Entangled Protocols and Non-Local Games for Testing Quantum Systems.

by

Matthew Ryan Coudron

Submitted to the Department of Electrical Engineering and Computer Science
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy in Computer Science and Electrical Engineering

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

June 2017

Author .. Signature redacted .....
Department of Electrical Engineering and Computer Science
May 19, 2017

Certified by ..... Signature redacted
Peter W. Shor
Morss Professor of Applied Mathematics
Thesis Supervisor

Accepted by ..... Signature redacted ...
Leslie A. Kolodziejski
Professor of Electrical Engineering and Computer Science
Chair, Department Committee on Graduate Students

Entangled Protocols and Non-Local Games for Testing Quantum Systems.

by

Matthew Ryan Coudron

Submitted to the Department of Electrical Engineering and Computer Science
on May 19, 2017, in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy in Computer Science and Electrical Engineering

Abstract

The field of quantum computing investigates the extent to which one can design a quantum system that outperforms all known classical hardware at a certain task. But, to what extent can a human being, capable only (perhaps) of classical computation and of observing classical bit-string messages, verify that a quantum device in their possession is performing the task that they wish? This is a fundamental question about the nature of quantum mechanics, and the extent to which humans can harness it in a trustworthy manner. It is also a natural and important consideration when quantum devices may be used to perform sensitive cryptographic tasks which have no known efficient classical witness of correctness (Quantum Key Distribution, and Randomness Expansion are two examples of such tasks). It is remarkable that any quantum behavior at all can be tested by a verifier under such a constraint, without trusting any other quantum mechanical device in the process! But, intriguingly, when there are two or more quantum provers available in an interactive proof, there exist protocols to verify many interesting and useful quantum tasks in this setting.

This thesis investigates multi-prover interactive proofs for verifying quantum behavior, and focuses on the stringent testing scenario in which the verifier in the interactive proof is completely classical as described above. It resolves the question of the maximum attainable expansion rate of a randomness expansion protocol by providing an adaptive randomness expansion protocol that achieves an arbitrary, or *infinite* rate of randomness expansion [29]. Secondly it presents a new rigidity result for the parallel repeated magic square game [24], which provides some improvements on previous rigidity results that play a pivotal role in existing interactive proofs for entangled provers, QKD, and randomness expansion results. This new rigidity result may be useful for improving such interactive proofs in the future.

The second half of this thesis investigates the problem of bounding the role of quantum

entanglement in non-local processes. This is important for understanding the upper limit on the power of multi-prover interactive proof systems with entangled provers. In particular it establishes that, assuming the Strong Kirchberg Conjecture, one can provide a doubly exponential upper bound on the class MIP* [25] (for comparison, the best known unconditional upper bound on MIP* is that its languages are recursively enumerable!). Finally this thesis presents a result which characterizes the *type* of entanglement that is useful in entanglement assisted quantum communication complexity by showing that any communication protocol using arbitrary shared entanglement can be simulated by a protocol using only EPR pairs for shared entanglement. Therefore all quantum communication protocols can be approximately simulated by a protocol using only the maximally entangled state as a shared resource.

Thesis Supervisor: Peter W. Shor
Title: Morss Professor of Applied Mathematics

Acknowledgments

This thesis is dedicated to my Mother and Father.

I have now journeyed far from home in pursuit of scientific research, adventure, and life. The further I go the more I value what my parents' example has taught me, not about science, but about life. I love you Mom and Dad.

My deep gratitude goes to my advisor, Peter Shor, for guidance in research throughout graduate school, and for supporting my own research endeavors. During a PhD a student's mind is full of many different considerations, both scientific and logistical. Peter's advice is an invaluable way to refocus on the heart of the research problem at hand and, with stunning consistency, to learn something amazing and new.

During my PhD I have had the privilege of collaborating with many talented researchers and good friends. What would the exploration process be without people share ideas with, and fellow researchers with which to share the thrill of discovery? Many thanks to my collaborators (listed here in no particular order)! I can only hope to continue to have such great collaborations again in the future: Thomas Vidick, Aram Harrow, Peter Shor, Gilad Lerman, Henry Yuen, Anand Natarajan, Ramis Movassagh, Dimiter Ostrev, Mohammad Bavarian, Shalom Abate.

This thanks goes double for the professors and senior researchers who have given me the opportunity to visit them, given their time and attention in many helpful research discussions, and otherwise aided me in my research pursuits: Peter Shor, Aram Harrow, Thomas Vidick, Ankur Moitra, William Slofstra, Gilad Lerman, Greg Anderson, Ezra Miller, Paul Garrett, John Watrous, Scott Aaronson.

At the beginning of my PhD program, looking forward, the experience seemed that it should be mostly characterized by accomplishments (or lack thereof). At the end of my PhD, looking back, the experience seems mostly characterized by the people I met along the way. I would especially like to thank all of my friends (again in no particular order) for making my graduate school experience an awesome one! : Henry Yuen, Moham-

mad Bavarian, Adam Bouland, Eirik Bakke, Dimiter Ostrev, Robin Kothari, Shalev Ben-David, Ramis Movassagh, Peter Shor, Scott Aaronson, Thomas Vidick, Aram Harrow, Ankur Moitra, Shalom Abate, Andrea Coladangelo, Cyril Stark, Madars Virza, Richard Peng, Ludwig Schmidt, Ilya Razensteyn, Arturs Backurs, Cristos Tzamos, Peter Lofgren, Scott Isaacson, Steve Brown, Jamie Wilcox, David Hong, Gautam Kamath, Adrian Vladu, Michael Forbes, Jerry Li, Adam Sealfon, Daniel Grier, Luke Schaeffer, Pritish Kamath, Aloni Cohen

I also want to thank the instructors of the Fall 2014 edition of the MIT course 6.046, of which I was head TA. In hindsight I can confidently say that when I was a college student I completely underestimated the complexity of teaching an algorithms course to 300 highly energetic undergraduates (and MIT undergrads, no less)! I remain thoroughly impressed by the work ethic, skill, and passion for the subject that I saw in the three course instructors: Dana Moshkovitz, Costis Daskalakis, and Richard Peng, as well as in the 9 other TAs who worked with me on the course!

Finally, among acknowledgements to people, I want to thank my thesis committee, Peter Shor, Aram Harrow, Vinod Vaikuntanathan, and Ryan Williams, for graciously agreeing to oversee my defense.

And for my many extracurricular experionces at MIT: First and foremost, thanks to "up", The MIT Ultimate Frisbee pick-up team, for many, many epic games of ultimate, all year around! Thanks to the MIT climbing club, for teaching me pretty much everything I know about rock climbing. And, thanks to the MIT gymnastics club, for having a well padded floor, which I am now very well acquainted with (but not from lack of great instruction!).

For my parents.

Contents

Chapter 1

Introduction

The field of quantum computing promises to provide both hardware and algorithms which are capable of vastly outperforming any previously known algorithm at certain tasks (factoring numbers, hidden shift problems, non-abelian hidden subgroup problems, database search, etc). Furthermore, while the construction of a quantum computer is a large scale effort spanning decades, there are already a number of functioning special purpose quantum devices, which exceed what is achievable classically, and can be constructed in the laboratory today. For example, devices for performing quantum key distribution, as well as the experimental apparatus for the violation of Bell's inequality with "no loopholes" [39] have already been built! With a growing number of quantum devices being constructed for a variety of applications, from cryptographic to computational, it is fundamentally important to develop tools which an experimenter can use to verify that untrusted (or imperfectly constructed) systems are indeed performing the tasks that they claim. Yet, the task of testing and controlling untrusted systems in this manner poses a unique difficulty in the context of quantum mechanics. All devices which have a quantum advantage over classical technology must make use of entangled quantum states, which are delicate and may "collapse" upon observation. One cannot merely look "under the hood" of a quantum device during it's operation without potentially ruining the entangled state resource on which the device relies, and thus compromising it's function.

Furthermore, in the absence of such methods of direct observation the very complexity which gives proposed quantum systems their power could also make it extremely difficult to test them for errors or flaws. Therefore, the design of protocols to test untrusted quantum devices for particular behavior, under the weakest possible assumptions, and in a computationally efficient manner, is an inherently important component of the push for more powerful quantum technology.

The simple test of running a quantum machine and it's classical counterpart side by side and comparing them directly is an important benchmark in the context of computation, but even in that context this test only provides a small fraction of the information that one might need to inform future development of a complex quantum machine. Furthermore, in other contexts, such as quantum cryptography, this sort of test is entirely insufficient to address subtle aspects of the security of quantum devices. To design a more stringent type of test it is useful to think of the quantum devices being tested as untrusted "provers", and to imagine that the experimenter ("verifier") may only interact with these provers as "black-boxes", merely providing inputs and observing their corresponding outputs. This model arises naturally within quantum computation/information, where the experimenter cannot look inside a device in their possession without potentially ruining it, but it is also an extension of the notion of an Interactive Proof from theoretical computer science. Among other advantages, the interactive proof approach to verifying quantum behavior is capable of guaranteeing a level of cryptographic security which may not be achievable, even in principle, by simply inspecting the hardware very carefully before operation (for example). Remarkably, several important and natural open problems about interactive proofs for quantum behavior are closely related to longstanding open problems in quantum information and mathematical physics (see Sections 1.3, 1.4.2 for more).

1.1 Concrete Examples

Interactive proofs in quantum information are protocols through which a verifier can interact with an *untrusted* quantum system (modeled by the untrusted "prover(s)" in the interactive proof), and certify that a particular quantum task is being performed by that system. Concrete examples of such interactive proofs include: protocols for delegating quantum computation to untrusted devices [82], protocols for device independent randomness expansion [22, 78, 93], and protocols for device independent quantum key distribution [94, 37, 58], as well as any interactive proof providing non-trivial bounds for the complexity class MIP*, or QMIP. These topics are related to each other by many shared mathematical and conceptual techniques, and thus the term "interactive proof" used here does not only refer to complexity classes such as MIP*, but also to a broader set of techniques which have an important practical impact in Quantum Cryptography, and the delegation of Quantum Computation, in addition to importance in Quantum Complexity.

1.2 Concepts

There is a fascinating interplay of different ideas in the study of interactive proofs in quantum information: On one hand the study employs and inspires techniques from computational complexity theory, quantum information and operator theory. On the other hand it focuses on tests which serve a basic practical purpose for any researcher running experiments related to the elusive properties of quantum computing or quantum mechanics. That is, these protocols allow a human observer (the "verifier"), to draw mathematically certifiable conclusions from an experiment run on *untrusted* quantum devices, often with error bounds that are suitable for cryptographic applications. For example, these untrusted devices may be prototype devices which a scientist has constructed (imperfectly) in their laboratory, or devices they may have purchased from some untrusted source.

The concrete examples, in Section 1.1, of interactive proofs for testing quantum systems, will be discussed in greater detail in sections below, along with related mathematical techniques. For now, it is amazing to note that in most of these examples the verifier is only required to exchange classical bit string messages with the quantum devices, and perform standard polynomial time *classical* computations. This means that these protocols allow the verifier to control the quantum behavior of the untrusted quantum system, *even though the verifier does not ever handle or observe any quantum states!* The mere intuition that such a stringent test of untrusted quantum devices is even conceivable is itself a non-trivial observation in quantum mechanics, and is drawn from the famous Bell's inequality [10]. Bell's inequality, and the more general concept of a non-local entangled game that it inspired (the CHSH game [17], the Magic Square game [67, 77], etc.), form the conceptual basis upon which the theory of interactive proofs for testing quantum systems is built.

This conceptual basis provides a precedent showing that it is possible to circumvent one of the most fundamental requirements in all of science: The requirement that an experimenter must *trust* the devices in their own laboratory to obey certain rules defined by their construction (or else the experimental result is invalid). Astoundingly, the intuition inspired by Bell's inequality, together with mathematical tools from quantum information and computer science, make it is possible to design protocols which *do not have this requirement.* Almost all of the concrete examples listed above allow the verifier to interact with the quantum devices as black-boxes, observing only the classical bit strings which form inputs and outputs to the devices, and assuming nothing about the construction of the devices, except that they obey the laws of physics (they cannot communicate faster than the speed of light, or violate the laws of quantum mechanics, etc). Indeed, these protocols are sound even in the case that the quantum devices were purchased or acquired from a possibly-malicious adversary, or were constructed in a manner that may have unforseen imperfections.

A key concept in the use of non-local entangled games in interactive proofs is the notion of the "Rigidity" of certain games. A non-local entangled game is said to exhibit "Rigidity"

if it has the property that any nearly optimal measurement strategy used by the players must be nearly equal to one unique "ideal" strategy (up to isometry, say). In other words, we say that a non-local entangled game is rigid if it has a unique optimal winning strategy that is robust in the sense that any nearly optimal strategy must be close to the unique optimum. Both the CHSH game, and the Magic Square game have this property. Rigidity was first discovered and proved for the CHSH game, and that is one of the biggest reasons that CHSH plays such a central role in the results in Section 1.1, and many more.

Rigidity in entangled games is a powerful tool because it effectively provides us with a type of interactive proof that the players (which we think of as untrusted provers) are performing specific quantum operations. In particular, if one observes that Alice and Bob have nearly optimal performance on repeated rounds of the CHSH game, then one can show that (up to isometry) Alice and Bob must be performing high-fidelity versions of the ideal CHSH measurements corresponding to their inputs. Formally proving certain variants of this fact, and achieving nearly optimal, cryptographically useful parameters is a central goal in quantum key distribution, device independent randomness expansion and many interactive proofs in quantum information. In the case of delegating quantum computation, or tasks in MIP*, one can employ a second technique. Now that the two untrusted provers, Alice and Bob, can be constrained to perform particular quantum measurements on command, the verifier can leverage the fact that Alice and Bob cannot communicate, and play them against each other during the protocol. The following is a common high-level protocol structure (variations are used in [82], and in a number of subsequent works): The verifier begins the protocol by asking the two provers to play many independent rounds of the CHSH game. At some randomly chosen point during the protocol Alice is instructed by the verifier to perform some more complicated task rather than simply playing CHSH (perhaps the task is to apply some more complex, multi-qubit unitary, etc). Bob, on the other hand, is told that both players are still playing yet more rounds CHSH and given his inputs for the next games. By leveraging a number of techniques from the theory of interactive proofs and quantum information, it is often

possible to use the specific measurements that Bob must perform in CHSH to force Bob to unwittingly check Alice's actions in carrying out her new more complicated task. Tests based on non-local entangled games in this manner have exciting potential to aid in overcoming both conceptual and logistical challenges of harnessing the power of a quantum computer, and other complex quantum systems.

1.3 Focus

This thesis is focused on establishing bounds on the types of quantum behavior that can be tested by a classical verifier: The first half (the "lower bound" half) studies the design of new interactive proofs in quantum information, and the sharpening of related techniques. The second half (the "upper bound" half) is focused on investigating and quantifying the role of quantum entanglement, which is a key resource in interactive proofs. This leads immediately to the need to quantify the role of entanglement in non-local entangled games, which is a problem closely related to providing a satisfactory upper bound on the class MIP* (the best currently known upper bound is that its languages are recursively enumerable!).

1.4 Results

1.4.1 Interactive Proofs with a Classical Verifier

Device Independent Randomness Expansion First proposed by Colbeck [21] in 2006, as a type of interactive proof by which a classical verifier can certify that untrusted quantum devices are producing new random bits (in an information theoretic sense), "device-independent randomness expansion" has flourished into an active area of research [22, 78, 93, 34, 26, 1, 88, 90, 79, 92, 36, 56, 3, 55, 87]. In joint work with Thomas Vidick and Henry Yuen [26], we showed the first upper bounds on randomness expansion proto-

cols, establishing that *non-adaptive* protocols that are robust to noise cannot surpass doubly exponential randomness expansion, and that techniques robust against non-signaling strategies (such as those in the state-of-the-art paper [93]), could not surpass (singly)-exponential randomness expansion.

Arbitrary Randomness Expansion With the above upper bounds in place, a fundamental conceptual open question in the field of randomness expansion was whether an *adaptive* protocol could exceed these established upper limits on *non-adaptive* protocols. In joint work with Henry Yuen [29], we showed that indeed this is possible, and more surprisingly, that *adaptive* randomness expansion protocols could provably achieve an arbitrarily high rate of randomness expansion. Through a novel application of a sequential rigidity result from [82] we designed a protocol using additional provers to "launder" the randomness produced by the provers in the [93] protocol and feed it back to those original provers who produced it. The result was an adaptive protocol that achieves *infinite* (or arbitrarily large) certifiable randomness expansion, using a *constant* number of non-signaling quantum devices! This result addressed a lack of understanding in the field about the extent to which the outputs of provers could be adaptively reused as inputs to those *same* provers, while provably maintaining the soundness of the protocol. It also solves an open problem of [34], which proposed a more direct scheme for adaptive randomness expansion, but required, for its analysis, the assumption that certain pairs of devices do not share any entanglement (an assumption that we do not require). Our protocol works even in the presence of arbitrary entanglement between the devices and an eavesdropper, and is sound against devices that can employ any physically implementable adversarial strategy, including simple tactics such as memorizing their own previous inputs and outputs, etc.

Rigidity Results for Parallel Repeated Games: The notion of Rigidity of Nonlocal Entangled Games is one of the most important and widespread tools used to study the complexity class MIP*, as well as many other topics, including self-testing quantum states

and device independent protocols. There has been a growing interest in improving these techniques to further basic goals in self-testing quantum states, and to improve bounds on MIP*[63, 95, 64, 70, 65]. In joint work with Anand Natarajan [24] we proved a rigidity result for the parallel-repeated magic square game, which shows that any ε-optimal strategy for the n-round game must have the property that the provers' measurements are $\text{poly}(n, \varepsilon)$-close (in expectation) to the ideal Pauli product operators on $2n$ qubits. For the purposes of certifying this measurement structure, this is an exponential improvement over the previous best result [64], which had an exponential (in n) error dependence. This work allows a verifier to test that the untrusted provers are applying specific Pauli-product measurements on all of the rounds of the game, which is a task that, if properly optimized, may have a number of potential uses in lower bounding MIP*, and improving protocols for device-independent delegation of quantum computation. Ideas in these directions are the object of our future research. For now it is interesting to note that one can use the main result of [24] to replace the role of [82] in the arbitrary randomness expansion protocol of [29], and this results in decreasing the runtime of the protocol from at least n^{16} to $O(n^2)$.

1.4.2 Entanglement in Non-Local Games and Communication Complexity

On the role of Entanglement in Nonlocal games It is a major open problem to upper bound the amount of entanglement required by a pair of players to win even relatively small nonlocal games. The heart of our lack of understanding on this matter is that there is no known bound on the dimension of the entangled state that the provers may need to share in order to implement a nearly optimal strategy to a general entangled game. Therefore, the dimension of the Hilbert space used by the provers is potentially unbounded, and the space of strategies available to the provers is *not even known to be compact*. This is the reason that there is no obvious "brute force" attempt at computing the winning prob-

ability of a general non-local entangled game, for example, by constructing an epsilon-net over the space of the provers' potential strategies, and evaluating every representative of the net, etc, etc. This lack of understanding is the very same issue that stands in the way of providing a more stringent upper bound for the complexity class MIP* (by perhaps improving over the best currently known upper bound, which is that its languages are recursively enumerable).

In joint work with Thomas Vidick [25], we show that by *assuming* a mathematical conjecture known as the Strong Kirchberg Conjecture, one can provide an upper bound for the amount of entanglement required in such games. If this conjecture were to hold, our result would provide a concrete upper bound on the dimension of entanglement needed to approximate a non-local game (as a function of the number of inputs and outputs of the game, and the approximation error ε) , and would also show that MIP* is contained in doubly-exponential time, which is a vastly better upper bound than is currently known. The main contribution of our work is a novel rounding scheme for the proposed Semidefinite Programing (SDP) hierarchy of [71, 31], by which we show that one can round an SDP certificate for an entangled game to produce an actual measurement strategy for two provers to play that game, with the caveat that the measurements for the two different provers will not commute *exactly*, as they should in any non-local strategy, but rather they will be $\frac{1}{\sqrt{L}}$-close to commuting in the operator norm (where L is the level of the SDP hierarchy which is used to produce the certificate). The task of further "rounding" such an approximately commuting measurement strategy to an exactly commuting measurement strategy is exactly the content of the Strong Kirchberg Conjecture, and so, that is the missing piece needed to prove an upper bound on MIP* itself via this approach. However, even without the Strong Kirchberg Conjecture, our result shows that MIP^*_δ is contained in doubly-exponential time, where MIP^*_δ is an analog of MIP*, in which the soundness condition is relaxed to allow δ-commuting strategies for the provers. Furthermore, we

establish the lower bound

$$\text{NEXP} \subseteq \bigcup_{p,q \in \text{poly}} \text{MIP}^*_{2^{-q}}(2, 1, 1 - 2^{-p}),$$

which provides a direct analogue of the same lower bound for MIP* [41], and is proven using the same technique. This demonstrates that our rounding scheme is accomplishing a non-trivial task, as it provides an unconditional upper bound on the complexity class MIP^*_δ, which also has a non-trivial lower bound.

Entanglement-Assisted Communication Complexity Another complexity-theoretic lens through which to study the power of prior entanglement is provided by the notion of Entanglement-Assisted Communication Complexity. For reasons closely related to our lack of understanding of entanglement in non-local games (see above), there is no known general bound on the amount of shared entanglement that may be required by two provers in order to perform a given communication protocol optimally (that is, to compute some joint function $f(x, y)$, when Alice is given only x and Bob is given only y). However, in joint work with Aram Harrow, we show that it is possible to characterize the *type* of entanglement necessary for a given communication protocol, at least up to some error. In particular, we show that every quantum communication protocol using Q qubits of communication and arbitrary shared entanglement can be ϵ-approximated by a protocol using $O(Q/\epsilon)$ qubits of communication and *only* EPR pairs as shared entanglement. Note that this conclusion is opposite of the common wisdom in the study of non-local games, where it has been shown, for example, that the I3322 inequality has a non-local strategy using a non-maximally entangled state, which surpasses the winning probability achievable by any strategy using only a maximally entangled state, regardless of the dimension [96]. This hints that the notion of entanglement-assisted communication complexity, even with very small amounts of allowed communication (and thus perhaps "approximating" the non-local games setting), may provide a setting in which it is easier to bound the

role of entanglement. As one of the tools in our analysis, we prove that any shared entangled state between two provers may be transformed into any other shared entangled state using a communication protocol the requires an amount of communication equal to the ℓ_∞-Earthmover Distance between the two states. This may be of independent interest.

Chapter 2

Arbitrary Randomness Expansion

In this chapter we present a device-independent randomness expansion protocol, involving only a constant number of non-signaling quantum devices, that achieves *unbounded expansion*: starting with m bits of uniform private randomness, the protocol can produce an unbounded amount of certified randomness that is $\exp(-\Omega(m^{1/3}))$-close to uniform and secure against a quantum adversary. The only parameters which depend on the size of the input are the soundness of the protocol and the security of the output (both are inverse exponential in m). This settles a long-standing open problem in the area of randomness expansion and device-independence.

The analysis of our protocols involves overcoming fundamental challenges in the study of *adaptive* device-independent protocols. Our primary technical contribution is the design and analysis of device-independent protocols which are *Input Secure*; that is, their output is guaranteed to be secure against a quantum eavesdropper, *even if the input randomness was generated by that same eavesdropper*!

The notion of Input Security may be of independent interest to other areas such as device-independent quantum key distribution.

2.1 Introduction

Bell's Theorem states that the outcomes of local measurements on spatially separated systems cannot be predetermined, due to the phenomenon of quantum entanglement [10]. This is one of the most important "no-go" results in physics because it rules out the possibility of a local hidden variable theory that reproduces the predictions of quantum mechanics. However, Bell's Theorem has also found application in quantum information as a *positive* result, in that it gives a way to certify the generation of genuine randomness: if measurement outcomes of separated systems exhibit non-local correlations (e.g. correlations that violate so-called Bell Inequalities), then the outcomes cannot be deterministic.

While Bell's Theorem does give a method to certify randomness, there is a caveat. The measurement settings used on the separated systems have to be chosen at random! Nevertheless, it is possible to choose the measurement settings in a randomness-efficient manner such that the measurement outcomes certifiably contain *more* randomness (as measured by, say, min-entropy) than the amount of randomness used as input. This is the idea behind *randomness expansion protocols*, in which a classical experimenter, starting with m-bits of uniform randomness, can interact with physically isolated devices to certifiably generate $g(m)$ bits of (information theoretic) randomness (ideally with $g(m) \gg m$). Furthermore, these protocols are *device-independent*: the only assumption made on the devices is that they cannot communicate, and obey the laws of quantum mechanics. In particular, there is no *a priori* assumption on the internal structure or dynamics of the devices. Indeed, the devices may even have been manufactured by an adversary!

First proposed by Colbeck [21] in 2006, device-independent randomness expansion has flourished into an active area of research [22, 78, 93, 34, 27, 1, 92, 36, 69]. Its study has synthesized a diverse array of concepts from quantum information theory, theoretical computer science, and quantum cryptography, including generalized Bell inequalities [78, 1, 79, 34], the monogamy of entanglement [93, 84], randomness extractors [85, 52, 30], and quantum key distribution [9, 58, 94, 69]. Randomness expansion has even been experi-

mentally realized by [78], who reported the generation of 42 bits of certified randomness (over the course of a month).

The fundamental problem in analyzing a randomness expansion protocol is in demonstrating a lower bound on the amount of certified randomness, usually measured by min-entropy. There have been a couple of different approaches. A line of works, starting with [78], gives bounds on the min-entropy by analytically relating the extent to which a Bell inequality is violated to the "guessing probability" of the protocol's output [78, 34, 1, 79]. Another approach, developed in [93], is to utilize the operational definition of min-entropy in a "guessing game", which establishes that a low min-entropy output implies that the non-signaling devices must have communicated during the protocol (a contradiction). This latter approach yields a protocol (which we will refer to as the Vazirani-Vidick protocol in this chapter) that not only achieves the state-of-the-art expansion factor $g(m) = \exp(m^{1/3})$, but is also *quantum secure*: that is, the output contains high min-entropy even from the perspective of a malicious eavesdropper that may be entangled with the protocol devices. Recently, a work by [69] not only achieves quantum security, but randomness expansion that tolerates a constant level of noise in the devices.

The original protocol of [21, 22] obtained $g(m) = \Theta(m)$, or linear expansion. This was improved by Pironio et al. [78] to achieve quadratic expansion $g(m) = \Theta(m^2)$. The protocols of [93, 34, 69] achieve exponential expansion. Perhaps the most tantalizing open question in randomness expansion is: how large an expansion factor $g(m)$ can we achieve? For example, is there a protocol with expansion factor $g(m)$ that is doubly-exponential in m? Is there any upper bound on randomness expansion in general?

The only known upper bounds on randomness expansion apply to *non-adaptive* protocols with two devices (i.e., where the referee's inputs to the devices do not depend on their previous outputs) [27]. There the authors showed that *noise robust*, non-adaptive protocols must have a finite bound on their expansion factor[1]. With the exception of [34], randomness expansion protocols prior to our work were *non-adaptive*, and hence the results

[1] They showed that $g(m) \leq \exp(\exp(m))$, or a doubly-exponential upper bound.

of [27] suggest those protocols have a bounded expansion factor. Thus, going beyond the the finite expansion barrier appears to require adaptivity – but it could, *a priori*, be the case that even adaptive protocols are inherently limited to finite randomness expansion.

We present an adaptive protocol that achieves *infinite* certifiable randomness expansion, using a *constant* number of non-signaling quantum devices. The output length of our protocol depends only on the number of rounds performed in the protocol (which can be arbitrarily large), and not on the size of the initial random seed! This shows that there is no finite upper bound on the expansion factor of adaptive protocols. Our protocol involves a constant number – eight, specifically – of non-communicating black-box quantum devices, and guarantees that the output of the protocol is close to uniformly random, even from the point of view of a quantum eavesdropper (where the closeness to uniformity is determined by the initial seed length). Our protocol works even in the presence of arbitrary entanglement between the devices and an eavesdropper.

The key technical component of the analysis of the InfiniteExpansion protocol is to show that a sub-protocol, which we call ClusterExpansion, is *Input Secure*: it generates uniform randomness secure against a quantum adversary, *even if that adversary generated the seed randomness earlier in the protocol*! Since the ClusterExpansion sub-protocol is Input Secure, composing ClusterExpansion with itself in sequence (i.e. using the outputs of one instance of the protocol as the inputs of another instance) yields another randomness expansion protocol, this time with much larger expansion factor. Our InfiniteExpansion protocol is the infinite composition of the ClusterExpansion sub-protocol.

In Section 2.2.2, we discuss two relevant and enlightening results about randomness expansion [16, 69], which were announced after the original posting of this work (though these results were discovered independently and, unbeknownst to the authors, developed in parallel with this work).

We note here that any exponential randomness expansion protocol with security against a quantum eavesdropper (such as the Vazirani-Vidick protocol, for example) readily yields a protocol using $2N$ devices, which has a randomness expansion given by an exponential

tower function of N (i.e. $2^{2^{2^{\cdots^{2^N}}}}$): after running such a quantum-secure expansion protocol on one pair of devices, the devices are discarded, and their outputs are fed into a fresh pair of devices (that did not communicate with any previous devices used in the protocol). This "exponential tower" protocol terminates when all $2N$ devices have been used. This was first observed by [101], and in [69] it is noted that the robust exponential expansion protocol given therein can be used to obtain an analogous "tower" randomness expansion protocol, which is also *robust*.

For all practical intents and purposes, a "tower" expansion protocol can certify much, much (... $\text{much}^{\text{much}^{\text{much}^{\cdots}}}$) more randomness than would ever be needed in practice, so one might consider it effectively an "infinite" randomness expansion protocol. However, such a protocol avoids the need to reuse devices, and hence sidesteps the need for Input Security – but secure device reuse is the key conceptual issue that we find interesting!

Finally, the work [16] serves as one very interesting example (discovered independently of this work) of how the concept of Input Security is relevant to problems other than infinite randomness expansion. We note that our result can be combined with a quantum-secure randomness amplification protocol (for example [16], or [14]) to produce an infinite randomness amplification protocol.

2.1.1 Barriers to infinite randomness expansion

Here we identify the inherent technical challenges in analyzing any adaptive randomness expansion protocol. In Section 4.1 we discuss how to overcome these challenges. Some of the technical issues discussed here have been identified in previous work (e.g., [34]) and in randomness expansion folklore.

The Extractor Seed and Input Security Problems

In any adaptive randomness expansion scheme there is a stage when intermediate outputs of the protocol are used to generate "derived" inputs for some devices in future stages of the protocol. This creates an inherent difficulty in analyzing adaptive protocols,

because the devices involved in the protocol may adversarially take advantage of memory and shared entanglement to attempt to create harmful correlations between intermediate outputs and the the internal state of the devices that receive the "derived" inputs. To prove the correctness of an adaptive randomness expansion protocol, one must show that the devices receiving these "derived" inputs cannot distinguish them from inputs generated by a truly private random seed. Because of this fundamental challenge, there are very few analyses of adaptive randomness expansion protocols (or key distribution protocols for that matter) in the existing literature. Prior to our work, [34] gave the only analysis of an adaptive randomness expansion protocol. However, their analysis requires the assumption that entanglement is only shared between certain pairs of devices, but otherwise that the devices are unentangled.

In the general case where devices can share arbitrary entanglement and may be entangled with an eavesdropper, we face the issue of the *quantum security* of the intermediate outputs against devices that will receive the derived inputs[2]. This issue manifests itself in two different forms: the Input Security Problem and the Extractor Seed Problem.

Generally, a randomness expansion protocol is comprised of two components: an expansion component and an extractor component. The expansion component will generate an output string that, while not necessarily close to uniformly random, will be guaranteed to have high min-entropy. The extractor component will then take this high min-entropy source, as well as a small polylogarithmic-sized uniformly random seed (taken, for example, from the initial seed of the randomness expansion protocol), and convert the high min-entropy source into a string that is close to uniform.

The Input Security Problem. In an adaptive protocol, we require that the output of the expansion component contains high min-entropy *relative to a quantum eavesdropper* (i.e. high conditional min-entropy) – where we treat the other devices in the protocol, collectively, as the eavesdropper. However, the Vazirani-Vidick protocol – an quantum-secure

[2]We say that a string X is quantum secure, or simply secure, against an eavesdropper E if the joint state of the string and eavesdropper ρ_{XE} is approximately equal to $U_{|X|} \otimes \rho_E$, where U_m denotes the uniform distribution on $|X|$ bits.

exponential randomness expansion protocol that produces an output with high conditional min-entropy[3] – uses, in its analysis, an assumption that the initial seed to the protocol is secure against the eavesdropper [93]. This is a condition that *cannot* be satisfied in an adaptive protocol. Suppose in an adaptive protocol some device D produced an intermediate output X, which we use as the derived input to some other device D' as input randomness. Note that X is *not* secure against D. Hence, we cannot use the analysis of [93] as is and treat D as an eavesdropper, and argue that D' produces an output Y that is secure against D. We refer to this issue as the Input Security Problem.

The Extractor Seed Problem. Even supposing that we had an expansion component that was immune to the Input Security Problem (i.e. produces output that contains high conditional min-entropy despite the input being known to the eavesdropper), we would still suffer from a similar problem with the extractor component. Here, we need to use a small polylogarithmic-sized uniform extractor seed to convert a source of high conditional min-entropy into a string that is nearly uniform, relative to a quantum adversary.

First, note that we cannot always take the extractor seed from the original random seed to the protocol, because this would limit us to exponential randomness expansion. Thus to achieve super-exponential expansion, the extractor seed must eventually be generated by intermediate outputs of the protocol.

Secondly, the existing quantum-secure extractors in the literature (e.g., see [30, 52, 85]) require that the extractor seed be secure against the quantum eavesdropper. As pointed out by [34], provably satisfying this requirement in an adaptive randomness expansion protocol involves overcoming a technical difficulty similar to that of the Input Security Problem. We refer to this technical barrier as the Extractor Seed Problem.

To summarize, in order to obtain quantum security of the output against an eavesdropper E, current quantum-secure expansion protocols and extraction procedures require the strong assumption that the joint state of the seed, the devices, and the eavesdropper ρ_{SDE}

[3]Recent work by [69] gives another such protocol with quantum security. See Section 2.2.2 for more information.

is such that $\rho_{SDE} \approx U_{|S|} \otimes \rho_{DE}$, where $U_{|S|}$ denotes the uniform distribution on $|S|$ bits, and ρ_{DE} denotes the internal state of the devices and adversary. In order to solve the Input Security and Extractor Seed Problems, we require randomness expansion protocols and extraction schemes that work with the weaker assumption that $\rho_{SD} \approx U_{|S|} \otimes \rho_D$ – with no mention of the eavesdropper! – while still obtaining the same quantum-security guarantees. We call this property *Input Security*, and say that protocols with this property are *Input Secure*.

It is interesting to note that extractors, by themselves, cannot satisfy a property like Input Security (i.e. we cannot guarantee that an extractor will produce private randomness when the seed is prepared by the adversary)[4].

The primary conceptual contribution of this chapter is the design and analysis of the first randomness expansion protocols and extraction schemes that are (provably) Input Secure.

The Conditioning Security Problem

The output guarantees of a randomness expansion protocol only hold *conditioned* on the protocol succeeding (i.e. conditioned on the event that the referee does not abort). Thus, the analysis of the security properties of the output of a protocol must take into account the fact that conditioning can skew the distribution of the output. Adversarially designed devices may, for example, coordinate to pass the protocol only when the first bit of the output is "1". This alone does not harm the min-entropy of the output by much, but suggests that there could be other strategies employed by adversarial devices to significantly weaken the security of the output. In [93], they show that such a collusion strategy would imply that the eavesdropper and the devices could communicate with each other, a contradiction. However, this analysis again relies on the assumption that the initial seed is secure against the eavesdropper. When analyzing an Input Secure protocol, we cannot

[4]Here's a counter-example: let D be an n-bit source that is uniformly random. Let S be a $O(\log n)$-bit seed that is uniform and independent of D. Let E denote the string $(S, \text{first bit of } \text{Ext}(D,S))$. The min-entropy of D with respect to E is at least $n-1$, and S is uniform and independent of D. However, the output of the extractor is *not* secure against E.

use this assumption, so resolving this Conditioning Security Problem requires different techniques.

The Compounding Error Problem

Another technical concern is the problem of error accumulation in an adaptive protocol. When using intermediate outputs to generate derived inputs for later stages in the protocol, we can only assume, at best, that the derived inputs are *approximately* secure and uniform. Furthermore, these errors will accumulate over the course of the protocol, and in an infinite expansion protocol, this accumulation could grow so large that the protocol will fail to work at some point. Depending on how one measures the security of a string against an quantum eavesdropper, errors may not accumulate in a linear fashion – as pointed out by [51], even if the *accessible information* of a string relative to an eavesdropper (which has been used as a standard security measure in quantum key distribution) is small, a tiny piece of classical side information could completely break the security of the string. Such an ill-behaved measure of quantum security would severely complicate the analysis of an adaptive randomness protocol.

2.2 Results

We present a protocol that attains *infinite randomness expansion*. Our protocol, which we denote the InfiniteExpansion protocol, involves a constant number of non-signaling devices (eight, specifically) that, with m bits of seed randomness, can produce an arbitrarily large amount of certified randomness. In particular, starting with m bits of random seed, if InfiniteExpansion is run for k iterations, the output of the k iterations is a random string that is $\exp(-\Omega(m^{1/3}))$-close to uniform, and has length

$$\underbrace{2^{2^{\cdot^{\cdot^{2^{\Omega(m^{1/3})}}}}}}_{k},$$

i.e., a k-height tower of exponentials in m. The initial seed length m controls soundness parameters of the protocol, but *has no bearing on the amount of certified output randomness!*

Our protocol uses as subroutines the exponential expansion protocol of [93] (which we denote VV)[5], and the sequential CHSH game protocol of Reichardt, et al. [84] (which we denote RUV). See Section 2.4 for more detail on these sub-protocols. We describe the protocol below, both algorithmically and schematically (see Figure 2-1).

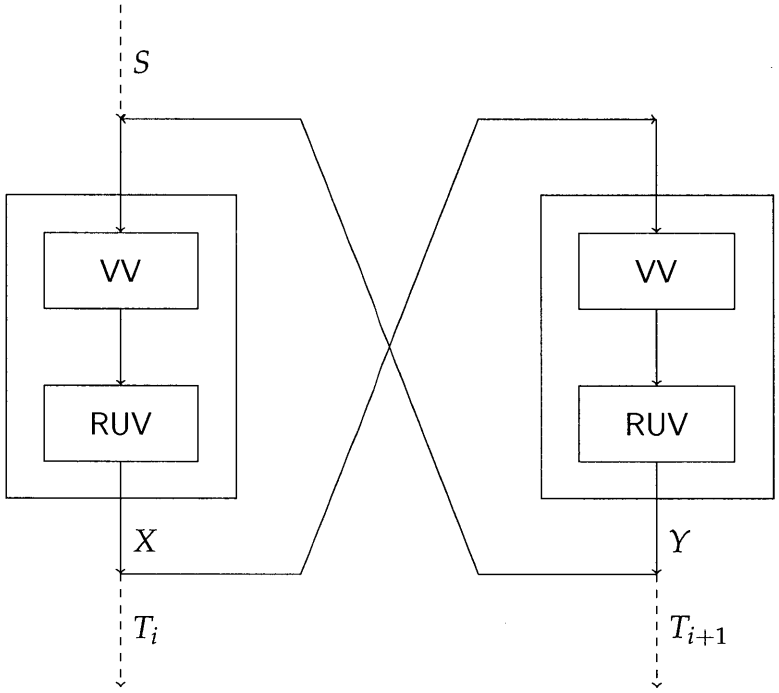

Figure 2-1: The InfiniteExpansion protocol. All arrows indicate classical operations performed by the referee. S denotes the initial seed to the protocol, and T_i denotes the output of the protocol at the ith iteration. Each of the VV and RUV boxes involve two devices, for a total of eight devices used in the protocol.

[5]We implicitly include the extraction procedure as part of the VV protocol, where the extractor seed is taken from the input seed of the VV protocol.

Non-signaling devices: $D_1, \ldots, D_8$.

Initial seed randomness: $S \sim U_m$.

