A^{\mathbf{c}}_{\mathbf{r},\mathbf{p}}(\tilde{A}^{c_1}_{r_1,1})^{p_1}|\psi'\rangle\right) + O(n\sqrt{\varepsilon}) \\
&= 2\,\mathbf{E}_{\mathbf{r}}\left(1 - \langle\psi'|(\prod_{k=n}^{2}(\tilde{B}^{r_k}_{c_k,k})^{p_k})(\prod_{k=n}^{1}A^{\mathbf{c}}_{\mathbf{r},p_k\cdot\mathbf{e}_k})(\tilde{A}^{c_1}_{r_1,1})^{p_1}|\psi'\rangle\right) + O(n\sqrt{\varepsilon}) \\
&\le 2\left|\mathbf{E}_{\mathbf{r}}\left(1 - \langle\psi'|A^{\mathbf{c}}_{\mathbf{r},p_n\cdot\mathbf{e}_n}(\tilde{A}^{c_n}_{r_n,n})^{p_n}|\psi'\rangle\right)\right| \\
&\qquad + 2\sum_{i=n-1}^{1}\left|\mathbf{E}_{\mathbf{r}}\left(\langle\psi'|(\prod_{k=n}^{i+2}(\tilde{B}^{r_k}_{c_k,k})^{p_k})(\prod_{k=n}^{i+1}A^{\mathbf{c}}_{\mathbf{r},p_k\cdot\mathbf{e}_k})(\tilde{A}^{c_{i+1}}_{r_{i+1},i+1})^{p_{i+1}}|\psi'\rangle\right.\right. \\
&\qquad \left.\left. - \langle\psi'|(\prod_{k=n}^{i+1}(\tilde{B}^{r_k}_{c_k,k})^{p_k})(\prod_{k=n}^{i}A^{\mathbf{c}}_{\mathbf{r},p_k\cdot\mathbf{e}_k})(\tilde{A}^{c_i}_{r_i,i})^{p_i}|\psi'\rangle\right)\right| + O(n\sqrt{\varepsilon}) \\
&\le 2\cdot O(\sqrt{\varepsilon}) + 2(n-1)O(\sqrt{\varepsilon}) + O(n\sqrt{\varepsilon}) = O(n\sqrt{\varepsilon})
\end{aligned}
$$

Where the last inequality follows by Lemma A.4.10.

□

A.4.3 The Isometry

Definition A.4.12. Define the *single round* "approximate Pauli" operators on Alice's space by:

$$\begin{aligned} X_{2k-1} &= \tilde{A}^1_{1,k} \\ X_{2k} &= \tilde{A}^0_{1,k} \\ Z_{2k-1} &= \tilde{A}^0_{0,k} \\ Z_{2k} &= \tilde{A}^1_{0,k}. \end{aligned}$$

Likewise define the single round approximate Pauli operators on Bob's space by

$$\begin{aligned} X^B_{2k-1} &= \tilde{B}^1_{1,k} \\ X^B_{2k} &= \tilde{B}^0_{1,k} \\ Z^B_{2k-1} &= \tilde{B}^0_{0,k} \\ Z^B_{2k} &= \tilde{B}^1_{0,k}. \end{aligned}$$

Lemma A.4.13 (Approximate single-round Pauli relations)**.** *Suppose Alice and Bob share an entangled strategy that wins with probability* $1-\varepsilon$*. Then the single-round Pauli operators as defined above satisfy the following relations:*

$$\begin{aligned} &\forall i, \quad d_\psi(X_i, X^B_i) && \leq \sqrt{\varepsilon} \\ &\forall i, \quad d_\psi(Z_i, Z^B_i) && \leq \sqrt{\varepsilon} \\ &\forall i, \quad d_\psi(X_iZ_i, -Z_iX_i) && \leq \sqrt{\varepsilon} \\ &\forall i \neq j, \quad d_\psi(X_iX_j, X_jX_i) && \leq \sqrt{\varepsilon} \\ &\forall i \neq j, \quad d_\psi(Z_iZ_j, Z_jZ_i) && \leq \sqrt{\varepsilon}. \end{aligned} \tag{A.14}$$

Proof. The consistency relations follow from Lemma A.4.8. The other relations come from Theorem A.4.1. □

We will now build up multi-round Paulis from products of these.

Lemma A.4.14 (Approximate Pauli relations)**.** *Suppose* X_i*,* Z_i *are observables on Alice and* X^B_i, Z^B_i *are observables on Bob indexed by* $i \in [n]$ *satisfying* (A.14)*. Let* $X^{\mathbf{a}} := \prod_{i=1}^n X_i^{a_i}$ *and* $Z^{\mathbf{b}} := \prod_{i=1}^n Z_i^{b_i}$*, and likewise let* $(X^B)^{\mathbf{a}} := \prod_{i=n}^1 (X^B_i)^{a_i}$ *and* $(Z^B)^{\mathbf{b}} := \prod_{i=n}^1 (Z^B_i)^{b_i}$*. Then*

$$\forall \mathbf{a}, \mathbf{b}, \mathbf{a}', \mathbf{b}', \quad d_\psi((X^{\mathbf{a}}Z^{\mathbf{b}})(X^{\mathbf{a}'}Z^{\mathbf{b}'}), (-1)^{\mathbf{a}'\cdot\mathbf{b}}X^{\mathbf{a}+\mathbf{a}'}Z^{\mathbf{b}+\mathbf{b}'}) \leq O(n^2\sqrt{\varepsilon}) \tag{A.15}$$

$$\forall \mathbf{a}, \mathbf{b}, \quad d_\psi((X^{\mathbf{a}}Z^{\mathbf{b}}), (Z^B)^{\mathbf{b}}(X^B)^{\mathbf{a}}) \leq O(n\sqrt{\varepsilon}). \tag{A.16}$$

Proof. (A.16) is an immediate consequence of Lemma A.6.6. We obtain (A.15) in two steps. First, by (A.17) of Lemma A.6.9, we have that

$$d_\psi(X^{\mathbf{a}}Z^{\mathbf{b}}, (-1)^{\mathbf{a}\cdot\mathbf{b}}Z^{\mathbf{b}}X^{\mathbf{a}}) \leq O(n^2\sqrt{\varepsilon}).$$

Further, by (A.18) of Lemma A.6.9 we have that

$$\begin{aligned} d_\psi(X^{\mathbf{a}}X^{\mathbf{a}'}, X^{\mathbf{a}+\mathbf{a}'}) &\leq O(n^2\sqrt{\varepsilon}) \\ d_\psi(Z^{\mathbf{b}}Z^{\mathbf{b}'}, Z^{\mathbf{b}+\mathbf{b}'}) &\leq O(n^2\sqrt{\varepsilon}). \end{aligned}$$

Hence,

$$\begin{aligned} &d_\psi(X^{\mathbf{a}}Z^{\mathbf{b}}X^{\mathbf{a}'}Z^{\mathbf{b}'}, (-1)^{\mathbf{a}'\cdot\mathbf{b}}X^{\mathbf{a}+\mathbf{a}'}Z^{\mathbf{b}+\mathbf{b}'}) \\ &\quad\leq d_\psi(X^{\mathbf{a}}Z^{\mathbf{b}}X^{\mathbf{a}'}Z^{\mathbf{b}'}, (Z^B)^{\mathbf{b}'}X^{\mathbf{a}}Z^{\mathbf{b}}X^{\mathbf{a}'}) \\ &\qquad + d_\psi((Z^B)^{\mathbf{b}'}X^{\mathbf{a}}Z^{\mathbf{b}}X^{\mathbf{a}'}, (-1)^{\mathbf{a}'\cdot\mathbf{b}}(Z^B)^{\mathbf{b}'}X^{\mathbf{a}}X^{\mathbf{a}'}Z^{\mathbf{b}}) \\ &\qquad + d_\psi((-1)^{\mathbf{a}'\cdot\mathbf{b}}(Z^B)^{\mathbf{b}'}X^{\mathbf{a}}X^{\mathbf{a}'}Z^{\mathbf{b}}, (-1)^{\mathbf{a}'\cdot\mathbf{b}}(Z^B)^{\mathbf{b}'}(Z^B)^{\mathbf{b}}X^{\mathbf{a}}X^{\mathbf{a}'}) \\ &\qquad + d_\psi((-1)^{\mathbf{a}'\cdot\mathbf{b}}(Z^B)^{\mathbf{b}'}(Z^B)^{\mathbf{b}}X^{\mathbf{a}}X^{\mathbf{a}'}, (-1)^{\mathbf{a}'\cdot\mathbf{b}}(Z^B)^{\mathbf{b}'}(Z^B)^{\mathbf{b}}X^{\mathbf{a}+\mathbf{a}'}) \\ &\qquad + d_\psi((-1)^{\mathbf{a}'\cdot\mathbf{b}}(Z^B)^{\mathbf{b}'}(Z^B)^{\mathbf{b}}X^{\mathbf{a}+\mathbf{a}'}, (-1)^{\mathbf{a}'\cdot\mathbf{b}}X^{\mathbf{a}+\mathbf{a}'}Z^{\mathbf{b}}Z^{\mathbf{b}'}) \\ &\qquad + d_\psi((-1)^{\mathbf{a}'\cdot\mathbf{b}}X^{\mathbf{a}+\mathbf{a}'}Z^{\mathbf{b}}Z^{\mathbf{b}'}, (-1)^{\mathbf{a}'\cdot\mathbf{b}}X^{\mathbf{a}+\mathbf{a}'}Z^{\mathbf{b}+\mathbf{b}'}) \\ &\quad\leq O(n^2\sqrt{\varepsilon}). \end{aligned}$$

□

Proof of Theorem A.4.2. Let $W^A{}_{\mathbf{a},\mathbf{b}} := X^{\mathbf{a}}Z^{\mathbf{b}}$ and $W^B{}_{\mathbf{a},vb} := (X^B)^{\mathbf{a}}(Z^B)^{\mathbf{b}}$, and let $\mathcal{H}$ be the provers' Hilbert space, together with the ancillas adjoined in Section A.4.2. Then we define the isometry $V : \mathcal{H} \to \mathcal{H} \otimes \mathbb{C}^{2n} \otimes \mathbb{C}^{2n} \otimes \mathbb{C}^{2n} \otimes \mathbb{C}^{2n}$ by

$$V(|\psi\rangle) = \frac{1}{2^{3n}} \sum_{\mathbf{a},\mathbf{b},\mathbf{c}} \sum_{\mathbf{d},\mathbf{e},\mathbf{f}} (-1)^{\mathbf{b}\cdot(\mathbf{a}+\mathbf{c})}(-1)^{\mathbf{e}\cdot(\mathbf{d}+\mathbf{f})} W^A{}_{\mathbf{a},\mathbf{b}} \otimes W^B{}_{\mathbf{d},\mathbf{e}} |\psi\rangle \otimes |\mathbf{a}+\mathbf{c}, \mathbf{c}\rangle \otimes |\mathbf{d}+\mathbf{f}, \mathbf{f}\rangle.$$

Here the second and the fourth register are the "output register" of the isometry, and the third and fifth register are "junk." This isometry was introduced by McKague [McK16a], and has an alternate description in terms of a circuit that "swaps" the input into the output register, which is initialized to be maximally entangled with the junk register.