1. Let $X_1 \leftarrow S$.
2. For $i = 1, 2, 3, \ldots$
   (a) $Y_i \leftarrow \mathsf{VV}(D_1, D_2, X_i)$.
   (b) $Z_i \leftarrow \mathsf{RUV}(D_3, D_4, Y_i)$.
   (c) $W_i \leftarrow \mathsf{VV}(D_5, D_6, Z_i)$.
   (d) $X_{i+1} \leftarrow \mathsf{RUV}(D_7, D_8, W_i)$.

Figure 2-2: The algorithmic specification of the InfiniteExpansion protocol. $\mathsf{VV}(A, B, X)$ (resp. $\mathsf{RUV}(A, B, X)$) denotes executing the VV (resp. RUV) sub-protocol with devices A and B using seed randomness X (for more details about these sub-protocols see Section 2.4). The X_i, Y_i, Z_i, and W_i registers are all classical, and managed by the referee.

The main result of this chapter is the following theorem, stated informally here (for the formal version see Theorems 12 and 11):

Theorem 1 (Infinite randomness expansion, informal). *Let $D = \{D_1, \ldots, D_8\}$ denote eight non-signaling quantum devices. Let E be an arbitrary quantum system that may be entangled with the D_i's, but cannot communicate with them. Suppose that a classical referee executes the* InfiniteExpansion *protocol with the $\{D_i\}$ devices, using an m-bit random seed S that is secure against the devices $\{D_i\}$. Then, for all $k \in \mathbb{N}$, if $\Pr(\text{Protocol has not aborted by round } k) = \exp(-O(m^{1/3}))$, then the output T_k of the protocol, conditioned on not aborting after k rounds, is $\exp(-\Omega(m^{1/3}))$-secure against E, and has length $\Omega(g^{(k)}(m))$, where $g^{(k)}$ denotes the k-fold composition of the function $g : \mathbb{N} \to \mathbb{N}$, defined as $g(m) = \exp(\Omega(m^{1/3}))$.*

Furthermore, there exists a quantum strategy for the devices such that, with high probability, they do not abort the protocol at any round.

The analysis of the InfiniteExpansion protocol overcomes the challenges described in the

previous section. We now give an overview of how we solve them.

2.2.1 Our proof strategy

Solving the Extractor Seed and Input Security Problems. The key technique for solving both the Extractor Seed and Input Security Problems is a powerful result of Reichardt, Unger, and Vazirani [84], which is based on the phenomenon of *CHSH game rigidity*. The CHSH game is a two-player game in which a classical referee chooses two input bits x and y uniformly at random, and gives them to non-communicating players Alice and Bob. Alice and Bob produce binary outputs a and b, and they win the game if $a \oplus b = x \wedge y$. If Alice and Bob employ classical strategies, they cannot win the CHSH game with probability exceeding 75%, but using shared quantum entanglement, there is a quantum strategy that allows them to win the game with probability $\cos^2(\pi/8) \approx 85\%$. The CHSH game is frequently used in the study of quantum entanglement and non-locality. More relevantly, it also serves as the basis for many randomness expansion protocols in the literature: protocols will often test for Bell inequality violations by measuring how often devices win the CHSH game.

The famous Tsirelson's Theorem states that $\cos^2(\pi/8)$ is the optimal winning probability using quantum strategies. Even more remarkable is that the CHSH game is *rigid*: there is essentially a *unique* quantum strategy that achieves this optimum. That is, any quantum strategy that achieves $\cos^2(\pi/8)$ winning probability must be, in a specific sense, isomorphic to the "canonical" CHSH strategy which involves Alice and Bob making specific measurements on separate halves of an EPR pair[6] (which we will call the *ideal CHSH strategy*). Furthermore, CHSH game rigidity is robust: any strategy that achieves $\cos^2(\pi/8) - \varepsilon$ winning probability must be isomorphic to a strategy that is $O(\sqrt{\varepsilon})$-close to the ideal CHSH strategy. A form of CHSH game rigidity was first proved by Mayers and Yao in the exact case [60] and later made robust by [61, 68].

[6]The EPR pair state is defined as $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

Reichardt et al. proved a far-reaching generalization of CHSH game rigidity to the situation where Alice and Bob play N independent CHSH games in sequence. This can be viewed as a larger game $\mathsf{CHSH}^{\otimes N}$, where Alice and Bob win $\mathsf{CHSH}^{\otimes N}$ if they win approximately $\cos^2(\pi/8)N$ games. Reichardt et al. prove the following theorem, stated informally here (for the precise version see [84] Theorem 5.38, or Theorem 2.8 in this chapter), which they call *sequential CHSH game rigidity*:

Theorem 2 (Sequential CHSH game rigidity, informal version)**.** *Suppose Alice and Bob play N instances of the CHSH game, where the inputs to Alice and Bob in each instance are uniform and independent of each other. Divide the N instances into N/t blocks of t games each, where $t = N^{1/\alpha}$ for some universal constant $\alpha > 1$. If Alice and Bob use a strategy that, with high probability, wins approximately $\cos^2(\pi/8)N$ instances, then in most blocks, Alice and Bob's strategy is approximately isomorphic to the ideal sequential strategy, in which the ideal CHSH strategy is applied t times in sequence to t EPR pairs that are in tensor product with each other.*

Sequential CHSH game rigidity is a powerful tool that allows one to characterize the behavior of separated quantum devices, simply from observing the correlations between their (classical) inputs and outputs. Reichardt et al. use sequential CHSH games as a primitive in a more general protocol that allows a classical computer to command non-signaling quantum devices to perform arbitrary quantum computation – and verify that this computation has been performed correctly! Here, in contrast, our goal is much more modest: we simply want to command non-signaling quantum devices to generate uniformly random bits.

The $\mathsf{CHSH}^{\otimes N}$ game already yields a protocol that produces certified randomness. In particular, we have two non-signaling devices play N games of CHSH. The referee will check whether the devices won approximately $\cos^2(\pi/8)N$ games. If so, the referee will select a block of t games at random, and use the output of one of the devices in that block of t games be the protocol's output – call this the RUV protocol.

We know from Theorem 2 that, with high probability, the outputs of the RUV protocol were generated by a strategy approximating the ideal sequential strategy. The ideal se-

quential strategy is the ideal CHSH measurement repeatedly applied to a tensor product of EPR pairs, so the measurement outcomes are necessarily in tensor product with an eavesdropper. Thus the outputs of RUV are approximately secure against a quantum adversary. The problem, of course, is that the amount of randomness needed by the referee to run this RUV protocol is much greater than the amount of certified randomness in the output ($\Theta(N)$ versus $N^{1/\alpha}$). So we can't use RUV by itself as a randomness expansion scheme.

However, sequential CHSH game rigidity offers more than just the guarantee of secure uniform randomness; observe that it *does not need to assume that the inputs to the N CHSH games were secure against an eavesdropper* – only that it was secure against the devices playing the CHSH games! This is precisely the Input Security property.

Thus, we can use the RUV protocol as a "scrambling" procedure that transforms an input that may not be secure against an eavesdropper into a shorter string that *is* secure against an eavesdropper. Recall that, because of the Input Security and Extractor Seed Problems, the output of the VV sub-protocol in the InfiniteExpansion protocol may not be secure against other devices (namely, the devices that produced the input to the VV sub-protocol). However, if we invoke the RUV protocol on the outputs of VV, we obtain secure outputs that can be used as input randomness for another VV instance.

Furthermore, observe that we still have achieved randomness expansion: the VV protocol attains exponential expansion, and the RUV protocol will only shrink that by a polynomial amount.

Solving the Conditioning Security Problem. The main technical contribution of this chapter is solving the Conditioning Security Problem. While combining the VV and RUV protocols conceptually yields an Input Secure randomness expansion protocol, there still is the technical issue of whether this protocol is Input Secure when we condition on the RUV protocol succeeding. There are simple examples that show that adversarial devices can, via conditioning, skew the distribution of their outputs, and even introduce entanglement between some bits of their outputs and an eavesdropper, despite most outputs

having been produced by an ideal strategy. The Sequential CHSH Game Rigidity Theorem of [84] does not take conditioning into account, because it is assumed that the devices pass the RUV protocol with probability extremely close to 1.

Here, we assume the RUV protocol passes with some small probability that is inverse polynomial in the number of games played, and show that the RUV protocol manages to obtain an approximately secure output conditioned on the protocol succeeding. We prove this in Lemma 15, and our proof employs tools from quantum information theory. Our approach is reminiscent of that used in the proofs of the classical Parallel Repetition Theorem (see, e.g., [40]).

Solving the compounding error problem. We use the strongest definition of the quantum security of a string against an eavesdropper: namely, a string X is (approximately) secure against an eavesdropper E iff the trace distance between the joint state ρ_{XE} and the ideal state $U_{|X|} \otimes \rho_E$ is small, where where $U_{|X|}$ denotes the uniform distribution on $|X|$ bits. To solve the compounding error problem, we first show that the errors incurred at each iteration of the InfiniteExpansion protocol accumulate *linearly* – this is because the trace distance satisfies the triangle inequality. Then, we show that the error added at iteration k is *exponentially* smaller than the error of iteration $k-1$. Thus, the infinite sum of errors converges to a constant multiple of the error incurred by the first iteration, which is exponentially small in the seed length m. Hence we avoid the potential problems raised by [51].

2.2.2 Related work

Here we discuss some relevant recent developments in the area of randomness expansion and amplification, which were announced after the original posting of this work. We note, however, that the results in the following works were discovered independently of the results in this work, and their relationship to each other was only realized after both works were essentially complete. In the following description we will occasionally

use the terminology of this chapter to restate results of these other works, though those papers used different terminology in the original statements.

In independent work by Chung, Shi, and Wu [16], the problem of Input Security was also studied, and played a key role in their construction of a device-independent protocol to amplify randomness, starting with any min-entropy source. The authors require an Input Secure randomness expansion protocol to use as a building block for their amplification protocol. They prove an elegant result called the Equivalence Lemma, which may be informally summarized as follows (see [16] for a formal statement):

Consider a device-independent randomness expansion protocol P, that starts with a seed S, uniform and in tensor product with the devices D involved in the protocol, as well as a quantum adversary E, and produces an output string X that is certifiably close to uniform and in tensor product with E and S. The Equivalence Lemma states that any such protocol P *also* certifies output randomness X with the same security guarantees, *without requiring that S is in tensor product with E* — in other words, any such protocol P is also Input Secure. In particular, this proves that the Vazirani-Vidick protocol (when implemented in composition with a strong quantum extractor) is, in fact, Input Secure, and can be composed with itself to perform unbounded randomness expansion in the same manner as we do here, without requiring the use of the RUV protocol.

Secondly, another independent work of Miller and Shi [69] gives the first provably robust protocol for randomness expansion (and, in fact, gives robust exponential expansion). Combining the main result of [69] with Equivalence Lemma of [16], allows one to obtain a provably *robust* infinite expansion protocol requiring only four non-communicating devices.

It is interesting to note that extractors (which have a similar input-output structure to randomness expansion protocols) cannot possess an analogous Input Security. Thus, there is no natural analogue of the Equivalence Lemma which will work for extractors. In this sense, the Equivalence Lemma represents an interesting phenomenon or property which is possessed by device independent (quantum) protocols, but not by (classical) protocols

such as extractors.

2.3 Preliminaries

2.3.1 Notation

We write $[N]$ for the set of integers $\{1, \ldots, N\}$. For a Hilbert space $\mathcal{H}$, let $D(\mathcal{H})$ denote the set of density matrices on $\mathcal{H}$. The classical state ρ_X corresponding to a discrete classical random variable X is defined as $\sum_x \Pr(X = x)|x\rangle\langle x|$ (where x ranges over the computational basis states). For a discrete classical random variable X, we use $|X|$ to denote X's length in bits. A classical-quantum state (or *cq-state*) $\rho_{XB} \in D(\mathcal{H}_X \otimes \mathcal{H}_B)$ is a density matrix where $\rho_{XB} = \sum_x p_x |x\rangle\langle x| \otimes \rho_B^x$, where p_x are probabilities and $\{|x\rangle\}$ is an orthonormal basis for $\mathcal{H}_X$. We write $\mathbb{1}_N$ to denote the $N \times N$ identity matrix. We write U_m to denote the density matrix $2^{-m}\mathbb{1}_{2^m}$ (i.e. the completely mixed state of dimension 2^m). For an arbitrary matrix A, we let $\|A\|_{\mathrm{tr}} := \frac{1}{2}\mathrm{tr}\sqrt{A^\dagger A}$ denote its trace norm (also known as its Schatten 1-norm).

Definition 3 (Secure cq-state)**.** *Let E be an arbitrary quantum system. Let ρ_{XE} be a cq-state. For state ρ_{XE}, X is ζ-**secure against** E iff*

$$\|\rho_{XE} - U_{|X|} \otimes \rho_E\|_{\mathrm{tr}} \leq \zeta.$$

2.3.2 Quantum information theory

For completeness we present a few key definitions and facts of quantum information theory that will be useful for us later. For a more comprehensive reference we refer the reader to, e.g., [74, 98].

For a density matrix ρ, its von Neumann entropy is defined as $H(\rho) := -\mathrm{tr}(\rho \log \rho)$. For a density matrix $\rho_{AB} \in D(\mathcal{H}_A \otimes \mathcal{H}_B)$, the conditional von Neumann entropy is defined

as $H(A|B)_\rho := H(AB)_\rho - H(B)_\rho$ where $H(AB)_\rho = H(\rho_{AB})$ and $H(B)_\rho = H(\rho_B)$. The quantum mutual information between A and B of ρ_{AB} is defined as $I(A:B)_\rho := H(A)_\rho - H(A|B)_\rho$. The conditional quantum mutual information $I(A:B|C)_\rho$ for a tripartite state ρ_{ABC} is defined as $H(A|C)_\rho - H(A|B,C)_\rho$. We will usually omit the subscript ρ when the state is clear from context.

We now list a few useful facts about these quantum information-theoretic quantities. Proofs of the following facts can be found in, e.g., [98].

Fact 4. 1. *Let X be a discrete random variable, and let ρ_X be its associated classical state. Then $H(\rho_X) = H(X)$, where $H(X)$ is the Shannon entropy of X.*

2. *(Conditioning reduces entropy) Let $\rho_{AB} \in D(\mathcal{H}_A \otimes \mathcal{H}_B)$. Then $H(A|B)_\rho \leq H(A)_\rho$.*

3. *(Chain rule) Let $\rho_{ABC} \in D(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C)$. Then*

$$I(A:BC)_\rho = I(A:B)_\rho + I(A:C|B)_\rho.$$

4. *(Pinsker's inequality) Let $\rho_{AB} \in D(\mathcal{H}_A \otimes \mathcal{H}_B)$. Then*

$$\|\rho_{AB} - \rho_A \otimes \rho_B\|_{\text{tr}}^2 \leq 2I(A:B)_\rho.$$

Finally, we define quantum min-entropy. Let ρ_{AB} be a bipartite density matrix. The min-entropy of A conditioned on B is defined as

$$H_{\min}(A|B)_\rho := \max\{\lambda \in \mathbb{R} : \exists \sigma_B \in D(\mathcal{H}_B) \text{ s.t. } 2^{-\lambda} \mathbb{1}_A \otimes \sigma_B \geq \rho_{AB}\}.$$

Let $\varepsilon > 0$. Then ε-smoothed min-entropy of A conditioned on B is defined as

$$H_{\min}^\varepsilon(A|B)_\rho := \max_{\tilde{\rho}_{AB} \in B(\rho_{AB}, \varepsilon)} H_{\min}(A|B)_{\tilde{\rho}},$$

where $B(\rho_{AB}, \varepsilon)$ is the set of sub-normalized density matrices within trace distance ε of

ρ_{AB}. For a detailed reference on quantum min-entropy, we refer the reader to [85].

2.3.3 Modelling protocols and input robustness

In this chapter we will consider several different randomness expansion procedures (e.g., the Vazirani-Vidick protocol, or the RUV protocol); a crucial element of our analysis is that these protocols are all *input robust* in the sense that slight deviations from uniformity in their input seed only mildly affect the expansion guarantees that we get when assuming the seed is perfectly uniform. To make this input robustness property formal, we introduce the quantum operation description of randomness expansion protocols.

In general, a randomness expansion protocol is an interaction between a classical referee R and a quantum device D, that is entirely unconstrained, except that D consists of two or more isolated, non-signaling sub-devices (but the sub-devices may be entangled).

The important Hilbert spaces we will consider are:

1. (**Pass/No Pass Flag**). $\mathcal{H}_F$ denotes a two-dimensional Hilbert space that the referee will use to indicate whether it accepts or rejects the interaction.

2. (**Protocol seed**). $\mathcal{H}_S$ denotes the 2^m-dimensional Hilbert space that corresponds to the (private) m-bit seed randomness that the referee will use for its interaction with the device D.

3. (**Protocol output**). $\mathcal{H}_X$ denotes the Hilbert space that corresponds to the output of the device D [7].

4. (**Device internal state**). $\mathcal{H}_D$ denotes the Hilbert space corresponding to the internal state of the device D.

5. (**Eavesdropper**). $\mathcal{H}_E$ denotes the Hilbert space corresponding to a potential quantum eavesdropper, which may be entangled with device D.

[7] Since D always consists of non-signaling subdevices, we will arbitrarily declare one of the sub-devices' output to be the output of the overall device D.

We can view a randomness expansion protocol as a quantum operation $\mathcal{E}$ acting on states in the space $\mathcal{H}_F \otimes \mathcal{H}_S \otimes \mathcal{H}_X \otimes \mathcal{H}_D$. Of the Hilbert spaces listed above, device D only has access to the Hilbert space $\mathcal{H}_D$; the other Hilbert spaces get updated by the referee's interaction with D (except for $\mathcal{H}_E$ which is controlled by the eavesdropper). For example, the referee, by interacting with D, will write D's outputs to register X. The states in the Hilbert spaces $\mathcal{H}_F$, $\mathcal{H}_S$, and $\mathcal{H}_X$ will always be classical mixed states (i.e. diagonal in the computational basis).

More precisely, let P be a randomness expansion protocol. We will model P as a quantum operation $\mathcal{E}$ acting on an initial state ρ^i_{FSXD} in the space $\mathcal{H}_F \otimes \mathcal{H}_S \otimes \mathcal{H}_X \otimes \mathcal{H}_D$, where ρ^i_D is the internal state of D before the protocol starts, and ρ^i_{FSX} is prepared by the referee. $\mathcal{E}$ will be some unitary map V_P applied to the joint state ρ^i_{FSXD}. Now, define the quantum operation $\mathcal{F}$ that takes a state ρ_{FSXD}, and produces the post-measurement state of ρ_{FSXD} *conditioned* on measuring $|1\rangle$ in the F register, and then traces out the F and S registers, leaving $\rho_{XD|F=1}$. We define $\mathcal{FE}$ to be the composition of the two quantum operations $\mathcal{E}$, followed by $\mathcal{F}$. Throughout this chapter, we will decorate density matrices by superscripts i and f to denote the states before and after the protocol, respectively. For example, we will often let ρ^f_{FSXD} denote the state of the $FSXD$ system after the execution of the protocol, conditioned on the protocol succeeding (i.e. $F = 1$).

The completeness and soundness of protocol P are statements about the post-measurement state $\mathcal{FE} \otimes \mathbb{1}_E(\rho^i_{FSXDE})$ (where $\mathbb{1}_E$ is the identity on $\mathcal{H}_E$), argued only with respect to an *ideal* initial state ρ^i_{FSXDE} such that $\rho^i_{FSXD} := |0\rangle\langle 0|_F \otimes U_m \otimes |0\rangle\langle 0|_X \otimes \rho^i_D$, (or, depending on the analysis, the stronger assumption that $\rho^i_{FSXDE} := |0\rangle\langle 0|_F \otimes U_m \otimes |0\rangle\langle 0|_X \otimes \rho^i_{DE}$). In other words, the initial seed is assumed to be perfectly uniform and unentangled with the device D. However, we also have a form of input robustness: if the initial state were instead δ-close in trace distance to the ideal initial state defined above, then we would obtain the same output parameters as P, up to an δ/λ additive factor in trace distance, where λ is the probability that $|1\rangle$ is measured in the F register. We prove this formally in Lemma 5 below.

Lemma 5. *Let D be a device, and E an arbitrary quantum system that may be entangled with D. Let $\sigma_{FSX} := |0\rangle\langle 0|_F \otimes U_{|S|} \otimes |0\rangle\langle 0|_X$. Let the quantum operations $\mathcal{F}$, $\mathcal{E}$, and $\mathcal{FE}$ be defined as above. Suppose for all states σ_{FSXDE} such that $\sigma_{FSXD} = \sigma_{FSX} \otimes \sigma_D$, there exists a state τ_{XDE} such that $\tau_{XE} = U_{|X|} \otimes \sigma_E$ and*

$$\|\mathcal{FE} \otimes \mathbb{1}_E(\sigma_{FSXDE}) - \tau_{XDE}\|_{\mathrm{tr}} \leq \varepsilon.$$

Let $\delta, \lambda > 0$. Let ρ^i_{FSXDE} be such that $\|\rho^i_{FSXDE} - \sigma_{FSXDE}\|_{\mathrm{tr}} \leq \delta$ for a state σ_{FSXDE} where $\sigma_{FSXD} = |0\rangle\langle 0|_F \otimes U_{|S|} \otimes |0\rangle\langle 0|_X \otimes \sigma_D$. Suppose that the probability of measuring $|1\rangle$ in the F register for the state $\mathcal{E} \otimes \mathbb{1}_E(\rho^i_{FSXDE})$ is at least λ. Then, there exists a state μ_{XDE} such that $\mu_{XE} = U_{|X|} \otimes \mu_E$ and

$$\|\rho^f_{XDE} - \mu_{XDE}\|_{\mathrm{tr}} \leq \varepsilon + \delta/\lambda,$$

where $\rho^f_{XDE} := \mathcal{FE} \otimes \mathbb{1}_E(\rho^i_{FSXDE})$.

The proof of Lemma 5 is deferred to Appendix A.1.

2.3.4 The Vazirani-Vidick protocol and quantum-secure extractors

Vazirani and Vidick exhibit a protocol that involves two non-signaling quantum devices and a classical referee, that achieves randomness expansion that is secure against a quantum eavesdropper [93, Protocol B]. We record a formulation of their result as it will be used by us here:

Theorem 6 (Vazirani-Vidick protocol [93]). *There exists a protocol P with the following properties. Let D_1 and D_2 be arbitrary non-signaling quantum devices. Let E be an arbitrary quantum system, possibly entangled with D_1 and D_2, but cannot communicate with D_1 and D_2 once the protocol begins. The protocol, executed with devices D_1 and D_2, has the following properties:*

1. *(Output length). The output of the protocol has length $n(m) = \exp(Cm^{1/3})$, for some constant C;*

2. *(Completeness). There exists a non-signaling quantum strategy for D_1 and D_2 to pass the protocol with probability* $1 - \exp(-\Omega(m^{2/3}))$;

3. *(Soundness). If the initial joint state $\rho^i_{SD_1D_2E}$ of the seed S, devices D_1, D_2, and eavesdropper E is such that $\rho^i_{SD_1D_2E} = U_m \otimes \rho^i_{D_1D_2E}$, then if* $\Pr(\textit{Protocol succeeds}) \geq \varepsilon$, *we have that*

$$H^{\varepsilon}_{\infty}(X|E)_{\rho^f} \geq h(m),$$

where $\varepsilon = \varepsilon(m)$, and ρ^f_{XE} denotes the joint state of device D_1's output and E, conditioned *on the protocol succeeding.*

where $h(m) := \exp(C'm^{1/3})$ and $\varepsilon(m) := 1/h(m)$, for a universal constant C'.

Another important primitive we will use is a *quantum-secure extractor.*

Definition 7 (Quantum-secure extractor). *A function* $\mathrm{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^r$ *is a (h, ε)-quantum-secure extractor iff for all cq-states ρ_{XE} classical on n-bit strings X with $H_{\infty}(X|E)_{\rho} \geq h$, and for uniform seed S secure against X and E (that is, the joint state ρ_{XES} is such that $\rho_{XES} = \rho_{XE} \otimes U_d$), we have*

$$\left\| \rho_{\mathrm{Ext}(X,S)ES} - U_r \otimes \rho_{ES} \right\|_{\mathrm{tr}} \leq \varepsilon,$$

where $\rho_{\mathrm{Ext}(X,S)ES}$ denotes the joint cqc-state on the extractor output, quantum side information E, and the seed S.

Theorem 8 ([30]). *For all positive integers n, r, there exists a function* $\mathsf{QExt} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^r$ *that is a $(r + O(\log r) + O(\log 1/\varepsilon), \varepsilon)$-quantum-secure extractor where $d = O(\log^2(n/\varepsilon) \log r)$.*

2.3.5 Sequential CHSH game rigidity

We can view a sequence of N CHSH games, played by non-signaling quantum devices D_1, D_2, as a protocol $\mathsf{CHSH}^{\otimes N}$, where the referee uses a private random seed S to generate

inputs $A_i, B_i \in \{0,1\}$ to the devices D_1 and D_2, and obtains their respective outputs $X_i, Y_i \in \{0,1\}$ for each round $i \in [N]$. The protocol succeeds if W, the number of rounds i such that $X_i \oplus Y_i = A_i \wedge B_i$, is at least $(\cos^2(\pi/8) - O(\frac{\log N}{\sqrt{N}}))N$.

Divide the N rounds of the $\mathsf{CHSH}^{\otimes N}$ protocol into *blocks* of t consecutive games each, where $t = \lfloor N^{1/\alpha} \rfloor$ for some fixed constant α. Let X be the output register of device D_1. Let X_i denote the t-qubit register of the ith block of X.

We paraphrase the sequential CHSH game rigidity theorem of [84] here. In the theorem, we imagine that for each block of games, the devices D_1, D_2 apply some local quantum operation on their respective systems to produce outputs for the block. We call the quantum operation applied in each block i their *block strategy* for i. We say that a block strategy is ζ-ideal if there is a local isometry $\mathcal{I}$ under which their quantum operation $\mathcal{E}$ and the state acted upon by $\mathcal{E}$ are together ζ-close to the ideal CHSH strategy (for a precise definition of ζ-ideal strategies, see [84]). The main property of ζ-ideal strategy that we will use is the following:

Lemma 9. *Let D_1, D_2 be non-signaling quantum devices. Suppose that D_1 and D_2 participate in the $\mathsf{CHSH}^{\otimes N}$ protocol. Let E be an arbitrary quantum system that may be entangled with D_1, D_2, but cannot communicate with them once the $\mathsf{CHSH}^{\otimes N}$ protocol begins. Let I_i be the indicator random variable denoting whether D_1 and D_2's block strategy for block i is ζ-ideal. Let X_i be the output of block i. Then,*

$$\|\rho_{X_i E|I_i=1} - U_n \otimes \rho_{E|I_i=1}\|_{\mathrm{tr}} \leq \zeta,$$

where $\rho_{X_i E|I_i=1}$ denotes the joint state of X_i and E, conditioned on the event $I_i = 1$.

Proof. This is straightforward given the definition of ζ-ideal strategy. See [84, Definitions 5.4, 5.5 and 5.37] for more detail. □

Theorem 10 (Sequential CHSH game rigidity; Theorem 5.38 of [84])**.** *Let D_1, D_2 be non-signaling quantum devices. Suppose that D_1 and D_2 participate in the $\mathsf{CHSH}^{\otimes N}$ protocol. Let E be an arbitrary quantum system that may be entangled with D_1, D_2, but cannot communicate with them once the $\mathsf{CHSH}^{\otimes N}$ protocol begins. Let W be the total number of CHSH games that D_1*

and D_2 win in the protocol. Let X be the output of D_1. Fix $\varepsilon > 0$, and let $G \leq N/t$ be the total number of blocks i such that the strategy employed by D_1 and D_2 in block i is $\kappa_* t^{-\kappa_*}$-ideal, where $\kappa_* > 1$ is a universal constant. Then,

$$\Pr(W \geq \cos^2(\pi/8)N - \frac{1}{2\sqrt{2}}\sqrt{N \log N} \text{ and } G \leq (1-\nu)N/t) \leq \frac{1}{t^2},$$

where $\nu = (12/\sqrt{2})\sqrt{\log N} t / N^{1/4}$, and $t > 85$.

Proof. This is Theorem 5.38 of [84], instantiated with the parameter settings used in Theorem 5.39. □

2.4 The Protocol

In this section we formally define the protocol for infinite certifiable randomness expansion, which we call the InfiniteExpansion protocol. The protocol uses eight non-signaling devices, which may all share entanglement, but cannot communicate with each other. The devices are partitioned into two *Expansion Clusters* C_0 and C_1 with four devices each. In each iteration, the InfiniteExpansion protocol alternates between clusters C_0 and C_1, performing a sub-protocol called ClusterExpansion. The output of one cluster is used as seed randomness for the next invocation of the ClusterExpansion sub-protocol with the other cluster. Only the first iteration requires some seed randomness, to "jumpstart" the randomness expansion process.

InfiniteExpansion **Protocol**

Non-signaling Clusters: C_0, C_1.

Initial seed randomness: $S \sim U_m$.

1. Let $X_1 \leftarrow S$.
2. For $i = 1, 2, 3, \ldots$
   (a) $X_{i+1} \leftarrow \mathsf{ClusterExpansion}(C_i, X_i)$.
   (b) If ClusterExpansion aborts, then abort the entire protocol, otherwise continue.

Figure 2-3: The InfiniteExpansion protocol. The classical registers X_i are maintained by the referee, and C_i denotes cluster $C_{i \bmod 2}$. $X_{i+1} \leftarrow \mathsf{ClusterExpansion}(C_i, X_i)$ denotes executing the ClusterExpansion sub-protocol with the devices in cluster C_i, using X_i as the seed randomness, and storing the sub-protocol output in register X_{i+1}.

We now specify the sub-protocol $\mathsf{ClusterExpansion}(C, S)$ for a 4-device cluster C and seed randomness S. As discussed earlier, two devices of a cluster C will be used to perform the Vazirani-Vidick near-exponential randomness expansion protocol, and the other two will be used to perform a variant of the $\mathsf{CHSH}^{\otimes N}$ protocol, which we call the RUV protocol.

ClusterExpansion(C, S) **Sub-Protocol**

Input Non-signaling Devices: $C := \{D_1, D_2, E_1, E_2\}$.

Input seed randomness: S

1. $Y \leftarrow \mathsf{VV}(D_1, D_2, S)$.
2. $Z \leftarrow \mathsf{RUV}(E_1, E_2, Y)$.
3. If either of the above instances of VV or RUV aborts, then abort ClusterExpansion. Otherwise continue.
4. Output Z.

It is important that no subset of these devices can communicate with (signal to) any other subset of the devices throughout the course of the subroutine. We now give precise definitions of the VV and RUV sub-protocols.

2.4.1 The VV sub-protocol

The VV sub-protocol consists of performing Protocol B from [93], and then applying a randomness extractor to the output of Protocol B. For any s, Protocol B takes in a uniformly random s-bit seed, and conditioned on the protocol succeeding, produces a string of length $n(s) = \exp(\Omega(s^{1/3}))$ with $h(s) = \exp(\Omega(s^{1/3}))$ bits of (smoothed) min-entropy (see Theorem 6). We give a detailed account of the particular parameter settings we use for Protocol B in Appendix A.3.

We use the QExt randomness extractor given by Theorem 8. More formally, by $\mathsf{QExt}_{n,r,\varepsilon}$ we denote the $(r + O(\log r) + O(\log 1/\varepsilon), \varepsilon)$-quantum-secure extractor mapping $\{0,1\}^n \times \{0,1\}^d$ to $\{0,1\}^r$, where $d = d(n, r, \varepsilon) = O(\log^2(n/\varepsilon) \log r)$.

For all s, the VV sub-protocol takes in a s-bit seed S, and outputs $v(s)$ bits, where $v(s) := \exp(\Omega(s^{1/3}))$ (for more detail, see Appendix A.3).

VV(A, B, S) **Sub-Protocol**

Input Non-signaling Devices: A, B

Input Seed : S

1. Let S_1 be the first $\lfloor s/2 \rfloor$ bits of S, and S_2 be the last $\lfloor s/2 \rfloor$ bits of S, where $s := |S|$.
2. Perform Protocol B of [93] with devices A and B, using S_1 as seed randomness, and store Protocol B's output in register Y.
3. If Protocol B aborts, then abort VV. Otherwise, continue.
4. Output $\mathsf{QExt}_{n,r,\varepsilon}(Y, S_2)$, where $n = n(\lfloor s/2 \rfloor)$, $r = v(s)$, and $\varepsilon = 1/h(\lfloor s/2 \rfloor)$.

Figure 2-4: The VV sub-protocol. The functions $n(s)$ and $h(s)$ denote the output length and min-entropy lower bound of Protocol B in Theorem 6 on s bits of seed.

2.4.2 The RUV sub-protocol

The RUV sub-protocol, using a random seed S, has two devices (call them A and B) play a number N of sequential CHSH games, where N is a function of $|S|$, and the inputs to the devices in each of the CHSH games are determined by half of S. The RUV sub-protocol aborts if they do not win nearly $\approx \cos^2(\pi/8)$ fraction of games. Then, the other half of S is used to select a random *sub-block* of A's outputs in the N CHSH games, and the sub-block is produced as the output of RUV.

More precisely, let $X \in \{0,1\}^N$ denote A's outputs. Divide X into blocks of t consecutive bits, and further subdivide each block into $\sqrt{t}$ sub-blocks of $\sqrt{t}$ bits each. We set $t = \lfloor N^{1/\alpha} \rfloor$, where $\alpha := \lceil 16\kappa_*^2 \rceil$ and κ_* is the constant from [84, Theorem 5.7].

For all s, the RUV sub-protocol takes in a s-bit seed S, and outputs $r(s)$ bits, where $r(s) := \lfloor (s/4)^{1/(2\alpha)} \rfloor$.

RUV(A, B, S) **Sub-Protocol**

Input Non-signaling Devices: A, B

Input Seed : S

1. Let S_1 be the first $\lfloor s/2 \rfloor$ bits of S, and S_2 be the last $\lfloor s/2 \rfloor$ bits of S, where $s := |S|$.

2. Let $a, b \in \{0,1\}^{\lfloor s/4 \rfloor}$ be the first and last halves of S_1, respectively.

3. For $i = 1, \ldots, N$, where $N := \lfloor s/4 \rfloor$:

   (a) Input a_i, b_i to devices A and B respectively, and collect outputs $x_i, y_i \in \{0,1\}$ from A and B respectively.

4. Let W be the number of indices i such that $x_i \oplus y_i = a_i \wedge b_i$. If

$$W < \cos^2(\pi/8)N - \frac{1}{2\sqrt{2}}\sqrt{N \log N},$$

   then abort RUV. Otherwise, continue.

5. Output Z, the $\sqrt{t}$-bit string that is the jth sub-block of the ith block of X, where X is the register that holds the outputs (x_i), and i and j are selected uniformly from $[N/t]$, $[\sqrt{t}]$, respectively, using the seed S_2.

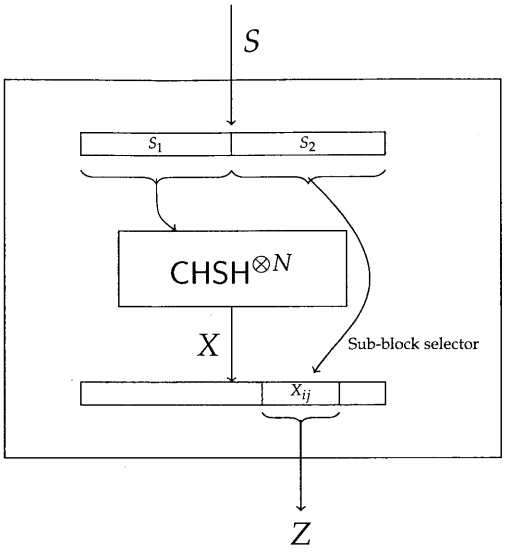

Figure 2-5: The RUV sub-protocol. All arrows indicate classical operations performed by the referee.

2.5 Analysis of the InfiniteExpansion Protocol

We now analyze the InfiniteExpansion protocol. As discussed in the Preliminaries (Section 4.2), we will use the notation ρ^i and ρ^f (or some variant thereof) to denote the state of the registers, devices, eavesdroppers, etc., before and after the execution of a protocol, respectively. We will use the following functions throughout this section: $v(s)$ and $r(s)$ to denote the output lengths of the VV and RUV sub-protocols on inputs of length s, respectively (defined in Section 2.4). The output length of the ClusterExpansion sub-protocol on an s-bit seed is $g(s) := r(v(s))$. We will use $g^{(k)}(s)$ to denote the k-fold composition of $g(s)$ (i.e. $g^{(1)}(s) = g(s), g^{(2)}(s) = g(g(s))$, etc.).

Theorem 11 establishes that there exists a quantum strategy by which the devices, with high probability, do not abort the InfiniteExpansion protocol. Theorem 12 establishes the soundness of the InfiniteExpansion protocol.

Theorem 11 (Completeness of the InfiniteExpansion protocol). *There exists a non-signalling*

quantum strategy for devices $D_1, \ldots, D_8$, such that the probability that the referee aborts in any round i in the execution of the InfiniteExpansion(C_1, C_2, S) *protocol is at most* $\exp(-\Omega(m^{1/3}))$, *where* $C_1 = \{D_1, \ldots, D_4\}$ *and* $C_2 = \{D_5, \ldots, D_8\}$, *and* S *is a uniformly random* m*-bit seed that is secure against* $D_1, \ldots, D_8$.

Proof. We group the devices into pairs $\{D_1, D_2\}$, $\{D_3, D_4\}$, $\{D_5, D_6\}$, and $\{D_7, D_8\}$, where pairs $\{D_1, D_2\}$ and $\{D_5, D_6\}$ will instantiate the ideal devices for the VV protocol (see [93] for more details), and the pairs $\{D_3, D_4\}$ and $\{D_7, D_8\}$ will instantiate the ideal devices for the RUV protocol (i.e. use the ideal CHSH strategy in every round). Fix a round i and assume, without loss of generality, that the referee interacts with the pairs $\{D_1, D_2\}$ (used for the VV protocol) and $\{D_3, D_4\}$ (used for the RUV protocol) in round i. The probability that $\{D_1, D_2\}$ abort the VV protocol is at most $\exp(-\Omega(m_i^{2/3}))$, and the probability that $\{D_3, D_4\}$ abort the RUV protocol is at most $\exp(-\Omega(m_i^{1/3}))$, where $m_i = g^{(i)}(m)$. Thus, by the union bound, the probability of aborting any round i is at most $\exp(-\Omega(m^{1/3}))$. □

Theorem 12 (Soundness of the InfiniteExpansion protocol). *Let C_0 and C_1 be non-signaling Expansion Clusters. Suppose that a classical referee executes the* InfiniteExpansion(C_0, C_1, S) *protocol, where S denotes the referee's classical register that holds an m-bit seed. Let WIN_i to be the event that the referee did not abort the* InfiniteExpansion *protocol in the ith round, and let $\mathrm{WIN}_{\leq i} = \mathrm{WIN}_1 \wedge \cdots \wedge \mathrm{WIN}_i$. Let E be an arbitrary quantum system that may be entangled with C_0 and C_1, but cannot communicate with C_0 and C_1 once the protocol has started. Let $\rho^0_{SC_0C_1}$ denote the initial joint state of the seed and the clusters. If $\rho_{SC_0C_1} = U_m \otimes \rho_{C_0C_1}$, then we have for all $k \in \mathbb{N}$ that if $\Pr(\mathrm{WIN}_{\leq k}) \geq \lambda \geq \exp(-C'm^{1/3})$ for some universal constant C', then*

$$\|\rho^k_{X_kE} - U_{g^{(k)}(m)} \otimes \rho^k_E\|_{\mathrm{tr}} \leq 4\exp(-C''m^{1/3})/\lambda^2,$$

where

- *C'' is the universal constant from Theorem 13, and*
- *$\rho^k_{X_kE}$ denotes the joint state of the referee's X_k register and E after k rounds of the* InfiniteExpansion(C_0, C_1)

Protocol, conditioned on the event $\text{WIN}_{\leq k}$.

Before presenting the proof of Theorem 12, we wish to direct the reader's attention to the Input Security of the InfiniteExpansion protocol: the assumption on the initial seed is that it is in tensor product with the cluster devices only, and not the eavesdropper E – however, the output at each iteration is close to being in tensor product with the eavesdropper E.

The proof of Theorem 12 assumes the correctness of the ClusterExpansion sub-protocol (Theorem 13), and shows that the InfiniteExpansion protocol maintains the property that at each iteration i, the output of X of cluster C_i (where C_i denotes Expansion Cluster $C_{i \mod 2}$) is approximately secure against the other cluster C_{i+1}. Thus, the the execution of the ClusterExpansion sub-protocol with C_{i+1}, conditioned on not aborting, will continue to produce a nearly uniform output. Furthermore, the errors accumulate linearly with each iteration.

Proof. Define $C_j := C_{j \mod 2}$. Divide the overall probability of success, $\Pr(\text{WIN}_{\leq k})$, into conditional probabilities: let $p = \Pr(\text{WIN}_{\leq k})$ and let $p_i = \Pr(\text{WIN}_i | \text{WIN}_{\leq i-1})$. Observe that we have $p = \prod p_i \geq \lambda$. We prove the claim by induction.

The inductive hypothesis: Recursively define $\delta(i) := \varepsilon_{\mathsf{EC}}(g^{(i-1)}(m), p_i) + \delta(i-1)/p_i$, where $\delta(1) := \varepsilon_{\mathsf{EC}}(m, p_1)$ and $\varepsilon_{\mathsf{EC}}(\cdot)$ is the error bound given by Theorem 13. For all $i = 1, \ldots, k-1$, there exists a state $\mu^i_{XC_iC_{i+1}E}$ such that $\mu^i_{X_iC_{i+1}E} = U_{g^{(i)}(m)} \otimes \mu^i_{C_{i+1}E}$ and

$$\|\rho^i_{X_iC_iC_{i+1}E} - \mu^i_{X_iC_iC_{i+1}E}\|_{\text{tr}} \leq \delta(i),$$

where $\rho^i_{X_iC_iC_{i+1}E}$ is the joint state of the X_i register, both clusters C_i and C_{i+1}, and E after the ith round, conditioned on $\text{WIN}_{\leq i}$.

Let $k = 1$. Then, by invoking Theorem 13 with $C = C_1$, and treating the quantum eavesdropper as C_2 and E together, we obtain that there exists a state $\mu^1_{X_1C_1C_2E}$ such that $\mu^1_{X_1C_2E} = U_{g(m)} \otimes \mu^1_{C_2E}$, and

$$\|\rho^1_{X_1C_1C_2E} - \mu^1_{X_1C_1C_2E}\|_{\text{tr}} \leq \varepsilon_{\mathsf{EC}}(m, p_1) = \delta(1).$$

This establishes the base case.

Now, suppose that we have run $k-1$ rounds of the InfiniteExpansion protocol for some $k > 1$. Using our inductive assumption for $i = k-1$, we invoke Theorem 13 along with Lemma 5 to conclude that there exists a state $\mu^k_{X_k C_k C_{k+1} E}$ such that $\mu^k_{X_k C_{k+1} E} = U_{g^{(k)}}(m) \otimes \mu^k_{C_{k+1} E}$ and

$$\|\rho^k_{X_k C_k C_{k+1} E} - \mu^k_{X_k C_k C_{k+1} E}\|_{\mathrm{tr}} \leq \varepsilon_{\mathsf{EC}}(g^{(k-1)}(m), p_k) + \delta(k-1)/p_k := \delta(k).$$

This completes the induction argument. We now bound $\delta(k)$:

$$\begin{aligned}
\delta(k) &= \varepsilon_k + \frac{1}{p_k}\left(\varepsilon_{k-1} + \frac{1}{p_{k-1}}\left(\varepsilon_{k-2} + \cdots\right)\right) \\
&\leq \frac{1}{\lambda}\left(\varepsilon_k + \varepsilon_{k-1} + \cdots + \varepsilon_1\right) \\
&\leq \frac{2\varepsilon_1}{\lambda},
\end{aligned}$$

where we write $\varepsilon_i := \varepsilon_{\mathsf{EC}}(g^{(i)}(m), p_i)$, and use the facts that $\prod p_i \geq \lambda$ and each ε_i is exponentially smaller than ε_{i-1}.

Finally, for every k, we have that

$$\begin{aligned}
\|\rho^k_{X_k E} - U_{g^{(k)}(m)} \otimes \rho^k_E\|_{\mathrm{tr}} &\leq \|\rho^k_{X_k E} - \mu^k_{X_k E}\|_{\mathrm{tr}} + \|\mu^k_{X_k E} - U_{g^{(k)}(m)} \otimes \rho^k_E\|_{\mathrm{tr}} \\
&\leq \delta(k) + \|U_{g^{(k)}}(m) \otimes \mu^k_E - U_{g^{(k)}(m)} \otimes \rho^k_E\|_{\mathrm{tr}} \\
&= \delta(k) + \|\mu^k_E - \rho^k_E\|_{\mathrm{tr}} \\
&\leq 2\delta(k).
\end{aligned}$$

□

Next, we argue that the ClusterExpansion sub-protocol is an Input Secure randomness expansion scheme. The correctness of the ClusterExpansion sub-protocol assumes the correctness of VV and RUV protocols (Lemmas 14 and 15, respectively).

Theorem 13. *Let C be an Expansion Cluster. Suppose that a classical referee executes the* $\mathsf{ClusterExpansion}(C, S)$ *protocol, where S denotes the referee's classical register that holds an m-bit seed. Let E be an arbitrary quantum system that may be entangled with C, but cannot communicate with C once the protocol has started. If $\rho^i_{SC} = U_m \otimes \rho^i_C$, and* $\Pr(\mathsf{ClusterExpansion}(C, S)$ *succeeds)* $\geq \lambda \geq \exp(-C' m^{1/3})$ *for some universal constant C', then there exists a state τ_{XCE} such that $\tau_{XE} = U_{g(m)} \otimes \tau_E$ and*

$$\|\rho^f_{XCE} - \tau_{XCE}\|_{\mathrm{tr}} \leq \varepsilon_{\mathsf{EC}}(m, \lambda),$$

where $\varepsilon_{\mathsf{EC}}(m, \lambda) := \exp(-C'' m^{1/3})/\lambda$ for some universal constant C'', and ρ^f_{XCE} is the joint state of the protocol's output X, the cluster C, and E conditioned on the protocol $\mathsf{ClusterExpansion}(C, S)$ *succeeding.*

Proof. Let λ_1 denote the probability that Step 1 of $\mathsf{ClusterExpansion}(C, S)$ succeeds, and let λ_2 denote the probability that Step 2 of $\mathsf{ClusterExpansion}(C, S)$ succeeds, conditioned on Step 1 succeeding, so that $\lambda_1 \lambda_2 \geq \lambda$. Let C consist of devices $D = \{D_1, D_2\}$ and $G = \{G_1, G_2\}$, where the D_i's are used for execution of the VV protocol, and the G_j's are used for the execution of the RUV protocol. Let Y be the output of $\mathsf{VV}(D_1, D_2, S)$ (which is Step 1 of $\mathsf{ClusterExpansion}(C, S)$). By definition of the VV protocol, $|Y| = v(m)$. By Lemma 14 and our assumption on S (in particular, that $\rho^i_{SDG} = U_m \otimes \rho^i_{DG}$), there exists a state τ^v_{YDGE} such that $\tau^v_{YG} = U_{v(m)} \otimes \tau^v_G$ and

$$\|\rho^v_{YDGE} - \tau^v_{YDGE}\|_{\mathrm{tr}} \leq \varepsilon_{\mathsf{VV}}(m), \tag{2.1}$$

where ρ^v denotes the state of the system after running the VV protocol (and conditioned on it succeeding) but before executing the RUV protocol, and $\varepsilon_{\mathsf{VV}}(\cdot)$ is the error bound given by Lemma 14. Let X be the output of $\mathsf{RUV}(G_1, G_2, Y)$ (which is Step 2 of $\mathsf{ClusterExpansion}(C, S)$). By definition of the RUV protocol, $|X| = r(|Y|) = r(v(m))$.

Imagine that we executed the RUV protocol on the "ideal" input τ^v_{YDGE}. By Lemma 15,

we would get that there existed a state τ^f_{XDGE} such that $\tau^f_{XE} = U_{g(m)} \otimes \tau^f_E$, and

$$\|\rho^f_{XDGE} - \tau^f_{XDGE}\|_{\mathrm{tr}} \leq \varepsilon_{\mathsf{RUV}}(v(m), \lambda_2),$$

where $\varepsilon_{\mathsf{RUV}}(\cdot,\cdot)$ is the error bound given by Lemma 15. However, we only have the approximate guarantee on Y given by (2.1). So, by Lemma 5, we instead get that there exists a state τ^f_{XDGE} such that $\tau^f_{XE} = U_{g(m)} \otimes \tau^f_E$, and

$$\|\rho^f_{XDGE} - \tau^f_{XDGE}\|_{\mathrm{tr}} \leq \varepsilon_{\mathsf{RUV}}(v(m), \lambda_2) + \frac{\varepsilon_{\mathsf{VV}}(m)}{\lambda_2}.$$

Plugging in the expressions for $\varepsilon_{\mathsf{RUV}}$ and $\varepsilon_{\mathsf{VV}}$, we get that this is at most

$$\frac{1}{\lambda_2}(\sqrt{192(v(m)/4)^{-1/(8\alpha)}} + \sqrt{3\exp(-C'm^{1/3})}) \leq \exp(-C''m^{1/3})/\lambda,$$

for some universal constant C''. □

2.5.1 Analysis of the VV protocol

In the next two sections, we analyze that the VV and the RUV components of the ClusterExpansion sub-protocol. As discussed in the introduction, the VV protocol in a cluster C will provide near-exponential randomness expansion, although the analysis of [93] does not allow us to conclude that the output is secure against the other cluster C' (i.e. the Input Security Problem) [8]. The RUV protocol in C will be used to transform the output of VV to be secure against C'. Observe that, qualitatively, the RUV protocol solves the Input Security Problem because in Lemma 15, the random seed is not required to be secure against an eavesdropper, yet the output is guaranteed to be! On the other hand, Lemma 14 below requires the assumption that the seed to the VV protocol is secure against the protocol's devices and the eavesdropper simultaneously.

[8] See 2.2.2 for more about this issue.

Lemma 14. *Let D_1, D_2 be non-signaling quantum devices. Suppose that a classical referee executes the $\mathsf{VV}(D_1, D_2, S)$ protocol, where S denotes the referee's classical register that holds an m-bit seed. Let E be an arbitrary quantum system that may be entangled with D_1 and D_2, but cannot communicate with them once the protocol begins. If the initial joint state of S, D_1, D_2, and E is $\rho^0_{SD_1D_2E} = U_m \otimes \rho^0_{D_1D_2E}$, and if $\Pr(\mathsf{VV}(D_1, D_2, S)$ succeeds$) \geq \exp(-C'm^{1/3})$ for some universal constant C', then there exists a state τ_{XDE} where $\tau_{XE} = U_{v(m)} \otimes \rho^f_E$ and*

$$\|\rho^f_{XDE} - \tau_{XDE}\|_{\mathrm{tr}} \leq \varepsilon_{\mathsf{VV}}(m),$$

where ρ^f_{XDE} is the joint state of E, the devices $D = \{D_1, D_2\}$, and the output X of the protocol conditioned on the $\mathsf{VV}(D_1, D_2, S)$ protocol succeeding, $\varepsilon_{\mathsf{VV}}(m) = \sqrt{3\exp(-C'm^{1/3})}$, and $v(m) = \exp(C'm^{1/3})/2$.

Proof. The VV protocol consists of two parts, executing Protocol B of [93] using half of the seed S (which we denote by S_1) to produce an output Y of length $\exp(\Omega(m^{1/3}))$ which contains high min-entropy (conditioned on Protocol B not aborting), and then applying a randomness extractor using Y as the source, and the other half of S (which we denote by S_2) as the extractor seed, to produce an output X that is close to uniform.

Let ρ^v_{YE} denote the joint state of the output of Protocol B (Step 2 of the VV protocol) and the eavesdropper E, conditioned on Protocol B not aborting. Then, by our assumption on S and by Theorem 6, we get that $H^\varepsilon_\infty(Y|E)_{\rho^v} \geq h(m)$, where $h(m) = \exp(C'm^{1/3})$ and $\varepsilon = \varepsilon(m) = 1/h(m)$ for a universal constant C'.

The VV protocol then applies a quantum-secure randomness extractor to the source Y, with seed S_2. The protocol uses the $\mathsf{QExt} : \{0,1\}^{|Y|} \times \{0,1\}^{d(m)} \to \{0,1\}^{h(m)/2}$ randomness extractor promised by Theorem 8, where $d(m) = \Theta(m)$. Let $\tilde{\rho}_{YE}$ be a cq-state that is ε-close to ρ^v_{YE} in trace distance, and is such that $H_\infty(Y|E)_{\tilde{\rho}} \geq h(m)$ [9]. Then, since QExt is

[9] Although the definition of smoothed min-entropy quantifies over *all* density states in the ε-ball around ρ_{YE}, there exists a cq-state with high min-entropy in the ε-ball – see, e.g., [85].

a $(h(m), \varepsilon)$-quantum-secure extractor, we have that

$$\|\tilde{\rho}_{XE} - U_{v(m)} \otimes \tilde{\rho}_E\|_{\text{tr}} \leq \varepsilon, \tag{2.2}$$

where $\tilde{\rho}_{XE}$ is the joint state of the output X of the extractor QExt and E, with $\tilde{\rho}_Y$ as the source. View the application of QExt to the Y and S_2 register as a trace-preserving quantum operation $\mathcal{E}$, which takes states $\rho^v_{YS_2}$ and outputs states $\rho^f_{\text{QExt}(Y,S_2)}$. Then, by the triangle inequality, we have

$$\begin{aligned}\|\mathcal{E} \otimes \mathbb{1}_E(\rho^v_{YS_2E}) - U_{v(m)} \otimes \rho^f_E\|_{\text{tr}} \leq & \|\mathcal{E} \otimes \mathbb{1}_E(\rho^v_{YS_2E}) - \mathcal{E} \otimes \mathbb{1}_E(\tilde{\rho}_{YS_2E})\|_{\text{tr}} + \\ & \|\mathcal{E} \otimes \mathbb{1}_E(\tilde{\rho}_{YS_2E}) - U_{v(m)} \otimes \tilde{\rho}_E\|_{\text{tr}} + \\ & \|U_{v(m)} \otimes \tilde{\rho}_E - U_{v(m)} \otimes \rho^f_E\|_{\text{tr}}.\end{aligned}$$

Since $\mathcal{E}$ is trace-preserving, we can bound the first term by ε. The second term is bounded by ε via equation (2.2). The third term is bounded by ε because the trace distance is non-increasing with respect to the partial trace. Thus,

$$\|\rho^f_{XE} - U_{v(m)} \otimes \rho^f_E\|_{\text{tr}} = \|\mathcal{E} \otimes \mathbb{1}_E(\rho^v_{YS_2E}) - U_{v(m)} \otimes \rho^f_E\|_{\text{tr}} \leq 3\varepsilon.$$

We then apply Lemma 18 to obtain that there exists a state τ_{XDE} such that $\tau_{XE} = U_{v(m)} \otimes \rho^f_E$ and

$$\|\rho^f_{XDE} - \tau_{XDE}\|_{\text{tr}} \leq \sqrt{3\varepsilon}.$$

which proves the claim. □

2.5.2 Analysis of the RUV protocol

In this section, we analyze the RUV protocol. Before stating Lemma 15, it will be necessary to give formal and precise definitions of several (classical) random variables, and how they interact with the relevant quantum states.

Let S be an m-bit seed used in the RUV protocol, performed with non-signaling devices D_1 and D_2. Half of S, call it S_1, is used for N CHSH games, where $N = m/4$. Recall that we divide the N CHSH games into blocks of $t = N^{1/\alpha}$ consecutive games. Define the following random variables:

1. Let F denote the indicator variable that is 1 iff the RUV protocol doesn't abort in Step 4 (i.e. the devices win $\approx \cos^2(\pi/8)N$ CHSH games). Note that F is a deterministic function of the devices' outputs and S_1.

2. For all $i \in [N/t]$, let I_i denote the indicator variable that is 1 iff the devices D_1 and D_2 used a ζ-ideal strategy to produce their outputs in the ith block of CHSH games, where $\zeta := \kappa_* t^{-\kappa_*}$ (see Section 4.2 and [84] for more details about ideal strategies).

3. Let H denote the indicator variable that is 1 iff $G \geq (1-\nu)N/t$, where $G := \sum I_i$ and $\nu := (12/\sqrt{2})\sqrt{\log N t}/N^{1/4} \leq t^{-\alpha/8}$.

In our proof of Claim 15, we will consider states such as ρ_{FI_iXDE}, where X denotes the output of device D_1 after N CHSH games, D denotes the devices D_1 and D_2 together, E denotes an arbitrary quantum system, F will contain the classical bit indicating whether the devices aborted the RUV protocol or not, and I_i will contain a classical bit denoting whether the devices used a ζ-ideal strategy for block i. Because F and I_i are classical variables, ρ_{FI_iXDE} is a cccqq-state, and thus there is an ensemble $\{\rho_{DE}^{fqx}\}$ that represents the states of the D and E systems conditioned on the classical events $F = f$, $I_i = q$, and $X = x$, where

$$\rho_{FI_iXDE} := \sum_{f,q,x} \Pr(F = f, I_i = q, X = x) |f\rangle\langle f|_F \otimes |q\rangle\langle q|_{I_i} \otimes |x\rangle\langle x|_X \otimes \rho_{DE}^{fqx}.$$

Thus, we can meaningfully condition the state ρ_{FI_iXDE} on various values of F and I_i. For example, when we refer to the state $\rho_{XE|F=1}$, we mean the state that is, up to a normaliza-

tion factor,

$$\sum_q \Pr(F = 1, I_i = q, X = x)|x\rangle\langle x|_X \otimes \rho_{DE}^{1qx}.$$

In particular, we will make use of the fact that $\rho_{XE|F=1} = \Pr(I_i = 0|F = 1)\rho_{XE|I_i=0,F=1} + \Pr(I_i = 1|F = 1)\rho_{XE|I_i=1,F=1}$, where $\rho_{XE|I_i=q,F=1}$ is defined similarly to $\rho_{XE|F=1}$.

Lemma 15. *Let D_1, D_2 be non-signaling quantum devices. Suppose that a classical referee executes the $\mathsf{RUV}(D_1, D_2, S)$ protocol, where S denotes the referee's classical register that holds an m-bit seed. Let E be an arbitrary quantum system that may be entangled with D_1 and D_2, but cannot communicate with them once the protocol begins. If the initial joint state of S, D_1, and D_2 is $\rho^i_{SD_1D_2} = U_m \otimes \rho^i_{D_1D_2}$, and $\Pr(\mathsf{RUV}(D_1, D_2, S)$ succeeds$) \geq \lambda$, then, we have that there exists a state τ_{ZDE} where $\tau_{ZE} = U_{r(m)} \otimes \tau_E$, and*

$$\|\rho^f_{ZDE|F=1} - \tau_{ZDE}\|_{\mathrm{tr}} \leq \varepsilon_{\mathsf{RUV}}(m, \lambda),$$

where $\varepsilon_{\mathsf{RUV}}(m, \lambda) \leq \sqrt{192(m/4)^{-1/(8\alpha)}/\lambda}$, and where $\rho^f_{ZDE|F=1}$ is the joint state of E, the devices $D = \{D_1, D_2\}$, and the output Z of the protocol, conditioned on $F = 1$ (i.e. the $\mathsf{RUV}(D_1, D_2, S)$ protocol does not abort).

Proof. Let ρ^i_{XDFE} be the joint state of the X, D, F, and E registers *before* the N CHSH games are played (so X and F are initialized to the all 0 state). For this proof, we will assume that E is such that ρ^i_{XDFE} is a *pure state*. This is without loss of generality, because we can take a non-pure state ρ^i_{XDFE} and augment it with some extension $E' \supset E$ such that $\rho^i_{XDFE'}$ is pure (e.g. via a purification of the state ρ^i_{XDFE}). Observe that $\|\rho^f_{ZE'|F=1} - U_{r(m)} \otimes \rho^f_{E'|F=1}\|_{\mathrm{tr}} \leq \varepsilon$ implies $\|\rho^f_{ZE|F=1} - U_{r(m)} \otimes \rho^f_{E|F=1}\|_{\mathrm{tr}} \leq \varepsilon$, because the trace distance is non-increasing under discarding the augmented system $E'\backslash E$.

For notational clarity, we shall omit the superscripts i and f, because we focus on the state ρ_{FSXDE} of the system *after* the N CHSH games (i.e. the X register holds the output of device D_1), but *before* conditioning on $F = 1$ and before using the seed S_2 to select a sub-block. The i^{th} block of X will be denoted X_i, and the j^{th} sub-block of the i^{th} block will

be denoted X_{ij}.

There are two main components to this proof.

1. We argue that, for the state $\rho_{XE|F=1}$, there is a $1-\delta$ fraction of sub-blocks X_{ij} such that

$$\|\rho_{X_{ij}E|F=1} - U_{\sqrt{t}} \otimes \rho_{E|F=1}\|_{\mathrm{tr}} \leq \eta,$$

   where we set η and δ later in the proof. We say that such sub-blocks are η-good with respect to E.

2. We argue that the string S_2 (substring of the seed S used to select the sub-block that $\mathsf{RUV}(D_1, D_2, S)$ will output) is in tensor product with a string describing the locations of the η-good sub-blocks of the state $\rho_{XE|F=1}$.

In particular, let $Z := X_{S_2}$ denote the sub-block selected by string S_2. From the above two components, it follows that, for the state $\rho_{XE|F=1}$, the the random variable Z is $(\eta+\delta)$-good with respect to E, i.e.,

$$\|\rho_{ZE|F=1} - U_{\sqrt{t}} \otimes \rho_{E|F=1}\|_{\mathrm{tr}} \leq \eta + \delta.$$

We then invoke Lemma 18 to argue that there exists a state τ_{ZDE} such that $\tau_{ZE} = U_{\sqrt{t}} \otimes \rho_{E|F=1}$ and

$$\|\rho_{ZDE|F=1} - \tau_{ZDE}\|_{\mathrm{tr}} \leq \sqrt{\eta+\delta},$$

and we are done. We now proceed to proving the first two components.

There are many good sub-blocks. By the definition of I_i and Lemma 9,

$$\|\rho_{X_iE|I_i=1} - U_t \otimes \rho_{E|I_i=1}\|_{\mathrm{tr}} \leq \zeta.$$

It follows by Proposition 16 that, for at least a $1 - t^{-1/4}$ fraction of sub-blocks j of block i we have that

$$\|\rho_{X_{ij}EF|I_i=1} - U_{\sqrt{t}} \otimes \rho_{EF|I_i=1}\|_{\mathrm{tr}} \leq \mu,$$

where $\mu := 2(\sqrt{\zeta} + t^{-1/8})$. If we then condition on the event $F = 1$ it follows that

$$\|\rho_{X_{ij}E|I_i=1,F=1} - U_{\sqrt{t}} \otimes \rho_{E|I_i=1,F=1}\|_{\mathrm{tr}} \leq \frac{\mu}{\Pr(F=1)} \leq \frac{\mu}{\lambda} \tag{2.3}$$

We wish to establish the above statement for the state $\rho_{X_{ij}E|F=1}$ rather than the state $\rho_{X_{ij}E|I_i=1,F=1}$. The key to making this transition is to establish that, for many values of i, the event $F = 1$ is approximately a sub-event of the event $I_i = 1$. To do so, it is helpful to consider the event $H = 1$.

Let $M := N/t$ denote the number of blocks of CHSH games. It follows from the definition of H that $\sum_{i\in[M]} \mathbb{E}[I_i = 0|H = 1] \leq \nu M$. Thus, by Markov's inequality we have that at most a $\sqrt{\nu}$ fraction of blocks $i \in [M]$ are such that $\Pr(I_i = 0|H = 1) > \sqrt{\nu}$. Thus, at least a $1 - \sqrt{\nu}$ fraction of blocks $i \in [M]$ have $\Pr(I_i = 0|H = 1) \leq \sqrt{\nu}$.

Consider such a block i. Note that by Theorem 10, $\Pr(H = 0, F = 1) \leq t^{-2}$. Thus

$$\begin{aligned}
\Pr(I_i = 0, F = 1) &= \Pr(I_i = 0|H = 1, F = 1)\Pr(H = 1, F = 1) + \Pr(I_i = 0|H = 0, F = 1)\Pr(H = 0, F = \\
&\leq \Pr(I_i = 0|H = 1, F = 1) + \Pr(I_i = 0|H = 0, F = 1)t^{-2} \\
&\leq \frac{\Pr(I_i = 0|H = 1)}{\Pr(F = 1)} + t^{-2} \\
&\leq \frac{\sqrt{\nu}}{\lambda} + t^{-2}.
\end{aligned}$$

Since $I_i = 1$ is a classical event, we have $\rho_{XE|F=1} = (1-\tau)\rho_{XE|I_i=1,F=1} + \tau\rho_{XE|I_i=0,F=1}$, where $\tau := \Pr(I_i = 0|F = 1)$. Thus,

$$\begin{aligned}
\|\rho_{X_iE|F=1} - \rho_{X_iE|I_i=1,F=1}\|_{\mathrm{tr}} &= \|(-\tau)\rho_{X_iE|I_i=1,F=1} + \tau\rho_{X_iE|I_i=0,F=1}\|_{\mathrm{tr}} \\
&\leq \tau(\|\rho_{X_iE|I_i=1,F=1}\|_{\mathrm{tr}} + \|\rho_{X_iE|I_i=0,F=1}\|_{\mathrm{tr}}) \\
&\leq 2\tau.
\end{aligned}$$

By definition, $\tau = \Pr(I_i = 0, F = 1)/\Pr(F = 1)$. Thus,

$$\|\rho_{X_i E|I_i=1,F=1} - \rho_{X_i E|F=1}\|_{\mathrm{tr}} \leq 2\frac{\sqrt{\nu} + \lambda t^{-2}}{\lambda^2}$$

By tracing over all except the j^{th} sub-block we get

$$\|\rho_{X_{ij} E|I_i=1,F=1} - \rho_{X_{ij} E|F=1}\|_{\mathrm{tr}} \leq 2\frac{\sqrt{\nu} + \lambda t^{-2}}{\lambda^2} \tag{2.4}$$

By tracing over the entire X_i register we get

$$\|\rho_{E|I_i=1,F=1} - \rho_{E|F=1}\|_{\mathrm{tr}} \leq 2\frac{\sqrt{\nu} + \lambda t^{-2}}{\lambda^2} \tag{2.5}$$

Thus, at least a $(1 - t^{-1/4})(1 - \sqrt{\nu})$ of all the sub-blocks X_{ij} have the property that equations (2.3), (2.5), and (2.4) all hold. It follows by the triangle inequality that

$$\begin{aligned}
\|\rho_{X_{ij} E|F=1} - U_{\sqrt{t}} \otimes \rho_{E|F=1}\|_{\mathrm{tr}} &\leq \|\rho_{X_{ij} E|F=1} - \rho_{X_{ij} E|I_i=1,F=1}\|_{\mathrm{tr}} + \|\rho_{X_{ij} E|I_i=1,F=1} - U_{\sqrt{t}} \otimes \rho_{E|I_i=1,F=1}\|_{\mathrm{tr}} \\
&\quad + \|U_{\sqrt{t}} \otimes \rho_{E|I_i=1,F=1} - U_{\sqrt{t}} \otimes \rho_{E|F=1}\|_{\mathrm{tr}} \\
&\leq 2\frac{\sqrt{\nu} + \lambda t^{-2}}{\lambda^2} + \frac{\mu}{\lambda} + \|\rho_{E|I_i=1,F=1} - \rho_{E|F=1}\|_{\mathrm{tr}} \\
&\leq 4\left(\frac{\sqrt{\nu} + \lambda t^{-2}}{\lambda^2}\right) + \frac{\mu}{\lambda} \\
&\leq \frac{96}{\lambda} t^{-1/8}.
\end{aligned} \tag{2.6}$$

Define $\eta := 96t^{-1/8}/\lambda$. Thus, we have that at least a $1 - \delta$ fraction of the sub-blocks X_{ij} are η-good with respect to E, where $\delta := t^{-1/4} + \sqrt{\nu} \leq 2t^{-1/4}$. It is easy to see that $\eta + \delta \leq 2\eta = 192(m/4)^{-1/(8\alpha)}/\lambda$.

S_2 is secure against the location of good sub-blocks. Although we have established that most of the sub-blocks of X are η-good, we need to show that the seed S_2 used to select the sub-block for the output of the RUV protocol is independent of the locations of the good sub-blocks (i.e. the indices i, j such that X_{ij} is η-good with respect to E). *A priori*,

since S_2 is entangled with the eavesdropper E (because S_2 was the output of a different expansion cluster), it could be that S_2 was somehow adversarially generated to select a bad sub-block. Here, we show that this cannot happen, because the locations of the good sub-blocks can be *locally computed* by the devices $D = \{D_1, D_2\}$. Since $\rho^i_{SD} = U_m \otimes \rho^i_D$ (where $\rho^i_D := \rho_{D_1 D_2}$), S_2 is independent of the good sub-block locations.

Consider the following thought experiment: the system $D = \{D_1, D_2\}$ is augmented with a *classical description* Δ of the state ρ^i_{XFD}, and a register Λ that will store the locally computed location of the good sub-blocks, so that we have a new system $D' = \{D_1, D_2, \Delta, \Lambda\}$. Throughout the RUV protocol, the D' system cannot communicate with the eavesdropper system E. At the beginning of the RUV protocol, we have that $\rho_{SD'} = U_{|S|} \otimes \rho_{D'}$. Imagine that we have measured the S_1 register (but the S_2 register remains unmeasured), so that it is now a deterministic value s_1. Let $\mathcal{E}_{s_1}$ denote the quantum operation that acts on the systems D_1, D_2, F that represents the strategy employed by devices D_1 and D_2, on the inputs determined by s_1, for the N CHSH games (Step 3 of the RUV protocol). That is, $\rho^f_{XFD} := \mathcal{E}_{s_1}(\rho^i_{XFD})$.

As part of this thought experiment, we imagine that, after the N CHSH games, the Δ system performs a quantum operation $\mathcal{S}_{s_1}$ on the Δ, and Λ systems (but not D_1 and D_2!) to classically simulate the strategy used by the devices D_1, D_2 on input s_1 in the N CHSH games, and compute the location of the good sub-blocks. The Δ will then contain a classical description of the state ρ^f_{XFD}. Note that at this point, S_2 is still secure against D'; that is, we have

$$\mathcal{S}_{s_1}(\mathcal{E}_{s_1}(\rho^i_{S_2 XFD\Delta\Lambda})) = U_{|S_2|} \otimes \mathcal{S}_{s_1}(\mathcal{E}_{s_1}(\rho^i_{XFD\Delta\Lambda})).$$

We elaborate on the classical simulation $\mathcal{S}$. Given the classical description Δ of ρ^i_{XFD}, the location of the good sub-blocks can be computed by using Δ in the following way:

1. Compute the classical description of a purification $\sigma^i_{XFDE'}$ of the state ρ^i_{XFD}. Note that in general, $\sigma^i_{XFDE'}$ is different from the "real" state ρ^i_{XFDE}, because the Δ system has no knowledge of the external system E.

2. Classically simulate the devices' strategy $\mathcal{E}$ on the state $\sigma^i_{XFDE'}$, i.e.,

$$\sigma^f_{XFDE'} = \mathcal{E}_{s_1}(\sigma^i_{XFDE'}).$$

Note that $\sigma^f_{XFD} = \rho^f_{XFD}$.

3. Compute the indices i, j, such that

$$\|\sigma^f_{X_{ij}E'|F=1} - U_{\sqrt{t}} \otimes \sigma^f_{E'|F=1}\|_{\mathrm{tr}} \leq \eta,$$

and store those indices in a register Λ.

We now argue that Λ will contain an accurate description of the locations of the η-good sub-blocks in the "real" state ρ^f_{XFDE}. From this, since $\rho^f_{S_2\Lambda} = \rho^f_{S_2} \otimes \rho^f_{\Lambda}$, it follows that S_2 is independent of the good sub-block locations.

Here we will use the assumption, stated at the beginning of this proof, that ρ^i_{XFDE} is a pure state. Let $\rho^i_{XFDE} := |\psi\rangle\langle\psi|$, and let $\sigma^i_{XFDE'} := |\phi\rangle\langle\phi|$. There exists a unitary V that takes the E system to the E' system and acts as the identity on all other systems, such that $|\phi\rangle = V|\psi\rangle$. Since V and $\mathcal{E}_{s_1}$ act on different systems, they commute, and hence $\sigma^f_{XFDE'} = V\rho^f_{XFDE}V^\dagger$. Furthermore, V commutes with the projector $\Pi_{F=1}$ that projects onto the $F = 1$ subspace, and thus

$$\sigma^f_{XDE'|F=1} = V\rho^f_{XDE|F=1}V^\dagger.$$

Thus,

$$\begin{aligned}
\|\sigma^f_{X_{ij}E'|F=1} - U_{\sqrt{t}} \otimes \sigma^f_{E'|F=1}\|_{\mathrm{tr}} &= \|\mathrm{tr}_{\neq(i,j),D}(V\rho^f_{XDE|F=1}V^\dagger) - U_{\sqrt{t}} \otimes \mathrm{tr}_{XD}(V\rho^f_{XDE|F=1}V^\dagger)\|_{\mathrm{tr}} \\
&= \|V\left(\mathrm{tr}_{\neq(i,j),D}(\rho^f_{XDE|F=1}) - U_{\sqrt{t}} \otimes \mathrm{tr}_{XD}(\rho^f_{XDE|F=1})\right)V^\dagger\|_{\mathrm{tr}} \\
&= \|\mathrm{tr}_{\neq(i,j),D}(\rho^f_{XDE|F=1}) - U_{\sqrt{t}} \otimes \mathrm{tr}_{XD}(\rho^f_{XDE|F=1})\|_{\mathrm{tr}} \\
&= \|\rho^f_{X_{ij}E|F=1} - U_{\sqrt{t}} \otimes \rho^f_{E|F=1}\|_{\mathrm{tr}},
\end{aligned}$$

where $\mathrm{tr}_{\neq(i,j),D}$ indicates tracing out over all sub-blocks except for the jth one in the ith block, and the system D. The second equality follows from the fact that V and the partial trace commute. The third equality follows because the trace norm is unitarily invariant. Thus, the indices i, j where $\|\sigma^f_{X_{ij}E'|F=1} - U_{\sqrt{t}} \otimes \sigma^f_{E'|F=1}\|_{\mathrm{tr}} \leq \eta$ are exactly those sub-blocks that are η-good in the state ρ^f_{XFDE}.

□

Proposition 16. *Let $i \in [N/t]$ be the index of a block. If*

$$\|\rho_{X_iE|I_i=1} - U_t \otimes \rho_{E|I_i=1}\| \leq \zeta,$$

then for at least a $1 - t^{-1/4}$ fraction of sub-blocks j of block i we have that

$$\|\rho_{X_{ij}EF|I_i=1} - U_{\sqrt{t}} \otimes \rho_{EF|I_i=1}\| \leq 2(\sqrt{\zeta} + t^{-1/8}).$$

Proof. By Lemma 18, there exists a state σ_{X_iFE} such that $\sigma_{X_iE} = U_t \otimes \rho_{E|I_i=1}$, and $\|\rho_{X_iFE|I_i=1} - \sigma_{X_iFE}\|_{\mathrm{tr}} \leq \sqrt{\zeta}$. Let $R := \sqrt{t}$ denote the number of sub-blocks in a block. We now prove the Proposition by showing that, for the state σ_{X_iFE}, at least $1 - t^{-1/4}$ fraction of sub-block indices $j \in [R]$ satisfy $I(X_{ij} : FE)_\sigma \leq 2t^{-1/4}$. For such j, we obtain:

$$\begin{aligned}
\|\rho_{X_{ij}FE|I_i=1} - U_{\sqrt{t}} \otimes \rho_{FE|I_i=1}\|_{\mathrm{tr}} &\leq \|\rho_{X_{ij}FE|I_i=1} - \sigma_{X_{ij}FE}\|_{\mathrm{tr}} + \|\sigma_{X_{ij}FE} - U_{\sqrt{t}} \otimes \sigma_{FE}\|_{\mathrm{tr}} \\
&\quad + \|U_{\sqrt{t}} \otimes \sigma_{FE} - U_{\sqrt{t}} \otimes \rho_{FE|I_i=1}\|_{\mathrm{tr}} \\
&\leq \sqrt{\zeta} + \sqrt{4t^{-1/4}} + \sqrt{\zeta}.
\end{aligned}$$

The bound on the second term in the second inequality is given via Pinsker's Inequality (see Fact 4), which states that $\|\sigma_{X_{ij}FE} - U_{\sqrt{t}} \otimes \sigma_{FE}\|_{\mathrm{tr}} \leq \sqrt{2I(X_{ij} : FE)_\sigma}$. The bounds on the first and third terms come from the fact that the trace distance is non-increasing with respect to the partial trace.

Thus we focus on analyzing the state σ_{X_iFE} for the remainder of this proof. We apply the

chain rule to obtain $I(X_i : FE)_\sigma = \sum_j I(X_{ij} : FE|X_{i,<j})_\sigma$. This is equivalent to

$$\mathbb{E}_j[I(X_{ij} : FE|X_{i,<j})_\sigma] = \frac{1}{R} I(X_i : FE)_\sigma,$$

where $X_{i,<j}$ denotes all the X_{ik} such that $k < j$. We will omit the subscript σ because the underlying state is clear from context. We upper-bound the quantity $I(X_i : FE)$ via the following calculation:

$$\begin{aligned}
I(X_i : FE) &= H(X_i) - H(X_i|FE) && (2.7)\\
&= H(X_i) - (H(X_iFE) - H(FE)) && (2.8)\\
&= H(X_i) - (H(X_iFE) - H(E) - H(F|E)) && (2.9)\\
&= H(X_i) - (H(X_iE) + H(F|X_iE) - H(E) - H(F|E)) && (2.10)\\
&= H(X_i) - (H(X_i) + H(E) + H(F|X_iE) - H(E) - H(F|E)) && (2.11)\\
&= H(F|E) - H(F|X_iE) && (2.12)\\
&\leq 2H(F) && (2.13)\\
&\leq 2 && (2.14)
\end{aligned}$$

Equation (2.7) is the definition of mutual information. Equations (2.8), (2.9), and (2.10) follow from the definition of conditional mutual entropy. Equation (2.11) follows from our assumption that $\sigma_{X_iE} = \sigma_{X_i} \otimes \sigma_E$. Equation (2.13) follows from the fact that conditioning can only reduce entropy, and that $-H(F|X_iE) \leq H(F)$.

We now lower bound the individual terms of the expectation $I(X_{ij} : FE|X_{i,<j})$.

$$\begin{aligned}
I(X_{ij} : FE|X_{i,<j}) &= H(X_{ij}|X_{i,<j}) - H(X_{ij}|FEX_{i,<j}) && (2.15)\\
&\geq H(X_{ij}) - H(X_{ij}|FE) && (2.16)\\
&= I(X_{ij} : FE). && (2.17)
\end{aligned}$$

Equation (2.15) is the definition of conditional mutual information. Equation (2.16) fol-

lows because $\sigma_{X_i} = U_t$ (hence $\sigma_{X_{ij}}$ is in tensor product with $\sigma_{X_{i,<j}}$), and conditioning can only reduce entropy. Finally, equation (2.17) is again the definition of mutual information. Thus,

$$\mathbb{E}_j[I(X_{ij} : FE)] \leq \frac{2}{R},$$

and by Markov's inequality, we get that $1 - \mu$ fraction of j's are such that $I(X_{ij} : FE) \leq \frac{2}{\mu R}$. Setting $\mu = t^{-1/4}$ completes the proof. □

2.6 Conclusion

We have presented a randomness expansion protocol that achieves infinite expansion: starting with m bits of uniform seed, the protocol produces an arbitrarily long output string that is $\exp(-\Omega(m^{\frac{1}{3}}))$-close to uniform. Furthermore, this protocol only requires eight non-signaling quantum devices (and can be performed with just six devices using a simple modification). In order to accomplish this we design an *Input Secure* adaptive randomness expansion protocol, which is then used as a sub-protocol in the infinite expansion protocol. We suspect that the existence of Input Secure randomness expansion protocols is also of independent interest. As evidence of their independent interest we note that Input Secure protocols play a key role as a building block in [16], where they were discovered independently from this work, and used to design a protocol for seedless randomness amplification from any min-entropy source (see Section 2.2.2).