We now show the expectation value of any multi-qubit Pauli operator on the output of the isometry is close to the corresponding expectation value of approximate Paulis in the isometry input. In the equations below, $|\phi\rangle = V(|\psi\rangle)$, the Paulis σ_X^A, σ_Z^A act on output register 2, and σ_X^B, σ_Z^B on output register 4.

$$\mathcal{P} = \langle\phi|\sigma_X^A(\mathbf{s})\sigma_Z^A(\mathbf{t})\sigma_X^B(\mathbf{u})\sigma_Z^B(\mathbf{v})|\phi\rangle$$

$$= \frac{1}{2^{6n}} \sum_{\mathbf{a},\mathbf{b},\mathbf{c}} \sum_{\mathbf{a}',\mathbf{b}',\mathbf{c}'} \sum_{\mathbf{d},\mathbf{e},\mathbf{f}} \sum_{\mathbf{d}',\mathbf{e}',\mathbf{f}'} \Big(\langle\psi| \otimes \langle \mathbf{a}'+\mathbf{c}', \mathbf{c}'| \otimes \langle \mathbf{d}'+\mathbf{f}', \mathbf{f}'|$$
$$\times {W^A}^\dagger_{\mathbf{a}',\mathbf{b}'} \otimes {W^B}^\dagger_{\mathbf{d}',\mathbf{e}'} (-1)^{\mathbf{b}'\cdot(\mathbf{a}'+\mathbf{c}')+\mathbf{e}'\cdot(\mathbf{d}'+\mathbf{f}')}$$
$$\times \sigma_X^A(\mathbf{s})\sigma_Z^A(\mathbf{t})\sigma_X^B(\mathbf{u})\sigma_Z^B(\mathbf{v})(-1)^{\mathbf{b}\cdot(\mathbf{a}+\mathbf{c})+\mathbf{e}\cdot(\mathbf{d}+\mathbf{f})} {W^A}_{\mathbf{a},\mathbf{b}} \otimes {W^B}_{\mathbf{d},\mathbf{e}}$$
$$\times |\psi\rangle \otimes |\mathbf{a}+\mathbf{c}, \mathbf{c}\rangle \otimes |\mathbf{d}+\mathbf{f}, \mathbf{f}\rangle \Big)$$
$$= \frac{1}{2^{6n}} \sum_{\mathbf{a},\mathbf{b},\mathbf{c}} \sum_{\mathbf{a}',\mathbf{b}',\mathbf{c}'} \sum_{\mathbf{d},\mathbf{e},\mathbf{f}} \sum_{\mathbf{d}',\mathbf{e}',\mathbf{f}'} \Big(\langle\psi| \otimes \langle \mathbf{a}'+\mathbf{c}', \mathbf{c}'| \otimes \langle \mathbf{d}'+\mathbf{f}', \mathbf{f}'|$$
$$\times {W^A}^\dagger_{\mathbf{a}',\mathbf{b}'} \otimes {W^B}^\dagger_{\mathbf{d}',\mathbf{e}'} (-1)^{\mathbf{b}'\cdot(\mathbf{a}'+\mathbf{c}')} (-1)^{\mathbf{e}'\cdot(\mathbf{d}'+\mathbf{f}')}$$
$$\times (-1)^{(\mathbf{b}+\mathbf{t})(\mathbf{a}+\mathbf{c})} (-1)^{(\mathbf{e}+\mathbf{v})(\mathbf{d}+\mathbf{f})} {W^A}_{\mathbf{a},\mathbf{b}} \otimes {W^B}_{\mathbf{d},\mathbf{e}}$$
$$\times |\psi\rangle \otimes |\mathbf{a}+\mathbf{c}+\mathbf{s}, \mathbf{c}\rangle |\mathbf{d}+\mathbf{f}+\mathbf{u}, \mathbf{f}\rangle \Big)$$
$$= \frac{1}{2^{6n}} \sum_{\mathbf{a},\mathbf{b},\mathbf{b}',\mathbf{c}} \sum_{\mathbf{d},\mathbf{e},\mathbf{e}',\mathbf{f}} \Big(\langle\psi| {W^A}^\dagger_{\mathbf{a}+\mathbf{s},\mathbf{b}'} \otimes {W^B}^\dagger_{\mathbf{d}+\mathbf{u},\mathbf{e}'} (-1)^{\mathbf{b}'\cdot(\mathbf{a}+\mathbf{s}+\mathbf{c})} (-1)^{\mathbf{e}'\cdot(\mathbf{d}+\mathbf{u}+\mathbf{f})}$$
$$\times (-1)^{(\mathbf{b}+\mathbf{t})\cdot(\mathbf{a}+\mathbf{c})} (-1)^{(\mathbf{e}+\mathbf{v})\cdot(\mathbf{d}+\mathbf{f})} {W^A}_{\mathbf{a},\mathbf{b}} \otimes {W^B}_{\mathbf{d},\mathbf{e}} |\psi\rangle \Big).$$

Now we do the sum over $\mathbf{c}$ and $\mathbf{f}$ to force $\mathbf{b}' = \mathbf{b}+\mathbf{t}$ and $\mathbf{e}' = \mathbf{e}+\mathbf{v}$:

$$= \frac{1}{2^{4n}} \sum_{\mathbf{a},\mathbf{b}} \sum_{\mathbf{d},\mathbf{e}} \Big((-1)^{(\mathbf{b}+\mathbf{t})\cdot\mathbf{s}} (-1)^{(\mathbf{e}+\mathbf{v})\cdot\mathbf{u}} \langle\psi| {W^A}^\dagger_{\mathbf{a}+\mathbf{s},\mathbf{b}+\mathbf{t}} {W^A}_{\mathbf{a},\mathbf{b}} \otimes {W^B}^\dagger_{\mathbf{d}+\mathbf{u},\mathbf{e}+\mathbf{v}} {W^B}_{\mathbf{d},\mathbf{e}} |\psi\rangle \Big).$$

Finally, we apply Lemma A.4.14 to merge the W^A and W^B operators, picking up an error of $O(n^2\sqrt{\varepsilon})$ in the process.

$$\approx_{O(n^2\sqrt{\varepsilon})} \langle\psi| {W^A}_{\mathbf{s},\mathbf{t}} {W^B}_{\mathbf{u},\mathbf{v}} |\psi\rangle.$$

□

Lemma A.4.15. *Let M_n be the $4n$-qubit operator defined by*

$$M_n = \Big(\frac{1}{2} IIII + \frac{1}{18} (IXIX + XIXI + XXXX + ZIZI + IZIZ + ZZZZ + XZXZ + ZXZX + YYYY) \Big)^{\otimes n}.$$

Then if a density matrix ρ satisfies $\mathrm{Tr}[M_n\rho] \geq 1-\delta$, $\langle \mathrm{EPR}|^{\otimes 2n} \rho |\mathrm{EPR}\rangle^{\otimes 2n} \geq 1 - \frac{9}{4}\delta$.

Proof. Observe that the highest eigenvalue of M_1 is 1, with unique eigenvector $|\mathrm{EPR}\rangle^{\otimes 2}$. Moreover all other eigenvalues of M_1 have absolute value at most 5/9. Hence, the highest eigenvalue of M_n is also 1 with the unique eigenvector is $|\mathrm{EPR}\rangle^{\otimes 2n}$, and all other eigenvalues have absolute value at most 5/9. Hence

$$M_n \leq |\mathrm{EPR}\rangle\langle\mathrm{EPR}|^{\otimes 2n} + \frac{5}{9}(I - |\mathrm{EPR}\rangle\langle\mathrm{EPR}|^{\otimes 2n}).$$

So

$$\begin{aligned}
1-\delta &\leq \mathrm{Tr}[M_n\rho] \\
&\leq \frac{4}{9}\mathrm{Tr}[\rho|\mathrm{EPR}\rangle\langle\mathrm{EPR}|^{\otimes 2n}] + \frac{5}{9} \\
\frac{4}{9}-\delta &\leq \frac{4}{9}\mathrm{Tr}[\rho|\mathrm{EPR}\rangle\langle\mathrm{EPR}|^{\otimes 2n}] \\
1-\frac{9}{4}\delta &\leq \mathrm{Tr}[\rho|\mathrm{EPR}\rangle\langle\mathrm{EPR}|^{\otimes 2n}].
\end{aligned}$$

□

Lemma A.4.16. *For every single round operator $\tilde{A}^c_{r,k}$, let $X^{\mathbf{a}}Z^{\mathbf{b}}$ be approximate Pauli operator formed by taking the row-r, column-c entry in the Magic Square (Figure A-2), and converting X and Z on the first and second qubits to the approximate Paulis on qubits $2k-1$ and $2k$, respectively. Then*

$$d_\psi(\tilde{A}^c_{r,k}, X^{\mathbf{a}}Z^{\mathbf{b}}) \leq O(\sqrt{\varepsilon}).$$

Likewise, for Bob,

$$d_\psi(\tilde{B}^r_{c,k}, (X^B)^{\mathbf{a}}(Z^B)^{\mathbf{b}}) \leq O(\sqrt{\varepsilon}).$$

Proof. First consider Alice. Then the conclusion follows by definition of the approximate Paulis for $r \in \{0,1\}$. When $r=2$, use the fact that $d_\psi(\tilde{A}^c_{2,k}, \tilde{B}^2_{c,k}) \leq O(\sqrt{\varepsilon})$. By definition, $\tilde{B}^2_{ck} = -\tilde{B}^1_{ck}\tilde{B}^0_{ck}$. Each of these two operators can be switched back to Alice, to yield

$$d_\psi(\tilde{A}^c_{2,k}, -\tilde{A}^c_{0k}\tilde{A}^c_{1k}) \leq O(\sqrt{\varepsilon}).$$

This establishes the result for single round operators. For the Bob, we follow the same argument, interchanging the role of the row and column indices. □

Lemma A.4.17. *For every product of single-round operators $\prod_{k=1}^n (\tilde{A}^{c_k}_{r_k,k})^{p_k}$, let $X^{\mathbf{a}}Z^{\mathbf{b}}$ be the approximate Pauli operator formed by applying the procedure of Lemma A.4.16 to each single-round operator. Then*

$$d_\psi(\prod_{k=1}^n (\tilde{A}^{c_k}_{r_k,k})^{p_k}, X^{\mathbf{a}}Z^{\mathbf{b}}) \leq O(n\sqrt{\varepsilon}).$$

The analogous statement holds for B.

Proof. This is a consequence of Lemma A.4.16 and Lemma A.6.7. □

Lemma A.4.18. *Suppose Alice and Bob win the test with probability $1-\varepsilon$. Then for the operator M_n defined in Lemma A.4.15. $\langle\phi|M_n|\phi\rangle \geq 1 - O(n^2\sqrt{\varepsilon})$, where $|\phi\rangle = V(|\psi\rangle)$ is the output of the isometry in Theorem A.4.2 applied to Alice and Bob's shared state $|\psi\rangle$.*

Proof. Recall from Fact A.3.6, we know that

$$\forall \mathbf{p}, \quad \mathbf{E}_{\mathbf{r},\mathbf{c}} \langle \psi | A^{\mathbf{c}}_{\mathbf{r},\mathbf{p}} B^{\mathbf{r}}_{\mathbf{c},\mathbf{p}} | \psi \rangle \geq 1 - \varepsilon.$$

By applying the consistency relations (A.4) and (A.5) guaranteed by Theorem A.4.1, we obtain that

$$\forall \mathbf{p}, \quad \mathbf{E}_{\mathbf{r},\mathbf{c}} \langle \psi | \prod_{k=1}^{n} (\tilde{A}^{c_k}_{r_k,k})^{p_k} \prod_{k=1}^{n} (\tilde{B}^{r_k}_{c_k,k})^{p_k} | \psi \rangle \geq 1 - O(n\sqrt{\varepsilon}).$$

Now, by Lemma A.4.17, we can switch the $\tilde{A}$ and $\tilde{B}$ operators to approximate Paulis:

$$\forall \mathbf{p}, \quad \mathbf{E}_{\mathbf{r},\mathbf{c}} \langle \psi | (X^{\mathbf{a}} Z^{\mathbf{b}})((X^B)^{\mathbf{c}} (Z^B)^{\mathbf{d}}) | \psi \rangle \geq 1 - O(n\sqrt{\varepsilon}).$$

Applying Theorem A.4.2, we obtain that

$$\forall \mathbf{p}, \quad \langle \phi | \, \mathbf{E}_{\mathbf{r},\mathbf{c}} (\sigma^A_X(\mathbf{a}) \sigma^A_Z(\mathbf{b}) \sigma^B_X(\mathbf{c}) \sigma^B_Z(\mathbf{d})) | \phi \rangle \geq 1 - O(n^2\sqrt{\varepsilon}).$$

In particular, taking an expectation over uniformly random choices of $\mathbf{p}$, we obtain that

$$\langle \phi | \, \mathbf{E}_{\mathbf{r},\mathbf{c},\mathbf{p}} (\sigma^A_X(\mathbf{a}) \sigma^A_Z(\mathbf{b}) \sigma^B_X(\mathbf{c}) \sigma^B_Z(\mathbf{d})) | \phi \rangle \geq 1 - O(n^2\sqrt{\varepsilon}).$$

It is not hard to see that $\mathbf{E}_{\mathbf{r},\mathbf{c},\mathbf{p}} (\sigma^A_X(\mathbf{a}) \sigma^A_Z(\mathbf{b}) \sigma^B_X(\mathbf{c}) \sigma^B_Z(\mathbf{d}))$ is precisely the operator M_n, corresponding to the magic square test performed on an unknown state $|\phi\rangle$ using the measurement operators of the ideal strategy. □

A.5 Discussion and open questions

The reader familiar with previous self-testing results may notice that our Theorem A.4.2 gives a robustness bound on the *expectation value* of operators without explicitly characterizing the state, whereas previous works often state a bound on the 2-norm $\| V(|\psi\rangle) - |\psi'\rangle \otimes |\text{junk}\rangle \|$, where $|\psi'\rangle$ is a fixed target state. While it is possible to translate from one to the other by means of the techniques in Lemma A.4.18, we think the guarantee on expectation values is more natural in applications where one does not want to test closeness to a fixed target state, but rather to test whether the state satisfies a certain *property* described by a measurement operator.

Self-testing and rigidity have been very active areas of research in recent years, and we believe that many more interesting questions remain to be answered. Perhaps the most interesting question is to understand the constant error regime. It is an open question whether the parallel-repeated magic square game, as described in this appendix, can in fact achieve constant robustness independent of n, by an improvement of our analysis. (See Appendix A.8 for a possible approach towards this goal). Relatedly, it would be interesting to explore the tradeoff between the bits of communication between the prover and verifier, and the robustness of the test. The constant error regime is especially interesting from the perspective of computational complexity, where self-testing results have been used to show computational hardness

for estimating the value of non-local games [Ji16b, NV15]. Rigidity has also been applied to secure delegated computation and quantum key distribution: in particular, the work of Reichardt, Unger, and Vazirani [RUV13b] achieves these applications using a serial (many-round) version of the CHSH test; it would be interesting to see if their results could be improved using the Magic Square test.

A further way to generalize our result would be to adapt it to test states made up of qudits, with local dimension $d \neq 2$. As our techniques relied heavily on the algebraic structure of the qubit Pauli group, this may require significant technical advances. In fact, a variant of the Magic Square game for which the ideal strategy consists of "generalized Paulis" (i.e. the mod d shift- and clock-matrices) was recently proposed by McKague [McK16b], and it would be interesting to see if our analysis could extend to the parallel repetition of this game. Likewise, it would be interesting to extend our analysis to states other than the EPR state—for instance, could we do something like McKague's self-test for n-qubit graph states [McK16a], but with only two provers instead of n?

A.6 Properties of the State-Dependent Distance

Definition A.6.1. Given a state $|\psi\rangle$ and two operators A, B, the *state-dependent distance* $d_\psi(A, B)$ between A and B is defined to be

$$d_\psi(A, B) := \||A|\psi\rangle - B|\psi\rangle\|.$$

Lemma A.6.2. *The state-dependent distance satisfies the triangle inequality*

$$\forall A, B, C, \quad d_\psi(A, C) \leq d_\psi(A, B) + d_\psi(B, C).$$

Lemma A.6.3. *Let A, B, C, D be bounded operators. Then*

$$d_\psi(DA, DC) \leq d_\psi(DA, DB) + \|D\| d_\psi(B, C).$$

Proof. By Lemma A.6.2,

$$d_\psi(DA, DC) \leq d_\psi(DA, DB) + d_\psi(DB, DC).$$

Expand the second term:

$$\begin{aligned} d_\psi(DB, DC) &= \|D(B|\psi\rangle - C|\psi\rangle)\|_2 \\ &\leq \|D\| \cdot \|B|\psi\rangle - C|\psi\rangle\|_2 \\ &= \|D\| d_\psi(B, C). \end{aligned}$$

□

The following lemma tells us that guarantees on the state-dependent distance on average can be made "coherent."

Lemma A.6.4. *Let $\{A_i\}$ and $\{B_i\}$ be two sets of operators indexed by $i \in [N]$, and suppose that*

$$\mathbf{E}_i \, d_\psi(A_i, B_i)^2 = \delta.$$

Define the extended state $|\psi'\rangle = \frac{1}{\sqrt{N}} \sum_{i \in [N]} |\psi\rangle \otimes |i\rangle$, and the extended operators $\tilde{A} = \sum_i A_i \otimes |i\rangle\langle i|$ and $\tilde{B} = \sum_i B_i \otimes |j\rangle\langle j|$. Then

$$d_{\psi'}(\tilde{A}, \tilde{B})^2 = \delta.$$

Proof.

$$\begin{aligned}
d_{\psi'}(\tilde{A}, \tilde{B}) &= \|\tilde{A}|\psi'\rangle - \tilde{B}|\psi'\rangle\|^2 \\
&= \|\frac{1}{\sqrt{N}} \sum_i A_i|\psi\rangle \otimes |i\rangle - \frac{1}{\sqrt{N}} \sum_i B_i|\psi\rangle \otimes |i\rangle\|^2 \\
&= \frac{1}{N} \sum_i \langle\psi|(A_i^\dagger A_i + B_i^\dagger B_i - A_i^\dagger B_i - B_i^\dagger A_i)|\psi\rangle \\
&= \mathbf{E}_i \, d_\psi(A_i, B_i)^2 \\
&= \delta.
\end{aligned}$$