Appendix A

A.1 Proof of Lemma 5

Proof of Lemma 5. Define μ_{XDE} to be the state τ_{XDE} as given by the assumption in the lemma on input σ_{FSXDE} where $\sigma_{FSXD} = \sigma_{FSX} \otimes \sigma_D$. By the triangle inequality, we have:

$$\begin{aligned} \|\rho^f_{XDE} - \mu_{XDE}\|_{\mathrm{tr}} \leq & \|\mathcal{F}\mathcal{E} \otimes \mathbb{1}_E(\rho^i_{FSXDE}) - \mathcal{F}\mathcal{E} \otimes \mathbb{1}_E(\sigma_{FSXDE})\|_{\mathrm{tr}} \\ & + \|\mathcal{F}\mathcal{E} \otimes \mathbb{1}_E(\sigma_{FSXDE}) - \mu_{XDE}\|_{\mathrm{tr}}. \end{aligned} \tag{A.1}$$

We bound the first term on the right hand side:

$$\begin{aligned} \|\mathcal{F}\mathcal{E} \otimes \mathbb{1}_E(\rho^i_{FSXDE}) - \mathcal{F}\mathcal{E} \otimes \mathbb{1}_E(\sigma_{FSXDE})\|_{\mathrm{tr}} &\leq \frac{1}{\lambda}\|\mathcal{E} \otimes \mathbb{1}_E(\rho^i_{FSXDE}) - \mathcal{E} \otimes \mathbb{1}_E(\sigma_{FSXDE})\|_{\mathrm{tr}} \\ &\leq \frac{1}{\lambda}\|\rho^i_{FSXDE} - \sigma_{FSXDE}\|_{\mathrm{tr}} \\ &\leq \delta/\lambda. \end{aligned}$$

Let λ' denote the probability that the F register of the state $\mathcal{E} \otimes \mathbb{1}_E(\sigma_{FSXDE})$, when measured, has outcome $|1\rangle$. Note that $\max\{\lambda, \lambda'\} \geq \lambda$, so the first inequality follows from Lemma 17. The second inequality follows because trace-preserving quantum operations are contractive with respect to the trace distance. The final inequality comes from our assumption on ρ^i_{FSXDE}.

The second term on the right hand side of (A.1) is bounded by ε from our assumption on the quantum operation $\mathcal{FE}$. □

A.2 Useful lemmata

Lemma 17. *Let ρ_{FQ}, σ_{FQ} be cq-states on the same classical-quantum Hilbert space $\mathcal{H}_F \otimes \mathcal{H}_Q$. Let E be a set of outcomes of the F register such that $\min\{\Pr_\rho(E), \Pr_\sigma(E)\} > 0$, where $\Pr_\rho(E)$, $\Pr_\sigma(E)$ denote the probabilities of obtaining outcome E when measuring ρ_F and σ_F in the computational basis. Then,*

$$\|\rho_{FQ|E} - \sigma_{FQ|E}\|_{\mathrm{tr}} \leq \frac{\|\rho_{FQ} - \sigma_{FQ}\|_{\mathrm{tr}}}{\max\{\Pr_\rho(E), \Pr_\sigma(E)\}},$$

where $\rho_{FQ|E}$ and $\sigma_{FQ|E}$ denote the post-measurement state of ρ_{FQ} and σ_{FQ}, respectively, conditioned on E.

Proof. We use the operational interpretation of the trace norm of two quantum states, namely, that $\|\rho - \sigma\|_{\mathrm{tr}} = \max_A \Pr(A(\rho) = 1) - \Pr(A(\sigma) = 1)$, where ρ and σ are arbitrary density matrices, and the maximization is over all possible 0/1-valued POVMs A.

Let λ_ρ and λ_σ denote $\Pr_\rho(E)$ and $\Pr_\sigma(E)$ respectively. We consider two cases: $\lambda_\rho \geq \lambda_\sigma$ and $\lambda_\rho < \lambda_\sigma$. Take the first case.

Consider the following two-outcome experiment A that tries to distinguish between ρ_{FQ} and σ_{FQ}. We first measure the F register in the computational basis. If the outcome E does not occur, we output "0". Suppose outcome E does occur. Let B be the optimal two-outcome POVM such that $\Pr(B(\rho_{FQ|E}) = 1) - \Pr(B(\sigma_{FQ|E}) = 1) = \|\rho_{FQ|E} - \sigma_{FQ|E}\|_{\mathrm{tr}}$. We then make the measurement dictated by B on the post-measurement state (which is either

$\rho_{FQ|E}$ or $\sigma_{FQ|E}$), and output "1" iff B outputs "1". Then, we have that

$$\begin{aligned}\|\rho_{FQ} - \sigma_{FQ}\|_{\mathrm{tr}} &\geq \Pr(A(\rho_{FQ}) = 1) - \Pr(A(\sigma_{FQ}) = 1) \\ &= \lambda_\rho \Pr(B(\rho_{FQ|E}) = 1) - \lambda_\sigma \Pr(B(\sigma_{FQ|E}) = 1) \\ &= \lambda_\rho \left(\|\rho_{FQ|E} - \sigma_{FQ|E}\|_{\mathrm{tr}} + \Pr(B(\sigma_{FQ|E}) = 1) \right) - \lambda_\sigma \Pr(B(\sigma_{FQ|E}) = 1).\end{aligned}$$

Solving for $\|\rho_{FQ|E} - \sigma_{FQ|E}\|_{\mathrm{tr}}$, we get that

$$\|\rho_{FQ|E} - \sigma_{FQ|E}\|_{\mathrm{tr}} \leq \frac{\|\rho_{FQ} - \sigma_{FQ}\|_{\mathrm{tr}} - \beta(\lambda_\rho - \lambda_\sigma)}{\lambda_\rho} \leq \frac{\|\rho_{FQ} - \sigma_{FQ}\|_{\mathrm{tr}}}{\lambda_\rho} \leq \frac{\|\rho_{FQ} - \sigma_{FQ}\|_{\mathrm{tr}}}{\max\{\lambda_\rho, \lambda_\sigma\}},$$

where $\beta := \Pr(B(\sigma_{FQ|E}) = 1)$. In the other case, we have that $\lambda_\rho < \lambda_\sigma$. We can then switch the order of ρ_{FQ} and σ_{FQ} in the previous argument, and obtain that

$$\|\rho_{FQ|E} - \sigma_{FQ|E}\|_{\mathrm{tr}} \leq \frac{\|\rho_{FQ} - \sigma_{FQ}\|_{\mathrm{tr}}}{\lambda_\sigma} \leq \frac{\|\rho_{FQ} - \sigma_{FQ}\|_{\mathrm{tr}}}{\max\{\lambda_\rho, \lambda_\sigma\}}.$$

□

Lemma 18. *Let $\rho_{A_1A_2B} \in \mathcal{D}(\mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2} \otimes \mathcal{H}_B)$, and $\sigma_{A_1A_2} \in \mathcal{D}(\mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2})$ be such that $\rho_{A_1A_2B}$ is a cqq-state, $\sigma_{A_1A_2}$ is a cq-state, and $\|\rho_{A_1A_2} - \sigma_{A_1A_2}\|_{\mathrm{tr}} \leq \varepsilon$. Then there exists a cqq-state $\tau_{A_1A_2B} \in \mathcal{D}(\mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2} \otimes \mathcal{H}_B)$ such that $\tau_{A_1A_2} = \sigma_{A_1A_2}$ and $\|\rho_{A_1A_2B} - \tau_{A_1A_2B}\|_{\mathrm{tr}} \leq \sqrt{\varepsilon}$.*

Proof. For notational brevity we will let $A = \{A_1, A_2\}$ so $\rho_{AB} := \rho_{A_1A_2B}$ and $\sigma_A := \sigma_{A_1A_2}$. Let $\mathcal{F}(\rho, \sigma)$ denote the fidelity between two quantum states ρ and σ. By Uhlmann's Theorem, there exists purifications $\rho_{AQ} := |\psi\rangle\langle\psi|$ and $\sigma_{AQ} := |\phi\rangle\langle\phi|$ of ρ_A and σ_A, respectively, such that $\mathcal{F}(\rho_A, \sigma_A) = |\langle\psi|\phi\rangle|$ [98]. But by the Fuchs-van de Graaf inequalities, we also have that $\mathcal{F}(\rho_A, \sigma_A) \geq 1 - \|\rho_A - \sigma_A\|_{\mathrm{tr}}/2 \geq 1 - \varepsilon/2$ [98]. Since $\|\rho_{AQ} - \sigma_{AQ}\|_{\mathrm{tr}} = \sqrt{1 - |\langle\psi|\phi\rangle|^2}$, we have that

$$\|\rho_{AQ} - \sigma_{AQ}\|_{\mathrm{tr}} \leq \sqrt{\varepsilon}.$$

Let $\rho_{ABR} = |\theta\rangle\langle\theta|$ be a purification of the state ρ_{AB}. Since ρ_{ABR} and ρ_{AQ} are both purifica-

tions of the state ρ_A, there exists a unitary map V that takes the Q space to the BR space such that $\rho_{ABR} = V\rho_{AQ}V^\dagger$. Define $\tau'_{ABR} := V\sigma_{AQ}V^\dagger$. Then, by the unitary invariance of the trace norm, we have that

$$\begin{aligned}
\|\rho_{ABR} - \tau'_{ABR}\|_{\mathrm{tr}} &= \|V\rho_{AQ}V^\dagger - V\tau'_{AQ}V^\dagger\|_{\mathrm{tr}} \\
&= \|V(\rho_{AQ} - \tau'_{AQ})V^\dagger\|_{\mathrm{tr}} \\
&= \|\rho_{AQ} - \tau'_{AQ}\|_{\mathrm{tr}} \\
&\leq \sqrt{\varepsilon}.
\end{aligned}$$

Since the trace norm cannot increase when discarding subsystems, we obtain $\|\rho_{AB} - \tau'_{AB}\|_{\mathrm{tr}} \leq \sqrt{\varepsilon}$. $\tau'_{AB} = \tau'_{A_1A_2B}$ is not guaranteed to be a cqq-state, but we can apply the trace-preserving quantum map $\mathcal{E}$ that measures the A_1 system in the computational basis and forgets the measurement outcome. Let $\tau_{A_1A_2B} := \mathcal{E}(\tau'_{A_1A_2B})$, and observe that this is a cqq-state. Since $\rho_{A_1A_2B}$ is already a cqq-state, $\rho_{A_1A_2B} = \mathcal{E}(\rho_{A_1A_2B})$. Because trace-preserving quantum maps are contractive under the trace norm, we obtain $\|\rho_{A_1A_2B} - \tau_{A_1A_2B}\|_{\mathrm{tr}} \leq \sqrt{\varepsilon}$, and we are done. □

A.3 Parameter settings for the VV sub-protocol

For the sake of concreteness, we specify the settings of parameters to be used in the instantiation of Protocol B of [93] in our VV sub-protocol (see Section 2.4). We choose constants $\alpha, \gamma > 0$ such that $\gamma \leq 1/(10 + 8\alpha)$. These constants are part of the definition of VV and will remain unchanged for every instance of VV throughout the InfiniteExpansion protocol.

In [93, Theorem 2], the parameter h specifies the min-entropy lower bound of Protocol B, which in turn governs the length of the seed to Protocol B and length of the output. By definition Protocol B implemented with parameter h requires at most $K_1\gamma^{-3}\log^3(h)$ bits of seed for some fixed constant K_1 (this constant may depend on α, but since α is a global constant here, we ignore this). When Protocol B is invoked by $\mathsf{VV}(A, B, S)$, we

will set $h = \left\lfloor 2^{\gamma\left(\lfloor s/2 \rfloor \frac{1}{K_1}\right)^{1/3}} \right\rfloor$, where $s := |S|$, and it follows that Protocol B, with these parameters, will require no more than $\lfloor s/2 \rfloor$ bits of seed.

We will now discuss parameters relevant to the quantum extractor which will be used in VV. Let us now define $t := h^{\frac{1}{\gamma}}$, $C := \lceil 100\alpha \rceil$ and $\varepsilon := \frac{1}{h}$. The output of Protocol B is a bit string of length $n := \lceil 10 \log^2(t) \rceil \cdot \lceil Ct \log^2(t) \rceil$. By Theorem 8 there exists a function $\mathsf{QExt} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^{\frac{h}{2}}$ that is a $(\frac{h}{2} + O(\log\left(\frac{h}{2}\right)) + O(\log 1/\varepsilon), \varepsilon)$-quantum-secure extractor as long as $d \geq O\left(\log^2(n/\varepsilon) \log\left(\frac{h}{2}\right)\right) = O\left(\log^3(h)\right) = O\left(\gamma^3 \lfloor s/2 \rfloor \frac{1}{K_1}\right)$. That is, as long as $d \geq K_4 \gamma^3 \lfloor s/2 \rfloor \frac{1}{K_1}$ for some fixed constant K_4.

Thus, in specifying the VV sub-protocol and throughout the chapter, we will set the following functions, where s is the length of input to the VV sub-protocol:

- Min-entropy lower bound of Protocol B:

$$h(s) := \left\lfloor 2^{\gamma\left(\lfloor s/2 \rfloor \frac{1}{K_1}\right)^{1/3}} \right\rfloor.$$

- Output length of Protocol B:

$$n(s) := \left\lfloor 10C \left(\frac{s}{2K_1}\right)^{4/3} 2^{(s/(2K_1))^{1/3}} \right\rfloor.$$

- Seed length of the extractor:

$$d(s) := \left\lceil \frac{K_4}{K_1} \gamma^3 \lfloor s/2 \rfloor \right\rceil.$$

- Output length of the extractor/VV sub-protocol:

$$v(s) := \lfloor h(s)/2 \rfloor.$$

Chapter 3

The Parallel-Repeated Magic Square Game is Rigid

In this chapter 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.

3.1 Introduction

Nonlocal games have long been a fundamental topic in quantum information, starting from Bell's pioneering work in the 1960s. In the langauge of games, Bell [10] showed that for a certain two-player nonlocal game, two players sharing a single 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 [17]

discovered a game (called the CHSH game) with similar properties, but with messages consisting of just one bit. The CHSH game can be viewed as 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 [91], even the optimal quantum strategy succeeds with probability at most $(2+\sqrt{2})/4 \approx 0.854$. To remedy this drawback, Mermin [67] and independently Peres [77] 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 [59] 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 it required the CHSH correlations to hold *exactly*: however, the subsequent work of McKague, Yang, and Scarani [62] was able to achieve a robust self-test based on CHSH 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. More recently, Wu et al. [99] showed rigidity for Mermin and Peres's

[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.

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*) [83]. 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 [83] uses a serially repeated CHSH test, and McKague [64] 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 chapter, 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 [64], 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

[2]Note that, by repeating the test in section 4 of [64] 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.

round of the Magic Square game, which was established in [99]. 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 [99], to a full n-round set of approximate anti-commutation relations for the provers measurements, which is expressed in Theorem 25. A second important technical tool in our proof is a theorem (Theorem 26) 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 26 relies on an isometry inspired by the works of McKague [63, 65], but is designed to take the guarantees produced by Theorem 25 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 [15], which proves a theorem similar to our Theorem 26. The second is a paper by Coladangelo [20], 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 [20] makes use of the same key theorem of [15], which is, in turn, similar to our own Theorem 26. The theorem of [15] (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 26 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.

3.2 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 chapter, 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

$$XZ = -ZX.$$

3.3 The Magic Square game

In this section we introduce the nonlocal game analyzed in this chapter: 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 [67] and Peres [77]. The rules of the game are described in Fig. 3-1.

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 3-1: The magic square game

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. 3-2, 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 3-2: The ideal strategy for a single round of magic square. Alice and Bob share the state $|\text{EPR}\rangle^{\otimes 2}$.

The game we study in this chapter is the n-fold parallel repetition of the above game.

Definition 19. *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 chapter we will refer to the non-local entangled strategy applied by the players according to the following definitions:

Definition 20. *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 21. *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 22. *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 3.3.1. 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 23. *Suppose Alice and Bob win the magic square game with probability $\geq 1-\varepsilon$. Then it holds that*

$$\forall \mathbf{p}, \quad \mathbb{E}_{\mathbf{r},\mathbf{c}} \langle \psi | A^{\mathbf{c}}_{\mathbf{r},\mathbf{p}} B^{\mathbf{r}}_{\mathbf{c},\mathbf{p}} | \psi \rangle \geq 1-\varepsilon. \tag{3.1}$$

In Remark 3.3.1, 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 24. *Suppose Alice and Bob have an ε-optimal strategy. Then, $\forall i, r, \mathbf{c}$,*

$$\left| 1 - \mathbb{E}_{\mathbf{r},\mathbf{r}' : r'_i = r_i = r} \langle \psi | A^{\mathbf{c}}_{\mathbf{r},\mathbf{e}_i} \cdot A^{\mathbf{c}}_{\mathbf{r}',\mathbf{e}_i} | \psi \rangle \right| \leq 36\varepsilon$$

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:

$$T \equiv \sum_{\mathbf{r}_{-i}} A^{\mathbf{c}}_{\mathbf{r},\mathbf{e}_i} \otimes |\mathbf{r}_{-i}\rangle\langle \mathbf{r}_{-i}| \otimes I \otimes I = \sum_{\mathbf{r}_{-i}} \sum_{\mathbf{s}_{-i}} A^{c_i \cup \mathbf{s}_{-i}}_{\mathbf{r},\mathbf{e}_i} \otimes |\mathbf{r}_{-i}\rangle\langle \mathbf{r}_{-i}| \otimes I \otimes |\mathbf{s}_{-i}\rangle\langle \mathbf{s}_{-i}|$$

Note that, by Remark 3.3.1, these two definitions are equivalent because $A^{\mathbf{c}}_{\mathbf{r},\cdot\mathbf{e}_i}$ is identically equal to $A^{c_i \cup \mathbf{s}_{-i}}_{\mathbf{r},\cdot\mathbf{e}_i}$ by definition, regardless of the value of $\mathbf{s}_{-i}$. Further define

$$T' \equiv \sum_{\mathbf{r}'_{-i}} A^{\mathbf{c}}_{\mathbf{r}',\mathbf{e}_i} \otimes I \otimes |\mathbf{r}'_{-i}\rangle\langle \mathbf{r}'_{-i}| \otimes I = \sum_{\mathbf{r}'_{-i}} \sum_{\mathbf{s}_{-i}} A^{c_i \cup \mathbf{s}_{-i}}_{\mathbf{r}',\mathbf{e}_i} \otimes I \otimes |\mathbf{r}'_{-i}\rangle\langle \mathbf{r}'_{-i}| \otimes |\mathbf{s}_{-i}\rangle\langle \mathbf{s}_{-i}|$$

and

$$
\begin{aligned}
S &\equiv \sum_{\mathbf{r}_{-i}} \sum_{\mathbf{s}_{-i}} B^{r_i \cup \mathbf{r}_{-i}}_{\mathbf{c}_i \cup s_{-i}, \mathbf{e}_i} \otimes |\mathbf{r}_{-i}\rangle\langle \mathbf{r}_{-i}| \otimes I \otimes |\mathbf{s}_{-i}\rangle\langle \mathbf{s}_{-i}| \\
&= \sum_{\mathbf{r}_{-i}} \sum_{\mathbf{s}_{-i}} B^{r_i \cup \mathbf{r}_{-i}}_{\mathbf{c}_i \cup s_{-i}, \mathbf{e}_i} \otimes |\mathbf{r}_{-i}\rangle\langle \mathbf{r}_{-i}| \otimes \sum_{\mathbf{r}'_{-i}} |\mathbf{r}'_{-i}\rangle\langle \mathbf{r}'_{-i}| \otimes |\mathbf{s}_{-i}\rangle\langle \mathbf{s}_{-i}| \\
&= \sum_{\mathbf{r}'_{-i}} \sum_{\mathbf{s}_{-i}} B^{r'_i \cup \mathbf{r}'_{-i}}_{\mathbf{c}_i \cup s_{-i}, \mathbf{e}_i} \otimes \sum_{\mathbf{r}_{-i}} |\mathbf{r}_{-i}\rangle\langle \mathbf{r}_{-i}| \otimes |\mathbf{r}'_{-i}\rangle\langle \mathbf{r}'_{-i}| \otimes |\mathbf{s}_{-i}\rangle\langle \mathbf{s}_{-i}| \\
&= \sum_{\mathbf{r}'_{-i}} \sum_{\mathbf{s}_{-i}} B^{r_i \cup \mathbf{r}'_{-i}}_{\mathbf{c}_i \cup s_{-i}, \mathbf{e}_i} \otimes I \otimes |\mathbf{r}'_{-i}\rangle\langle \mathbf{r}'_{-i}| \otimes |\mathbf{s}_{-i}\rangle\langle \mathbf{s}_{-i}|
\end{aligned}
$$

Where, to conclude equivalence of the different versions of the last definition, we are using Remark 3.3.1 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) \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) \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 = \mathbb{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 follows by Fact 23. Similarly,

$$\begin{aligned}
\langle\sigma|T'\cdot S|\sigma\rangle &= \left(\langle\psi|\otimes\frac{1}{\sqrt{3^{-(n-1)}}}\sum_{\mathbf{r}_{-i}}\langle\mathbf{r}_{-i}|\otimes\frac{1}{\sqrt{3^{-(n-1)}}}\sum_{\mathbf{r}'_{-i}}\langle\mathbf{r}'_{-i}|\otimes\frac{1}{\sqrt{3^{-(n-1)}}}\sum_{\mathbf{s}_{-i}}\langle\mathbf{s}_{-i}|\right)\\
&\times\left(\sum_{\mathbf{r}'_{-i}}\sum_{\mathbf{s}_{-i}}A^{c_i\cup\mathbf{s}_{-i}}_{\mathbf{r}',\mathbf{e}_i}\otimes I\otimes|\mathbf{r}'_{-i}\rangle\langle\mathbf{r}'_{-i}|\otimes|\mathbf{s}_{-i}\rangle\langle\mathbf{s}_{-i}|\right)\left(\sum_{\mathbf{r}'_{-i}}\sum_{\mathbf{s}_{-i}}B^{r_i\cup\mathbf{r}'_{-i}}_{\mathbf{c}_i\cup s_{-i},\mathbf{e}_i}\otimes I\otimes|\mathbf{r}'_{-i}\rangle\langle\mathbf{r}'_{-i}|\otimes|\mathbf{s}_{-i}\rangle\langle\mathbf{s}_{-i}|\right)\\
&\times\left(|\psi\rangle\otimes\frac{1}{\sqrt{3^{-(n-1)}}}\sum_{\mathbf{r}_{-i}}|\mathbf{r}_{-i}\rangle\otimes\frac{1}{\sqrt{3^{-(n-1)}}}\sum_{\mathbf{r}'_{-i}}|\mathbf{r}'_{-i}\rangle\otimes\frac{1}{\sqrt{3^{-(n-1)}}}\sum_{\mathbf{s}_{-i}}|\mathbf{s}_{-i}\rangle\right)\\
&=\frac{1}{3^{-2(n-1)}}\sum_{\mathbf{r}'_{-i},\mathbf{s}_{-i}}\langle\psi|A^{c_i\cup\mathbf{s}_{-i}}_{\mathbf{r}',\mathbf{e}_i}B^{r_i\cup\mathbf{r}'_{-i}}_{\mathbf{c}_i\cup s_{-i},\mathbf{e}_i}|\psi\rangle\cdot\left(\frac{1}{\sqrt{3^{-(n-1)}}}\sum_{\mathbf{r}_{-i}}\langle\mathbf{r}_{-i}|\right)\left(\frac{1}{\sqrt{3^{-(n-1)}}}\sum_{\mathbf{r}_{-i}}|\mathbf{r}_{-i}\rangle\right)\\
&=\frac{1}{3^{-2(n-1)}}\sum_{\mathbf{r}'_{-i},\mathbf{s}_{-i}}\langle\psi|A^{c_i\cup\mathbf{s}_{-i}}_{\mathbf{r}',\mathbf{e}_i}B^{r_i\cup\mathbf{r}'_{-i}}_{\mathbf{c}_i\cup s_{-i},\mathbf{e}_i}|\psi\rangle=\mathbb{E}_{\mathbf{r}'_{-i},\mathbf{s}_{-i}}\langle\psi|A^{c_i\cup\mathbf{s}_{-i}}_{\mathbf{r}',\mathbf{e}_i}B^{r_i\cup\mathbf{r}'_{-i}}_{\mathbf{c}_i\cup s_{-i},\mathbf{e}_i}|\psi\rangle\geq 1-9\varepsilon
\end{aligned}$$

Where the last line again follows by Fact 23. It follows by Lemma 47, that

$$\langle\sigma|T\cdot T'|\sigma\rangle\geq 1-36\varepsilon$$

Noting that

$$\begin{aligned}
\langle\sigma|T\cdot T'|\sigma\rangle &= \left(\langle\psi|\otimes\frac{1}{\sqrt{3^{-(n-1)}}}\sum_{\mathbf{r}_{-i}}\langle\mathbf{r}_{-i}|\otimes\frac{1}{\sqrt{3^{-(n-1)}}}\sum_{\mathbf{r}'_{-i}}\langle\mathbf{r}'_{-i}|\otimes\frac{1}{\sqrt{3^{-(n-1)}}}\sum_{\mathbf{s}_{-i}}\langle\mathbf{s}_{-i}|\right)\\
&\times\left(\sum_{\mathbf{r}_{-i}}A^{\mathbf{c}}_{\mathbf{r},\mathbf{e}_i}\otimes|\mathbf{r}_{-i}\rangle\langle\mathbf{r}_{-i}|\otimes I\otimes I\right)\left(\sum_{\mathbf{r}'_{-i}}A^{\mathbf{c}}_{\mathbf{r}',\mathbf{e}_i}\otimes I\otimes|\mathbf{r}'_{-i}\rangle\langle\mathbf{r}'_{-i}|\otimes I\right)\\
&\times\left(|\psi\rangle\otimes\frac{1}{\sqrt{3^{-(n-1)}}}\sum_{\mathbf{r}_{-i}}|\mathbf{r}_{-i}\rangle\otimes\frac{1}{\sqrt{3^{-(n-1)}}}\sum_{\mathbf{r}'_{-i}}|\mathbf{r}'_{-i}\rangle\otimes\frac{1}{\sqrt{3^{-(n-1)}}}\sum_{\mathbf{s}_{-i}}|\mathbf{s}_{-i}\rangle\right)\\
&=\frac{1}{3^{-2(n-1)}}\sum_{\mathbf{r}_{-i},\mathbf{r}'_{-i}}\langle\psi|A^{\mathbf{c}}_{\mathbf{r},\mathbf{e}_i}A^{\mathbf{c}}_{\mathbf{r}',\mathbf{e}_i}|\psi\rangle=\mathbb{E}_{\mathbf{r}_{-i},\mathbf{r}'_{-i}::r'_i=r_i=r}\langle\psi|A^{\mathbf{c}}_{\mathbf{r},\mathbf{e}_i}A^{\mathbf{c}}_{\mathbf{r}',\mathbf{e}_i}|\psi\rangle
\end{aligned}$$

So, we have,

$$\left|1 - \mathbb{E}_{\mathbf{r},\mathbf{r}':r'_i=r_i=r} \langle\psi| A^{\mathbf{c}}_{\mathbf{r},\mathbf{e}_i} \cdot A^{\mathbf{c}}_{\mathbf{r}',\mathbf{e}_i} |\psi\rangle\right| = \left|1 - \langle\sigma| T \cdot T' |\sigma\rangle\right| \leq 36\varepsilon$$

□

3.4 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.

3.4.1 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. For a single round of Magic Square one expects to be able to derive these results directly from previously existing rigidity results. The novelty of our result is to produce a rigidity statement which shows that individual rounds of the parallel repeated game must nearly commute with each other, where the commutation bound is polynomial in the number of rounds. That is the key to proving the following theorem.

Theorem 25. *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

$$\begin{aligned} &\forall k, r, c, r', c', \qquad d_{\psi'}(\tilde{A}^{c}_{r,k}\tilde{A}^{c'}_{r',k}, (-1)^{f(r,r',c,c')}\tilde{A}^{c'}_{r',k}\tilde{A}^{c}_{r,k}) \quad \leq O(\sqrt{\varepsilon}) \\ &\forall k \neq k', r, c, r', c', \qquad d_{\psi'}(\tilde{A}^{c}_{r,k}\tilde{A}^{c'}_{r',k'}, \tilde{A}^{c'}_{r',k'}\tilde{A}^{c}_{r,k}) \qquad \leq O(\sqrt{\varepsilon}). \end{aligned} \tag{3.2}$$

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*

$$\begin{aligned} &\forall k, r, c, r', c', \qquad d_{\psi'}(\tilde{B}^{r}_{c,k}\tilde{B}^{r'}_{c',k}, (-1)^{f(r,r',c,c')}\tilde{B}^{r'}_{c',k}\tilde{B}^{r}_{c,k}) \quad \leq O(\sqrt{\varepsilon}) \\ &\forall k \neq k', r, c, r', c', \qquad d_{\psi'}(\tilde{B}^{r}_{c,k}\tilde{B}^{r'}_{c',k'}, \tilde{B}^{r'}_{c',k'}\tilde{B}^{r}_{c,k}) \qquad \leq O(\sqrt{\varepsilon}). \end{aligned} \tag{3.3}$$

Moreover, the following consistency relations hold in expectation:

$$\forall \mathbf{c}, \mathbf{p}, \quad \mathbb{E}_{\mathbf{r}} d_{\psi'}(A^{\mathbf{c}}_{\mathbf{r},\mathbf{p}} \otimes I_{ancilla}, \prod_{k=1}^{n} (\tilde{A}^{c_k}_{r_k,k})^{p_k})^2 \leq O(n\sqrt{\varepsilon}) \tag{3.4}$$

$$\forall \mathbf{r}, \mathbf{p}, \quad \mathbb{E}_{\mathbf{c}} d_{\psi'}(B^{\mathbf{r}}_{\mathbf{c},\mathbf{p}} \otimes I_{ancilla}, \prod_{k=1}^{n} (\tilde{B}^{r_k}_{c_k,k})^{p_k})^2 \leq O(n\sqrt{\varepsilon}) \tag{3.5}$$

Proof of Theorem 25. The single-round phase relations in Equations (3.2) and (3.3) follow from Lemma 30. The commutation relations between rounds follow from Lemma 31. The consistency relations (Equations (3.4) and (3.5)) follow from Lemma 35. □

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 26. *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* (3.2) *and* (3.3)*. 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 $\left(\text{which is a polynomial in the } \tilde{A}^c_{r,k}\right)$, 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 $\left(\text{which is a polynomial in the } \tilde{B}^r_{c,k}\right)$, such that

$$\forall \mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d}, \qquad \left| \langle \phi | \sigma_X^A(\mathbf{s}) \sigma_Z^A(\mathbf{t}) \sigma_X^B(\mathbf{u}) \sigma_Z^B(\mathbf{v}) | \phi \rangle - \langle \psi | W^A{}_{\mathbf{s},\mathbf{t}} W^B{}_{\mathbf{u},\mathbf{v}} | \psi \rangle \right| \leq O(n^2 \sqrt{\varepsilon}), \quad (3.6)$$

where $|\phi\rangle = V(|\psi\rangle)$, σ_X^A, σ_Z^A are Pauli operators acting on the second output register of V, and σ_X^B, σ_Z^B are Pauli operators acting on the fourth output register of V.

The proof of this theorem is deferred to Section 3.4.3. As a corollary, we show that the output state of the isometry has high overlap with the state $|\text{EPR}\rangle^{\otimes 2n}$ consisting of $2n$ EPR pairs shared between Alice and Bob.

Corollary 27. *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 26,*

$$\langle \phi | |\text{EPR}\rangle\langle\text{EPR}|^{\otimes 2n} \otimes I_{junk} | \phi \rangle \geq 1 - O(n^2 \sqrt{\varepsilon}),$$

whwere the identity operator I_{juk} acts on the first, third, and fifth register of the isometry output.

Proof. This follows from Lemma 42 and Lemma 39. □

3.4.2 Single-round observables

Definition 28. *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 29. *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

$$\begin{aligned}\tilde{A}_{r,k}^c &:= \sum_{\mathbf{r}_{-k}} \sum_{\mathbf{a}_0,\mathbf{a}_1} (-1)^{(\mathbf{a}_c)_k} P_{\mathbf{r}}^{\mathbf{a}_0,\mathbf{a}_1} \otimes I_1 \otimes \ldots \otimes I_{k-1} \otimes |\mathbf{r}_{-k}\rangle\langle\mathbf{r}_{-k}| \otimes I_{k+1} \ldots \otimes I_n \\ &= \sum_{\mathbf{r}_{-k}} A_{\mathbf{s},\mathbf{e}_k}^{\mathbf{c}} \otimes I_1 \otimes \ldots \otimes I_{k-1} \otimes |\mathbf{r}_{-k}\rangle\langle\mathbf{r}_{-k}| \otimes I_{k+1} \ldots \otimes I_n\end{aligned}$$

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 $\tilde{A}_{r,k}^c$ *are true observables, i.e. they are Hermitian and square to* I*. Moreover,* $\tilde{A}_{r,k}^c$ *simulates the two-outcome POVM whose elements are given by* $M^{a_c} := \mathbb{E}_{\mathbf{r}_{-k}} P_{\mathbf{r},k}^{a_c}$*.*

Similarly, define dilated observables on Bob's side

$$\begin{aligned}\tilde{B}_{c,k}^r &:= \sum_{\mathbf{c}_{-k}} \sum_{\mathbf{b}_0,\mathbf{b}_1} (-1)^{(\mathbf{b}_r)_k} Q_{\mathbf{c}}^{\mathbf{b}_0,\mathbf{b}_1} \otimes I_1 \otimes \ldots \otimes I_{k-1} \otimes |\mathbf{r}_{-k}\rangle\langle\mathbf{r}_{-k}| \otimes I_{k+1} \ldots \otimes I_n \\ &= \sum_{\mathbf{c}_{-k}} B_{\mathbf{c},\mathbf{e}_k}^{\mathbf{r}} \otimes I_1 \otimes \ldots \otimes I_{k-1} \otimes |\mathbf{r}_{-k}\rangle\langle\mathbf{r}_{-k}| \otimes I_{k+1} \ldots \otimes I_n\end{aligned}$$

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 $\tilde{B}_{c,k}^r$ *are true observables, i.e. they are Hermitian and square to* I*. Moreover,* $\tilde{B}_{c,k}^r$ *simulates the two-outcome POVM whose elements are given by* $M^{b_c} := \mathbb{E}_{\mathbf{c}_{-k}} P_{\mathbf{c},k}^{b_r}$*.*

Lemma 30. *For all* k, r, r', c, c'*, it holds that*

$$\|(\tilde{A}_{r,k}^c \tilde{A}_{r',k}^{c'} - (-1)^{f(r,r',c,c')} \tilde{A}_{r',k}^{c'} \tilde{A}_{r,k}^c)|\psi'\rangle\| \leq O(\sqrt{\varepsilon}).$$

The analogous statement also holds for Bob operators.