□

Lemma A.6.5. *Given three Hermitian, unitary operators T, T', S, and a unit vector $|\sigma\rangle$, if: $\langle\sigma|T \cdot S|\sigma\rangle \geq 1 - \delta$ and $\langle\sigma|T' \cdot S|\sigma\rangle \geq 1 - \delta$, then $\langle\sigma|T \cdot T'|\sigma\rangle \geq 1 - 4\delta$.*

Proof. Note that

$$\|(T - S)|\sigma\rangle\|^2 = 2 - 2\langle\sigma|T \cdot S|\sigma\rangle \leq 2\delta$$

and, similarly,

$$\|(T' - S)|\sigma\rangle\|^2 = 2 - 2\langle\sigma|T' \cdot S|\sigma\rangle \leq 2\delta.$$

So, by the Cauchy-Schwarz inequality,

$$|\langle\sigma|(T - S)(T' - S)|\sigma\rangle| \leq \|(T - S)|\sigma\rangle\| \cdot \|(T' - S)|\sigma\rangle\| \leq \sqrt{2\delta} \cdot \sqrt{2\delta} = 2\delta.$$

Expanding out the Left Hand Side, now gives

$$\begin{aligned}
2\delta \geq |\langle\sigma|(T - S)(T' - S)|\sigma\rangle| &= |\langle\sigma|T \cdot T'|\sigma\rangle - \langle\sigma|T \cdot S|\sigma\rangle - \langle\sigma|S \cdot T'|\sigma\rangle + \langle\sigma|S \cdot S|\sigma\rangle| \\
&= |\langle\sigma|T \cdot T'|\sigma\rangle - \langle\sigma|T \cdot S|\sigma\rangle - \langle\sigma|S \cdot T'|\sigma\rangle + 1|
\end{aligned}$$

So,

$$-2\delta \leq \langle\sigma|T \cdot T'|\sigma\rangle - \langle\sigma|T \cdot S|\sigma\rangle - \langle\sigma|S \cdot T'|\sigma\rangle + 1$$

and

$$\langle\sigma|T\cdot T'|\sigma\rangle \geq \langle\sigma|T\cdot S|\sigma\rangle + \langle\sigma|S\cdot T'|\sigma\rangle - 1 - 2\delta \geq (1-\delta) + (1-\delta) - 1 - 2\delta = 1 - 4\delta,$$

where the last inequality again uses the assumption of this lemma. □

We now state and prove some "utility" lemmas, about what happens when we commute words of operators past each other.

Lemma A.6.6. *Let $A_1, \ldots, A_k$ be Hermitian operators on Alice's space, and $B_1, \ldots, B_k$ be Hermitian operators on Bob's space, such that*

$$\forall i, \quad d_\psi(A_i, B_i) \leq \varepsilon_i.$$

Then

$$d_\psi(\prod_{i=1}^{k} A_i, \prod_{i=k}^{1} B_i) \leq \sum_{i=1}^{k} \varepsilon_i$$

Proof.

$$\begin{aligned} d_\psi(\prod_{i=1}^{k} A_i, \prod_{i=k}^{1} B_i) &\leq d_\psi(A_1 \ldots A_k, B_k A_1 \ldots A_{k-1}) + d_\psi(B_k A_1 \ldots A_{k-1}, B_k B_{k-1} A_1 \ldots A_{k-2}) \\ &\quad + \cdots + d_\psi(B_k \ldots B_2 A_1, B_k \ldots B_1) \\ &\leq d_\psi(A_k, B_k) + d_\psi(A_{k-1}, B_{k-1}) + \cdots + d_\psi(A_1, B_1) \\ &= \sum_i \varepsilon_i \end{aligned}$$

□

Lemma A.6.7. *Let $A_1, \ldots A_k$ and $A'_1, \ldots A'_k$ be operators on Alice, and $B_1, \ldots B_k$ be operators on Bob, such that*

$$\begin{aligned} \forall i, \quad & d_\psi(A_i, B_i) \leq \varepsilon_1 \\ \forall i, \quad & d_\psi(A'_i, B_i) \leq \varepsilon_2. \end{aligned}$$

Then

$$d_\psi(A_1 \ldots A_k, A'_1 \ldots A'_k) \leq n(\varepsilon_1 + \varepsilon_2).$$

Proof. This is a straightforward application of the Lemma A.6.6.

$$\begin{aligned} d_\psi(A_1 \ldots A_k, A'_1 \ldots A'_k) &\leq d_\psi(A_1 \ldots A_k, B_k \ldots B_1) + d_\psi(B_k \ldots B_1, A'_1 \ldots A'_k) \\ &\leq n\varepsilon_1 + n\varepsilon_2. \end{aligned}$$

□

Lemma A.6.8. *Let $A_1, \ldots A_k$ be Hermitian operators on Alice's space, and $B_1, \ldots, B_k$ be Hermitian operators on Bob's space. Suppose that*

$$\forall i, \quad d_\psi(A_i, B_i) \leq \varepsilon_1$$

and

$$\forall i, j \in \{1, \ldots, k-1\}, j \in \{k\}, \quad d_\psi(A_i A_j, \alpha_{ij} A_j A_i) \leq \varepsilon_2$$

where $\alpha_{ij} \in \{\pm 1\}$ for each choice of i, j. Then

$$d_\psi(A_1 \ldots A_k, \alpha_{1k}\alpha_{2k} \ldots \alpha_{k-1,k} A_k A_1 A_2 \ldots A_{k-1}) \leq 2(k-2)\varepsilon_1 + (k-1)\varepsilon_2.$$

Proof.

$$\begin{aligned}
&d_\psi(A_1 \ldots A_k, (\prod_{i=1}^{k-1} \alpha_{ik}) A_k A_1 \ldots A_{k-1}) \\
&\quad \leq d_\psi(A_1 \ldots A_k, \alpha_{k-1,k} A_1 \ldots A_{k-2} A_k A_{k-1}) \\
&\qquad + d_\psi(\alpha_{k-1,k} A_1 \ldots A_{k-2} A_k A_{k-1}, \alpha_{k-1,k} B_{k-1} A_1 \ldots A_{k-2} A_k) \\
&\qquad + d_\psi(\alpha_{k-1,k} B_{k-1} A_1 \ldots A_{k-2} A_k, \alpha_{k-1,k}\alpha_{k-2,k} B_{k-1} A_1 \ldots A_{k-3} A_k A_{k-2}) \\
&\qquad + d_\psi(\alpha_{k-1,k}\alpha_{k-2,k} B_{k-1} A_1 \ldots A_{k-3} A_k A_{k-2}, \\
&\qquad\quad \alpha_{k-1,k}\alpha_{k-2,k} B_{k-1} B_{k-2} A_1 \ldots A_{k-3} A_k) \\
&\qquad + \ldots \\
&\qquad + d_\psi(\prod_{i=2}^{k-1} \alpha_{ik} B_{k-1} \ldots B_2 A_1 A_k, \prod_{i=1}^{k-1} \alpha_{ik} B_{k-1} \ldots B_2 A_k A_1) \\
&\qquad + d_\psi(\prod_{i=1}^{k-1} \alpha_{ik} B_{k-1} \ldots B_2 A_k A_1, \prod_{i=1}^{k-1} \alpha_{ik} A_k A_1 \ldots A_{k-1}) \\
&\quad \leq d_\psi(A_{k-1} A_k, \alpha k-1, k A_k A_{k-1}) + d_\psi(A_{k-1}, B_{k-1}) + \ldots \\
&\qquad + d_\psi(A_2 A_k, \alpha 2k A_k A_2) + d_\psi(A_2, B_2) \\
&\qquad + d_\psi(A_1 A_k, \alpha 1k A_k A_1) + d_\psi(B_2, A_2) + \cdots + d_\psi(B_k, A_k) \\
&\quad \leq 2(k-2)\varepsilon_1 + (k-1)\varepsilon_2.
\end{aligned}$$

□

As a consequence of the preceding lemma

Lemma A.6.9. *Let $S_1, \ldots, S_k, T_1, \ldots, T_k$ be Hermitian operators on Alice's space and let $S_1^B, \ldots S_k^B, T_1^B \ldots T_k^B$ be Hermitian operators on Bob's space, satisfying*

$$\begin{aligned}
\forall i, \quad & d_\psi(S_i, S_i^B) \leq \varepsilon_1 \\
\forall i, \quad & d_\psi(T_i, T_i^B) \leq \varepsilon_2 \\
\forall i, j, \quad & d_\psi(S_i T_j, \alpha_{ij} T_j S_i) \leq \varepsilon_3.
\end{aligned}$$

Then

$$d_\psi(S_1 \dots S_k T_1 \dots T_k, \prod_{i,j=1}^{k} \alpha_{ij} T_1 \dots T_k S_1 \dots S_k) \leq 2(k-1)\varepsilon_2 + k(2(k-1)\varepsilon_1 + k\varepsilon_3). \tag{A.17}$$

Likewise,

$$d_\psi(S_1 \dots S_k T_1 \dots T_k, \prod_{i=2}^{k} \prod_{j=1}^{i-1} \alpha_{ij} S_1 T_1 S_2 T_2 \dots S_k T_k) \leq 2(k-1)\varepsilon_2 + \sum_{j=2}^{k} (2(j-2)\varepsilon_2 + (j-1)\varepsilon_3) \tag{A.18}$$

Proof. We first prove (A.17).

$$\begin{aligned}
&d_\psi(S_1 \dots S_k T_1 \dots T_k, \prod_{i,j=1}^{k} \alpha_{ij} T_1 \dots T_k S_1 \dots S_k) \\
&\quad \leq d_\psi(S_1 \dots S_k T_1 \dots T_k, T_k^B \dots T_2^B S_1 \dots S_k T_1) \\
&\qquad + d_\psi(T_k^B \dots T_2^B S_1 \dots S_k T_1, \prod_{i=1}^{k} \alpha_{i1} T_k^B \dots T_2^B T_1 S_1 \dots S_k) \\
&\qquad + d_\psi(\prod_{i=1}^{k} \alpha_{i1} T_k^B \dots T_2^B T_1 S_1 \dots S_k, \prod_{i=1}^{k} \alpha_{i1} T_k^B \dots T_3^B T_1 S_1 \dots S_k T_2) \\
&\qquad + d_\psi(\prod_{i=1}^{k} \alpha_{i1} T_k^B \dots T_3^B T_1 S_1 \dots S_k T_2, \prod_{i=1}^{k} \alpha_{i1}\alpha_{i2} T_k^B \dots T_3^B T_1 T_2 S_1 \dots S_k) \\
&\qquad + \dots \\
&\qquad + d_\psi(\prod_{i=1}^{k} \prod_{j=1}^{k-1} \alpha_{ij} T_k^B T_1 \dots T_{k-1} S_1 \dots S_k, \prod_{i=1}^{k} \prod_{j=1}^{k-1} \alpha_{ij} T_1 \dots T_{k-1} S_1 \dots S_k T_k) \\
&\qquad + d_\psi(\prod_{i=1}^{k} \prod_{j=1}^{k-1} \alpha_{ij} T_1 \dots T_{k-1} S_1 \dots S_k T_k, \prod_{i,j=1}^{k} \alpha_{ij} T_1 \dots T_k S_1 \dots S_k) \\
&\quad \leq 2(k-1)\varepsilon_2 + k(2(k-1)\varepsilon_1 + k\varepsilon_3).
\end{aligned}$$

The derivation of (A.18) is very similar. The only difference is that the number of commutations of S with T is different. □

A.7 The Single Round Case

In this section, we review the self-testing result of [WBMS16b] on the single-round magic square game, and write out the measurement definitions concretely for use in our setting. The rules of the game are described in Fig. A-1. Any entangled strategy for this game is described by a shared quantum state $|\psi\rangle_{AB}$ and projectors $P_r^{a_0,a_1}$ for

Alice and $Q_c^{b_0,b_1}$ for Bob. It can be seen that the game can be won with certainty for the following strategy:

$$
\begin{aligned}
|\psi\rangle &= \frac{1}{2} \sum_{i,j\in\{0,1\}} |ij\rangle_A \otimes |ij\rangle_B \\
P_0^{a_0,a_1} &= \frac{1}{4}(I + (-1)^{a_0} Z)_{A1} \otimes (I + (-1)^{a_1} Z)_{A2} \otimes I_B \\
P_1^{a_0,a_1} &= \frac{1}{4}(I + (-1)^{a_1} X)_{A1} \otimes (I + (-1)^{a_0} X)_{A2} \otimes I_B \\
Q_0^{b_0,b_1} &= \frac{1}{4} I_A \otimes (I + (-1)^{b_0} Z)_{B1} \otimes (I + (-1)^{b_1} X)_{B2} \\
Q_1^{b_0,b_1} &= \frac{1}{4} I_A \otimes (I + (-1)^{b_1} X)_{B1} \otimes (I + (-1)^{b_0} Z)_{B2}
\end{aligned}
$$

This strategy is represented pictorially in Fig. A-2, where each row contains a set of simultaneously-measurable observables that give Alice's answers, and likewise each column for Bob.

Inspired by this ideal strategy, for *any* strategy we can define the following induced observables on Alice's system:

$$
\begin{aligned}
X_1 &= \sum_{a_0,a_1} (-1)^{a_1} P_1^{a_0,a_1} = A_1^1 \\
X_2 &= \sum_{a_0,a_1} (-1)^{a_0} P_1^{a_0,a_1} = A_1^0 \\
Z_1 &= \sum_{a_0,a_1} (-1)^{a_0} P_0^{a_0,a_1} = A_0^0 \\
Z_2 &= \sum_{a_0,a_1} (-1)^{a_1} P_0^{a_0,a_1} = A_0^1,
\end{aligned}
$$

and on Bob's system:

$$
\begin{aligned}
X_3 &= \sum_{b_0,b_1} (-1)^{b_1} Q_1^{b_0,b_1} = B_1^1 \\
X_4 &= \sum_{b_0 b_1} (-1)^{b_1} Q_0^{b_0,b_1} = B_0^1 \\
Z_3 &= \sum_{b_0,b_1} (-1)^{b_0} Q_0^{b_0,b_1} = B_0^0 \\
Z_4 &= \sum_{b_0,b_1} (-1)^{b_0} Q_1^{b_0 b_1} = B_1^0.
\end{aligned}
$$

The X and Z observables correspond to the first two rows and columns of the square.

From the third row and third column, we obtain four more observables; two for Alice:

$$W_1 = \sum_{a_0,a_1} (-1)^{a_0} P_2^{a_0,a_1} = A_2^0$$
$$W_2 = \sum_{a_0,a_1} (-1)^{a_1} P_2^{a_0,a_1} = A_2^1,$$

and two for Bob:

$$W_3 = \sum_{b_0,b_1} (-1)^{b_0} Q_2^{b_0,b_1} = B_2^0$$
$$W_4 = \sum_{b_0,b_1} (-1)^{b_1} Q_2^{b_0,b_1} = B_2^1.$$

There are nine consistency conditions implied by winning the game with probability $1 - \varepsilon$:

$$\langle\psi|Z_1 Z_3|\psi\rangle \geq 1 - 9\varepsilon \tag{A.19}$$
$$\langle\psi|Z_2 Z_4|\psi\rangle \geq 1 - 9\varepsilon \tag{A.20}$$
$$\langle\psi|Z_1 Z_2 W_3|\psi\rangle \geq 1 - 9\varepsilon \tag{A.21}$$
$$\langle\psi|X_2 X_4|\psi\rangle \geq 1 - 9\varepsilon \tag{A.22}$$
$$\langle\psi|X_1 X_3|\psi\rangle \geq 1 - 9\varepsilon \tag{A.23}$$
$$\langle\psi|X_1 X_2 W_4|\psi\rangle \geq 1 - 9\varepsilon \tag{A.24}$$
$$-\langle\psi|W_1 Z_3 X_4|\psi\rangle \geq 1 - 9\varepsilon \tag{A.25}$$
$$-\langle\psi|W_2 Z_4 X_3|\psi\rangle \geq 1 - 9\varepsilon \tag{A.26}$$
$$-\langle\psi|W_1 W_2 W_3 W_4|\psi\rangle \geq 1 - 9\varepsilon. \tag{A.27}$$

From this we obtain anticommutation conditions

$$\begin{aligned}
X_1 Z_1 &\approx X_1 Z_2 W_3 && \text{(by (A.21))} \\
&= W_3 X_1 Z_2 \\
&\approx W_3 X_1 Z_4 && \text{(by (A.20))} \\
&\approx W_3 Z_4 X_3 && \text{(by (A.23))} \\
&\approx -W_3 W_2 && \text{(by (A.26))} \\
&\approx W_3 W_1 W_3 W_4 && \text{(by (A.27))} \\
&= W_1 W_4 \\
&\approx -W_4 Z_3 X_4 && \text{(by (A.25))} \\
&\approx -Z_1 W_4 X_4 && \text{(by (A.19))} \\
&\approx -Z_1 X_2 W_4 && \text{(by (A.22))} \\
&\approx -Z_1 X_2 X_2 X_1 && \text{(by (A.24))} \\
&= -Z_1 X_1.
\end{aligned}$$

We can also get commutation relations on different qubits:

$$\begin{aligned} X_1 Z_2 &\approx X_1 Z_4 && \text{(by (A.20))} \\ &\approx Z_4 X_3 && \text{(by (A.23))} \\ &= X_3 Z_4 && \text{(by construction)} \\ &\approx X_3 Z_2 && \text{(by (A.20))} \\ &\approx Z_2 X_1 && \text{(by (A.23)).} \end{aligned}$$

The other cases follow similarly. See [WBMS16b] for further details.

A.8 Group Structure of Magic Square Game

In this section, we show that the global (n-round) operators applied in any near-optimal strategy approximately satisfy certain anticommutaiton relations in expectation, up to an error that is independent of n. We consider this result to be a first step towards showing a *constant* robustness for the Magic Square game. To obtain these results, in this section we use a different notation for the row and column indices $\mathbf{r}$ and $\mathbf{c}$, which makes manifest an underlying group structure in the Magic Square game.

Definition A.8.1. We now define an addition operation on the indices of $A^{\mathbf{c}}_{\mathbf{r}}$ as follows. We first define addition for single round indices, and addition of n-round indices will follow by applying this rule round by round. The single round rule is:

$$\begin{aligned} &0+1=2 \\ &1+2=0 \\ &2+0=1 \\ &0+0=1+1=2+2=\phi \\ &0+\phi=0 \\ &1+\phi=1 \\ &2+\phi=2 \end{aligned}$$

Where ϕ is an additional "null" symbol. This addition rule is defined to be commutative, and therefore this is a complete set of rules. (Note that these rules are simply the addition rules for Z_2^2 with the identifications $\phi \to 00$, $0 \to 01$, $1 \to 10$, and $2 \to 11$.)

Under this new addition rule it follows by Definition A.3.3 that,

$$A^{\mathbf{c}}_{\mathbf{r}} A^{\mathbf{c}'}_{\mathbf{r}} = A^{\mathbf{c}+\mathbf{c}'}_{\mathbf{r}} \tag{A.28}$$

and for Bob operators

$$B^{\mathbf{r}}_{\mathbf{c}} B^{\mathbf{r}'}_{\mathbf{c}} = (-1)^{h(r,r')} B^{\mathbf{r}+\mathbf{r}'}_{\mathbf{c}}, \tag{A.29}$$

where $h : Z_2^{2n} \times Z_2^{2n} \mapsto$ is defined as $h(\mathbf{r}, \mathbf{r}', \mathbf{c}) = \oplus_{i=1}^{n}([\mathbf{c}_i \neq \phi] \cap [\mathbf{r}_i \neq \phi] \cap [\mathbf{r}'_i \neq \phi] \cap [\mathbf{r}_i \neq \mathbf{r}'_i])$.