Proof. Follows from single round analysis. See Appendix B.2. 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 B.2 still holds. □

Lemma 31. *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 (3.1) we have that

$$\forall \mathbf{p}, \quad \mathbb{E}_{\mathbf{r},\mathbf{c}} \langle\psi| A_{\mathbf{r},\mathbf{p}}^{\mathbf{c}} B_{\mathbf{c},\mathbf{p}}^{\mathbf{r}} |\psi\rangle \geq 1 - \varepsilon. \tag{3.7}$$

Setting $\mathbf{p} = \mathbf{e}_k$ gives that, for all fixed values of r_k and c_k,

$$\forall k, \quad \mathbb{E}_{\mathbf{r}_{-k},\mathbf{c}_{-k}} \langle\psi| A_{\mathbf{r},\mathbf{e}_k}^{\mathbf{c}} B_{\mathbf{c},\mathbf{e}_k}^{\mathbf{r}} |\psi\rangle \geq 1 - 9\varepsilon. \tag{3.8}$$

So,

$$\forall k, \quad \mathbb{E}_{\mathbf{r}_{-k},\mathbf{c}_{-k}} d_\psi \left(A_{\mathbf{r},\mathbf{e}_k}^{\mathbf{c}} B_{\mathbf{c},\mathbf{e}_k}^{\mathbf{r}} \right)^2 \leq 18\varepsilon \tag{3.9}$$

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 $\mathbb{E}_{\mathbf{c}|k,k'}$ the uniform distribution over choices of column vector $\mathbf{c}$ such that $c_k = c$ and

$c_{k'} = c'$. Then

$$d_\psi(\tilde{A}^{c}_{r,k}\tilde{A}^{c'}_{r',k'}, \tilde{A}^{c'}_{r'k'}, \tilde{A}^{c}_{r,k}) = \mathbb{E}_{\mathbf{c}|k,k'} d_{\psi'}\Big(\sum_{\mathbf{r}_{-k}}\sum_{\mathbf{r}'_{-k'}} A^{\mathbf{c}}_{\mathbf{r},\mathbf{e}_k} A^{\mathbf{c}}_{\mathbf{r}',\mathbf{e}_{k'}} \otimes |\mathbf{r}_{-k}, \mathbf{r}'_{-k'}\rangle\langle \mathbf{r}_{-k}, \mathbf{r}'_{-k'}|_{k,k'},$$
$$\sum_{\mathbf{r}_{-k}}\sum_{\mathbf{r}'_{-k'}} A^{\mathbf{c}}_{\mathbf{r}',\mathbf{e}_{k'}} A^{\mathbf{c}}_{\mathbf{r},\mathbf{e}_k} \otimes |\mathbf{r}_{-k}, \mathbf{r}'_{-k'}\rangle\langle \mathbf{r}_{-k}, \mathbf{r}'_{-k'}|_{k,k'}\Big)$$

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 44 to move the leftmost A operator to Bob.

$$\leq \mathbb{E}_{\mathbf{c}|k,k'}\Big[d_{\psi'}\Big(\sum_{\mathbf{r}_{-k}}\sum_{\mathbf{r}'_{-k'}} A^{\mathbf{r}}_{\mathbf{c},\mathbf{e}_k} B^{\mathbf{r}'}_{\mathbf{c},\mathbf{e}_{k'}} \otimes |\mathbf{r}_{-k}, \mathbf{r}'_{-k'}\rangle\langle \mathbf{r}_{-k}, \mathbf{r}'_{-k'}|_{k,k'},$$
$$\sum_{\mathbf{r}_{-k}}\sum_{\mathbf{r}'_{-k'}} A^{\mathbf{c}}_{\mathbf{r}',\mathbf{e}_{k'}} A^{\mathbf{c}}_{\mathbf{r},\mathbf{e}_k} \otimes |\mathbf{r}_{-k}, \mathbf{r}'_{-k'}\rangle\langle \mathbf{r}_{-k}, \mathbf{r}'_{-k'}|_{k,k'}\Big) +$$
$$d_{\psi'}\Big(\sum_{\mathbf{r}_{-k}} A^{\mathbf{c}}_{\mathbf{r},\mathbf{e}_k} \otimes |\mathbf{r}_{-k}\rangle\langle \mathbf{r}_{-k}| \otimes I_{k'} \sum_{\mathbf{r}'_{-k'}} A^{\mathbf{c}}_{\mathbf{r}',\mathbf{e}_{k'}} \otimes I_k \otimes |\mathbf{r}'_{-k'}\rangle\langle \mathbf{r}'_{-k'}|,$$
$$\sum_{\mathbf{r}_{-k}} A^{\mathbf{c}}_{\mathbf{r},\mathbf{e}_k} \otimes |\mathbf{r}_{-k}\rangle\langle \mathbf{r}_{-k}| \otimes I_{k'} \sum_{\mathbf{r}'_{-k'}} B^{\mathbf{r}'}_{\mathbf{c},\mathbf{e}_{k'}} \otimes I_k \otimes |\mathbf{r}'_{-k'}\rangle\langle \mathbf{r}'_{-k'}|\Big)\Big]$$

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 45 and Lemma 46, we get

$$\leq \mathbb{E}_{\mathbf{c}|k,k'}\Big[d_{\psi'}\Big(\sum_{\mathbf{r}_{-k}}\sum_{\mathbf{r}'_{-k'}} A^{\mathbf{r}}_{\mathbf{c},\mathbf{e}_k} B^{\mathbf{r}'}_{\mathbf{c},\mathbf{e}_{k'}} \otimes |\mathbf{r}_{-k}, \mathbf{r}'_{-k'}\rangle\langle \mathbf{r}_{-k}, \mathbf{r}'_{-k'}|_{k,k'},$$
$$\sum_{\mathbf{r}_{-k}}\sum_{\mathbf{r}'_{-k'}} A^{\mathbf{c}}_{\mathbf{r}',\mathbf{e}_{k'}} A^{\mathbf{c}}_{\mathbf{r},\mathbf{e}_k} \otimes |\mathbf{r}_{-k}, \mathbf{r}'_{-k'}\rangle\langle \mathbf{r}_{-k}, \mathbf{r}'_{-k'}|_{k,k'}\Big) +$$
$$\mathbb{E}_{\mathbf{r}'_{-k'}} d_\psi(A^{\mathbf{c}}_{\mathbf{r}',\mathbf{e}_{k'}}, B^{\mathbf{r}'}_{\mathbf{c},\mathbf{e}_{k'}})\Big]$$

By performing the same steps on the other A operator, we obtain

$$\leq \mathbb{E}_{\mathbf{c}|k,k'}\Big[d_{\psi'}\big(\sum_{\mathbf{r}_{-k}}\sum_{\mathbf{r}'_{-k'}} B^{\mathbf{r}'}_{\mathbf{c},\mathbf{e}_{k'}} B^{\mathbf{r}}_{\mathbf{c},\mathbf{e}_k} \otimes |\mathbf{r}_{-k},\mathbf{r}'_{-k'}\rangle\langle\mathbf{r}_{-k},\mathbf{r}'_{-k'}|_{k,k'},$$
$$\sum_{\mathbf{r}_{-k}}\sum_{\mathbf{r}'_{-k'}} A^{\mathbf{c}}_{\mathbf{r}',\mathbf{e}_{k'}} A^{\mathbf{c}}_{\mathbf{r},\mathbf{e}_k} \otimes |\mathbf{r}_{-k},\mathbf{r}'_{-k'}\rangle\langle\mathbf{r}_{-k},\mathbf{r}'_{-k'}|_{k,k'}\big) +$$
$$\mathbb{E}_{\mathbf{r}_{-k}} d_\psi(A^{\mathbf{c}}_{\mathbf{r},\mathbf{e}_k}, B^{\mathbf{r}}_{\mathbf{c},\mathbf{e}_k}) + \mathbb{E}_{\mathbf{r}'_{-k'}} d_\psi(A^{\mathbf{c}}_{\mathbf{r}',\mathbf{e}_{k'}}, B^{\mathbf{r}'}_{\mathbf{c},\mathbf{e}_{k'}})\Big]$$

Now the B operators can be commuted exactly since they share the same input $\mathbf{c}$.

$$\leq \mathbb{E}_{\mathbf{c}|k,k'}\Big[d_{\psi'}\big(\sum_{\mathbf{r}_{-k}}\sum_{\mathbf{r}'_{-k'}} B^{\mathbf{r}}_{\mathbf{c},\mathbf{e}_k} B^{\mathbf{r}'}_{\mathbf{c},\mathbf{e}_{k'}} \otimes |\mathbf{r}_{-k},\mathbf{r}'_{-k'}\rangle\langle\mathbf{r}_{-k},\mathbf{r}'_{-k'}|_{k,k'},$$
$$\sum_{\mathbf{r}_{-k}}\sum_{\mathbf{r}'_{-k'}} A^{\mathbf{c}}_{\mathbf{r}',\mathbf{e}_{k'}} A^{\mathbf{c}}_{\mathbf{r},\mathbf{e}_k} \otimes |\mathbf{r}_{-k},\mathbf{r}'_{-k'}\rangle\langle\mathbf{r}_{-k},\mathbf{r}'_{-k'}|_{k,k'}\big) +$$
$$\mathbb{E}_{\mathbf{r}_{-k}} d_\psi(A^{\mathbf{c}}_{\mathbf{r},\mathbf{e}_k}, B^{\mathbf{r}}_{\mathbf{c},\mathbf{e}_k}) + \mathbb{E}_{\mathbf{r}'_{-k'}} d_\psi(A^{\mathbf{c}}_{\mathbf{r}',\mathbf{e}_{k'}}, B^{\mathbf{r}'}_{\mathbf{c},\mathbf{e}_{k'}})\Big]$$

We move the Bs back to Alice by reversing the previous steps, again using Lemmas 44, 45, and 46

$$\leq \mathbb{E}_{\mathbf{c}|k,k'}\Big[d_{\psi'}\big(\sum_{\mathbf{r}_{-k}}\sum_{\mathbf{r}'_{-k'}} A^{\mathbf{c}}_{\mathbf{r}',\mathbf{e}_{k'}} A^{\mathbf{c}}_{\mathbf{r},\mathbf{e}_k} \otimes |\mathbf{r}_{-k},\mathbf{r}'_{-k'}\rangle\langle\mathbf{r}_{-k},\mathbf{r}'_{-k'}|_{k,k'},$$
$$\sum_{\mathbf{r}_{-k}}\sum_{\mathbf{r}'_{-k'}} A^{\mathbf{c}}_{\mathbf{r}',\mathbf{e}_{k'}} A^{\mathbf{c}}_{\mathbf{r},\mathbf{e}_k} \otimes |\mathbf{r}_{-k},\mathbf{r}'_{-k'}\rangle\langle\mathbf{r}_{-k},\mathbf{r}'_{-k'}|_{k,k'}\big) +$$
$$2\mathbb{E}_{\mathbf{r}_{-k}} d_\psi(A^{\mathbf{c}}_{\mathbf{r},\mathbf{e}_k}, B^{\mathbf{r}}_{\mathbf{c},\mathbf{e}_k}) + 2\mathbb{E}_{\mathbf{r}'_{-k'}} d_\psi(A^{\mathbf{c}}_{\mathbf{r}',\mathbf{e}_{k'}}, B^{\mathbf{r}'}_{\mathbf{c},\mathbf{e}_{k'}})\Big]$$
$$= \mathbb{E}_{\mathbf{c}|k,k'}(2\mathbb{E}_{vr_{-k}} d_\psi(A^{\mathbf{c}}_{\mathbf{r},\mathbf{e}_k}, B^{\mathbf{r}}_{\mathbf{c},\mathbf{e}_k}) + 2\mathbb{E}_{\mathbf{r}'_{-k'}} d_\psi(A^{\mathbf{c}}_{\mathbf{r}',\mathbf{e}_{k'}}, B^{\mathbf{r}'}_{\mathbf{c},\mathbf{e}_{k'}}))$$

Finally, we bound this by Equation (3.9). Note that Equation (3.9) is stated with $\mathbb{E}_{\mathbf{r}_{-k},\mathbf{c}_{-k'}}$ but this implies the same statement with $\mathbb{E}_{\mathbf{c}|k,k'}\mathbb{E}_{\mathbf{r}_{-k}}$ with an additional constant factor of 3. Similarly for $\mathbb{E}_{\mathbf{c}|k,k'}\mathbb{E}_{\mathbf{r}_{-k'}}$. So, continuing our computation:

$$\leq 4 \cdot 3 \cdot 3\sqrt{2\varepsilon} = 36\sqrt{2\varepsilon}.$$

□

Lemma 32.

$$\forall r, c, k, \quad d_{\psi'}\left(\tilde{A}^c_{r,k}, \tilde{B}^r_{c,k}\right) \leq O(\sqrt{\varepsilon})$$

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 46 with $i = (\mathbf{r}_{-k}, \mathbf{c}_{-k})$,

$$= \mathbb{E}_{\mathbf{r}_{-k},\mathbf{c}_{-k}} d_{\psi'}(A^{\mathbf{c}}_{\mathbf{r},k}, B^{\mathbf{r}}_{\mathbf{c},k})^2$$

This is bounded by the probability that round k of the test succeeds with inputs r and c

$$\leq O(\varepsilon).$$

□

Lemma 33. $\forall \mathbf{r}, \mathbf{c}, \mathbf{p}$ *and* $\forall i \in [n]$

$$\left|\langle\psi'|(\prod_{k=n}^{i+1}(\tilde{B}_{c_k,k}^{r_k})^{p_k})A_{\mathbf{r},\mathbf{p}}^{\mathbf{c}}(\prod_{k=1}^{i}\tilde{A}_{r_k,k}^{c_k})|\psi'\rangle - \langle\psi'|(\prod_{k=n}^{i}(\tilde{B}_{c_k,k}^{r_k})^{p_k})A_{\mathbf{r},\mathbf{p}}^{\mathbf{c}}(\prod_{k=1}^{i-1}\tilde{A}_{r_k,k}^{c_k})|\psi'\rangle\right| \leq O(\sqrt{\varepsilon})$$

Proof. Fixing $\mathbf{r}, \mathbf{c}, \mathbf{p}$, and fixing $i \in [n]$ we have

$$\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}\tilde{A}_{r_k,k}^{c_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})|\psi'\rangle\right| \\
&= \Bigg|\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})\tilde{B}_{c_i,i}^{r_i}|\psi'\rangle + \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})\left(\tilde{A}_{c_i,i}^{r_i} - \tilde{B}_{c_i,i}^{r_i}\right)|\psi'\rangle \\
&\quad - \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})|\psi'\rangle\Bigg| \\
&\leq \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})\tilde{B}_{c_i,i}^{r_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})|\psi'\rangle\right| \\
&\quad + \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})\left(\tilde{A}_{c_i,i}^{r_i} - \tilde{B}_{c_i,i}^{r_i}\right)|\psi'\rangle\right| \\
&\leq \left|\langle\psi'|(\prod_{k=n}^{i+1}(\tilde{B}_{c_k,k}^{r_k})^{p_k})\tilde{B}_{c_i,i}^{r_i}A_{\mathbf{r},\mathbf{p}}^{\mathbf{c}}(\prod_{k=1}^{i-1}\tilde{A}_{r_k,k}^{c_k})\tilde{B}_{c_i,i}^{r_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})|\psi'\rangle\right| \\
&\quad + d_{\psi'}(\tilde{A}_{r_i,i}^{c_i}, \tilde{B}_{c_i,i}^{r_i}) \\
&\leq 0 + O(\sqrt{\varepsilon}) = O(\sqrt{\varepsilon}).
\end{aligned}$$

Here the last inequality uses Lemma 32, and the second to last inequality uses that $\tilde{B}_{c_i,i}^{r_i}$ commutes with all Alice operators, and that $(\prod_{k=n}^{i+1}(\tilde{B}_{c_k,k}^{r_k})^{p_k})A_{\mathbf{r},\mathbf{p}}^{\mathbf{c}}(\prod_{k=1}^{i-1}\tilde{A}_{r_k,k}^{c_k})$ is a unitary, so that

$$\left|\langle\psi'|(\prod_{k=n}^{i+1}(\tilde{B}_{c_k,k}^{r_k})^{p_k})A_{\mathbf{r},\mathbf{p}}^{\mathbf{c}}(\prod_{k=1}^{i-1}\tilde{A}_{r_k,k}^{c_k})\left(\tilde{A}_{c_i,i}^{r_i} - \tilde{B}_{c_i,i}^{r_i}\right)|\psi'\rangle\right| \leq \left\|\left(\tilde{A}_{c_i,i}^{r_i} - \tilde{B}_{c_i,i}^{r_i}\right)|\psi'\rangle\right\| = d_{\psi'}(\tilde{A}_{r_i,i}^{c_i}, \tilde{B}_{c_i,i}^{r_i}).$$

□

Lemma 34.

$$\Big|\mathbb{E}_{\mathbf{r}}\Big(\langle\psi'|(\prod_{k=n}^{i+2}(\tilde{B}^{r_k}_{c_k,k})^{p_k})(\prod_{k=n}^{i+1}A^{\mathbf{c}}_{\mathbf{r},p_k\cdot\mathbf{e}_k}\otimes I)(\tilde{A}^{c_{i+1}}_{r_{i+1},i+1})|\psi'\rangle$$
$$-\langle\psi'|(\prod_{k=n}^{i+1}(\tilde{B}^{r_k}_{c_k,k})^{p_k})(\prod_{k=n}^{i}A^{\mathbf{c}}_{\mathbf{r},p_k\cdot\mathbf{e}_k}\otimes I)(\tilde{A}^{c_i}_{r_i,i})|\psi'\rangle\Big)\Big|\leq O(\sqrt{\varepsilon}) \tag{3.10}$$

and

$$\mathbb{E}_{\mathbf{r}}\left(1-\langle\psi'|A^{\mathbf{c}}_{\mathbf{r},p_n\cdot\mathbf{e}_n}(\tilde{A}^{c_n}_{r_n,n})|\psi'\rangle\right)\leq O(\sqrt{\varepsilon}) \tag{3.11}$$

Proof.

$$\begin{aligned}
&\left|\mathbb{E}_{\mathbf{r}}\left(\langle\psi'|(\prod_{k=n}^{i+2}\tilde{B}^{r_k}_{c_k,k})(\prod_{k=n}^{i+1}A^{\mathbf{c}}_{\mathbf{r},p_k\cdot\mathbf{e}_k}\otimes I)(\tilde{A}^{c_{i+1}}_{r_{i+1},i+1})|\psi'\rangle-\langle\psi'|(\prod_{k=n}^{i+1}\tilde{B}^{r_k}_{c_k,k})(\prod_{k=n}^{i}A^{\mathbf{c}}_{\mathbf{r},p_k\cdot\mathbf{e}_k}\otimes I)(\tilde{A}^{c_i}_{r_i,i})|\psi'\rangle\right)\right|\\
&=\left|\mathbb{E}_{\mathbf{r}}\left(\langle\psi'|(\prod_{k=n}^{i+2}\tilde{B}^{r_k}_{c_k,k})(\prod_{k=n}^{i+1}A^{\mathbf{c}}_{\mathbf{r},p_k\cdot\mathbf{e}_k}\otimes I)(\tilde{A}^{c_{i+1}}_{r_{i+1},i+1})|\psi'\rangle-\langle\psi'|(\prod_{k=n}^{i+2}\tilde{B}^{r_k}_{c_k,k})(\prod_{k=n}^{i+1}A^{\mathbf{c}}_{\mathbf{r},p_k\cdot\mathbf{e}_k}\otimes I)(\tilde{B}^{r_{i+1}}_{c_{i+1},i+1})|\psi'\rangle\right.\right.\\
&\left.\left.+\langle\psi'|(\prod_{k=n}^{i+2}\tilde{B}^{r_k}_{c_k,k})(\prod_{k=n}^{i+1}A^{\mathbf{c}}_{\mathbf{r},p_k\cdot\mathbf{e}_k}\otimes I)(\tilde{B}^{r_{i+1}}_{c_{i+1},i+1})|\psi'\rangle-\langle\psi'|(\prod_{k=n}^{i+1}\tilde{B}^{r_k}_{c_k,k})(\prod_{k=n}^{i}A^{\mathbf{c}}_{\mathbf{r},p_k\cdot\mathbf{e}_k}\otimes I)(\tilde{A}^{c_i}_{r_i,i})|\psi'\rangle\right)\right|\\
&\leq\left|\mathbb{E}_{\mathbf{r}}\left(\langle\psi'|(\prod_{k=n}^{i+2}\tilde{B}^{r_k}_{c_k,k})(\prod_{k=n}^{i+1}A^{\mathbf{c}}_{\mathbf{r},p_k\cdot\mathbf{e}_k}\otimes I)(\tilde{A}^{c_{i+1}}_{r_{i+1},i+1})|\psi'\rangle-\langle\psi'|(\prod_{k=n}^{i+2}\tilde{B}^{r_k}_{c_k,k})(\prod_{k=n}^{i+1}A^{\mathbf{c}}_{\mathbf{r},p_k\cdot\mathbf{e}_k}\otimes I)(\tilde{B}^{r_{i+1}}_{c_{i+1},i+1})|\psi'\rangle\right)\right|\\
&+\left|\mathbb{E}_{\mathbf{r}}\left(\langle\psi'|(\prod_{k=n}^{i+2}\tilde{B}^{r_k}_{c_k,k})(\prod_{k=n}^{i+1}A^{\mathbf{c}}_{\mathbf{r},p_k\cdot\mathbf{e}_k}\otimes I)(\tilde{B}^{r_{i+1}}_{c_{i+1},i+1})|\psi'\rangle-\langle\psi'|(\prod_{k=n}^{i+1}\tilde{B}^{r_k}_{c_k,k})(\prod_{k=n}^{i}A^{\mathbf{c}}_{\mathbf{r},p_k\cdot\mathbf{e}_k}\otimes I)(\tilde{A}^{c_i}_{r_i,i})|\psi'\rangle\right)\right|\\
&\leq\left|\mathbb{E}_{\mathbf{r}}\left(d_{\psi'}(\tilde{A}^{c_{i+1}}_{r_{i+1},i+1},\tilde{B}^{r_{i+1}}_{c_{i+1},i+1})\right)\right|\\
&+\left|\mathbb{E}_{\mathbf{r}}\left(\langle\psi'|(\prod_{k=n}^{i+1}\tilde{B}^{r_k}_{c_k,k})(\prod_{k=n}^{i+1}A^{\mathbf{c}}_{\mathbf{r},p_k\cdot\mathbf{e}_k}\otimes I)|\psi'\rangle-\langle\psi'|(\prod_{k=n}^{i+1}\tilde{B}^{r_k}_{c_k,k})(\prod_{k=n}^{i+1}A^{\mathbf{c}}_{\mathbf{r},p_k\cdot\mathbf{e}_k}\otimes I)\cdot A^{\mathbf{c}}_{\mathbf{r},p_i\cdot\mathbf{e}_i}\otimes I\cdot(\tilde{A}^{c_i}_{r_i,i})|\psi'\rangle\right)\right|\\
&\leq\left|\mathbb{E}_{\mathbf{r}}\left(d_{\psi'}(\tilde{A}^{c_{i+1}}_{r_{i+1},i+1},\tilde{B}^{r_{i+1}}_{c_{i+1},i+1})\right)\right|+\left|\mathbb{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})\right)\right|
\end{aligned}$$

Where the second to last inequality uses the fact that $\|\langle\psi'|(\prod_{k=n}^{i+2}\tilde{B}^{r_k}_{c_k,k})(\prod_{k=n}^{i+1}A^{\mathbf{c}}_{\mathbf{r},p_k\cdot\mathbf{e}_k}\otimes I)\|=1$, and the third inequality uses that fact that $\|\langle\psi'|(\prod_{k=n}^{i+1}\tilde{B}^{r_k}_{c_k,k})(\prod_{k=n}^{i+1}A^{\mathbf{c}}_{\mathbf{r},p_k\cdot\mathbf{e}_k}\otimes$

$I)\| = 1$. Now, applying Lemma 32, we have

$$\left|\mathbb{E}_{\mathbf{r}}\left(\langle\psi'|(\prod_{k=n}^{i+2}\tilde{B}^{r_k}_{c_k,k})(\prod_{k=n}^{i+1}A^{\mathbf{c}}_{\mathbf{r},p_k\cdot\mathbf{e}_k}\otimes I)(\tilde{A}^{c_{i+1}}_{r_{i+1},i+1})|\psi'\rangle - \langle\psi'|(\prod_{k=n}^{i+1}\tilde{B}^{r_k}_{c_k,k})(\prod_{k=n}^{i}A^{\mathbf{c}}_{\mathbf{r},p_k\cdot\mathbf{e}_k}\otimes I)(\tilde{A}^{c_i}_{r_i,i})|\psi'\rangle\right)\right|$$
$$\leq \mathbb{E}_{\mathbf{r}}\left(d_{\psi'}(\tilde{A}^{c_{i+1}}_{r_{i+1},i+1},\tilde{B}^{r_{i+1}}_{c_{i+1},i+1})\right) + \mathbb{E}_{\mathbf{r}}\left(d_{\psi'}(I,(A^{\mathbf{c}}_{\mathbf{r},p_i\cdot\mathbf{e}_i}\otimes I)\cdot\tilde{A}^{c_i}_{r_i,i})\right)$$
$$\leq O(\sqrt{\varepsilon}) + \mathbb{E}_{\mathbf{r}}\left(d_{\psi'}(I,(A^{\mathbf{c}}_{\mathbf{r},p_i\cdot\mathbf{e}_i}\otimes I)\cdot\tilde{A}^{c_i}_{r_i,i})\right) \tag{3.12}$$
$$\tag{3.13}$$

And we note that

$$\mathbb{E}_{\mathbf{r}}\left(d_{\psi'}(I,(A^{\mathbf{c}}_{\mathbf{r},p_i\cdot\mathbf{e}_i}\otimes I)\cdot\tilde{A}^{c_i}_{r_i,i})^2\right)$$
$$= \mathbb{E}_{\mathbf{r}}\left(\||\psi'\rangle - (A^{\mathbf{c}}_{\mathbf{r},p_i\cdot\mathbf{e}_i}\otimes I)\cdot\tilde{A}^{c_i}_{r_i,i}|\psi'\rangle\|^2\right)$$
$$= \mathbb{E}_{\mathbf{r}}\left(2 - 2\langle\psi'|(A^{\mathbf{c}}_{\mathbf{r},p_i\cdot\mathbf{e}_i}\otimes I)\cdot\tilde{A}^{c_i}_{r_i,i}|\psi'\rangle\right)$$
$$= \mathbb{E}_{\mathbf{r}}\left(2 - 2\left(\langle\psi|\otimes\frac{1}{\sqrt{3^{n-1}}}\sum_{\mathbf{r}_{-k}\in\{0,1,2\}^{n-1}}\langle\mathbf{r}_{-k}|\right)(A^{\mathbf{c}}_{\mathbf{r},p_i\cdot\mathbf{e}_i}\otimes I)\cdot\left(\sum_{\mathbf{r}':r'_i=r_i}A^{\mathbf{c}}_{\mathbf{r}',\mathbf{e}_i}\otimes|\mathbf{r}'_{-i}\rangle\langle\mathbf{r}'_{-i}|\right)\times\ldots\right.$$
$$\left.\ldots\times\left(|\psi\rangle\otimes\frac{1}{\sqrt{3^{n-1}}}\sum_{\mathbf{r}_{-k}\in\{0,1,2\}^{n-1}}|\mathbf{r}_{-k}\rangle\right)\right)$$
$$= \mathbb{E}_{\mathbf{r}}\left(2 - 2\cdot\frac{1}{3^{n-1}}\sum_{\mathbf{r}':r'_i=r_i}\langle\psi|A^{\mathbf{c}}_{\mathbf{r},p_i\cdot\mathbf{e}_i}\cdot A^{\mathbf{c}}_{\mathbf{r}',\mathbf{e}_i}|\psi\rangle\cdot\langle\mathbf{r}'_{-i}||\mathbf{r}'_{-i}\rangle\langle\mathbf{r}'_{-i}||\mathbf{r}'_{-i}\rangle\right)$$
$$= \mathbb{E}_{\mathbf{r}}\left(2 - 2\cdot\mathbb{E}_{\mathbf{r}':r'_i=r_i}\langle\psi|A^{\mathbf{c}}_{\mathbf{r},p_i\cdot\mathbf{e}_i}\cdot A^{\mathbf{c}}_{\mathbf{r}',\mathbf{e}_i}|\psi\rangle\right) = 2\left(1 - \mathbb{E}_{\mathbf{r},\mathbf{r}':r'_i=r_i}\langle\psi|A^{\mathbf{c}}_{\mathbf{r},p_i\cdot\mathbf{e}_i}\cdot A^{\mathbf{c}}_{\mathbf{r}',\mathbf{e}_i}|\psi\rangle\right)$$
$$\leq 2\cdot 3\cdot 36\varepsilon \tag{3.14}$$

Where the last inequality follows from Lemma 24. Furthermore, by Jensen's inequality it follows that:

$$\mathbb{E}_{\mathbf{r}}\left(d_{\psi'}(I,(A^{\mathbf{c}}_{\mathbf{r},p_i\cdot\mathbf{e}_i}\otimes I)\cdot\tilde{A}^{c_i}_{r_i,i})\right)\leq\sqrt{\mathbb{E}_{\mathbf{r}}\left(d_{\psi'}(I,(A^{\mathbf{c}}_{\mathbf{r},p_i\cdot\mathbf{e}_i}\otimes I)\cdot\tilde{A}^{c_i}_{r_i,i})^2\right)}\leq O(\sqrt{\varepsilon})$$

Now, resuming the calculation in equation (3.12), we have that

$$\left|\mathbb{E}_{\mathbf{r}}\left(\langle\psi'|(\prod_{k=n}^{i+2}\tilde{B}^{r_k}_{c_k,k})(\prod_{k=n}^{i+1}A^{\mathbf{c}}_{\mathbf{r},p_k\cdot\mathbf{e}_k}\otimes I)(\tilde{A}^{c_{i+1}}_{r_{i+1},i+1})|\psi'\rangle-\langle\psi'|(\prod_{k=n}^{i+1}\tilde{B}^{r_k}_{c_k,k})(\prod_{k=n}^{i}A^{\mathbf{c}}_{\mathbf{r},p_k\cdot\mathbf{e}_k}\otimes I)(\tilde{A}^{c_i}_{r_i,i})|\psi'\rangle\right)\right|$$
$$\leq O(\sqrt{\varepsilon})+\mathbb{E}_{\mathbf{r}}\left(d_{\psi'}(I,(A^{\mathbf{c}}_{\mathbf{r},p_i\cdot\mathbf{e}_i}\otimes I)\cdot\tilde{A}^{c_i}_{r_i,i})\right)\leq O(\sqrt{\varepsilon})$$

Finally, note that, since Equation 3.14 is valid for every i, it follows by the same calculation, with $i=n$, that:

$$\left|\mathbb{E}_{\mathbf{r}}\left(1-\langle\psi'|A^{\mathbf{c}}_{\mathbf{r},p_n\cdot\mathbf{e}_n}(\tilde{A}^{c_n}_{r_n,n})|\psi'\rangle\right)\right|\leq O(\varepsilon)\leq O(\sqrt{\varepsilon})$$

□

Lemma 35.

$$\forall\mathbf{c},\mathbf{p},\quad\mathbb{E}_{\mathbf{r}}d_{\psi'}\left(A^{\mathbf{c}}_{\mathbf{r},\mathbf{p}}\otimes I,\prod_{k=1}^{n}(\tilde{A}^{c_k}_{r_k,k})^{p_k}\right)^2\leq O(n\sqrt{\varepsilon})$$

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

$$A^{\mathbf{c}}_{\mathbf{r},\mathbf{p}} = A^{\mathbf{c}}_{\mathbf{r},p_1} \dots A^{\mathbf{c}}_{\mathbf{r},p_k}.$$

So, fixing any value of $\mathbf{c}$, and $\mathbf{p}$, we have

$$\begin{aligned}
&\mathbb{E}_{\mathbf{r}} d_{\psi'} \left(A^{\mathbf{c}}_{\mathbf{r},\mathbf{p}}, \prod_{k=1}^{n} (\tilde{A}^{c_k}_{r_k,k})^{p_k} \right)^2 \\
&= \mathbb{E}_{\mathbf{r}} \left(\langle \psi' | A^{\mathbf{c}\dagger}_{\mathbf{r},\mathbf{p}} A^{\mathbf{c}}_{\mathbf{r},\mathbf{p}} | \psi' \rangle + \langle \psi' | (\prod_{k=1}^{n} (\tilde{A}^{c_k}_{r_k,k})^{p_k})^\dagger (\prod_{k=1}^{n} (\tilde{A}^{c_k}_{r_k,k})^{p_k}) | \psi' \rangle - \langle \psi' | A^{\mathbf{c}\dagger}_{\mathbf{r},\mathbf{p}} (\prod_{k=1}^{n} (\tilde{A}^{c_k}_{r_k,k})^{p_k}) | \psi' \rangle \right. \\
&\left. - \langle \psi' | (\prod_{k=1}^{n} (\tilde{A}^{c_k}_{r_k,k})^{p_k})^\dagger A^{\mathbf{c}}_{\mathbf{r},\mathbf{p}} | \psi' \rangle \right) = 2\mathbb{E}_{\mathbf{r}} \left(1 - \langle \psi' | A^{\mathbf{c}}_{\mathbf{r},\mathbf{p}} (\prod_{k=1}^{n} (\tilde{A}^{c_k}_{r_k,k})^{p_k}) | \psi' \rangle \right)
\end{aligned}$$

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

$$\begin{aligned}
&\mathbb{E}_{\mathbf{r}} d_{\psi'} \left(A^{\mathbf{c}}_{\mathbf{r},\mathbf{p}}, \prod_{k=1}^{n} (\tilde{A}^{c_k}_{r_k,k})^{p_k} \right)^2 \\
&\quad = 2\mathbb{E}_{\mathbf{r}} \left(1 - \langle \psi' | A^{\mathbf{c}}_{\mathbf{r},\mathbf{p}} (\prod_{k=1}^{n} (\tilde{A}^{c_k}_{r_k,k})^{p_k}) | \psi' \rangle \right) \\
&\quad = 2\mathbb{E}_{\mathbf{r}} \left(1 - \langle \psi' | (\prod_{k=n}^{2} (\tilde{B}^{r_k}_{c_k,k})^{p_k}) A^{\mathbf{c}}_{\mathbf{r},\mathbf{p}} (\tilde{A}^{c_1}_{r_1,1}) | \psi' \rangle \right. \\
&\qquad \left. - \sum_{i=n}^{1} \left(\langle \psi' | (\prod_{k=n}^{i+1} (\tilde{B}^{r_k}_{c_k,k})^{p_k}) A^{\mathbf{c}}_{\mathbf{r},\mathbf{p}} (\prod_{k=1}^{i} (\tilde{A}^{c_k}_{r_k,k})^{p_k}) | \psi' \rangle - \langle \psi' | (\prod_{k=n}^{i} (\tilde{B}^{r_k}_{c_k,k})^{p_k}) A^{\mathbf{c}}_{\mathbf{r},\mathbf{p}} (\prod_{k=1}^{i-1} (\tilde{A}^{c_k}_{r_k,k})^{p_k}) | \psi' \rangle \right) \right) \\
&\quad \leq 2\mathbb{E}_{\mathbf{r}} \left(1 - \langle \psi' | (\prod_{k=n}^{2} (\tilde{B}^{r_k}_{c_k,k})^{p_k}) A^{\mathbf{c}}_{\mathbf{r},\mathbf{p}} (\tilde{A}^{c_1}_{r_1,1}) | \psi' \rangle \right) \\
&\quad + \sum_{i=n}^{1} 2\mathbb{E}_{\mathbf{r}} \left(\left| \langle \psi' | (\prod_{k=n}^{i+1} (\tilde{B}^{r_k}_{c_k,k})^{p_k}) A^{\mathbf{c}}_{\mathbf{r},\mathbf{p}} (\prod_{k=1}^{i} (\tilde{A}^{c_k}_{r_k,k})^{p_k}) | \psi' \rangle - \langle \psi' | (\prod_{k=n}^{i} (\tilde{B}^{r_k}_{c_k,k})^{p_k}) A^{\mathbf{c}}_{\mathbf{r},\mathbf{p}} (\prod_{k=1}^{i-1} (\tilde{A}^{c_k}_{r_k,k})^{p_k}) | \psi' \rangle \right| \right).
\end{aligned}$$

We now apply Lemma 33 inside the expectation:

$$
\begin{aligned}
&\leq 2\mathbb{E}_{\mathbf{r}}\left(1-\langle\psi'|(\prod_{k=n}^{2}(\tilde{B}_{c_k,k}^{r_k})^{p_k})A_{\mathbf{r},\mathbf{p}}^{\mathbf{c}}(\tilde{A}_{r_1,1}^{c_1})|\psi'\rangle\right)+\sum_{i=1}^{n}2\cdot O(\sqrt{\varepsilon})\\
&=2\mathbb{E}_{\mathbf{r}}\left(1-\langle\psi'|(\prod_{k=n}^{2}(\tilde{B}_{c_k,k}^{r_k})^{p_k})A_{\mathbf{r},\mathbf{p}}^{\mathbf{c}}(\tilde{A}_{r_1,1}^{c_1})|\psi'\rangle\right)+O(n\sqrt{\varepsilon})\\
&=2\mathbb{E}_{\mathbf{r}}\left(1-\langle\psi'|(\prod_{k=n}^{2}(\tilde{B}_{c_k,k}^{r_k})^{p_k})(\prod_{k=n}^{1}A_{\mathbf{r},p_k\cdot\mathbf{e}_k}^{\mathbf{c}})(\tilde{A}_{r_1,1}^{c_1})|\psi'\rangle\right)+O(n\sqrt{\varepsilon})\\
&\leq 2\left|\mathbb{E}_{\mathbf{r}}\left(1-\langle\psi'|A_{\mathbf{r},p_n\cdot\mathbf{e}_n}^{\mathbf{c}}(\tilde{A}_{r_n,n}^{c_n})|\psi'\rangle\right)\right|+2\sum_{i=n-1}^{1}\left|\mathbb{E}_{\mathbf{r}}\Big(\langle\psi'|(\prod_{k=n}^{i+2}(\tilde{B}_{c_k,k}^{r_k})^{p_k})(\prod_{k=n}^{i+1}A_{\mathbf{r},p_k\cdot\mathbf{e}_k}^{\mathbf{c}})(\tilde{A}_{r_{i+1},i+1}^{c_{i+1}})|\psi'\rangle\right.\\
&\qquad\left.-\langle\psi'|(\prod_{k=n}^{i+1}\tilde{B}_{c_k,k}^{r_k})(\prod_{k=n}^{i}A_{\mathbf{r},p_k\cdot\mathbf{e}_k}^{\mathbf{c}})(\tilde{A}_{r_i,i}^{c_i})|\psi'\rangle\Big)\right|+O(n\sqrt{\varepsilon})\\
&\leq 2\cdot O(\sqrt{\varepsilon})+2(n-1)O(\sqrt{\varepsilon})+O(n\sqrt{\varepsilon})=O(n\sqrt{\varepsilon})
\end{aligned}
$$

Where the last inequality follows by Lemma 34.

□

3.4.3 The Isometry

Definition 36. *Define the* single round *"approximate Pauli" operators on Alice's space by:*

$$
\begin{aligned}
X_{2k-1}&=\tilde{A}_{1,k}^{1}\\
X_{2k}&=\tilde{A}_{1,k}^{0}\\
Z_{2k-1}&=\tilde{A}_{0,k}^{0}\\
Z_{2k}&=\tilde{A}_{0,k}^{1}.
\end{aligned}
$$

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 37 (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:*

$$\begin{aligned} &\forall i, \quad d_\psi(X_i, X^B_i) && \leq \sqrt{\varepsilon} \\ &\forall i, \quad d_\psi(Z_i, Z^B_i) && \leq \sqrt{\varepsilon} \\ &\forall i, \quad d_\psi(X_iZ_i, -Z_iX_i) && \leq \sqrt{\varepsilon} \\ &\forall i \neq j, \quad d_\psi(X_iX_j, X_jX_i) && \leq \sqrt{\varepsilon} \\ &\forall i \neq j, \quad d_\psi(Z_iZ_j, Z_jZ_i) && \leq \sqrt{\varepsilon}. \end{aligned} \tag{3.15}$$

Proof. The consistency relations follow from Lemma 32. The other relations come from Theorem 25. □

We will now build up multi-round Paulis from products of these.

Lemma 38 (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 Equation* (3.15). *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*

$$\forall \mathbf{a}, \mathbf{b}, \mathbf{a}', \mathbf{b}', \quad d_\psi((X^{\mathbf{a}}Z^{\mathbf{b}})(X^{\mathbf{a}'}Z^{\mathbf{b}'}), (-1)^{\mathbf{a}'\cdot\mathbf{b}}X^{\mathbf{a}+\mathbf{a}'}Z^{\mathbf{b}+\mathbf{b}'}) \leq O(n^2\sqrt{\varepsilon}) \tag{3.16}$$

$$\forall \mathbf{a}, \mathbf{b}, \quad d_\psi((X^{\mathbf{a}}Z^{\mathbf{b}}), (Z^B)^{\mathbf{b}}(X^B)^{\mathbf{a}}) \leq O(n\sqrt{\varepsilon}). \tag{3.17}$$

Proof. Equation (3.17) is an immediate consequence of Lemma 48. We obtain Equation (3.16) in two steps. First, by Equation (B.1) of Lemma 51, 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 Equation (B.2) of Lemma 51 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,

$$\begin{aligned} d_\psi(X^{\mathbf{a}}Z^{\mathbf{b}}X^{\mathbf{a}'}Z^{\mathbf{b}'}, (-1)^{\mathbf{a}'\cdot\mathbf{b}}X^{\mathbf{a}+\mathbf{a}'}Z^{\mathbf{b}+\mathbf{b}'}) &\leq d_\psi(X^{\mathbf{a}}Z^{\mathbf{b}}X^{\mathbf{a}'}Z^{\mathbf{b}'}, (Z^B)^{\mathbf{b}'}X^{\mathbf{a}}Z^{\mathbf{b}}X^{\mathbf{a}'}) \\ &\quad + d_\psi((Z^B)^{\mathbf{b}'}X^{\mathbf{a}}Z^{\mathbf{b}}X^{\mathbf{a}'}, (-1)^{\mathbf{a}'\cdot\mathbf{b}}(Z^B)^{\mathbf{b}'}X^{\mathbf{a}}X^{\mathbf{a}'}Z^{\mathbf{b}}) \\ &\quad + d_\psi((-1)^{\mathbf{a}'\cdot\mathbf{b}}(Z^B)^{\mathbf{b}'}X^{\mathbf{a}}X^{\mathbf{a}'}Z^{\mathbf{b}}, (-1)^{\mathbf{a}'\cdot\mathbf{b}}(Z^B)^{\mathbf{b}'}(Z^B)^{\mathbf{b}}X^{\mathbf{a}}X^{\mathbf{a}'}) \\ &\quad + d_\psi((-1)^{\mathbf{a}'\cdot\mathbf{b}}(Z^B)^{\mathbf{b}'}(Z^B)^{\mathbf{b}}X^{\mathbf{a}}X^{\mathbf{a}'}, (-1)^{\mathbf{a}'\cdot\mathbf{b}}(Z^B)^{\mathbf{b}'}(Z^B)^{\mathbf{b}}X^{\mathbf{a}+\mathbf{a}} \\ &\quad + d_\psi((-1)^{\mathbf{a}'\cdot\mathbf{b}}(Z^B)^{\mathbf{b}'}(Z^B)^{\mathbf{b}}X^{\mathbf{a}+\mathbf{a}'}, (-1)^{\mathbf{a}'\cdot\mathbf{b}}X^{\mathbf{a}+\mathbf{a}'}Z^{\mathbf{b}}Z^{\mathbf{b}'}) \\ &\quad + d_\psi((-1)^{\mathbf{a}'\cdot\mathbf{b}}X^{\mathbf{a}+\mathbf{a}'}Z^{\mathbf{b}}Z^{\mathbf{b}'}, (-1)^{\mathbf{a}'\cdot\mathbf{b}}X^{\mathbf{a}+\mathbf{a}'}Z^{\mathbf{b}+\mathbf{b}'}) \\ &\leq O(n^2\sqrt{\varepsilon}). \end{aligned}$$

□

Proof of Theorem 26. 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 3.4.2. 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 [65], 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.

$$\begin{aligned}
\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}'| {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}')} \\
&\qquad \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}} |\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}'| {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}'} \\
&\qquad \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}} |\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})} \\
&\qquad \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).
\end{aligned}$$

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 38 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 39. *Let M_n be the 4n-qubit operator defined by*

$$M_n = \left(\frac{1}{2}IIII + \frac{1}{18}(IXIX + XIXI + XXXX + ZIZI + IZIZ + ZZZZ + XZXZ + ZXZX + YYYY)\right)^{\otimes n}.$$

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 40. *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 3-2), 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 41. *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 40 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 40 and Lemma 49. □

Lemma 42. *Suppose Alice and Bob win the test with probability $1 - \varepsilon$. Then for the operator M_n defined in Lemma 39. $\langle\phi|M_n|\phi\rangle \geq 1 - O(n^2\sqrt{\varepsilon})$, where $|\phi\rangle = V(|\psi\rangle)$ is the output of the isometry in Theorem 26 applied to Alice and Bob's shared state $|\psi\rangle$.*

Proof. Recall from Fact 23, we know that

$$\forall \mathbf{p}, \quad \mathbb{E}_{\mathbf{r},\mathbf{c}} \langle\psi|A^{\mathbf{c}}_{\mathbf{r},\mathbf{p}} B^{\mathbf{r}}_{\mathbf{c},\mathbf{p}}|\psi\rangle \geq 1 - \varepsilon.$$

By applying the consistency relations Equation (3.4) and Equation (3.5) guaranteed by

Theorem 25, we obtain that

$$\forall \mathbf{p}, \quad \mathbb{E}_{\mathbf{r},\mathbf{c}} \langle \psi | \prod_{k=1}^{n} (\tilde{A}^{c_k}_{r_k,k})^{p_k} \prod_{k=1}^{n} (\tilde{B}^{r_k}_{c_k,k})^{p_k} | \psi \rangle \geq 1 - O(n\sqrt{\varepsilon}).$$

Now, by Lemma 41, we can switch the $\tilde{A}$ and $\tilde{B}$ operators to approximate Paulis:

$$\forall \mathbf{p}, \quad \mathbb{E}_{\mathbf{r},\mathbf{c}} \langle \psi | (X^{\mathbf{a}} Z^{\mathbf{b}}) ((X^B)^{\mathbf{c}} (Z^B)^{\mathbf{d}}) | \psi \rangle \geq 1 - O(n\sqrt{\varepsilon}).$$

Applying Theorem 26, we obtain that

$$\forall \mathbf{p}, \quad \langle \phi | \mathbb{E}_{\mathbf{r},\mathbf{c}} (\sigma^A_X(\mathbf{a}) \sigma^A_Z(\mathbf{b}) \sigma^B_X(\mathbf{c}) \sigma^B_Z(\mathbf{d})) | \phi \rangle \geq 1 - O(n^2\sqrt{\varepsilon}).$$

In particular, taking an expectation over uniformly random choices of $\mathbf{p}$, we obtain that

$$\langle \phi | \mathbb{E}_{\mathbf{r},\mathbf{c},\mathbf{p}} (\sigma^A_X(\mathbf{a}) \sigma^A_Z(\mathbf{b}) \sigma^B_X(\mathbf{c}) \sigma^B_Z(\mathbf{d})) | \phi \rangle \geq 1 - O(n^2\sqrt{\varepsilon}).$$

It is not hard to see that $\mathbb{E}_{\mathbf{r},\mathbf{c},\mathbf{p}} (\sigma^A_X(\mathbf{a}) \sigma^A_Z(\mathbf{b}) \sigma^B_X(\mathbf{c}) \sigma^B_Z(\mathbf{d}))$ 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. □

3.5 Discussion and open questions

The reader familiar with previous self-testing results may notice that our Theorem 26 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 42, 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. One open question of interest is to reduce the question and answer length of the test without sacrificing the error scaling. This 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 [45, 70]. Rigidity has also been applied to secure delegated computation and quantum key distribution: in particular, the work of Reichardt, Unger, and Vazirani [83] 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 [66], 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 [65], but with only two provers instead of n?