It is important to note that the above relations hold *exactly*, as they follow from the definition of the "third row" and "third column" in the Magic Square as a function of the other two rows/columns.

Using these relations, we obtain the following approximate anticommutation result in expectation.

Lemma A.8.2. *If Alice and Bob win the parallel repeated magic square game with probability $\geq 1 - \varepsilon$, then*

$$\mathbf{E}_{\mathbf{r},\mathbf{r}',\mathbf{c},\mathbf{c}'} \| A^{\mathbf{c}}_{\mathbf{r}} A^{\mathbf{c}'}_{\mathbf{r}'} |\psi\rangle - (-1)^{f(\mathbf{r},\mathbf{r}',\mathbf{c},\mathbf{c}')} A^{\mathbf{c}'}_{\mathbf{r}'} A^{\mathbf{c}}_{\mathbf{r}} |\psi\rangle \| \leq O(\sqrt{\varepsilon}),$$

where the indices $\mathbf{r}, \mathbf{r}', \mathbf{c}, \mathbf{c}'$ are taken to be independently and uniformly distributed.

Proof. The proof proceeds by repeatedly applying the algebraic relations (A.28) and (A.29), as well as shifting operators from Alice's system to Bob's system by using Lemma A.6.6 together with Fact A.3.6. An additive approximation error of $O(\sqrt{\varepsilon})$ is incurred whenever the latter step is preformed. For simplicity, we do not indicate all the details.

$$\begin{aligned}
&\mathbf{E}\, d_\psi(A^{\mathbf{c}}_{\mathbf{r}} A^{\mathbf{c}'}_{\mathbf{r}'}, (-1)^{f(\mathbf{r},\mathbf{r}',\mathbf{c},\mathbf{c}')} A^{\mathbf{c}'}_{\mathbf{r}'} A^{\mathbf{c}}_{\mathbf{r}}) \\
&\quad = \mathbf{E}\, d_\psi(A^{\mathbf{c}'+\mathbf{c}}_{\mathbf{r}} A^{\mathbf{c}'}_{\mathbf{r}} A^{\mathbf{c}'}_{\mathbf{r}'}, (-1)^{f(\mathbf{r},\mathbf{r}',\mathbf{c},\mathbf{c}')} A^{\mathbf{c}'}_{\mathbf{r}'} A^{\mathbf{c}}_{\mathbf{r}}) \\
&\quad \leq \mathbf{E}\, d_\psi(B^{\mathbf{r}'}_{\mathbf{c}'} B^{\mathbf{r}}_{\mathbf{c}'} B^{\mathbf{r}}_{\mathbf{c}'+\mathbf{c}}, (-1)^{f(\mathbf{r},\mathbf{r}',\mathbf{c},\mathbf{c}')} A^{\mathbf{c}'}_{\mathbf{r}'} A^{\mathbf{c}}_{\mathbf{r}}) + O(\sqrt{\varepsilon}) \\
&\quad \leq \mathbf{E}\, d_\psi((-1)^{h(\mathbf{r},\mathbf{r}',\mathbf{c}')} B^{vr'+\mathbf{r}}_{\mathbf{c}'} B^{\mathbf{r}}_{\mathbf{c}+\mathbf{c}'}, (-1)^{f(\mathbf{r},\mathbf{r}',\mathbf{c},\mathbf{c}')} A^{\mathbf{c}'}_{\mathbf{r}'} A^{\mathbf{c}}_{\mathbf{r}}) + O(\sqrt{\varepsilon}) \\
&\quad \leq \mathbf{E}\, d_\psi((-1)^{h(\mathbf{r},\mathbf{r}',\mathbf{c}')} A^{\mathbf{c}+\mathbf{c}'}_{\mathbf{r}} A^{\mathbf{c}'}_{\mathbf{r}'+\mathbf{r}}, (-1)^{f(\mathbf{r},\mathbf{r}',\mathbf{c},\mathbf{c}')} A^{\mathbf{c}'}_{\mathbf{r}'} A^{\mathbf{c}}_{\mathbf{r}}) + O(\sqrt{\varepsilon}) \\
&\quad \leq \mathbf{E}\, d_\psi((-1)^{h(\mathbf{r},\mathbf{r}',\mathbf{c}')} A^{\mathbf{c}+\mathbf{c}'}_{\mathbf{r}} A^{\mathbf{c}+\mathbf{c}'}_{\mathbf{r}+\mathbf{r}'} A^{\mathbf{c}}_{\mathbf{r}+\mathbf{r}'}, (-1)^{f(\mathbf{r},\mathbf{r}',\mathbf{c},\mathbf{c}')} A^{\mathbf{c}'}_{\mathbf{r}'} A^{\mathbf{c}}_{\mathbf{r}}) + O(\sqrt{\varepsilon}) \\
&\quad \leq \mathbf{E}\, d_\psi((-1)^{h(\mathbf{r},\mathbf{r}',\mathbf{c}')} B^{\mathbf{r}+\mathbf{r}'}_{\mathbf{c}} B^{\mathbf{r}+\mathbf{r}'}_{\mathbf{c}+\mathbf{c}'} B^{\mathbf{r}}_{\mathbf{c}+\mathbf{c}'}, (-1)^{f(\mathbf{r},\mathbf{r}',\mathbf{c},\mathbf{c}')} A^{\mathbf{c}'}_{\mathbf{r}'} A^{\mathbf{c}}_{\mathbf{r}}) + O(\sqrt{\varepsilon}) \\
&\quad \leq \mathbf{E}\, d_\psi((-1)^{h(\mathbf{r},\mathbf{r}',\mathbf{c}')+h(\mathbf{r},\mathbf{r}+\mathbf{r}',\mathbf{c}+\mathbf{c}')} B^{\mathbf{r}+\mathbf{r}'}_{\mathbf{c}} B^{\mathbf{r}'}_{\mathbf{c}+\mathbf{c}'}, (-1)^{f(\mathbf{r},\mathbf{r}',\mathbf{c},\mathbf{c}')} A^{\mathbf{c}'}_{\mathbf{r}'} A^{\mathbf{c}}_{\mathbf{r}}) + O(\sqrt{\varepsilon}) \\
&\quad \leq \mathbf{E}\, d_\psi((-1)^{h(\mathbf{r},\mathbf{r}',\mathbf{c}')+h(\mathbf{r},\mathbf{r}+\mathbf{r}',\mathbf{c}+\mathbf{c}')} A^{\mathbf{c}+\mathbf{c}'}_{\mathbf{r}'} A^{\mathbf{c}}_{\mathbf{r}+\mathbf{r}'}, (-1)^{f(\mathbf{r},\mathbf{r}',\mathbf{c},\mathbf{c}')} A^{\mathbf{c}'}_{\mathbf{r}'} A^{\mathbf{c}}_{\mathbf{r}}) + O(\sqrt{\varepsilon}) \\
&\quad \leq \mathbf{E}\, d_\psi((-1)^{h(\mathbf{r},\mathbf{r}',\mathbf{c}')+h(\mathbf{r},\mathbf{r}+\mathbf{r}',\mathbf{c}+\mathbf{c}')} A^{\mathbf{c}'}_{\mathbf{r}'} A^{\mathbf{c}}_{\mathbf{r}'} A^{\mathbf{c}}_{\mathbf{r}+\mathbf{r}'}, (-1)^{f(\mathbf{r},\mathbf{r}',\mathbf{c},\mathbf{c}')} A^{\mathbf{c}'}_{\mathbf{r}'} A^{\mathbf{c}}_{\mathbf{r}}) + O(\sqrt{\varepsilon}) \\
&\quad \leq \mathbf{E}\, d_\psi((-1)^{h(\mathbf{r},\mathbf{r}',\mathbf{c}')+h(\mathbf{r},\mathbf{r}+\mathbf{r}',\mathbf{c}+\mathbf{c}')} B^{\mathbf{r}+\mathbf{r}'}_{\mathbf{c}} B^{|vr'}_{\mathbf{c}} B^{\mathbf{r}'}_{\mathbf{c}'}, (-1)^{f(\mathbf{r},\mathbf{r}',\mathbf{c},\mathbf{c}')} A^{\mathbf{c}'}_{\mathbf{r}'} A^{\mathbf{c}}_{\mathbf{r}}) + O(\sqrt{\varepsilon}) \\
&\quad \leq \mathbf{E}\, d_\psi((-1)^{h(\mathbf{r},\mathbf{r}',\mathbf{c}')+h(\mathbf{r},\mathbf{r}+\mathbf{r}',\mathbf{c}+\mathbf{c}')+h(\mathbf{r}',\mathbf{r}+\mathbf{r}',\mathbf{c})} B^{\mathbf{r}}_{\mathbf{c}} B^{\mathbf{r}'}_{\mathbf{c}'}, (-1)^{f(\mathbf{r},\mathbf{r}',\mathbf{c},\mathbf{c}')} A^{\mathbf{c}'}_{\mathbf{r}'} A^{\mathbf{c}}_{\mathbf{r}}) + O(\sqrt{\varepsilon}) \\
&\quad \leq \mathbf{E}\, d_\psi((-1)^{h(\mathbf{r},\mathbf{r}',\mathbf{c}')+h(\mathbf{r},\mathbf{r}+\mathbf{r}',\mathbf{c}+\mathbf{c}')+h(\mathbf{r}',\mathbf{r}+\mathbf{r}',\mathbf{c})} A^{\mathbf{c}'}_{\mathbf{r}'} A^{\mathbf{c}}_{\mathbf{r}}, (-1)^{f(\mathbf{r},\mathbf{r}',\mathbf{c},\mathbf{c}')} A^{\mathbf{c}'}_{\mathbf{r}'} A^{\mathbf{c}}_{\mathbf{r}}) + O(\sqrt{\varepsilon})
\end{aligned}$$

To complete the proof, it remains to verify that $h(\mathbf{r}, \mathbf{r}', \mathbf{c}') + h(\mathbf{r}, \mathbf{r} + \mathbf{r}', \mathbf{c} + \mathbf{c}') + h(\mathbf{r}', \mathbf{r} + \mathbf{r}', \mathbf{c}) \equiv f(\mathbf{r}, \mathbf{r}', \mathbf{c}, \mathbf{c}') \pmod 2$. Both functions are defined coordinatewise, so it suffices to check that they agree for a single coordinate. This can be verified with a computer by explicitly computing the function values for all 4^4 possible values of $\mathbf{r}_i, \mathbf{r}'_i, \mathbf{c}_i, \mathbf{c}'_i$. □

Bibliography

[AALV09] Dorit Aharonov, Itai Arad, Zeph Landau, and Umesh Vazirani. The detectability lemma and quantum gap amplification. In *Proc. 41st STOC*, pages 417–426, New York, NY, USA, 2009. ACM.