Appendix B

B.1 Properties of the State-Dependent Distance

Definition 43. *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 44. *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 45. *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 44,

$$d_\psi(DA, DC) \leq d_\psi(DA, DB) + d_\psi(DB, DC).$$

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 46. *Let $\{A_i\}$ and $\{B_i\}$ be two sets of operators indexed by $i \in [N]$, and suppose that*

$$\mathbb{E}_i d_\psi(A_i, B_i)^2 = \delta.$$

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.

$$\begin{aligned} d_{\psi'}(\tilde{A}, \tilde{B}) &= \|\tilde{A}|\psi'\rangle - \tilde{B}|\psi'\rangle\|^2 \\ &= \|\frac{1}{\sqrt{N}} \sum_i A_i|\psi\rangle \otimes |i\rangle - \frac{1}{\sqrt{N}} \sum_i B_i|\psi\rangle \otimes |i\rangle\|^2 \\ &= \frac{1}{N} \sum_i \langle\psi|(A_i^\dagger A_i + B_i^\dagger B_i - A_i^\dagger B_i - B_i^\dagger A_i)|\psi\rangle \\ &= \mathbb{E}_i d_\psi(A_i, B_i)^2 \\ &= \delta. \end{aligned}$$

□

Lemma 47. *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,

$$\left|\langle\sigma|(T-S)(T'-S)|\sigma\rangle\right| \leq \|(T-S)|\sigma\rangle\| \cdot \|(T'-S)|\sigma\rangle\| \leq \sqrt{2\delta} \cdot \sqrt{2\delta} = 2\delta.$$

Expanding out the Left Hand Side, now gives

$$\begin{aligned} 2\delta &\geq \left|\langle\sigma|(T-S)(T'-S)|\sigma\rangle\right| = \left|\langle\sigma|T \cdot T'|\sigma\rangle - \langle\sigma|T \cdot S|\sigma\rangle - \langle\sigma|S \cdot T'|\sigma\rangle + \langle\sigma|S \cdot S|\sigma\rangle\right| \\ &= \left|\langle\sigma|T \cdot T'|\sigma\rangle - \langle\sigma|T \cdot S|\sigma\rangle - \langle\sigma|S \cdot T'|\sigma\rangle + 1\right| \end{aligned}$$

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 48. *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 49. *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 48.

$$\begin{aligned} d_\psi(A_1 \dots A_k, A'_1 \dots A'_k) &\leq d_\psi(A_1 \dots A_k, B_k \dots B_1) + d_\psi(B_k \dots B_1, A'_1 \dots A'_k) \\ &\leq n\varepsilon_1 + n\varepsilon_2. \end{aligned}$$

□

Lemma 50. *Let $A_1, \dots A_k$ be Hermitian operators on Alice's space, and $B_1, \dots, B_k$ be Hermitian operators on Bob's space. Suppose that*

$$\forall i, \quad d_\psi(A_i, B_i) \leq \varepsilon_1$$

and

$$\forall i, j \in \{1, \dots, k-1\}, j \in \{k\}, \quad d_\psi(A_i A_j, \alpha_{ij} A_j A_i) \leq \varepsilon_2$$

where $\alpha_{ij} \in \{\pm 1\}$ for each choice of i, j. Then

$$d_\psi(A_1 \dots A_k, \alpha_{1k}\alpha_{2k} \dots \alpha_{k-1,k} A_k A_1 A_2 \dots A_{k-1}) \leq 2(k-2)\varepsilon_1 + (k-1)\varepsilon_2.$$

Proof.

$$
\begin{aligned}
&d_\psi(A_1 \dots A_k, (\prod_{i=1}^{k-1} \alpha_{ik}) A_k A_1 \dots A_{k-1}) \\
&\quad \le d_\psi(A_1 \dots A_k, \alpha_{k-1,k} A_1 \dots A_{k-2} A_k A_{k-1}) \\
&\qquad + d_\psi(\alpha_{k-1,k} A_1 \dots A_{k-2} A_k A_{k-1}, \alpha_{k-1,k} B_{k-1} A_1 \dots A_{k-2} A_k) \\
&\qquad + d_\psi(\alpha_{k-1,k} B_{k-1} A_1 \dots A_{k-2} A_k, \alpha_{k-1,k} \alpha_{k-2,k} B_{k-1} A_1 \dots A_{k-3} A_k A_{k-2}) \\
&\qquad + d_\psi(\alpha_{k-1,k} \alpha_{k-2,k} B_{k-1} A_1 \dots A_{k-3} A_k A_{k-2}, \alpha_{k-1,k} \alpha_{k-2,k} B_{k-1} B_{k-2} A_1 \dots A_{k-3} A_k) \\
&\qquad + \dots \\
&\qquad + d_\psi(\prod_{i=2}^{k-1} \alpha_{ik} B_{k-1} \dots B_2 A_1 A_k, \prod_{i=1}^{k-1} \alpha_{ik} B_{k-1} \dots B_2 A_k A_1) \\
&\qquad + d_\psi(\prod_{i=1}^{k-1} \alpha_{ik} B_{k-1} \dots B_2 A_k A_1, \prod_{i=1}^{k-1} \alpha_{ik} A_k A_1 \dots A_{k-1}) \\
&\quad \le d_\psi(A_{k-1} A_k, \alpha k-1, k A_k A_{k-1}) + d_\psi(A_{k-1}, B_{k-1}) + \dots + d_\psi(A_2 A_k, \alpha 2k A_k A_2) + d_\psi(A_2, B_2) \\
&\qquad + d_\psi(A_1 A_k, \alpha 1k A_k A_1) + d_\psi(B_2, A_2) + \dots + d_\psi(B_k, A_k) \\
&\quad \le 2(k-2)\varepsilon_1 + (k-1)\varepsilon_2
\end{aligned}
$$

□

As a consequence of the preceding lemma

Lemma 51. *Let $S_1, \dots, S_k, T_1, \dots, T_k$ be Hermitian operators on Alice's space and let $S_1^B, \dots S_k^B, T_1^B \dots T_k^B$ be Hermitian operators on Bob's space, satisfying*

$$
\begin{aligned}
\forall i, \quad & d_\psi(S_i, S_i^B) \le \varepsilon_1 \\
\forall i, \quad & d_\psi(T_i, T_i^B) \le \varepsilon_2 \\
\forall i, j, \quad & d_\psi(S_i T_j, \alpha_{ij} T_j S_i) \le \varepsilon_3.
\end{aligned}
$$

Then

$$d_\psi(S_1 \dots S_k T_1 \dots T_k, \prod_{i,j=1}^{k} \alpha_{ij} T_1 \dots T_k S_1 \dots S_k) \leq 2(k-1)\varepsilon_2 + k(2(k-1)\varepsilon_1 + k\varepsilon_3). \quad \text{(B.1)}$$

Likewise,

$$d_\psi(S_1 \dots S_k T_1 \dots T_k, \prod_{i=2}^{k} \prod_{j=1}^{i-1} \alpha_{ij} S_1 T_1 S_2 T_2 \dots S_k T_k) \leq 2(k-1)\varepsilon_2 + \sum_{j=2}^{k} (2(j-2)\varepsilon_2 + (j-1)\varepsilon_3) \quad \text{(B.2)}$$

Proof. We first prove Equation (B.1).

$$\begin{aligned}
&d_\psi(S_1 \dots S_k T_1 \dots T_k, \prod_{i,j=1}^{k} \alpha_{ij} T_1 \dots T_k S_1 \dots S_k) \\
&\quad \leq d_\psi(S_1 \dots S_k T_1 \dots T_k, T_k^B \dots T_2^B S_1 \dots S_k T_1) \\
&\qquad + d_\psi(T_k^B \dots T_2^B S_1 \dots S_k T_1, \prod_{i=1}^{k} \alpha_{i1} T_k^B \dots T_2^B T_1 S_1 \dots S_k) \\
&\qquad + d_\psi(\prod_{i=1}^{k} \alpha_{i1} T_k^B \dots T_2^B T_1 S_1 \dots S_k, \prod_{i=1}^{k} \alpha_{i1} T_k^B \dots T_3^B T_1 S_1 \dots S_k T_2) \\
&\qquad + d_\psi(\prod_{i=1}^{k} \alpha_{i1} T_k^B \dots T_3^B T_1 S_1 \dots S_k T_2, \prod_{i=1}^{k} \alpha_{i1}\alpha_{i2} T_k^B \dots T_3^B T_1 T_2 S_1 \dots S_k) \\
&\qquad + \dots \\
&\qquad + d_\psi(\prod_{i=1}^{k} \prod_{j=1}^{k-1} \alpha_{ij} T_k^B T_1 \dots T_{k-1} S_1 \dots S_k, \prod_{i=1}^{k} \prod_{j=1}^{k-1} \alpha_{ij} T_1 \dots T_{k-1} S_1 \dots S_k T_k) \\
&\qquad + d_\psi(\prod_{i=1}^{k} \prod_{j=1}^{k-1} \alpha_{ij} T_1 \dots T_{k-1} S_1 \dots S_k T_k, \prod_{i,j=1}^{k} \alpha_{ij} T_1 \dots T_k S_1 \dots S_k) \\
&\quad \leq 2(k-1)\varepsilon_2 + k(2(k-1)\varepsilon_1 + k\varepsilon_3).
\end{aligned}$$

The derivation of Equation (B.2) is very similar. The only difference is that the number of commutations of S with T is different. □

B.2 The Single Round Case

In this section, we review the self-testing result of [99] 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. 3-1. 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. 3-2, 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:

$$
\begin{aligned}
W_1 &= \sum_{a_0,a_1} (-1)^{a_0} P_2^{a_0,a_1} && = A_2^0 \\
W_2 &= \sum_{a_0,a_1} (-1)^{a_1} P_2^{a_0,a_1} && = A_2^1,
\end{aligned}
$$

and two for Bob:

$$
\begin{aligned}
W_3 &= \sum_{b_0,b_1} (-1)^{b_0} Q_2^{b_0,b_1} && = B_2^0 \\
W_4 &= \sum_{b_0,b_1} (-1)^{b_1} Q_2^{b_0,b_1} && = B_2^1.
\end{aligned}
$$

There are nine consistency conditions implied by winning the game with probability $1-\varepsilon$:

$$\langle\psi|Z_1Z_3|\psi\rangle \geq 1-9\varepsilon \tag{B.3}$$

$$\langle\psi|Z_2Z_4|\psi\rangle \geq 1-9\varepsilon \tag{B.4}$$

$$\langle\psi|Z_1Z_2W_3|\psi\rangle \geq 1-9\varepsilon \tag{B.5}$$

$$\langle\psi|X_2X_4|\psi\rangle \geq 1-9\varepsilon \tag{B.6}$$

$$\langle\psi|X_1X_3|\psi\rangle \geq 1-9\varepsilon \tag{B.7}$$

$$\langle\psi|X_1X_2W_4|\psi\rangle \geq 1-9\varepsilon \tag{B.8}$$

$$-\langle\psi|W_1Z_3X_4|\psi\rangle \geq 1-9\varepsilon \tag{B.9}$$

$$-\langle\psi|W_2Z_4X_3|\psi\rangle \geq 1-9\varepsilon \tag{B.10}$$

$$-\langle\psi|W_1W_2W_3W_4|\psi\rangle \geq 1-9\varepsilon. \tag{B.11}$$

From this we obtain anticommutation conditions

$$\begin{aligned}
X_1Z_1 &\approx X_1Z_2W_3 && \text{(by (B.5))}\\
&= W_3X_1Z_2\\
&\approx W_3X_1Z_4 && \text{(by (B.4))}\\
&\approx W_3Z_4X_3 && \text{(by (B.7))}\\
&\approx -W_3W_2 && \text{(by (B.10))}\\
&\approx W_3W_1W_3W_4 && \text{(by (B.11))}\\
&= W_1W_4\\
&\approx -W_4Z_3X_4 && \text{(by (B.9))}\\
&\approx -Z_1W_4X_4 && \text{(by (B.3))}\\
&\approx -Z_1X_2W_4 && \text{(by (B.6))}\\
&\approx -Z_1X_2X_2X_1 && \text{(by (B.8))}\\
&= -Z_1X_1.
\end{aligned}$$

We can also get commutation relations on different qubits:

$$\begin{aligned} X_1 Z_2 &\approx X_1 Z_4 && \text{(by (B.4))} \\ &\approx Z_4 X_3 && \text{(by (B.7))} \\ &= X_3 Z_4 && \text{(by construction)} \\ &\approx X_3 Z_2 && \text{(by (B.4))} \\ &\approx Z_2 X_1 && \text{(by (B.7)).} \end{aligned}$$

The other cases follow similarly. See [99] for further details.

Chapter 4

Interactive proofs with approximately commuting provers

The class MIP* of promise problems that can be decided through an interactive proof system with multiple entangled provers provides a complexity-theoretic framework for the exploration of the nonlocal properties of entanglement. Very little is known in terms of the power of this class. The only proposed approach for establishing upper bounds is based on a hierarchy of semidefinite programs introduced independently by Pironio et al. and Doherty et al. in 2006. This hierarchy converges to a value, the field-theoretic value, that is only known to coincide with the provers' maximum success probability in a given proof system under a plausible but difficult mathematical conjecture, Connes' embedding conjecture. No bounds on the rate of convergence are known.

In this chapter we introduce a rounding scheme for the hierarchy, establishing that any solution to its N-th level can be mapped to a strategy for the provers in which measurement operators associated with distinct provers have pairwise commutator bounded by $O(\ell^2/\sqrt{N})$ in operator norm, where ℓ is the number of possible answers per prover.

Our rounding scheme motivates the introduction of a variant of quantum multiprover interactive proof systems, called MIP^*_δ, in which the soundness property is required to

hold against provers allowed to operate on the same Hilbert space as long as the commutator of operations performed by distinct provers has norm at most δ. Our rounding scheme implies the upper bound $\mathrm{MIP}^*_\delta \subseteq \mathrm{DTIME}(\exp(\exp(\mathrm{poly})/\delta^2))$. In terms of lower bounds we establish that $\mathrm{MIP}^*_{2^{-\mathrm{poly}}}$, with completeness 1 and soundness $1 - 2^{-\mathrm{poly}}$, contains NEXP. The relationship of MIP^*_δ to MIP^* has connections with the mathematical literature on approximate commutation. Our rounding scheme gives an elementary proof that the Strong Kirchberg Conjecture implies that MIP^* is computable. We also discuss applications to device-independent cryptography.

4.1 Introduction

In a multiprover interactive proof system, a *verifier* with bounded resources (a polynomial-time Turing machine) interacts with multiple all-powerful but non-communicating *provers* in an attempt to verify the truth of a mathematical statement — the membership of some input x, a string of bits, in a language L, such as 3-SAT. The provers always collaborate to maximize their chances of making the verifier accept the statement, and their maximum probability of success in doing so is called the *value* $\omega = \omega(x)$ of the protocol. (We will sometimes refer to a given protocol as an "interactive game".) A proof system's *completeness* c is the smallest value of $\omega(x)$ over all $x \in L$, while its soundness s is the largest value of $\omega(x)$ over $x \notin L$; a protocol is sound if $s < c$.

The class of all languages that have multiprover interactive proof systems with $c \geq 2/3$ and $s \leq 1/3$, denoted MIP, is a significant broadening of its non-interactive, single-prover analogue MA, as is witnessed by the characterization MIP = NEXP [7]. This result is one of the cornerstones on which the PCP theorem [6, 5] was built, with consequences ranging from cryptography [11] to hardness of approximation [35].

Quantum information suggests a natural extension of the class MIP. The laws of quantum mechanics assert that, in the physical world, a set of non-communicating provers may share an arbitrary entangled quantum state, a physical resource which strictly ex-

tends their set of strategies but provably does not allow them to communicate. The corresponding extension of MIP is the class MIP* of all languages that have multiprover interactive proof systems with entangled provers [50].

Physical intuition for the significance of the prover's new resource, entanglement, dates back to Einstein, Podolsky and Rosen's paradoxical account [32] of the consequences of quantum entanglement, later clarified through Bell's pioneering work [10]. To state the relevance of Bell's results more precisely in our context we first introduce the mathematical formalism used by Bell to model locality. With each prover's private space is associated a separate Hilbert space. The joint quantum state of the provers is specified by a unit vector $|\Psi\rangle$ in the tensor product of their respective Hilbert spaces. Upon receiving its query from the verifier, each prover applies a local measurement (a positive operator supported on its own Hilbert space) the outcome of which is sent back to the verifier as its answer. The supremum of the provers' probability of being accepted by the verifier, taken over all Hilbert spaces, states in their joint tensor product, and local measurements, is called the entangled value ω^* of the game. The analogue quantity for "classical" provers (corresponding to shared states which are product states) is denoted ω.

Bell's work and the extensive literature on Bell inequalities [18, 4] and quantum games [19] establishes that there are protocols, or interactive games, for which $\omega^* > \omega$. This simple fact has important consequences for interactive proof systems. First, a proof system sound with classical provers may no longer be so in the presence of entanglement. Cleve et al. [19] exhibit a class of restricted interactive proof systems, XOR proof systems, such that the class with classical provers equals NEXP while the same proof systems with entangled provers cannot decide any language beyond EXP. Second, the completeness property of a proof system may also increase through the provers' use of entanglement. As a result optimal strategies may require the use of arbitrarily large Hilbert spaces for the provers — no explicit bound on the dimension of these spaces is known as a function of the size of the game. In fact no better upper bound on the class MIP* is known other than its

languages being recursively enumerable: they may not even be decidable! This unfortunate state of affairs stems from the fact that, while the value ω^* may be approached from below through exhaustive search in increasing dimensions, there is no verifiable criterion for the termination of such a procedure.

Bounding entangled-prover strategies. The question of deriving algorithmic methods for placing upper bounds on the entangled value ω^* of a given protocol has long frustrated researchers' efforts. Major progress came in 2006 through the introduction of a hierarchy of relaxations based on semidefinite programming [31, 71] that we will refer to as the QC SDP hierarchy.[1] These relaxations follow a similar spirit as e.g. the Lasserre hierarchy in combinatorial optimization [53], and can be formulated using the language of sums of squares of *non-commutative* polynomials. In contrast with the commutative setting, this leads to a hierarchy that is in general infinite and need not converge at any finite level.

The limited convergence results that are known for the QC SDP hierarchy involve a formalization of locality for quantum provers which originates in the study of infinite-dimensional systems such as those that arise in quantum field theory. Here the idea is that observations made at different space-time locations should be represented by operators which, although they may act on the same Hilbert space, should nevertheless commute — a minimal requirement ensuring that the joint outcome of any two measurements made by distinct parties should be well-defined and independent of the order in which the measurements were performed.

For the case of finite-dimensional systems this seemingly weaker condition is equivalent to the existence of a tensor product representation [31]. In contrast, for the case of infinite-dimensional systems the two formulations are not known to be equivalent. This question, known as Tsirelson's problem in quantum information, was recently shown to be equivalent to a host of deep mathematical conjectures [86, 47], in particular Connes' embedding

[1] Here "QC" stands for "Quantum Commuting".

conjecture [23] and Kirchberg's QWEP conjecture [49]. The validity of these conjectures has a direct bearing on our understanding of MIP*. The QC SDP hierarchy is known to converge to a value called the *field-theoretic value* ω^f of the game, which is the maximum success probability achievable by commuting strategies of the type described above. A positive answer to Tsirelson's conjecture thus implies that $\omega^* = \omega^f$ and both quantities are computable. However, even assuming the conjecture and in spite of strong interest (the use of the first few levels of the hierarchy has proven extremely helpful to study a range of questions in device independence [8, 100] and the study of nonlocality [76]) absolutely no bounds have been obtained on the convergence rate of the hierarchy. It is only known that if a certain technical condition, called a rank loop, holds, then convergence is achieved [72]; unfortunately the condition is computationally expensive to verify (even for low levels of the hierarchy) and, in general, may not be satisfied at any finite level.

Beyond the obvious limitations for practical applications, these severe computational difficulties are representative of the intrinsic difficulty of working with the model of entangled provers. Our work is motivated by this state of affairs: we establish the first quantitative convergence results for the quantum SDP hierarchy. Our main observation is that successive levels of the hierarchy place bounds on the value achievable by provers employing a relaxed notion of strategy in which measurements applied by distinct provers are allowed to *approximately commute*: their commutator is bounded, in operator norm, by a quantity that tends to zero as the number of levels in the hierarchy grows.

A rounding scheme for the QC SDP hierarchy

Our main technical result is a rounding procedure for the QC SDP hierarchy of semidefinite programs. The procedure maps any feasible solution to the N-th level of the hierarchy to a set of measurement operators for the provers that approximately commute. For simplicity we state and prove our results for the case of a single round of interaction with two provers and classical messages only. Extension to multiple provers is straightforward; we

expect generalizations to multiple rounds and quantum messages to be possible but leave them for future work.

Definition 52. *An (m, ℓ) strategy for the provers is specified by two sets of m POVMS $\{A_x^a\}_{1\leq a\leq \ell}$ and $\{B_y^b\}_{1\leq b\leq \ell}$ with ℓ outcomes each, where $x, y \in \{1, \ldots, m\}$.*

A strategy is said to be δ-AC if for every x, y, a and b, $\|A_x^a B_y^b - B_y^b A_x^a\| \leq \delta$, where $\|\cdot\|$ denotes the operator norm.

Our main theorem on the QC SDP hierarchy can be stated as follows. (We refer to Section 4.2.2 for a definition of the hierarchy.)

Theorem 53. *Let G be a 2-prover one-round game with classical messages in which each prover has ℓ possible answers, and $\omega_{QCSDP}^N(G)$ the optimum of the N-th level of the QC SDP hierarchy. Then there exists a $\delta = O(\ell^2/\sqrt{N})$ and a δ-AC strategy for the provers with success probability $\omega_{QCSDP}^N(G)$ in G.*[2]

Our result is the first to derive the condition that the *operator norm* of commutators is small. In contrast it is not hard to show that a feasible solution to the first level of the hierarchy already gives rise to measurement operators that exactly satisfy a commutation relation *when evaluated on the state* (corresponding to the zeroth-order vector provided by the hierarchy). While the latter condition can be successfully exploited to give an exact rounding procedure from the first level for the class of XOR games [19], and an approximate rounding for the more general class of unique games [48], we do not expect it to be sufficient in general. In particular, even approximate tightness of the first level of the hierarchy for three-prover games would imply EXP = NEXP [95]. We will further show that the problem of optimizing over strategies which approximately commute, to within sufficiently small error and in *operator norm*, is NEXP-hard (see Section 4.1 for details).

[2]Due to the approximate commutation of the provers' strategies the success probability of δ-AC strategies may a priori depend on the order in which the measurement operators are applied. In our context the parameter δ will always be small enough that we can neglect this effect. Moreover, for the particular kind of strategies constructed in our rounding scheme the value will not be affected by the order.

The proof of Theorem 53 is constructive: starting from any feasible solution to the N-th level of the QC SDP hierarchy we construct measurement operators for the provers with pairwise commutators bounded by δ in operator norm, and which achieve a value in the game that equals the objective value of the N-th level SDP. Recall that this SDP has $O(m\ell)^N$ vector variables indexed by strings of length at most N over the formal alphabet $\{P_x^a, Q_y^b\}$ containing a symbol for each possible (question,answer) pair to any of the provers. Our main idea is to introduce a "graded" variant of the construction in [72] (which was used to show convergence under the rank loop constraint). Rather informally, the rounded measurement operators, $\{\tilde{P}_x^a\}$ for the first prover and $\{\tilde{Q}_y^b\}$ for the second, can be defined as follows:

$$\tilde{P}_x^a \equiv \frac{1}{N-1}\sum_{i=1}^{N-1} \Pi_{\leq i}\Pi_{P_x^a}\Pi_{\leq i} \quad \text{and} \quad \tilde{Q}_y^b \equiv \frac{1}{N-1}\sum_{j=1}^{N-1} \Pi_{\leq j}\Pi_{Q_y^b}\Pi_{\leq j}.$$

Here $\Pi_{P_x^a}$ and $\Pi_{Q_y^b}$ are projectors as defined in [72], i.e. as the projection onto vectors associated with strings ending in the formal label P_x^a, Q_y^b of the corresponding operator. The novelty is the introduction of the $\Pi_{\leq i}$, which project onto the subspace spanned by all vectors associated with strings of length at most i. Thus $\tilde{P}_x^a$ itself is not a projector, and it gives more weight to vectors indexed by shorter strings.

The intuition behind this rounding scheme is as follows. The winning probability is unchanged because it is determined by the action of the measurement operators on the subspace $\mathrm{Im}(\Pi_{\leq 1})$. On the other hand, the rounded operators approximately commute in the operator norm because the original operators commuted exactly on the subspace $\mathrm{Im}(\Pi_{\leq N-1})$, and we have now shifted the weight of the operators so that they are supported on that subspace. Furthermore, while truncating the operators abruptly at level $N-1$ (by conjugating by $\Pi_{\leq N-1}$ for example) could result in a large commutator, we perform a "smooth" truncation across vectors indexed by strings of increasing length.

Interactive proofs with approximately commuting provers

Motivated by the rounding procedure ascertained in Theorem 53 we propose a modification of the class MIP* in which the assumption that isolated provers must perform perfectly commuting measurements is relaxed to a weaker condition of *approximately commuting* measurements.

Definition 54. *Let* $\mathrm{MIP}^*_\delta(k, c, s)$ *be the class of promise problems* (L_{yes}, L_{no}) *that can be decided by an interactive proof system in which the verifier exchanges a single round of classical messages with k quantum provers* $P_1, \ldots, P_k$ *and such that:*

- *If the input* $x \in L_{yes}$ *then there exists a perfectly commuting strategy for the provers that is accepted with probability at least c,*
- *If* $x \in L_{no}$ *then any* δ*-AC strategy is accepted with probability at most s.*

Note that the definition of MIP^*_δ requires the completeness property to be satisfied with perfectly commuting provers; indeed we would find it artificial to seek protocols for which optimal strategies in the "honest" case would be required to depart from the commutation condition. Instead, only the soundness condition is relaxed by giving *more* power to the provers, who are now allowed to apply any "approximately commuting" strategy. The "approximately" is quantified by the parameter δ,[3] and for any $\delta' \leq \delta$ the inclusions $\mathrm{MIP}^*_\delta \subseteq \mathrm{MIP}^*_{\delta'} \subseteq \mathrm{MIP}^*$ trivially hold. It is important to keep in mind that while δ can be a function of the size of the protocol it must be independent of the dimension of the provers' operators, which is unrestricted.

δ-AC strategies were previously considered by Ozawa [75] in connection with Tsirelson's problem. Ozawa proposes a conjecture, the "Strong Kirchberg Conjecture (I)", which if true implies the equality $\mathrm{MIP}^* = \cup_{\delta>0} \mathrm{MIP}^*_\delta$. We state and discuss the conjecture further as Conjecture 80 below. Unfortunately the conjecture seems well beyond the reach of

[3] As a first approximation the reader may think of δ as a parameter that is inverse exponential in the input length $|x|$. In terms of games, this corresponds to δ being inverse polynomial in the number of questions in the game, which is arguably the most natural setting of parameters.

current techniques (Ozawa himself formulates doubts as to its validity). However, in our context less stringent formulations of the conjecture would still imply conclusive results relating MIP^*_δ to MIP^*; we discuss such variants in Section 4.5.

Further motivation for the definition of MIP^*_δ may be found by thinking operationally — with e.g. cryptographic applications in mind, how does one ascertain that "isolated" provers indeed apply commuting measurements? The usual line of reasoning applies the laws of quantum mechanics and special relativity to derive the tensor product structure from space-time separation. However, not only is strict isolation virtually impossible to enforce in all but the simplest experimental scenarios, but the implication "separation $\Longrightarrow$ tensor product" may itself be subject to questioning — in particular it may not be a testable prediction, at least not to precision that exceeds the number of measurements, or observations, performed. Relaxations of the tensor product condition have been previously considered in the context of device-independent cryptography; for instance Silman et al. [89] require that the joint measurement performed by two isolated devices be close, in operator norm, to a tensor product measurement. Our approximate commutation condition imposes a weaker requirement, and thus our convergence results on the hierarchy also apply to their setting; we discuss this in more detail in Section 4.5.2.

Theorem 53 can be interpreted as evidence that the hierarchy converges at a polynomial rate to the maximum success probability for MIP^*_{ac} provers. More formally, it implies the inclusion $\mathrm{MIP}^*_\delta \subseteq \mathrm{TIME}(\exp(\exp(\mathrm{poly})/\delta^2))$ for any $\delta > 0$, thereby justifying our claim that the class MIP^*_δ is computationally bounded. This stands in stark contrast with $\mathrm{MIP}^* = \mathrm{MIP}^*_0$, for which no quantitative upper bound is known (We note, however, that MIP^* is known to be recursively enumerable).

Having shown that the new class has "reasonable" complexity, it is natural to ask whether the additional power granted to the provers might actually make the class trivial — could provers that are δ-AC be no more useful than a single quantum prover, even for very small δ? The following theorem shows that this is not the case.

Theorem 55. *Every language in* NEXP *has a 2-prover* MIP^* *protocol in which completeness* 1

holds with classical provers and soundness $2^{-\text{poly}}$ *holds even against provers thate are* $2^{-\text{poly}}$*-AC. More formally,*

$$\text{NEXP} \subseteq \bigcup_{p,q \in \text{poly}} \text{MIP}^*_{2^{-q}}(2, 1, 1 - 2^{-p}).$$

Theorem 55 provides a direct analogue of the same lower bound for MIP* [41], and is proven using the same technique. We conjecture that the inclusion $\text{NEXP} \subseteq \text{MIP}^*_{2^{-\text{poly}}}(3, 1, 2/3)$ also holds, and that this can be derived by a careful extension of the results in [42, 95].

Organization. Section 4.2 contains some preliminaries, including the definition of MIP^*_{ac} and the QC SDP hierarchy. In Section 4.3 we present and analyze our rounding scheme for the hierarchy. In Section 4.4 we prove our lower bound on MIP*. We end in Section 4.5 with a discussion of the relevance of the study of MIP^*_{ac} for that of MIP* and closely related results from the mathematical literature.

4.2 Preliminaries

Notation. Given an integer N, we use $[N]$ to refer to the set $\{1, \ldots, N\}$. We use the symbol $\equiv$ to mark a definition. $\mathfrak{S}_k$ is the set of all permutations $\sigma : [k] \to [k]$. poly denotes the set of all polynomials. We write $\|X\|$ for the operator norm of a matrix X. Given matrices A, B, $[A, B] \equiv AB - BA$ denotes their commutator.

4.2.1 Approximately commuting provers

In this section we define the class MIP^*_δ for $\delta > 0$ and state some basic properties. We assume the reader is familiar with quantum interactive proof systems and the definition of the class MIP*; we refer to e.g. [50] for details. Throughout we will use k to denote the number of provers and c, s the completeness and soundness parameters. Although one could define the class more generally, we restrict our attention to protocols involving a

single round of interaction between the verifier and the provers. As is customary we will also call such one-round protocols *games*.

Definition 56. *A k-prover game G is specified by the following: integers $Q_1, \ldots, Q_k$, representing the number of possible questions to each prover, and a distribution π on $[Q_1] \times \cdots \times [Q_k]$; integers $A_1, \ldots, A_k$, representing the number of possible answers from each prover; a mapping $V : ([Q_1] \times \cdots \times [Q_k]) \times ([A_1] \times \cdots \times [A_k]) \to \{0, 1\}$ representing the referee's acceptance criterion.*

Next we introduce a notion of *approximately commuting* strategies for the provers.

Definition 57. *Given a game G, a* strategy *for the provers consists of the following:*

- *A finite-dimensional Hilbert space $\mathcal{H}$,*
- *For every $i \in [k]$ and $q \in [Q_i]$, a POVM $\{(A^{(i)})_q^a\}_{a \in [A_i]}$, where each $(A^{(i)})_q^a \in \mathrm{Pos}(\mathcal{H})$ and $\sum_a (A^{(i)})_q^a = \mathrm{Id}$,*
- *A density matrix $\rho \in \mathrm{D}(\mathcal{H})$.*

For any $\delta > 0$ we say that the strategy $((A^{(1)})_q^a, \ldots, (A^{(k)})_{q'}^{a'}, \rho)$ is δ-AC if $\|[(A^{(i)})_q^a, (A^{(j)})_{q'}^{a'}]\| \leq \delta$ for every $i \neq j \in [k]$ and $q \in [Q_i]$, $q' \in [Q_j]$, $a \in [A_i]$ and $a' \in [A_j]$.

Finally we define the success probability, or *value*, achieved by a given strategy in a game.

Definition 58. *Let G be a game and $((A^{(1)})_q^a, \ldots, (A^{(k)})_{q'}^{a'}, \rho)$ a strategy in G. The strategy's value is defined as*

$$\omega^*\big(((A^{(1)})_q^a, \ldots, (A^{(k)})_{q'}^{a'}, \rho); G\big) := \max_{\sigma \in \mathfrak{S}_k} \left| \sum_{q_i \in Q_i} \pi(q_i) \sum_{a_1, \ldots, a_k} V(a_i, q_i) \mathrm{Tr}\big((A^{(\sigma(1))})_{q_{\sigma(1)}}^{a_{\sigma(1)}} \cdots (A^{(\sigma(k))})_{q_{\sigma(k)}}^{a_{\sigma(k)}} \rho\big) \right|.$$

The δ-AC value $\omega_\delta^*(G)$ of the game G is the supremum over all δ-AC strategies of the strategy's value in G.

In the above definition the introduction of the supremum over all permutations of the provers amounts to allowing the provers to choose the order in which their respective

POVM are applied to the shared state (the ordering should be the same throughout, independently of the questions asked). Since POVM elements applied by distinct provers do not necessarily commute the choice of ordering may affect a strategy's value. Nevertheless, for δ-AC strategies it is easy to see that any two orderings will result in values that differ by at most $k^2\delta$; for our purposes the parameter δ will always be small enough that different choices of orderings would not matter and we will mostly ignore this issue throughout. Since we consider only finite-dimensional strategies, for $\delta = 0$ the value $\omega_0^*(G)$ reduces to what is usually called the *entangled value* $\omega^*(G)$, corresponding to strategies that are perfectly commuting, or equivalently strategies that can be put in tensor product form.

Having introduced games, strategies, and values, we are ready to define the class MIP_δ^*.

Definition 59. *Let $\delta, c, s : \mathbb{N} \to [0,1]$ be computable functions and $k \in$ poly. A language L is in $\mathrm{MIP}_\delta^*(k,c,s)$ if and only if there exists a polynomial-time computable mapping from inputs $x \in \{0,1\}^*$ to k-prover games G_x such that:*

- *In the game G_x, the distribution π can be sampled in time polynomial in $|x|$, and the predicate V can be computed in time polynomial in $|x|$,*
- *(Completeness) If $x \in L$ then $\omega^*(G_x) \geq c$, i.e. there exist a k-prover strategy that is 0-AC and has value at least c in G_x,*
- *(Soundness) If $x \notin L$ then $\omega_\delta^*(G_x) \leq s$, i.e. every δ-AC k-prover strategy has value at most s in G_x.*

Throughout this chapter we use poly *to represent any polynomial in $|x|$, or equivalently, any polynomial in the length of the messages passed in the protocol.*

Since for every $\delta < \delta'$ a δ'-AC strategy is also δ-AC, it follows that $\mathrm{MIP}_{\delta'}^*(k,c,s) \subseteq \mathrm{MIP}_\delta^*(k,c,s)$. A choice of parameter δ that is inverse exponential in the input length seems

to be the most natural, and we define

$$\mathrm{MIP}^*_{ac}(k,c,s) := \cup_{\delta \in 2^{-\mathrm{poly}}} \mathrm{MIP}^*_{\delta}(k,c,s).$$

We end this subsection with a simple claim on δ-AC strategies that is well-known to hold for the case of perfectly commuting strategies: up to a small loss in the commutation parameter we may without loss of generality restrict ourselves to strategies that apply projective measurements.