[AAV13] Dorit Aharonov, Itai Arad, and Thomas Vidick. The quantum PCP conjecture. Technical report, 2013, `arXiv:1309.7495`. Appeared as guest column in ACM SIGACT News archive Volume 44 Issue 2, June 2013, Pages 47–79.

[AE13] Dorit Aharonov and Lior Eldar. Quantum locally testable codes. 2013, `arXiv:1310.5664`.

[AE15] Dorit Aharonov and Lior Eldar. The commuting local Hamiltonian problem on locally expanding graphs is approximable in NP. *Quantum Information Processing*, 14(1):83–101, January 2015.

[AFB17] Rotem Arnon-Friedman and Jean-Daniel Bancal. Device-independent certification of one-shot distillable entanglement. 2017, `arXiv:1712.09369`.

[AFY17] Rotem Arnon-Friedman and Henry Yuen. Noise-tolerant testing of high entanglement of formation. 2017, `arXiv:1712.09368`.

[ALM+98] 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.

[AMN98] Yossi Azar, Rajeev Motwani, and Joseph Seffi Naor. Approximating probability distributions using small sample spaces. *Combinatorica*, 18(2):151–171, 1998.

[AN02] Dorit Aharonov and Tomer Naveh. Quantum NP – a survey. 2002, `arXiv:quant-ph/0210077`.

[Ara02] P. K. Aravind. The magic squares and Bell's theorem. Technical report, 2002, `arXiv:quant-ph/0206070`.

[AS98] Sanjeev Arora and Shmuel Safra. Probabilistic checking of proofs: A new characterization of NP. *J. ACM*, 45(1):70–122, 1998.

[AW02] Rudolf Ahlswede and Andreas Winter. Strong converse for identification via quantum channels. *IEEE Transactions on Information Theory*, 48(3):569–579, 2002, arXiv:quant-ph/0012127.

[BCH+96] Mihir Bellare, Don Coppersmith, JOHAN Hastad, Marcos Kiwi, and Madhu Sudan. Linearity testing in characteristic two. *IEEE Transactions on Information Theory*, 42(6):1781–1795, 1996.

[Bel64] John S. Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1:195–200, 1964.

[BFL91] László Babai, Lance Fortnow, and Carsten Lund. Non-deterministic exponential time has two-prover interactive protocols. *Computational Complexity*, 1:3–40, 1991.

[BH13] Fernando G.S.L. Brandao and Aram W. Harrow. Product-state approximations to quantum ground states. In *Proc. 45th STOC*, 2013.

[BHK05] Jonathan Barrett, Lucien Hardy, and Adrian Kent. No signaling and quantum key distribution. *Physical review letters*, 95(1):010503, 2005, arXiv:quant-ph/0405101.

[BLR93] Manuel Blum, Michael Luby, and Ronitt Rubinfeld. Self-testing/correcting with applications to numerical problems. *Journal of Computer and System Sciences*, 47:549–595, 1993.

[BNS+15] Jean-Daniel Bancal, Miguel Navascués, Valerio Scarani, Tamás Vértesi, and Tzyh Haur Yang. Physical characterization of quantum devices from nonlocal correlations. *Phys. Rev. A*, 91:022115, Feb 2015.

[BP15] Cédric Bamps and Stefano Pironio. Sum-of-squares decompositions for a family of clauser-horne-shimony-holt-like inequalities and their application to self-testing. *Phys. Rev. A*, 91:052111, May 2015.

[BSGH+05] Eli Ben-Sasson, Oded Goldreich, Prahladh Harsha, Madhu Sudan, and Salil Vadhan. Short pcps verifiable in polylogarithmic time. In *Computational Complexity, 2005. Proceedings. Twentieth Annual IEEE Conference on*, pages 120–134. IEEE, 2005.

[BVY17] Mohammad Bavarian, Thomas Vidick, and Henry Yuen. Hardness amplification for entangled games via anchoring. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, pages 303–316. ACM, 2017.

[CGJV17] Andrea Coladangelo, Alex Grilo, Stacey Jeffery, and Thomas Vidick. Verifier-on-a-leash: new schemes for verifiable delegated quantum computation, with quasilinear resources. 2017, arXiv:1708.07359.

[CHSH69] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23:880–884, Oct 1969.

[CHTW04] Richard Cleve, Peter Høyer, Ben Toner, and John Watrous. Consequences and limits of nonlocal strategies. 2004, `arXiv:arXiv:quant-ph/0404076`.

[Cir80a] B. S. Cirel'son. Quantum generalizations of bell's inequality. *Letters in Mathematical Physics*, 4(2):93–100, 1980.

[Cir80b] Boris S Cirel'son. Quantum generalizations of Bell's inequality. *Letters in Mathematical Physics*, 4(2):93–100, 1980.

[CM14] Toby Cubitt and Ashley Montanaro. Complexity classification of local Hamiltonian problems. In *Foundations of Computer Science (FOCS), 2014 IEEE 55th Annual Symposium on*, pages 120–129. IEEE, 2014.

[CN16] Matthew Coudron and Anand Natarajan. The parallel-repeated Magic Square game is rigid. 2016, `arXiv:1609.06306`.

[Col06] Roger Colbeck. *Quantum And Relativistic Protocols For Secure Multi-Party Computation.* PhD thesis, University of Cambridge, 2006, `arXiv:0911.3814`.

[Col16] Andrea W. Coladangelo. Parallel self-testing of (tilted) EPR pairs via copies of (tilted) CHSH. Technical report, 2016, `arXiv:1609.03687`.

[CRSV16] R. Chao, B. W. Reichardt, C. Sutherland, and T. Vidick. Overlapping qubits. Manuscript in preparation, 2016.

[CRSV17] Rui Chao, Ben W. Reichardt, Chris Sutherland, and Thomas Vidick. Test for a large amount of entanglement, using few measurements. In *Proceedings of the 2017 Conference on Innovations in Theoretical Computer Science (ITCS)*, 2017.

[CS96] A. R. Calderbank and Peter W. Shor. Good quantum error-correcting codes exist. *Phys. Rev. A*, 54:1098–1105, 1996, `arXiv:quant-ph/9512032`.

[CS17] Andrea Coladangelo and Jalex Stark. Robust self-testing for linear constraint system games. 2017, `arXiv:1709.09267`.

[DFK+11] Irit Dinur, Eldar Fischer, Guy Kindler, Ran Raz, and Shmuel Safra. PCP characterizations of NP: Toward a polynomially-small error-probability. *Computational Complexity*, 20(3):413, 2011.

[Din07] Irit Dinur. The PCP theorem by gap amplification. *J. ACM*, 54(3), June 2007.

[DSV15] Irit Dinur, David Steurer, and Thomas Vidick. A parallel repetition theorem for entangled projection games. *Comput. Complex.*, 24(2):201–254, June 2015.

[EH15] Lior Eldar and Aram W Harrow. Local Hamiltonians whose ground states are hard to approximate. 2015, `arXiv:1510.02082`.

[Eke91] Artur K Ekert. Quantum cryptography based on Bell's theorem. *Physical review letters*, 67(6):661, 1991.

[EPR35] Albert Einstein, Boris Podolsky, and Nathan Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical review*, 47(10):777, 1935.

[FGL+96] Uriel Feige, Shafi Goldwasser, Laszlo Lovász, Shmuel Safra, and Mario Szegedy. Interactive proofs and the hardness of approximating cliques. *J. ACM*, 43(2):268–292, 1996.

[FH15] Joseph Fitzsimons and Michal Hajdušek. Post hoc verification of quantum computing. Technical report, 2015, `arXiv:1512.04375`.

[FNT14] Tobias Fritz, Tim Netzer, and Andreas Thom. Can you compute the operator norm? *Proceedings of the American Mathematical Society*, 142(12):4265–4276, 2014, `arXiv:1207.0975`.

[FV15] Joseph Fitzsimons and Thomas Vidick. A multiprover interactive proof system for the local Hamiltonian problem. In *Proceedings of the 2015 Conference on Innovations in Theoretical Computer Science*, pages 103–112. ACM, 2015.

[GH15] W. T. Gowers and O. Hatami. Inverse and stability theorems for approximate representations of finite groups. 2015, `arXiv:1510.04085`.

[GKP16] Alex B Grilo, Iordanis Kerenidis, and Attila Pereszlényi. Pointer quantum PCPs and multi-prover games. 2016, `arXiv:1603.00903`.

[Gle10] Lev Glebsky. Almost commuting matrices with respect to normalized Hilbert-Schmidt norm. 2010, `arXiv:1002.3082`.

[Got97] Daniel Gottesman. Stabilizer codes and quantum error correction, 1997, `arXiv:quant-ph/9705052`. arXiv:quant-ph/9705052.

[Got99] Daniel Gottesman. Fault-tolerant quantum computation with higher-dimensional systems. *Chaos Solitons and Fractals*, 10(10):1749, 1999.

[IKM09] Tsuyoshi Ito, Hirotada Kobayashi, and Keiji Matsumoto. Oracularization and two-prover one-round interactive proofs against nonlocal strategies. In *Proceedings: Twenty-Fourth Annual IEEE Conference on Computational Complexity (CCC 2009)*, pages 217–228, July 2009.

[IKP+08] Tsuyoshi Ito, Hirotada Kobayashi, Daniel Preda, Xiaoming Sun, and Andrew C-C Yao. Generalized tsirelson inequalities, commuting-operator provers, and multi-prover interactive proof systems. In *Computational Complexity, 2008. CCC'08. 23rd Annual IEEE Conference on*, pages 187–198. IEEE, 2008.

[IV12] Tsuyoshi Ito and Thomas Vidick. A multi-prover interactive proof for NEXP sound against entangled provers. *Proc. 53rd FOCS*, pages 243–252, 2012, `arXiv:arXiv:1207.0550`.

[Ji16a] Zhengfeng Ji. Classical verification of quantum proofs. In *Proceedings of the 48th Annual ACM SIGACT Symposium on Theory of Computing*, pages 885–898. ACM, 2016.

[Ji16b] Zhengfeng Ji. Classical verification of quantum proofs. In *Proceedings of the 48th Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2016, pages 885–898, New York, NY, USA, 2016. ACM.

[Ji16c] Zhengfeng Ji. Compression of quantum multi-prover interactive proofs. Technical report, arXiv:1610.03133, 2016.

[KKKS06] Avanti Ketkar, Andreas Klappenecker, Santosh Kumar, and Pradeep Kiran Sarvepalli. Nonbinary stabilizer codes over finite fields. *IEEE Transactions on Information Theory*, 52(11):4892–4914, 2006.

[KKM+11] 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.

[KM03] Hirotada Kobayashi and Keiji Matsumoto. Quantum multi-prover interactive proof systems with limited prior entanglement. *JCSS*, 66:429–450, 2003. arXiv:cs/0102013.

[KRR14] Yael Tauman Kalai, Ran Raz, and Ron D. Rothblum. How to delegate computations: The power of no-signaling proofs. In *Proceedings of the Forty-sixth Annual ACM Symposium on Theory of Computing*, STOC '14, pages 485–494, New York, NY, USA, 2014. ACM.

[KSV02] Alexei Yu. Kitaev, Alexander H. Shen, and Mikhail N. Vyalyi. *Classical and Quantum Computation*, volume 47 of *Graduate Studies in Mathematics*. American Mathematical Society, 2002.

[LFKN92] Carsten Lund, Lance Fortnow, Howard Karloff, and Noam Nisan. Algebraic methods for interactive proof systems. *Journal of the ACM (JACM)*, 39(4):859–868, 1992.

[MBG+13] Alfred J Menezes, Ian F Blake, XuHong Gao, Ronald C Mullin, Scott A Vanstone, and Tomik Yaghoobian. *Applications of finite fields*, volume 199. Springer Science & Business Media, 2013.

[McK10] Matthew McKague. Self-testing graph states. Technical report, arXiv:1010.1989, 2010.

[McK14] Matthew McKague. Self-testing graph states. In *Theory of Quantum Computation, Communication, and Cryptography*, pages 104–120. Springer, 2014.

[McK15a] Matthew McKague. Self-testing in parallel, 2015, `arXiv:1511.04194`. arXiv:1511.04194.

[McK15b] Matthew McKague. Self-testing in parallel. Technical report, arXiv:1511.04194, 2015.

[McK16a] Matthew McKague. Interactive proofs for BQP via self-tested graph states. *Theory of Computing*, 12(3):1–42, 2016.

[McK16b] Matthew McKague. Self-testing high dimensional states using the generalized magic square game. Technical report, arXiv:1605.09435, 2016.

[MdW13] Ashley Montanaro and Ronald de Wolf. A survey of quantum property testing. *arXiv preprint arXiv:1310.2035*, 2013.

[Mer90] N David Mermin. Simple unified form for the major no-hidden-variables theorems. *Physical Review Letters*, 65(27):3373, 1990.

[MMMO06a] Frédéric Magniez, Dominic Mayers, Michele Mosca, and Harold Ollivier. Self-testing of quantum circuits. In *International Colloquium on Automata, Languages, and Programming*, pages 72–83. Springer, 2006, `arXiv:quant-ph/0512111`.

[MMMO06b] Frédéric Magniez, Dominic Mayers, Michele Mosca, and Harold Ollivier. Self-testing of quantum circuits. In *International Colloquium on Automata, Languages, and Programming*, pages 72–83. Springer Berlin Heidelberg, 2006.

[MS12] Carl A. Miller and Yaoyun Shi. Optimal robust quantum self-testing by binary nonlocal XOR games. Technical report, arXiv:1207.1819, 2012.

[MS14] Carl A. Miller and Yaoyun Shi. Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices. In *Proceedings of the 46th Annual ACM Symposium on Theory of Computing*, STOC '14, pages 417–426, New York, NY, USA, 2014. ACM.

[MY98] Dominic Mayers and Andrew Yao. Quantum cryptography with imperfect apparatus. In *Proceedings of the 39th Annual Symposium on Foundations of Computer Science*, FOCS '98, pages 503–, Washington, DC, USA, 1998. IEEE Computer Society.

[MY04] Dominic Mayers and Andrew Yao. Self testing quantum apparatus. *Quantum Information & Computation*, 4(4):273–286, 2004, arXiv:quant-ph/0307205.

[MYS12a] M McKague, T H Yang, and V Scarani. Robust self-testing of the singlet. *Journal of Physics A: Mathematical and Theoretical*, 45(45):455304, 2012.

[MYS12b] M. McKague, T. H. Yang, and V. Scarani. Robust self-testing of the singlet. *Journal of Physics A: Mathematical and Theoretical*, 45(45):455304, 2012.

[NC01] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2001.

[NV15] Anand Natarajan and Thomas Vidick. Constant-soundness interactive proofs for local hamiltonians. Technical report, arXiv:1512.02090, 2015.

[NV17a] Anand Natarajan and Thomas Vidick. A quantum linearity test for robustly verifying entanglement. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2017, pages 1003–1015, New York, NY, USA, 2017. ACM, arXiv:1610.03574.

[NV17b] Anand Natarajan and Thomas Vidick. Two-player entangled games are NP-hard. 2017, arXiv:1710.03062. To appear in the proceedings of CCC'18.

[NV18] Anand Natarajan and Thomas Vidick. Low-degree testing for quantum states, and a quantum entangled games PCP. 2018, arXiv:1801.03821v2.

[OV16] Dimiter Ostrev and Thomas Vidick. Entanglement of approximate quantum strategies in XOR games. Technical report, 2016, arXiv:1609.01652.

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

[Per90] Asher Peres. Incompatible results of quantum measurements. *Physics Letters A*, 151(3-4):107–108, 1990.

[Pre18] John Preskill. Quantum computing in the NISQ era and beyond. 2018, arXiv:1801.00862.

[PVN14] Károly F. Pál, Tamás Vértesi, and Miguel Navascués. Device-independent tomography of multipartite quantum states. *Phys. Rev. A*, 90:042340, Oct 2014.

[RRR16] Omer Reingold, Guy N. Rothblum, and Ron D. Rothblum. Constant-round interactive proofs for delegating computation. In *Proceedings of the Forty-eighth Annual ACM Symposium on Theory of Computing*, STOC '16, pages 49–62, New York, NY, USA, 2016. ACM.

[RS97] Ran Raz and Shmuel Safra. A sub-constant error-probability low-degree test, and a sub-constant error-probability PCP characterization of NP. In *Proceedings of the Twenty-ninth Annual ACM Symposium on Theory of Computing*, STOC '97, pages 475–484, New York, NY, USA, 1997. ACM.

[RUV13a] Ben Reichardt, Falk Unger, and Umesh Vazirani. A classical leash for a quantum system: Command of quantum systems via rigidity of CHSH games. *Nature*, 496(7446):456–460, 2013.

[RUV13b] Ben Reichardt, Falk Unger, and Umesh Vazirani. A classical leash for a quantum system: Command of quantum systems via rigidity of CHSH games. *Nature*, 496(7446):456–460, 2013.

[Sch80] J. T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *Journal of the ACM*, 27(4):701–717, 1980.

[Ste96] Andrew Steane. Multiple-particle interference and quantum error correction. In *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, volume 452, pages 2551–2577. The Royal Society, 1996, `arXiv:quant-ph/9601029`.

[SW88] Stephen J. Summers and Reinhard Werner. Maximal violation of Bell's inequalities for algebras of observables in tangent spacetime regions. *Annales de l'I.H.P. Physique théorique*, 49(2):215–243, 1988.

[Ton09] Ben Toner. Monogamy of non-local quantum correlations. *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 465(2101):59–69, 2009, `arXiv:arXiv:quant-ph/0601172`.

[Vid13] Thomas Vidick. Three-player entangled XOR games are NP-hard to approximate. In *Proc. 54th FOCS*, 2013, `arXiv:1302.1242`.

[VV14] Umesh Vazirani and Thomas Vidick. Fully device-independent quantum key distribution. *Phys. Rev. Lett.*, 113:140501, Sep 2014.

[WBMS16a] Xingyao Wu, Jean-Daniel Bancal, Matthew McKague, and Valerio Scarani. Device-independent parallel self-testing of two singlets. *Physical Review A*, 93(6):062121, 2016.

[WBMS16b] Xingyao Wu, Jean-Daniel Bancal, Matthew McKague, and Valerio Scarani. Device-independent parallel self-testing of two singlets. *Phys. Rev. A*, 93:062121, Jun 2016.

[WCY+14] Xingyao Wu, Yu Cai, Tzyh Haur Yang, Huy Nguyen Le, Jean-Daniel Bancal, and Valerio Scarani. Robust self-testing of the three-qubit w state. *Phys. Rev. A*, 90:042339, Oct 2014.

[YN13] Tzyh Haur Yang and Miguel Navascués. Robust self-testing of unknown quantum systems into any entangled two-qubit states. *Phys. Rev. A*, 87:050102, May 2013.

[Zip79] Richard Zippel. Probabilistic algorithms for sparse polynomials. In *Proceedings of the International Symposiumon on Symbolic and Algebraic Computation*, EUROSAM '79, pages 216–226, London, UK, UK, 1979. Springer-Verlag.