Claim 60. *Let $(A^a_q, B^{a'}_{q'}, \rho)$ be a δ-AC strategy with success probability p in a certain game. Then there exists a $(|A||A'|\delta)$-AC strategy in which all POVM are projective and that achieves the same success probability p.*

Proof. We can make $(A^a_q, B^{a'}_{q'}, \rho)$ (which is defined on some Hilbert space $\mathcal{H}$) into a projective strategy $(\tilde{A}^a_q, \tilde{B}^{a'}_{q'}, \tilde{\rho})$ on an extended Hilbert space $\mathcal{H}' \equiv \mathcal{H} \otimes \mathbb{C}^{|A|} \otimes \mathbb{C}^{|A'|}$ by extending ρ to $\rho \otimes |0\rangle_A\langle 0| \otimes |0\rangle_B\langle 0|$, and defining the norm preserving maps :

$$U^q_A : |\psi\rangle|0\rangle_A|0\rangle_B \to \sum_a (\sqrt{A^a_q}|\psi\rangle)|a\rangle_A|0\rangle_B$$

and

$$U^{q'}_B : |\psi\rangle|0\rangle_A|0\rangle_B \to \sum_{a'} (\sqrt{B^{a'}_{q'}}|\psi\rangle)|0\rangle_A|a'\rangle_B$$

Since the maps are norm-preserving they can be extended to unitary maps $\tilde{U}^q_A \otimes I_B$ and $\tilde{U}^{q'}_B \otimes I_A$ respectively on $\mathcal{H} \otimes \mathbb{C}^{|A|} \otimes \mathbb{C}^{|A'|}$ (note that the unitary for each prover acts as the identity on the ancilla for each other prover). We now define the new POVM operators as

$$\tilde{A}_q^a \equiv \left(\tilde{U}_A^q \otimes I_B\right)\left(I_{\mathcal{H}} \otimes |a\rangle_A\langle a| \otimes I_B\right)\left(\tilde{U}_A^q \otimes I_B\right)^\dagger$$

and

$$\tilde{B}_{q'}^{a'} \equiv \left(\tilde{U}_B^{q'} \otimes I_A\right)\left(I_{\mathcal{H}} \otimes I_A \otimes |a'\rangle_B\langle a'|\right)\left(\tilde{U}_B^{q'} \otimes I_A\right)^\dagger$$

The new operators now form projective POVM strategies, and the transformation clearly preserves the strategy's success probability. Since different provers act on distinct ancilla qubits, and as the identity on the ancillas for all other provers, we see that: $[\tilde{A}_q^a, \tilde{B}_{q'}^{a'}] \leq |A||A'|\delta$. □

4.2.2 The QC SDP Hierarchy

Fix a two-prover game G. Let $X = [Q_1]$ (resp. $Y = [Q_2]$) be the first (resp. second) prover's input alphabet, and $A = [A_1]$ (resp. $B = [A_2]$) the first (resp. second) prover's answer alphabet. Let $V : X \times Y \times A \times B \to \{0,1\}$ be the referee's decision predicate, and $\mu : X \times Y \to [0,1]$ the distribution on inputs. Consider the alphabet of formal symbols $\mathcal{A} \equiv \{P_x^a : \forall x, a\} \cup \{Q_y^b : \forall y, b\}$,[4] and let $W_m \equiv \cup_{i=1}^m \mathcal{A}^i \cup \{\phi\}$ be the set of all words of length at most m on the alphabet $\mathcal{A}$ (here ϕ is a formal symbol representing the empty string). The N^{th} level of QC SDP hierarchy for G defines an optimization problem over the space of positive semidefinite matrices $\Gamma_N \in \mathbb{C}^{|W_N| \times |W_N|}$ with entries $\Gamma_{s,t}^N$ indexed by words $s, t \in W_N$. As in [73], we will let $\{|v_s\rangle : s \in W_N\}$ be vectors in $\mathbb{C}^{|W_N|}$ such that $\Gamma_{s,t}^N = \langle v_s | v_t \rangle$. We can find such vectors by computing, for example, the Cholesky decomposition of Γ^N, which can be done in time polynomial in $|W_N|$.

Definition 61. *The N^{th} level of QC SDP hierarchy is defined to be the following optimization*

[4] Although this is a formal alphabet, P_x^a (resp. Q_y^b) is meant to represent the first (resp. second) provers' POVM element associated with input x (resp. y) and answer a (resp. b).

problem:

$$\textit{maximize} \sum_{(x,y,a,b)} \mu(x,y)\Gamma^N_{P^a_x,Q^b_y} V(x,y,a,b)$$

subject to:

$$\Gamma^N \succeq 0$$

$$\Gamma^N_{\phi,\phi} = 1$$

$$\forall C \in \mathcal{A}, \forall s,t \in W_{N-1}, \Gamma^N_{sC,t} = \Gamma^N_{s,Ct}$$

$$\forall P^a_x, Q^b_y \in \mathcal{A}, \forall s,t \in W_{N-1}, \Gamma^N_{sP^a_x,Q^b_y t} = \Gamma^N_{sQ^b_y,P^a_x t} \tag{4.1}$$

$$\forall x \in X, s \in W_{N-1}, t \in W_N, \sum_{a\in A} \Gamma^N_{sP^a_x,t} = \Gamma^N_{s,t} \tag{4.2}$$

$$\forall y \in Y, s \in W_{N-1}, t \in W_N, \sum_{b\in B} \Gamma^N_{sQ^b_y,t} = \Gamma^N_{s,t}$$

$$\forall x \in X, \forall s,t \in W_{N-1}, \textit{and for } a \neq a', \Gamma^N_{sP^a_x,P^{a'}_x t} = 0 \tag{4.3}$$

$$\forall y \in Y, \forall s,t \in W_{N-1}, \textit{and for } b \neq b', \Gamma^N_{sQ^b_y,Q^{b'}_y t} = 0$$

Note that, in order to make the constraints intuitive, we use the non-standard notation that, whenever as vector $|v_s\rangle$ is transposed, the result of the transpose is written as $\langle v_s| := (|v_{s^\dagger}\rangle)^\dagger$, where $s^\dagger$ is the string written in the reverse order. That is, we use the convention that transposing vectors also reverses the order of their labels.

From here on we let $\Gamma^N_{s,t} = \langle v_s|v_t\rangle$ represent an optimal solution to the N^{th} level of the QC SDP hierarchy. By definition,

$$\omega^N_{QCSDP}(G) = \sum_{(x,y,a,b)} \mu(x,y)\Gamma^N_{P^a_x,Q^b_y} V(x,y,a,b) = \sum_{(x,y,a,b)} \mu(x,y)\langle v_{P^a_x}|v_{Q^b_y}\rangle V(x,y,a,b).$$

Definition 62. *Let $V_j \equiv Span\{|v_s\rangle : s \in W_j\}$ denote the vector space spanned by all the vectors*

with labels of length $\leq j$. Note that, for a solution to the N^{th} level of the QC SDP hierarchy, V_N is the entire space spanned by all the vectors in the Cholesky decomposition of Γ^N.

Observation 63.

$$\forall x \in X, s \in W_{N-1}, t \in W_N, \sum_{a \in A} \langle v_{sP_x^a}| = \langle v_s| \tag{4.4}$$

$$\forall y \in Y, s \in W_{N-1}, t \in W_N, \sum_{b \in B} \langle v_{sQ_y^b}| = \langle v_s| \tag{4.5}$$

Proof. We give the proof of equation (4.4). The proof for equation (4.5) is completely analogous. Consider the vector $|z\rangle \equiv |v_s\rangle - \sum_{a \in A} |v_{sP_x^a}\rangle$. By definition we have that $|z\rangle \in V_N$. On the other hand, for every vector $|v_t\rangle$ (for any $t \in W_N$), it follows from equation (4.2) that $\langle z|v_t\rangle = \langle v_s|v_t\rangle - \sum_{a \in A} \langle v_{sP_x^a}|v_t\rangle = 0$. Thus we must have $|z\rangle = 0$, and the claim follows. □

Definition 64. *As in [73], for each $P_x^a \in \mathcal{A}$, let $\Pi_{P_x^a}$ denote the projector onto $Span\{|v_{P_x^a s}\rangle : s \in W_{N-1}\}$. Similarly, for each $Q_y^b \in \mathcal{A}$, let $\Pi_{Q_y^b}$ denote the projector onto $Span\{|v_{Q_y^b s}\rangle : s \in W_{N-1}\}$.*

Observation 65. *Note that, as observed in [73], for each $P_x^{a'} \in \mathcal{A}$, and for all $s \in W_{N-1}$ we have that:*

$$\Pi_{P_x^{a'}}|v_s\rangle = \Pi_{P_x^{a'}} \sum_{a \in A} |v_{P_x^a s}\rangle = \Pi_{P_x^{a'}}|v_{P_x^{a'} s}\rangle = |v_{P_x^{a'} s}\rangle \tag{4.6}$$

This follows from equation (4.3) *and Observation 63. The analogous statement holds for $Q_y^{b'} \in \mathcal{A}$, and $\Pi_{Q_y^{b'}}$.*

Definition 66. *For each $j \leq N$, let $\Pi_{\leq j}$ denote the orthogonal projector onto V_j, and $\Pi_{\leq j}^{\perp} \equiv I - \Pi_{\leq j}$.*

4.2.3 Useful identities

The following identities involving the projection operators defined in the previous section will be used in the analysis of our rounding scheme in Section 4.3.

Proposition 67. $\forall i, j \in [N]$:

$$\Pi_{\leq i}\Pi_{\leq j} = \Pi_{\leq j}\Pi_{\leq i} = \Pi_{\leq \min(i,j)} \tag{4.7}$$

$$\Pi^{\perp}_{\leq i}\Pi^{\perp}_{\leq j} = \Pi^{\perp}_{\leq j}\Pi^{\perp}_{\leq i} = \Pi^{\perp}_{\leq \max(i,j)}. \tag{4.8}$$

Furthermore, for $i \geq j \in [N]$,

$$\Pi_{\leq j}\Pi^{\perp}_{\leq i} = \Pi^{\perp}_{\leq i}\Pi_{\leq j} = 0, \tag{4.9}$$

Proof. All three equations follow trivially from the definition of $\Pi_{\leq i}$ as the orthogonal projector on V_i and the inclusion $V_j \subseteq V_i$ for $j \leq i$. □

Proposition 68. $\forall (x, y, a, b) \in X \times Y \times A \times B$, *and* $\forall i, j < N$,

$$\Pi_{\leq i}\Pi_{P^a_x}\Pi_{Q^b_y}\Pi_{\leq j} = \Pi_{\leq i}\Pi_{Q^b_y}\Pi_{P^a_x}\Pi_{\leq j}.$$

Proof. Consider any two vectors $|z\rangle, |w\rangle \in V_N$. By definition, we have that $\Pi_{\leq i}|z\rangle \in \mathrm{Im}\,(\Pi_{\leq i}) \equiv V_i = \mathrm{Span}\{|v_s\rangle : s \in W_i\}$, so we can expand them in this vector space: $\Pi_{\leq i}|z\rangle \equiv \sum_{s\in W_i} \lambda_s |v_s\rangle$. Similarly, $\Pi_{\leq j}|w\rangle \equiv \sum_{t\in W_j} \gamma_t |v_t\rangle$. So,

$$\begin{aligned}
\langle z|\Pi_{\leq i}\Pi_{P^a_x}\Pi_{Q^b_y}\Pi_{\leq j}|w\rangle &= \Big(\sum_{s\in W_i} \lambda_s^* \langle v_{s^\dagger}|\Big)\Pi_{P^a_x}\Pi_{Q^b_y}\Big(\sum_{t\in W_j} \gamma_t |v_t\rangle\Big) = \sum_{s\in W_i}\sum_{t\in W_j} \lambda_s^*\gamma_t \langle v_{s^\dagger}|\Pi_{P^a_x}\Pi_{Q^b_y}|v_t\rangle \\
&= \sum_{s\in W_i}\sum_{t\in W_j} \lambda_s^*\gamma_t \langle v_{s^\dagger P^a_x}|v_{Q^b_y t}\rangle = \sum_{s\in W_i}\sum_{t\in W_j} \lambda_s^*\gamma_t \langle v_{s^\dagger Q^b_y}|v_{P^a_x t}\rangle \\
&= \sum_{s\in W_i}\sum_{t\in W_j} \lambda_s^*\gamma_t \langle v_{s^\dagger}|\Pi_{Q^b_y}\Pi_{P^a_x}|v_t\rangle = \Big(\sum_{s\in W_i} \lambda_s^* \langle v_{s^\dagger}|\Big)\Pi_{Q^b_y}\Pi_{P^a_x}\Big(\sum_{t\in W_j} \gamma_t |v_t\rangle\Big) \\
&= \langle z|\Pi_{\leq i}\Pi_{Q^b_y}\Pi_{P^a_x}\Pi_{\leq j}|w\rangle
\end{aligned} \tag{4.10}$$

In (4.10), since we know that $s \in W_i$, $t \in W_j$ and $W_i, W_j \subseteq W_{N-1}$, the third equality follows by Observation 65, the fourth equality follows by equation (4.1), and the fifth equality follows by Observation 65 again.

Since this holds for arbitrary $|z\rangle, |w\rangle$, it follows that $\Pi_{\leq i}\Pi_{P_x^a}\Pi_{Q_y^b}\Pi_{\leq j} = \Pi_{\leq i}\Pi_{Q_y^b}\Pi_{P_x^a}\Pi_{\leq j}$, as claimed. □

Proposition 69. *For any $j < N$, and any $P_x^a \in \mathcal{A}$, or $Q_y^b \in \mathcal{A}$ we have that*

$$Im\big(\Pi_{P_x^a}\Pi_{\leq j}\big) \subseteq Im\big(\Pi_{\leq j+1}\big) \qquad \text{and} \qquad Im\big(\Pi_{Q_y^b}\Pi_{\leq j}\big) \subseteq Im\big(\Pi_{\leq j+1}\big)$$

Proof. Let $|z\rangle$ be an arbitrary vector in V_N. By definition, $\Pi_{\leq j}|z\rangle \in \mathrm{Im}\left(\Pi_{\leq j}\right) \equiv V_j = \mathrm{Span}\{|v_s\rangle : s \in W_j\}$. So, there exist coefficients $\lambda_s \in \mathbb{C}$ such that $\Pi_{\leq j}|z\rangle = \sum_{s\in W_j} \lambda_s |v_s\rangle$. Now, by invoking Observation 65 we see that

$$\Pi_{P_x^a}\Pi_{\leq j}|z\rangle = \sum_{s\in W_j} \lambda_s \Pi_{P_x^a}|v_s\rangle = \sum_{s\in W_j} \lambda_s |v_{P_x^a s}\rangle \in \mathrm{Im}\left(\Pi_{\leq j+1}\right) \equiv V_{j+1} = \mathrm{Span}\{|v_s\rangle : s \in W_{j+1}\}$$

$$\Pi_{Q_y^b}\Pi_{\leq j}|z\rangle = \sum_{s\in W_j} \lambda_s \Pi_{Q_y^b}|v_s\rangle = \sum_{s\in W_j} \lambda_s |v_{Q_y^b s}\rangle \in \mathrm{Im}\left(\Pi_{\leq j+1}\right) \equiv V_{j+1} = \mathrm{Span}\{|v_s\rangle : s \in W_{j+1}\}$$

Since this is true for arbitrary $|z\rangle$, the desired result follows. □

4.2.4 Some bounds

In this section we collect a few identities that will be useful in the proof of Theorem 55. We first note the bound

$$\|[A, B^r]\| \leq 2\|B\|^{1-r}\|[A, B]\|^r, \tag{4.11}$$

valid for $A, B \geq 0$ and $0 \leq r \leq 1$, that will be useful in our analysis. See Problem X.5.3 in [13] for a tighter bound from which (4.11) follows.

Claim 70. *For $i = 1, \ldots, M$ let $A_i, B_i \geq 0$ be such that (A_i) and (B_i) are δ-AC, and $\sum_i \mathrm{Tr}(A_i\sqrt{B_i}\rho\sqrt{B_i}) \geq 1 - \varepsilon$. Then*

$$\sum_i \mathrm{Tr}\Big(\big(A_i^{1/2} - B_i^{1/2}\big)^2 \rho\Big) \leq 2\varepsilon + O\big(\delta^{1/8} M\big), \tag{4.12}$$

and

$$\Big\| \sum_i A_i^{1/2} \rho A_i^{1/2} - \sum_i B_i^{1/2} \rho B_i^{1/2} \Big\|_1 \leq 2\sqrt{2\varepsilon} + O\big(\delta^{1/16} M^{1/2}\big), \tag{4.13}$$

Proof. We first evaluate

$$\begin{aligned}
\sum_i \mathrm{Tr}\big(A_i^{1/2} B_i^{1/2} \rho\big) &= \sum_i \mathrm{Tr}\big(A_i^{1/4} B_i^{1/2} A_i^{1/4} \rho\big) - \sum_i \mathrm{Tr}\big([A_i^{1/4}, B_i^{1/2}] A_i^{1/4} \rho\big) \\
&\geq \sum_i \mathrm{Tr}\big(A_i^{1/4} B_i A_i^{1/4} \rho\big) - 2\delta^{1/8} M \\
&= \sum_i \mathrm{Tr}\big(A_i^{1/2} B_i \rho\big) - \sum_i \mathrm{Tr}\big(A_i^{1/4} [A_i^{1/4}, B_i] \rho\big) - 2\delta^{1/8} M \\
&\geq \sum_i \mathrm{Tr}\big(B_i^{1/2} A_i^{1/2} B_i^{1/2} \rho\big) - \sum_i \mathrm{Tr}\big([B_i^{1/2}, A_i^{1/2}] B_i^{1/2} \rho\big) - 4\delta^{1/8} M \\
&\geq \sum_i \mathrm{Tr}\big(B_i^{1/2} A_i B_i^{1/2} \rho\big) - 6\delta^{1/8} M
\end{aligned} \tag{4.14}$$

where we repeatedly used the bound (4.11). To obtain (4.12) it suffices to expand the square in (4.12) and use the assumption $\sum_i \mathrm{Tr}(A_i\sqrt{B_i}\rho\sqrt{B_i}) \geq 1 - \varepsilon$ together with (4.14). Finally, (4.13) follows easily from (4.12) (see e.g. Claim 36 in [43]). □

4.3 A rounding scheme for approximately commuting provers

We introduce a rounding scheme for the QC SDP hierarchy which, given the optimal N^{th}-level QC SDP solution for a certain game G, constructs an $O\left(\frac{A^2}{\sqrt{N}}\right)$-AC strategy for the provers (here A is the number of possible answers in G, which for simplicity we assume to be the same for each prover). The resulting strategy for G has value equal to the value

of N^{th} level of the QC SDP hierarchy, which we denote $\omega^N_{QCSDP}(G)$ (see Definition 61 below for a precise definition). To the best of our knowledge this is the first proposal of a rounding scheme for the QC SDP hierarchy for which one is able to provide any quantitative error estimate whatsoever.

In [73] and [31] it is shown that $\omega^N_{QCSDP}(G)$ is an upper bound on the value of 0-AC strategies, that is, $\omega^N_{QCSDP}(G) \geq \omega^*(G)$. Our rounding result implies that for all $\delta = O\left(\frac{|A|^2}{\sqrt{N}}\right)$ the quantity $\omega^N_{QCSDP}(G)$ is also a *lower* bound on the optimal success probability achievable by any δ-AC strategy. This additional result allows us to place an upper bound on the complexity class MIP^*_δ introduced in Section 4.2.1. Precisely, we obtain the following:

Theorem 71. *For any $\delta > 0$, $k \in \mathbb{N}$ and $c, s : \mathbb{N} \to [0,1]$ such that $c - s = \Omega(2^{-\mathrm{poly}})$ it holds that $\mathrm{MIP}^*_\delta(k, c, s) \subseteq \mathrm{TIME}(\exp(\exp(\mathrm{poly})/\delta^2))$. Furthermore, the upper bound can be brought down to $\mathrm{TIME}(\exp(\mathrm{poly}/\delta^2))$ when considering only protocols with constant answer size.*

Combining Theorem 71 with Theorem 55 we obtain that for any constant k it holds that

$$\mathrm{NEXP} \subseteq \bigcup_{p \in \mathrm{poly}} \mathrm{MIP}^*_{ac}(2, 1, 1 - 2^{-p}) \subseteq \mathrm{TIME}\left(2^{2^{\mathrm{poly}}}\right).$$

4.3.1 Rounding Scheme

In this section we introduce a rounding scheme for the QC SDP hierarchy. First we briefly argue that the most natural rounding scheme suggested by the definition of the hierarchy, which was first proposed in [71], is actually not the best for our purposes. In [72] it is proposed that any solution, Γ^N, to the N^{th} level of the QC SDP hierarchy be rounded to a strategy consisting of state $\rho \equiv |v_\phi\rangle\langle v_\phi|$, and projective measurement operators $\Pi_{P^a_x}$ for the first prover and $\Pi_{Q^b_y}$ for the second. It is further proved that, assuming a technical condition called the "rank loop" condition, this rounded strategy gives valid POVMs for the two provers, and that those POVMs are exactly commuting ($[\Pi_{P^a_x}, \Pi_{Q^b_y}] = 0$). Unfortunately, the "rank loop" condition is computationally difficult to verify, and in general it may not hold at any level of the hierarchy. Even without assuming the "rank loop" condi-

tion, it is true that, for all $j < N$, $\Pi_{\leq j}\Pi_{P_x^a}\Pi_{Q_y^b}\Pi_{\leq j} = \Pi_{\leq j}\Pi_{Q_y^b}\Pi_{P_x^a}\Pi_{\leq j}$ (see Proposition 68). However, while this tells us that $[\Pi_{P_x^a}, \Pi_{Q_y^b}] = 0$ *exactly* when restricted to the space V_{N-1}, it is hard to control the size of $\|[\Pi_{P_x^a}, \Pi_{Q_y^b}]\|$ on the space $V_{N-1}^{\perp} \equiv \mathrm{Im}\left(\Pi_{\leq N-1}^{\perp}\right)$ without making additional assumptions about the structure of G, etc. Furthermore, when using this rounding scheme, it is not clear that there is any quantitative benefit from increasing the number of levels N of the QC SDP hierarchy.

We introduce a rounding scheme which will ultimately allow us to control the operator norm of commutators of the rounded strategy on the entire space V_N, without making any assumptions whatsoever about the structure of G.

Definition 72 (Rounding Scheme for the QC SDP hierarchy). *Fix probability distributions $\{p_i\}_{i=0}^N$, and $\{q_j\}_{j=1}^N$. In what follows we will assume that $p_0 = q_0 = p_N = q_N = 0$. Given a solution Γ^N to the N^{th} level of the QC SDP hierarchy for G, the probability distributions p_i and q_j specify a rounding scheme as follows. The state shared by the provers is $\rho \equiv |v_\phi\rangle\langle v_\phi|$. Their measurement operators, $\{\tilde{P}_x^a\}$ for the first prover and $\{\tilde{Q}_y^b\}$ for the second, are defined as*

$$\tilde{P}_x^a \equiv \sum_i p_i \Pi_{\leq i}\Pi_{P_x^a}\Pi_{\leq i}, \qquad \tilde{P}_x^{garbage} \equiv I - \sum_{a\in\mathcal{A}} \tilde{P}_x^a$$
$$\tilde{Q}_y^b \equiv \sum_j q_j \Pi_{\leq j}\Pi_{Q_y^b}\Pi_{\leq j}, \qquad \tilde{Q}_y^{garbage} \equiv I - \sum_{b\in\mathcal{B}} \tilde{Q}_y^b$$

We first verify that the rounding scheme defined in Definition 72 defines valid POVM measurements, and leads to a strategy whose value in G exactly matches $\omega_{QCSDP}^N(G)$. (As we defined it, it may seem that the strategy sometimes outputs a symbol "garbage". As we show below this has probability 0, and we can safely ignore the event.)

Claim 73. *The strategy defined in Definition 72 has value exactly $\omega_{QCSDP}^N(G)$ in G.*

Proof. First we note that the $\tilde{P}_x$ and $\tilde{Q}_y$ define valid POVM. Indeed, using that each $\Pi_{\leq i}$, $\Pi_{P_x^a}$ and $\Pi_{Q_y^b}$ is a projector, it is clear that the $\tilde{P}_x^a$ (resp. $\tilde{Q}_y^b$) are positive semidefinite. Furthermore, using $\sum_a \Pi_{P_x^a} \leq \mathrm{Id}$ (since the projectors are, by definition, orthogonal), $\sum_i p_i = 1$ and $\Pi_{\leq i} \leq \mathrm{Id}$ for every i we get $\sum_a \tilde{P}_x^a \leq \mathrm{Id}$ and hence $\tilde{P}_x^{garbage} \geq 0$ as well.

Next we evaluate the strategy's success probability in the game. From the definition,

$$\begin{aligned}
\langle v_\phi | \tilde{P}_x^a \tilde{Q}_y^b | v_\phi \rangle &= \langle v_\phi | \Big(\sum_i p_i \Pi_{\leq i} \Pi_{P_x^a} \Pi_{\leq i} \Big) \Big(\sum_j q_j \Pi_{\leq j} \Pi_{Q_y^b} \Pi_{\leq j} \Big) | v_\phi \rangle \\
&= \sum_i p_i \sum_j q_j \langle v_\phi | \Pi_{\leq i} \Pi_{P_x^a} \Pi_{\leq i} \Pi_{\leq j} \Pi_{Q_y^b} \Pi_{\leq j} | v_\phi \rangle \\
&= \sum_i p_i \sum_j q_j \langle v_\phi | \Pi_{P_x^a} \Pi_{\leq i} \Pi_{\leq j} \Pi_{Q_y^b} | v_\phi \rangle \\
&= \sum_i p_i \sum_j q_j \langle v_{P_x^a} | \Pi_{\leq i} \Pi_{\leq j} | v_{Q_y^b} \rangle \\
&= \langle v_{P_x^a} | v_{Q_y^b} \rangle. \qquad (4.15)
\end{aligned}$$

Here the third equality follows since $|v_\phi\rangle$ is in the image of $\Pi_{\leq i}$ for all i, the fourth equality follows from observation 65 and the last from the definition of $\Pi_{\leq i}$ (using $i, j \geq 1$ wlog since $p_0 = q_0 = 0$). Furthermore,

$$\begin{aligned}
\langle v_\phi | \tilde{P}_x^{garbage} \tilde{Q}_y^b | v_\phi \rangle &= \langle v_\phi | \Big(I - \sum_{a \in \mathcal{A}} \tilde{P}_x^a \Big) \tilde{Q}_y^b | v_\phi \rangle \\
&= \langle v_\phi | \tilde{Q}_y^b | v_\phi \rangle - \sum_{a \in \mathcal{A}} \langle v_\phi | \tilde{P}_x^a \tilde{Q}_y^b | v_\phi \rangle \\
&= \langle v_\phi | v_{Q_y^b} \rangle - \sum_{a \in \mathcal{A}} \langle v_{P_x^a} | v_{Q_y^b} \rangle \\
&= 0,
\end{aligned}$$

where the fourth equality follows by equation (4.15), and the third equality follows by reasoning very similar to that used to prove equation (4.15). Using similar arguments one can verify that $\langle v_\phi | \tilde{P}_x^a \tilde{Q}_y^{garbage} | v_\phi \rangle = 0$ and $\langle v_\phi | \tilde{P}_x^{garbage} \tilde{Q}_y^{garbage} | v_\phi \rangle = 0$ as well. Hence the "garbage" outcomes have probability zero of occurring (given the shared state is $\rho = |v_\phi\rangle\langle v_\phi|$) and we may ignore them. □

4.3.2 Commutator Bound

Theorem 74. *Suppose the p_i, q_j are such that*

$$\max\Big(\sum_i p_i^2, \sum_j q_j^2, \sum_i p_i q_i\Big) = O\Big(\frac{1}{N}\Big),$$

for instance $p_i = q_j = 1/(N-1)$ for $0 < i, j < N$). Then, for each value of $a, b, x, y \in A \times B \times X \times Y$, we have that

$$\left\| \left[\tilde{P}_x^a, \tilde{Q}_y^b\right] \right\| = O\left(\frac{1}{\sqrt{N}}\right).$$

Proof. Fix $(a, b, x, y) \in A \times B \times X \times Y$. In order to simplify notation within this proof we write $\tilde{P}$ for $\tilde{P}_x^a$, P for $\Pi_{P_x^a}$, $\tilde{Q}$ for $\tilde{Q}_y^b$, and Q for $\Pi_{Q_y^b}$. For any $1 \leq i \leq N$ let $\Pi_{=i} = (\mathrm{Id} - \Pi_{<i})\Pi_{\leq i}(\mathrm{Id} - \Pi_{<i})$. Using that $\Pi_{<i} \leq \Pi_{\leq i}$ for each i, we get that the $\Pi_{=i}$ are orthogonal projectors and, taking the convention that $\Pi_{\leq 0} = 0$, $\sum_{i \leq N} \Pi_{=i} = \Pi_{\leq N}$.

Proposition 69 immediately implies that for any $i < N$ and $k > i+1$ it holds that $\Pi_{=k} P \Pi_{\leq i} = 0$. Thus $\Pi_{\leq i} P \Pi_{\leq i} = (\mathrm{Id} - \Pi_{=i+1}) P \Pi_{\leq i}$ and similarly for Q. Expand

$$\begin{aligned}
[\tilde{P}, \tilde{Q}] &= \sum_{i,j} p_i q_j \left[\Pi_{\leq i} P \Pi_{\leq i}, \Pi_{\leq j} Q \Pi_{\leq j}\right] \\
&= \sum_{i,j} p_i q_j \left(\Pi_{\leq i} P (\mathrm{Id} - \Pi_{=i+1})(\mathrm{Id} - \Pi_{=j+1}) Q \Pi_{\leq j} - \Pi_{\leq j} Q (\mathrm{Id} - \Pi_{=j+1})(\mathrm{Id} - \Pi_{=i+1}) P \Pi_{\leq i}\right) \\
&= \sum_{i,j} p_i q_j \Big(\Pi_{\leq i}[P, Q]\Pi_{\leq j} + \left(\Pi_{\leq i} P \Pi_{=i+1} \Pi_{=j+1} Q \Pi_{\leq j} - \Pi_{\leq j} Q \Pi_{=j+1} \Pi_{=i+1} P \Pi_{\leq i}\right) \\
&\qquad - \left(\Pi_{\leq i} P (\Pi_{=i+1} + \Pi_{=j+1}) Q \Pi_{\leq j} - \Pi_{\leq j} Q (\Pi_{=i+1} + \Pi_{=j+1}) P \Pi_{\leq i}\right)\Big). \qquad (4.16)
\end{aligned}$$

The second equality above follows by using Propositions 67, and 69. We bound each of the four terms in (4.16) separately. Using $i, j < N$ terms of the form $\Pi_{\leq i}[P, Q]\Pi_{\leq j}$ evaluate

to zero by Proposition 68. The second term

$$\sum_{i,j} p_i q_j \left(\Pi_{\leq i} P \Pi_{=i+1} \Pi_{=j+1} Q \Pi_{\leq j} - \Pi_{\leq j} Q \Pi_{=j+1} \Pi_{=i+1} P \Pi_{\leq i}\right)$$
$$= \sum_i p_i q_i \, \Pi_{\leq i} \big(P \Pi_{=i+1} Q - Q \Pi_{=i+1} P\big) \Pi_{\leq i},$$

which using $\|P\Pi_{=i+1}Q - Q\Pi_{=i+1}P\| \leq 2$ and $\sum_i p_i q_i = O(N^{-1})$ has norm $O(N^{-1})$. It remains to bound the last two terms in (4.16). Towards this we first claim that

$$\Big\| \sum_i \Pi_{\leq i} P \Pi_{=i+1} \Big\| = O\Big(\frac{1}{\sqrt{N}}\Big). \tag{4.17}$$

This can be seen by evaluating

$$\Big(\sum_i p_i \Pi_{\leq i} P \Pi_{=i+1}\Big)\Big(\sum_i p_i \Pi_{\leq i} P \Pi_{=i+1}\Big)^\dagger = \sum_i p_i^2 \Pi_{\leq i} P \Pi_{=i+1} P \Pi_{\leq i}$$
$$\leq \sum_i p_i^2 \Pi_{\leq i} P \Pi_{\leq i}$$
$$\leq \sum_i p_i^2 \, \mathrm{Id},$$

from which the bound (4.17) follows since $\sum_i p_i^2 = O(1/N)$. Together with the fact that $\|\sum_i p_i P \Pi_{\leq i}\| \leq 1$, and using analogous bounds for Q, the last two terms in (4.16) each has norm at most $O(N^{-1/2})$. This concludes the proof. □

Corollary 75. *Let us specify $p_i = q_j = \frac{1}{N-1}$ when $0 < i, j < N$ (and $p_0 = q_0 = p_N = q_N = 0$). Then, for each value of $a, b, x, y \in A \times B \times X \times Y$, we have that*

$$\Big\| \Big[\tilde{P}_x^{garbage}, \tilde{Q}_y^b\Big] \Big\|_2 = O\left(\frac{|A|}{\sqrt{N}}\right),$$
$$\Big\| \Big[\tilde{P}_x^a, \tilde{Q}_y^{garbage}\Big] \Big\|_2 = O\left(\frac{|B|}{\sqrt{N}}\right),$$
$$\Big\| \Big[\tilde{P}_x^{garbage}, \tilde{Q}_y^{garbage}\Big] \Big\|_2 = O\left(\frac{|A||B|}{\sqrt{N}}\right),$$

Proof.

$$
\begin{aligned}
[\tilde{P}_x^{garbage}, \tilde{Q}_y^b] &= \Big[\Big(I - \sum_{a\in\mathcal{A}} \tilde{P}_x^a\Big), \tilde{Q}_y^b\Big] = [I, \tilde{Q}_y^b] - \sum_{a\in\mathcal{A}} [\tilde{P}_x^a, \tilde{Q}_y^b] = 0 - \sum_{a\in\mathcal{A}} [\tilde{P}_x^a, \tilde{Q}_y^b], \\
[\tilde{P}_x^a, \tilde{Q}_y^{garbage}] &= \Big[\tilde{P}_x^a, \Big(I - \sum_{b\in\mathcal{B}} \tilde{Q}_y^b\Big)\Big] = -[\tilde{P}_x^a, I] + \sum_{b\in\mathcal{B}} [\tilde{P}_x^a, \tilde{Q}_y^b] = 0 + \sum_{b\in\mathcal{B}} [\tilde{P}_x^a, \tilde{Q}_y^b], \\
[\tilde{P}_x^{garbage}, \tilde{Q}_y^{garbage}] &= \Big[\Big(I - \sum_{a\in\mathcal{A}} \tilde{P}_x^a\Big), \Big(I - \sum_{b\in\mathcal{B}} \tilde{Q}_y^b\Big)\Big] \\
&= \Big[I, \Big(I - \sum_{b\in\mathcal{B}} \tilde{Q}_y^b\Big)\Big] - \sum_{a\in\mathcal{A}} \Big[\tilde{P}_x^a, \Big(I - \sum_{b\in\mathcal{B}} \tilde{Q}_y^b\Big)\Big] \\
&= 0 - \sum_{a\in\mathcal{A}} \Big(- [\tilde{P}_x^a, I] + \sum_{b\in\mathcal{B}} [\tilde{P}_x^a, \tilde{Q}_y^b]\Big) \\
&= \sum_{a\in\mathcal{A}} \sum_{b\in\mathcal{B}} [\tilde{P}_x^a, \tilde{Q}_y^b],
\end{aligned}
$$

Using the triangle inequality and Theorem 74 then gives

$$
\begin{aligned}
\Big\| \Big[\tilde{P}_x^{garbage}, \tilde{Q}_y^b\Big] \Big\| &= \Big\| - \sum_{a\in\mathcal{A}} \Big[\tilde{P}_x^a, \tilde{Q}_y^b\Big] \Big\| \leq \sum_{a\in\mathcal{A}} \Big\| \Big[\tilde{P}_x^a, \tilde{Q}_y^b\Big] \Big\| \leq |A| O\left(\frac{1}{\sqrt{N}}\right) = O\left(\frac{|A|}{\sqrt{N}}\right), \\
\Big\| \Big[\tilde{P}_x^a, \tilde{Q}_y^{garbage}\Big] \Big\| &= \Big\| \sum_{b\in\mathcal{B}} \Big[\tilde{P}_x^a, \tilde{Q}_y^b\Big] \Big\| \leq \sum_{b\in\mathcal{B}} \Big\| \Big[\tilde{P}_x^a, \tilde{Q}_y^b\Big] \Big\| \leq |B| O\left(\frac{1}{\sqrt{N}}\right) = O\left(\frac{|B|}{\sqrt{N}}\right), \\
\Big\| \Big[\tilde{P}_x^{garbage}, \tilde{Q}_y^{garbage}\Big] \Big\| &= \Big\| \sum_{a\in\mathcal{A}} \sum_{b\in\mathcal{B}} \Big[\tilde{P}_x^a, \tilde{Q}_y^b\Big] \Big\| \leq \sum_{a\in\mathcal{A}} \sum_{b\in\mathcal{B}} \Big\| \Big[\tilde{P}_x^a, \tilde{Q}_y^b\Big] \Big\| \\
&\leq |A||B| O\left(\frac{1}{\sqrt{N}}\right) = O\left(\frac{|A||B|}{\sqrt{N}}\right),
\end{aligned}
$$

This is the desired result. □

4.4 A lower bound on MIP^*_δ

In this section we give a detailed sketch of the proof of Theorem 55. The proof closely follows the lines of Theorem 2 in [?], where the same result is proved for the case of provers that are restricted to be perfectly commuting. Most of the work consists in carefully going through the argument in [?] and verifying that the commutation condition, provided it is

satisfied for a sufficiently small δ, suffices to preserve soundness. Although intuitively one expects this to be the case, one still has to be a little careful in order to avoid any dimension dependence coming into the argument.

4.4.1 Proof outline

Our starting point is a non-adaptive 3-query PCP for NEXP with perfect completeness and soundness bounded away from 1 and in which the alphabet size is a single bit. Fix an input x, let N be the length of the PCP and $\pi : [N]^3 \to [0,1]$ the distribution on queries. We may assume that the marginal distribution of π on any of its three coordinates is uniform. Let $V : [N]^3 \times \{0,1\}^3 \to \{0,1\}$ be the acceptance predicate. We consider the following protocol in which the verifier interacts with two provers only:

1. The verifier chooses a triple (i_1, i_2, i_3) according to π, $i \in \{i_1, i_2, i_3\}$ uniformly at random and $j \in [N]$ uniformly at random. He sends (lexicographically ordered) tuples $\{i_1, i_2, i_3\}$ to the first prover and $\{i, j\}$ to the second.
2. A replies with three bits $a_{i_1}, a_{i_2}, a_{i_3}$. B replies with two bits b_i, b_j.
3. The referee accepts if and only if $V(i_1, i_2, i_3, a_{i_1}, a_{i_2}, a_{i_3}) = 1$ and $a_i = b_i$.

This protocol is obtained through the standard oracularization technique, except for the additional question j sent to the second prover. This is called a "dummy question" in [?] and it plays an important role in the analysis.

First we note that the completeness property of the protocol trivially holds. Hence it remains to establish soundness. This is done in the following lemma, which is proved in the following section:

Lemma 76. *There exists a universal constant $c_1 > 0$ such that the following holds. Let $(A_{i_1 i_2 i_3}^{a_1 a_2 a_3}, B_{ij}^{b_i b_j}, \rho)$ be a 2-prover δ-AC projective strategy that succeeds with probability at least $1 - \varepsilon$ in the protocol. Then there exists an assignment to the variables $[N]$ that satisfies the PCP verifier's queries with probability at least $1 - O(N^2(\varepsilon^{1/2} + \delta^{c_1}))$.*

Theorem 55 follows immediately from the above lemma (using Claim 60 to argue that the assumption that the provers' measurements are projective is without loss of generality).

4.4.2 Soundness analysis

In this section we sketch the proof of Lemma 76. Given a strategy for the provers for every $i \in [N]$ we define the following POVM with outcomes in $\{0,1\}$:

$$C_i^c := \mathrm{E}_{j\in[N]} \sum_{c'\in\{0,1\}} B_{ij}^{cc'}, \tag{4.18}$$

where the expectation is taken with respect to the uniform distribution. Define a (probabilistic) assignment $(c_i)_{i\in[N]}$ to the PCP proof according to the distribution

$$\mathrm{Prob}\big((c_i)\big) := \mathrm{Tr}\big(\sqrt{C_N^{c_N}}\cdots\sqrt{C_1^{c_1}}\rho\sqrt{C_1^{c_1}}\cdots\sqrt{C_N^{c_N}}\big). \tag{4.19}$$

We will show that this assignment satisfies the acceptance predicate with good probability. First we prove the following claim, which gives a simpler form for the marginals of the distribution on assignments to any three fixed variables.

Claim 77. *There exists a constant $c_1 > 0$ such that the following holds for any $i,j,k \in [N]$:*

$$\sum_{a,b,c} \Big|\mathrm{Tr}\Big(\sqrt{C_i^c}\sqrt{C_j^b}\sqrt{C_k^a}\rho\sqrt{C_i^a}\sqrt{C_j^b}\sqrt{C_k^c}\Big) - \sum_{\substack{c_\ell \\ \ell\notin\{i,j,k\}}} \mathrm{Tr}\Big(\sqrt{C_N^{c_N}}\cdots\sqrt{C_1^{c_1}}\rho\sqrt{C_1^{c_1}}\cdots\sqrt{C_N^{c_N}}\Big)\Big| = O\big(N^2(\varepsilon^{1/2}+\delta^{c_1})\big) \tag{4.20}$$

Proof sketch. First we note that the bound (4.20) follows by an easy induction once the

following has been established: for any t and $j_1, \ldots, j_t \in [N]$,

$$\mathrm{E}_i \sum_{c_1,\ldots,c_t} \Big| \sum_a \mathrm{Tr}\Big(\sqrt{C_{j_t}^{c_t}} \cdots \sqrt{C_{j_1}^{c_1}} \sqrt{C_i^a} \rho \sqrt{C_i^a} \sqrt{C_{j_1}^{c_1}} \cdots \sqrt{C_{j_t}^{c_t}}\Big) - \mathrm{Tr}\Big(\sqrt{C_{j_t}^{c_t}} \cdots \sqrt{C_{j_1}^{c_1}} \rho \sqrt{C_{j_1}^{c_1}} \cdots \sqrt{C_{j_t}^{c_t}}\Big)\Big| = O\big(t\,(\varepsilon^{1/2} + \delta^{1/16})\big). \tag{4.21}$$

To prove (4.21), for any $i \in [N]$ and $a \in \{0,1\}$ we introduce the POVM element

$$\hat{A}_i^a := \mathrm{E}_{j,k} \sum_{a_j, a_k} A_{ijk}^{a a_j a_k},$$

where the expectation is taken according to the conditional distribution $\pi(\cdot,\cdot|i)$. Note that $\sum_a \hat{A}_i^a = \mathrm{Id}$, and success in the consistency check of the protocol implies

$$\mathrm{E}_i \sum_a \mathrm{Tr}\big(\hat{A}_i^a \sqrt{C_i^a} \rho \sqrt{C_i^a}\big) \geq 1 - \varepsilon. \tag{4.22}$$

This justifies applying Claim 70, and from (4.13) we get

$$\mathrm{E}_i \Big\| \sum_a \sqrt{C_i^a} \rho \sqrt{C_i^a} - \sqrt{\hat{A}_i^a} \rho \sqrt{\hat{A}_i^a} \Big\|_1 = O\big(\varepsilon^{1/2} + \delta^{1/16}\big). \tag{4.23}$$

Using (4.23) we obtain

$$\mathrm{E}_i \sum_{c_1,\ldots,c_t} \Big| \sum_a \mathrm{Tr}\big(\sqrt{C_{j_t}^{c_t}} \cdots \sqrt{C_{j_1}^{c_1}} \sqrt{C_i^a} \rho \sqrt{C_i^a} \sqrt{C_{j_1}^{c_1}} \cdots \sqrt{C_{j_t}^{c_t}}\big) - \sum_a \mathrm{Tr}\big(\sqrt{C_{j_t}^{c_t}} \cdots \sqrt{C_{j_1}^{c_1}} \sqrt{\hat{A}_i^a} \rho \sqrt{\hat{A}_i^a} \sqrt{C_{j_1}^{c_1}} \cdots \sqrt{\hat{C}_{j_t}^{c_t}}\big)\Big| = O\big(\varepsilon^{1/2} + \delta^{1/16}\big). \tag{4.24}$$

Applying the (4δ)-AC condition (together with (4.11) in order to apply it to the square roots) between $\hat{A}$ and C $(2t)$ times leads to (4.21). To conclude the proof of (4.20) we start from the second term in the absolute value and apply (4.21) $(N-3)$ times to eliminate the C that are being summed over. □

Our second claim relates the marginal computed in Claim 77 to the original provers' strategy.

Claim 78. *There exists a constant $c_1 > 0$ such that the following holds:*

$$\mathrm{E}_{ijk} \sum_{a,b,c} \left| \mathrm{Tr}\left(\sqrt{C_i^c}\sqrt{C_j^b}\sqrt{C_k^a}\rho\sqrt{C_i^a}\sqrt{C_j^b}\sqrt{C_k^c} \right) - \mathrm{Tr}\left(A_{ijk}^{abc}\rho \right) \right| = O(\varepsilon^{1/2} + \delta^{1/16}), \quad (4.25)$$

where the expectation is taken according to the distribution π used in the protocol.

Sketch. We first proceed as in the proof of Claim 77 and note that success in the consistency check of the protocol implies, through Claim 70, the bound

$$\mathrm{E}_{ijk} \left\| \sum_a \sqrt{C_i^a}\rho\sqrt{C_i^a} - \sqrt{A_{ijk}^a}\rho\sqrt{A_{ijk}^a} \right\|_1 = O(\varepsilon^{1/2} + \delta^{1/16}). \quad (4.26)$$

Note however the slightly different formulation from (4.23), where we left the expectation on j and k outside, and slightly abused notation to write A_{ijk}^a for $\sum_{b,c} A_{ijk}^{abc}$. Applying (4.26) thrice, using the (4δ)-AC condition between A and C and the fact that we assumed the A_{ijk} to be projective measurements, we get

$$\mathrm{E}_{ijk} \left\| \sum_{a,b,c} \sqrt{C_i^c}\sqrt{C_j^b}\sqrt{C_k^a}\rho\sqrt{C_i^a}\sqrt{C_j^b}\sqrt{C_k^c} - \sum_{a,b,c} A_{ijk}^{abc}\rho A_{ijk}^{abc} \right\|_1 = O(\varepsilon^{1/2} + \delta^{1/16}).$$

The claimed bound (4.25) follows by noting that the A_{ijk}^{abc} are orthogonal for different outputs, and using the following pinching inequality: for any X and projection P, $\|PXP + (1-P)X(1-P)\|_1 \leq \|X\|_1$. □

Let $(c_i)_{i\in[N]}$ be sampled according to the distribution (4.19). Combining the bounds from Claim 77 and Claim 78 we see that for any query (i,j,k) made by the PCP verifier the marginal distribution on assignments induced by (c_i) is within statistical distance $O(N^2(\varepsilon^{1/2} + \delta^{c_1}))$ from the distribution on assignments obtained from the entangled provers' answers in the protocol. Since by assumption the latter satisfies the PCP

predicate with probability $1 - \varepsilon$, we deduce that the assignment $(c_i)_{i\in[N]}$ satisfies a randomly chosen query of the PCP verifier with probability (over the sampling of (c_i) as well as over the PCP verifier's random choice of query) at least $1 - O(N^2(\varepsilon^{1/2} + \delta^{c_1}))$. This completes the proof of Lemma 76, from which Theorem 55 follows easily.

4.5 Discussion

The rounding scheme for the QC SDP hierarchy in Section 4.3, and our introduction of the corresponding class MIP^*_{ac} in Section 4.4, are motivated by a desire to develop a framework for the study of quantum multiprover interactive proof systems that is both computationally bounded and relevant for typical applications of such proof systems. Our main technical result, Theorem 53, demonstrates the first aspect. In this section we discuss the relevance of the new model, its connection with the standard definition of MIP*, and applications to quantum information.

4.5.1 Commuting approximants: some results, limits, and possibilities

While we believe MIP^*_{ac} is of interest in itself, we do not claim that approximately commuting provers are more natural than commuting provers, or provers in tensor product form; the main goal in introducing the new class is to shed light on its thus-far-intractable parent MIP*. In light of the results from Section 4.3 the relationship between the two classes seems to hinge on the general mathematical problem of finding exactly commuting approximants to approximately commuting matrices.

Limits for commuting approximants

The main objection to the existence of a positive answer for the "commuting approximants" question is revealed by a beautiful construction of Voiculescu who exhibits a surprisingly simple scenario in which commuting approximants provably do not exist [97].

The following is a direct consequence of Voiculescu's result.

Theorem 79 (Voiculescu). *For every $d \in \mathbb{N}$ there exists a pair of unitary matrices $U_1, U_2 \in \mathbb{C}^{d\times d}$ with $\|[U_1, U_2]\| = O(\frac{1}{d})$, such that for any pair of complex matrices $A, B \in \mathbb{C}^{d\times d}$ satisfying $[A, B] = 0$, $\max(\|U_1 - A\|, \|U_2 - B\|) = \Omega(1)$.*

In Voiculescu's example U_1 is a d-dimensional cyclic permutation matrix, and U_2 is a diagonal matrix whose eigenvalues are the d^{th} roots of unity. The proof draws on a connection to homology, in particular using a homotopy invariant to establish the lower bound on the distance to commuting approximants. A succinct and elementary proof of the result is given by Exel and Loring [33].

In the context of entangled strategies one is most concerned with Hermitian matrices representing measurements, rather than unitaries. However, as a consequence of Theorem 79 we see that if one considers the Hermitian operators $M_k^j = \frac{(-i)^j}{2}(U_k + (-1)^j U_k^\dagger)$ ($j \in \{0, 1\}$) we have that $\|[M_1^j, M_2^{j'}]\| = O(\frac{1}{d})$, and yet any exactly commuting set of matrices must be a constant distance away in the operator norm. Thus Theorem 79 rules out the strongest form of a "commuting approximants" statement, which would ask for approximants in the same space as the original matrices, and with a commutator bound that does not depend on the dimension of the matrices.

Thus Theorem 79 invites us to refine the "commuting approximants" question and distinguish ways in which it may avoid the counter-example; we describe some possibilities in the following subsections.

Ozawa's conjecture

Motivated by the study of Tsirelson's problem [86] and the relationship with Tsirelson's conjecture, Ozawa [75] introduces two equivalent conjectures, the "Strong Kirchberg Conjecture (I)" and "Strong Kirchberg Conjecture (II)" respectively, which postulate the existence of commuting approximants to approximately commuting sets of POVM measurements and unitaries respectively. The novelty of these conjectures, which allows them

to avoid the immediate pitfall given by Voiculescu's example, is that Ozawa considers approximants in a larger Hilbert space than the original approximately commuting operators. Precisely, his Strong Kirchberg Conjecture (I) states the following:

Conjecture 80 (Ozawa). *Let $m, \ell \geq 2$ be such that $(m, \ell) \neq (2,2)$* [5]*. For every $\kappa > 0$ there exists $\varepsilon > 0$ such that, if $\dim \mathcal{H} < \infty$ and (P_i^k), (Q_j^l) is a pair of m projective ℓ-outcome POVMs on $\mathcal{H}$ satisfying $\|[P_i^k, Q_j^l]\| \leq \varepsilon$, then there is a finite-dimensional Hilbert space $\tilde{H}$ containing $\mathcal{H}$ and projective POVMs $\tilde{P}_i^k$, $\tilde{Q}_j^l$ on $\tilde{\mathcal{H}}$ such that $\|[\tilde{P}_i^k, \tilde{Q}_j^l]\| = 0$ and $\|\Phi_{\mathcal{H}}(\tilde{P}_i^k) - P_i^k\| \leq \kappa$ and $\|\Phi_{\mathcal{H}}(\tilde{Q}_j^l) - Q_j^l\| \leq \kappa$. Here $\Phi_{\mathcal{H}}$ denotes the compression to $\mathcal{H}$, defined by $\Phi_{\mathcal{H}}(M) \equiv P_{\mathcal{H}} M P_{\mathcal{H}}$, where $P_{\mathcal{H}}$ is the projection onto $\mathcal{H}$.*

Ozawa gives an elegant proof of a variant of the conjecture that applies to just two approximately commuting unitaries, thereby establishing that extending the Hilbert space can allow one to avoid the complications in Voiculescu's example. He also establishes that the conjecture is *stronger* than Kirchberg's conjecture (itself equivalent to Tsirelson's problem and Connes' embedding conjecture [47]), casting doubt, if not on its validity, at least on its approachability.

Nevertheless, we can mention the following facts. First, it follows from Theorem 74 that Conjecture 80 implies the equality $\text{MIP}^*_{ac} = \text{MIP}^*$; in fact it implies that $\text{MIP}^*_{\delta} = \text{MIP}^*$ for small enough δ, depending on how the parameter ε in Conjecture 80 depends on κ, m and d. For this it suffices to verify that a state ρ optimal for a strategy based on POVMs P_i^k and Q_j^l in a given protocol can be lifted to a state $\tilde{\rho}$ on $\tilde{\mathcal{H}}$ such that the correlations exhibited by performing the POVMs $\tilde{P}_i^k$, $\tilde{Q}_j^l$ on $\tilde{\rho}$ approximately reproduce those generated by P_i^k, Q_j^l on ρ; this is easily seen to be the case provided κ is small enough. Therefore, Theorem 74 may be seen as an elementary proof that Conjecture 80 implies that MIP* is computable (this result was previously known, but previous methods use a series of reductions connecting Kirchberg's Conjecture to Tsirelson's problem, see [75]).

[5] The case $(m, \ell) = (2,2)$ is the only nontrivial setting for which we have some understanding. In particular nonlocal games with two inputs and two outputs per party can be analyzed via an application of Jordan's lemma [57].

Second, Conjecture 80 can be weakened in several ways without losing the implication that $\text{MIP}^*_{ac} = \text{MIP}^*$. For instance, it is not necessary for the exactly commuting $\tilde{P}_i^k$, $\tilde{Q}_j^l$ to approximate P_i^k, Q_j^l in operator norm — in our context of interactive proofs, only the correlations obtained by measuring a particular state need to be preserved, and this does not in general imply an approximation as strong as that promised in Conjecture 80.

Dimension dependent bounds

An alternative relaxation for the "commuting approximants" question is to allow the approximation error to depend explicitly on the dimension of the matrices. A careful analysis of the rounding scheme from Theorem 53 shows that it produces d-dimensional POVM elements with an $O(1/\sqrt{\log(d)})$ bound on the commutators (this is because the dimension of the subspace $\text{Im}(\Pi_{\leq N-1})$ is exponential in N). Unfortunately, Voiculescu's result (Theorem 79) shows that one can only hope for good approximants in the operator norm if the commutator bound is $o(1/d)$. It remains instructive to find *any* explicit existence result for commuting approximants in the general case, regardless of dimension dependence. Concretely, we conjecture that Conjecture 80 may be true with a parameter κ that scales with the dimension d of the operators $\{P_i^k, Q_j^l\}$ as $\kappa = \varepsilon^c \,\text{poly}(d)^{(ml)^2}$ for some constant $0 < c \leq 1$.

An alternative norm

Another relaxation of the "commuting approximants" question, which would be sufficient to imply $\text{MIP}^*_{ac} = \text{MIP}^*$, is to allow for any set of commuting approximants which approximately preserves the winning probability of the game. For concreteness we include a precise version of a possible statement along these lines:

Conjecture 81. *There exists a function $f(\varepsilon, k) : \mathbb{R}^+ \times \mathbb{N} \to \mathbb{R}^+$ satisfying $\lim_{\varepsilon \to 0} f(\varepsilon, k) = 0$ for all $k \in \mathbb{N}$, such that for every game G and (m, ℓ) strategy (A_x^a, B_y^b, ρ) which is δ-AC, there*

exists a 0*-AC strategy* $(\tilde{A}_x^a, \tilde{B}_y^b, \rho)$ *for* G *satisfying*

$$\left|\omega^*\big(((A_x^a, B_y^b, \rho); G\big) - \omega^*\big((\tilde{A}_x^a, \tilde{B}_y^b, \rho); G\big)\right| \leq f(\delta, m\ell).$$

4.5.2 Device-independent randomness expansion and weak cross-talk

A device-independent randomness expansion (DIRE) protocol is a protocol which may be used by a classical verifier to certify that a pair of untrusted devices are producing true randomness. Under the sole assumptions that the devices do not communicate with each other, and that the verifier has access to a small initial seed of uniform randomness, the protocol allows for the generation of much larger quantities of certifiably uniform random bits; hence the term "randomness expansion". This conclusion relies only on the assumption that the two devices do not communicate, and in particular does not require any limit on the computational power of the devices, as is typically the case in the study of pseudorandomness. The precise formalization of DIRE protocols is rather involved, and we direct the interested reader to the flourishing collection of works on the topic [22, 78, 93, 34, 1, 92, 36, 69, 16]. In particular the precise formulation of the model is a focus of [28].

Our definition of MIP^*_{ac} is directly relevant to the notion of devices with *weak cross-talk* introduced in [89] as a model which relaxes the assumption that the devices must not communicate, leading to protocols that are more robust to leakage than the traditional model of device-independence. [89] proposes the use of the QC SDP hierarchy in order to optimize over the set of "weakly interacting" quantum strategies that they introduce, but no bounds are shown on the rate of convergence. This is where MIP^*_{ac} becomes relevant. Our notion of δ-AC strategies is easily seen to be a relaxation of weak cross-talk, and thus the analogue of the approach in [89] when performed with a δ-AC constraint is at least as robust as the weak cross-talk approach. Our rounding scheme for the QC SDP hierarchy thus provides a specific algorithm and complexity bound that applies to both δ-AC strategies and strategies with weak cross-talk.

Chapter 5

The Communication Cost of State Conversion, with application to Entanglement-Assisted Communication Complexity

In this chapter we present a series of results about communication complexity that culminate in a proof that any Entanglement-assisted communication protocol can be simulated by a communication protocol using only EPR pairs as an entangled resource. Our first result concerns an old question in quantum information theory: how much quantum communication is required to approximately convert one pure bipartite entangled state into another? We give a simple and efficiently computable bound in terms of the earth mover or Wasserstein distance. We show that the communication cost of converting between two pure states is bounded (up to a constant factor) by the ℓ_∞ Earth Mover distance between the distributions of the negative logarithm of the Schmidt coefficients of each state. Here the ℓ_∞ Earth Mover distance may be informally described as the minimum, over all transports between the two distributions, of the maximum distance that any amount of mass must be moved in that transport.

Using this result we consider the nature of entanglement-assistance in quantum communication protocols. Maximally entangled states are known to be less useful than partially entangled states such as embezzling states for tasks that involve quantum communication between players and referee, for nonlocal games, and for simulating bipartite unitaries or communication channels. By contrast, we prove that the bounded-error one-way or two-way quantum entanglement-assisted communication complexity of a partial or total function cannot be improved by more than a constant factor by replacing maximally entangled states with arbitrary entangled states. In particular, we show that every quantum communication protocol using Q qubits of communication and arbitrary shared entanglement can be ϵ-approximated by a protocol using $O(Q/\epsilon)$ qubits of communication and *only* EPR pairs as shared entanglement. Note that this conclusion is opposite of the common wisdom in the study of non-local games, where it has been shown, for example, that the I3322 inequality has a non-local strategy using a non-maximally entangled state, which surpasses the winning probability achievable by any strategy using only a maximally entangled state of any dimension [96].

This leaves open the question of how much maximally entangled states can reduce the quantum communication complexity of functions.

5.1 Introduction

5.1.1 Communication cost of state transformations

Suppose that $|\chi\rangle$ and $|\nu\rangle$ are bipartite pure quantum states, with vectors of Schmidt coefficients denoted respectively by χ and ν. In this setting it is known that $|\chi\rangle$ can be exactly converted into $|\nu\rangle$ using LOCC if any only if χ is majorized by ν. But the communication cost of this transformation is known only in a few special cases. If $|\chi\rangle = |\chi_0\rangle^{\otimes n}$ and $|\nu\rangle = |\nu_0\rangle^{\otimes n}$ for some states $|\chi_0\rangle, |\nu_0\rangle$, then this cost is $O(\sqrt{n})$ or less in some special cases (e.g. $|\nu_0\rangle$ is maximally entangled). More generally there is, in principle, an exact charac-

terization of the communication cost of state transformation using the Schubert calculus due to Daftuar and Hayden [quant-ph/0410052], but in practice it is difficult to extract concrete bounds from their main theorem.

We give a simple bound of the amount of quantum communication required to transform $|\chi\rangle$ to $|v\rangle$ that is based on the ℓ_∞ earth mover (or Wasserstein) distance, which is defined as follows:

Definition 82 (ℓ_∞ Earth Mover's Distance). *Let* $|\chi\rangle = \sum_{i\in X} \sqrt{\chi_i}|i\rangle \otimes |i\rangle$ *and* $|v\rangle = \sum_{j\in Y} \sqrt{v_j}|j\rangle \otimes |j\rangle$ *be two states. Let* p_χ *be the distribution of a random variable taking value* $\ln \chi_i$ *with probability* χ_i*, and* p_v *be defined analogously. We define* $d_\infty(|\chi\rangle, |v\rangle)$ *to be the* ℓ_∞ *Earth Mover's distance between* $|\chi\rangle$ *and* $|v\rangle$*, which is equal to the minimum* $\mu \geq 0$ *such that there exists a joint distribution* $\omega(x, y)$ *on* $X \times Y$ *with* x *and* y *marginals equal to* p_χ *and* p_v *respectively, and such that* $\omega(x, y) = 0$ *whenever* $|x - y| > \mu$.

In particular we show that there is a quantum communication protocol which can transform the shared state $|\chi\rangle$ to a shared state $|v\rangle$ using $O(d_\infty(|\chi\rangle, |v\rangle))$ communication and only EPR pairs as an additional entangled resource.

5.1.2 Entanglement-assisted communication complexity

In classical communication complexity, Newman's theorem states that arbitrarily large amounts of shared randomness can be replaced with a distribution with only $O(\log n/\varepsilon)$ bits of entropy while only reducing the success probability of a protocol by ε. (Here n is the input size of each party.) Is there a quantum analogue to this result?

In one sense the answer is no. Given a two-party entanglement-assisted protocol for, say, computing the value of some function, we cannot replace the shared entanglement with some different, less entangled, state, without causing large errors [44, 2]. It is an open question whether it is possible to replace a large entangled state with a less entangled one while also changing the communication protocol.

However, we can prove that non maximally entangled states can be replaced, without loss of generality, by maximally entangled states. The protocol is nearly oblivious in the following sense. Given a protocol $\mathcal{P}$ using Q qubits of entanglement and a shared entangled state $|\psi\rangle$, we can replace $|\psi\rangle$ with a state $|\varphi\rangle$ at the cost of error ε. This state $|\varphi\rangle$ can then be prepared from a maximally entangled state using $O(Q/\varepsilon)$ communication. For constant ε this implies that the EPR-assisted communication complexity is at most $O(1)$ times the arbitrary-entanglement-assisted communication complexity.

This contrasts with channel simulation [12], nonlocal games [46, 81], unitary gate simulation [38], and communication tasks involving quantum communication between referees and players [54]. In each of those cases there are large asymptotic separations between the EPR-assisted costs and the general-entanglement-assisted costs.

5.2 Results

The first result is an upper bound on the amount of communication required for two parties to begin with shared state $|\chi\rangle$, and transform it into shared state $|v\rangle$. As discussed in the introduction, one appealing property of this bound, which is given by the Earthmover distance between the two state, is that it is easy to produce from the definition of the states, in contrast to the more exact characterization of the communication complexity of this task, using Schubert calculus. The usefulness of such a bound will later be exhibited in the second result, where the relationship to Earthmover distance is utilized, along with other techniques, to prove a new result about entanglement assisted communication complexity.

Theorem 83. *Let* $|\chi\rangle = \sum_{i\in X} \sqrt{\chi_i}|i\rangle \otimes |i\rangle$ *and* $|v\rangle = \sum_{j\in Y} \sqrt{v_j}|j\rangle \otimes |j\rangle$ *be two states. There is a protocol* $\mathcal{M}$ *which can prepare* $|v\rangle$ *from* $|\chi\rangle$*, while using* $O(d_\infty(|\chi\rangle, |v\rangle))$ *classical communication, and using only EPR pairs as an entangled resource.*

The main result of this chapter, below, is a statement about the way that entanglement

assisted communication complexity depends on the *type* of entangled shared state that the two parties may share. In particular, using the first result, above, together with other techniques, our main result establishes that every entanglement assisted communication with *any* shared state, can be simulated by a protocol using only EPR pairs as the shared state.

Theorem 84. *Consider a one-way or two-way quantum communication protocol $\mathcal{P}$ whose goal it is to compute a joint function $f(x,y) \in \{0,1\}$. Suppose that $\mathcal{P}$ uses an arbitrary entangled state $|\varphi\rangle^{AB}$ (of unbounded size), as well as Q qubits of communication total, in either direction. Then, for every $\varepsilon > 0$, there exists a communication protocol $\mathcal{P}'$ which simulates $\mathcal{P}$ with error ϵ, while using only EPR pairs as an entangled resource (rather than $|\varphi\rangle^{AB}$ or any other state), and using $O(Q/\epsilon)$ qubits of communication. Thus, if $\mathcal{P}$ computes f with error ε' it follows that $\mathcal{P}'$ computes f with error $\epsilon + \varepsilon'$, while using only a maximally entangled state of some dimension, and $O(Q/\epsilon)$ qubits of communication.*

5.3 Earth Mover's Distance and State Transformation

In this section we will give a proof of Theorem 83. The proof is divided into two parts which are proved separately in Lemma 87, and Lemma 90 together with Corollary 91. At a high level Lemma 87 tells us that one can map the Schmidt coefficients of $|\chi\rangle$ directly onto the Schmidt coefficients of $|v\rangle$ using a series of bipartite "flows" that have small degree (defined below). Lemma 90 and Corollary 91 then tell us that any such "flow", which has small degree can be implemented as an actual bipartite state transformation, with correspondingly small communication required.

We prove Lemmas 87 and 90, which, together, prove the desired theorem. We begin by defining the concept of flows, as we use it here.

Definition 85 (Right (Left) Index-1 Flow). *Given two states $|\chi\rangle = \sum_{i\in X} \sqrt{\chi_i}|i\rangle \otimes |i\rangle$ and $|v\rangle = \sum_{j\in Y} \sqrt{v_j}|j\rangle \otimes |j\rangle$ we say that there is a Right Index-1 Flow from $|\chi\rangle$ to $|v\rangle$ if there exists a bipartite graph $G_{X,Y}$ with vertices given by $X \cup Y$, and edge set $E_{X,Y}$, such that:*

- *Each vertex in $j \in Y$ has index 1 in $G_{X,Y}$.*
- *For all $i \in X$, $\chi_i = \sum_{j \in Y:(i,j) \in E_{X,Y}} v_j$*

  If the roles of $|\chi\rangle$ and $|v\rangle$ are reversed in the above, then we say that there is a Left Index-1 Flow from $|v\rangle$ to $|\chi\rangle$ (equivalently, there is a Left Index-1 Flow from $|v\rangle$ to $|\chi\rangle$ exactly when there is a a Right Index-1 Flow from $|\chi\rangle$ to $|v\rangle$).

Definition 86 (Degree of a Right (Left) Index-1 Flow). *We define the degree of a Right (Left) Index-1 Flow from $|\chi\rangle = \sum_{i \in X} \sqrt{\chi_i}|i\rangle \otimes |i\rangle$ to $|v\rangle = \sum_{j \in Y} \sqrt{v_j}|j\rangle \otimes |j\rangle$ to be the maximum index of any vertex in the bipartite graph $G_{X,Y}$.*

Lemma 87. *Given two states $|\chi\rangle = \sum_{i \in X} \sqrt{\chi_i}|i\rangle \otimes |i\rangle$ and $|v\rangle = \sum_{j \in Y} \sqrt{v_j}|j\rangle \otimes |j\rangle$, there exist two "intermediate" states $|\gamma\rangle$ and $|\rho\rangle$, such that there is a Right Index-1 Flow from $|\chi\rangle$ to $|\gamma\rangle$ of degree at most $2^{O(\lceil d_\infty(|\chi\rangle,|v\rangle)\rceil)}$, a Left Index-1 Flow from $|\gamma\rangle$ to $|\rho\rangle$ of degree at most $2^{O(\lceil d_\infty(|\chi\rangle,|v\rangle)\rceil)}$, and a Left Index-1 Flow from $|\rho\rangle$ to $|v\rangle$ of degree at most $2^{O(\lceil d_\infty(|\chi\rangle,|v\rangle)\rceil)}$.*

Proof. Given two states $|\chi\rangle = \sum_{i \in X} \sqrt{\chi_i}|i\rangle \otimes |i\rangle$ and $|v\rangle = \sum_{j \in Y} \sqrt{v_j}|j\rangle \otimes |j\rangle$, and an arbitrary $\varepsilon > 0$, let $\omega(i,j) : X \times Y \to \mathbb{R}_{\geq 0}$ be the joint distribution on $X \times Y$ which satisfies the ℓ_∞ Earth Mover conditions for $|\chi\rangle$ and $|v\rangle$, and acheives the optimal earth mover bound $d_\infty(|\chi\rangle,|v\rangle)$. That is, for all $i \in X$, $\sum_{j \in Y} \omega(i,j) = \chi_i$, for all $j \in Y$, $\sum_{i \in X} \omega(i,j) = v_j$, and $\omega(i,j) = 0$ whenever $|\ln(\chi_i) - \ln(v_j)| > d_\infty(|\chi\rangle,|v\rangle)$.

Define

$$|\rho\rangle \equiv \sum_{j \in Y} \sum_{k \in [2^{\lceil d_\infty(|\chi\rangle,|v\rangle)\rceil+2}]} \sqrt{v_j/2^{\lceil d_\infty(|\chi\rangle,|v\rangle)\rceil+2}}|j\rangle \otimes |k\rangle \otimes |j\rangle \otimes |k\rangle$$

In other words, we define $|\rho\rangle \equiv \sum_{j \in Y} \sum_{k \in [2^{\lceil d_\infty(|\chi\rangle,|v\rangle)\rceil}]} \sqrt{\rho_{j,k}}|j\rangle \otimes |k\rangle \otimes |j\rangle \otimes |k\rangle$, where

$$\rho_{j,k} \equiv v_j/2^{\lceil d_\infty(|\chi\rangle,|v\rangle)\rceil+2}$$

We now define the intermediate state:

$$|\gamma\rangle \equiv \sum_{j\in Y} \sum_{k\in[2^{\lceil d_\infty(|\chi\rangle,|v\rangle)\rceil+2}]} \sum_{c\in\{0,1\}} \sqrt{\gamma_{j,k,c}}|j\rangle \otimes |k\rangle \otimes |c\rangle \otimes |j\rangle \otimes |k\rangle|c\rangle$$

Where we will leave the Schmidt coefficients $\gamma_{j,k,c}$ unspecified for now.

In order to specify the Schmidt coefficients of the intermediate state $|\gamma\rangle$ as well as the Right Index-1 Flow from $|\chi\rangle$ to $|\gamma\rangle$, and the Left Index-1 Flow from $|\gamma\rangle$ to $|\rho\rangle$ we will first define "bins" for the Schmidt coefficients of $|v\rangle$ as follows:

For $l \in \mathbb{N} \cup \{0\}$ let $Y_l \equiv \{j \in Y : e^{-l} \geq v_j \geq e^{-(l+1)}\}$, and $X_l \equiv \{i \in X : e^{-l} \geq \chi_i \geq e^{-(l+1)}\}$. Define $\omega(X_m, Y_l) \equiv \sum_{(i,j)\in X_m \times Y_l} \omega(i,j)$.

Fact 88. *If* $|m-l| > d_\infty(|\chi\rangle, |v\rangle) + 1$, *then* $\omega(X_m, Y_l) = 0$

Proof. Given $i \in X_m$, and $j \in Y_l$ we have by definition that $e^{-l} \geq v_j \geq e^{-(l+1)}$, and $e^{-m} \geq \chi_i \geq e^{-(m+1)}$, and therefore that $|\ln(\chi_i) - \ln(v_j)| \geq |m-l| - 1 > d_\infty(|\chi\rangle, |v\rangle)$, where the last equality follows by assumption. It follows by definition of $d_\infty(|\chi\rangle, |v\rangle)$ and of ω, that $\omega(i,j) = 0$. Since this is true for all $(i,j) \in X_m \times Y_l$, the claim follows. □

Definition 89. *For a set of indices* $S \subseteq \mathbb{N}$ *we define* $\min(S) \equiv \min\{i \in S\}$.

We will now specify an iterative, "greedy" procedure to define the Schmidt coefficients $\gamma_{j,k,c}$ as a function of the $|\chi\rangle$ and $|\rho\rangle$.

For each $(m,l) \in \mathbb{N} \cup \{0\} \times \mathbb{N} \cup \{0\}$ such that $\omega(X_m, Y_l) > 0$ we first note that by Fact 88 that $|m-l| < d_\infty(|\chi\rangle, |v\rangle) + 1$. Thus, for each $(i,j) \in X_m \times Y_l$,

$$\chi_i \geq 2^{-(m+1)} \geq 2^{-l-d_\infty(|\chi\rangle,|v\rangle)-2} \geq 2^{-l}/2^{\lceil d_\infty(|\chi\rangle,|v\rangle)\rceil+2} \geq v_j/2^{\lceil d_\infty(|\chi\rangle,|v\rangle)\rceil+2} \equiv \rho_{j,k}$$

for all $k \in [2^{\lceil d_\infty(|\chi\rangle,|v\rangle)\rceil+2}]$.

One may check that Algorithm 1 defines Schmidt coefficients $\gamma_{j,k,r}$, satisfying

$$\sum_{j\in Y} \sum_{k\in[2^{\lceil d_\infty(|\chi\rangle,|v\rangle)\rceil+2}]} \sum_{r\in[2^{\lceil d_\infty(|\chi\rangle,|v\rangle)\rceil+2}]} \gamma_{j,k,r} = \sum_{i\in X} \chi_i = 1,$$

1

For all i set $temp_i = \chi_i$
Set $i_m = \min\{X_m\}$ for all m
for $l \in \mathbb{N} \cup \{0\}$ **do**
    Set $j := \min\{Y_l\}$;
    Set $k = 0$;
    Set $overflow = 0$
    for $m \in \mathbb{N} \cup \{0\}$ **do**
        if $\omega(X_m, Y_l) > 0$ **then**
            Set $temp_\omega = \omega(X_m, Y_l)$
            while $temp_\omega > 0$ **do**
                if $\sum_{r \leq overflow} \gamma_{j,k,0,overflow} \neq \rho_{j,k}$ **then**
                    while $temp_\omega \geq \rho_{j,k} - \sum_{r \leq overflow} \gamma_{j,k,0,overflow}$ **do**
                        if $k = 2^{\lceil d_\infty(|\chi\rangle,|v\rangle)\rceil+2}$ **then**
                            Set $j = j + 1$
                            Set $overflow = 0$
                            Set $k = 0$
                        end if
                        if $temp_{i_m} < \rho_{j,k} - \sum_{r \leq overflow} \gamma_{j,k,0,overflow}$ **then**
                            Set $\gamma_{j,k,0,overflow+1} = temp_{i_m}$
                            Set $temp_\omega = temp_\omega - temp_{i_m}$
                            Set $temp_{i_m} = 0$
                            Add an edge in the flow graph from i_m to $(j, k, 0, overflow + 1)$
                            Set $i_m = i_m + 1$
                            Set $overflow = overflow + 1$
                        end if
                        if $temp_{i_m} \geq \rho_{j,k} - \sum_{r \leq overflow} \gamma_{j,k,0,overflow}$ and $temp_\omega \geq \rho_{j,k} - \sum_{r \leq overflow} \gamma_{j,k,0,overflow}$ **then**
                            Set $\gamma_{j,k,0,overflow+1} = \rho_{j,k} - \sum_{r \leq overflow} \gamma_{j,k,0,overflow}$
                            Set $temp_\omega = temp_\omega - \gamma_{j,k,0,overflow+1}$
                            Set $temp_{i_m} = temp_{i_m} - \gamma_{j,k,0,overflow+1}$
                            Add an edge in the flow graph from i_m to $(j, k, 0, overflow + 1)$
                            $k = k + 1$
                            Set $overflow = 0$
                        end if
                    end while

My algorithm (continued)

```
                    if k = 2^⌈d_∞(|χ⟩,|v⟩)⌉+2 then
                        Set j = j + 1
                        Set overflow = 0
                        Set k = 0
                    end if
                    if temp_ω < ρ_{j,k} − Σ_{r≤overflow} γ_{j,k,0,overflow} then
                        if temp_{i_m} ≤ temp_ω then
                            Set γ_{j,k,0,overflow+1} = temp_{i_m}
                            Set temp_ω = temp_ω − temp_{i_m}
                            Set temp_{i_m} = 0
                            Add an edge in the flow graph from i_m to (j, k, 0, overflow + 1)
                            Set i_m = i_m + 1
                            Set overflow = overflow + 1
                        end if
                        if temp_{i_m} ≥ temp_ω then
                            Set γ_{j,k,0,overflow+1} = temp_ω
                            Set temp_ω = 0
                            Set temp_{i_m} = temp_{i_m} − temp_ω
                            Add an edge in the flow graph from i_m to (j, k, 0, overflow +
  1)
                            Set overflow = overflow + 1
                        end if
                        if k = 2^⌈d_∞(|χ⟩,|v⟩)⌉+2 then
                            Set j = j + 1
                            Set overflow = 0
                            Set k = 0
                        end if
                    end if
                end if
            end while
        end if
    end for
end for
```

as well as a Right Index-1 Flow from $|\chi\rangle$ to $|\gamma\rangle$, with degree at most $2^{\lceil d_\infty(|\chi\rangle,|v\rangle)\rceil+2} \cdot 2^{\lceil d_\infty(|\chi\rangle,|v\rangle)\rceil+2} = 2^{2\lceil d_\infty(|\chi\rangle,|v\rangle)\rceil+4}$. Furthermore,

$$\sum_{r\in[2^{\lceil d_\infty(|\chi\rangle,|v\rangle)\rceil+2}]} \gamma_{j,k,r} = \rho_{j,k}$$

So that there is a Left Index-1 flow from $|\gamma\rangle$ to $|\rho\rangle$ defined by a bipartite graph between the Schmidt coefficients of $|\gamma\rangle$ and $|\rho\rangle$ respectively, in which, for every $(j,k,r) \in Y \times [2^{\lceil d_\infty(|\chi\rangle,|v\rangle)\rceil+2}] \times [2^{\lceil d_\infty(|\chi\rangle,|v\rangle)\rceil+2}]$, there is an edge from $\gamma_{j,k,r}$ to $\rho_{j,k}$ of weight $\gamma_{j,k,r}$. This Left Index-1 flow then clearly has degree $2^{\lceil d_\infty(|\chi\rangle,|v\rangle)\rceil+2}$.

Finally, recall that,

$$\sum_{k\in[2^{\lceil d_\infty(|\chi\rangle,|v\rangle)\rceil+2}]} \rho_{j,k} = \sum_{k\in[2^{\lceil d_\infty(|\chi\rangle,|v\rangle)\rceil+2}]} v_j/2^{\lceil d_\infty(|\chi\rangle,|v\rangle)\rceil+2} = v_j$$

So, by very similar reasoning, there is a Left Index-1 flow from $|\rho\rangle$ to $|\nu\rangle$ with degree exactly $2^{\lceil d_\infty(|\chi\rangle,|v\rangle)\rceil+2}$.

□

Lemma 90. *Given two states $|\tau\rangle = \sum_{i\in X} \sqrt{\tau_i}|i\rangle \otimes |i\rangle$ and $|\kappa\rangle = \sum_{j\in Y} \sqrt{\kappa_j}|j\rangle \otimes |j\rangle$ such that there is a Right Index-1 Flow from $|\tau\rangle$ to $|\kappa\rangle$ with degree at most 2^Q, then, for two parties sharing entangled state $|\tau\rangle$, there exists a two-way quantum communication protocol $\mathcal{P}$, which uses Q qubits of communication (in total, in either direction), and converts the shared state $|\tau\rangle$ to the shared state $|\kappa\rangle$.*

Proof. By assumption there is a Right Index-1 Flow from $|\tau\rangle$ to $|\kappa\rangle$ with degree at most 2^Q, so there exists a bipartite graph $G_{X,Y}$ with vertices given by $X \cup Y$, and edge set $E_{X,Y}$, such that:

- Each vertex in $j \in Y$ has index 1 in $G_{X,Y}$.
- For all $i \in X$, $\tau_i = \sum_{j\in Y:(i,j)\in E_{X,Y}} \kappa_j$.

- The maximum degree of any vertex $i \in X$ in $G_{X,Y}$ is 2^Q.

The protocol for Alice and Bob to start with shared state $|\tau\rangle$ and end up with shared state $|\kappa\rangle$ will proceed as follows: Beginning with the state $|\tau\rangle$ shared between Alice and Bob, we will refer to the register containing the Alice half of $|\tau\rangle$ as A, and the register containing the Bob half as B. Alice will append two additional registers, of Q qubits each, and initialize each of them to the all zeros state. We will call these two new registers C_1 and C_2 respectively. Alice will then perform a controlled unitary operation between A and the registers C_1 and C_2. She will then pass the register C_2 to Bob using Q qubits of quantum communication to do so. Bob will then perform a controlled unitary between B and C_2, Alice will perform a controlled unitary between A and C_1, and after that Alice and Bob will share the state $|\kappa\rangle$.

To describe the protocol more precisely we will define the specific controlled unitaries performed by Alice and Bob at each step. Beginning with a shared state $|\tau\rangle$, after Alice appends the two additional Q-qubit registers to her side of $|\tau\rangle$, the shared state looks as follows:

$$|\tau\rangle = \sum_{i \in X} \sqrt{\tau_i} |0^{\otimes Q}\rangle_{C_1} \otimes |0^{\otimes Q}\rangle_{C_2} \otimes |i\rangle_A \otimes |i\rangle_B$$

Where, initially, Alice holds the registers A, C_1, and C_2. Alice now performs a controlled unitary operation, acting on registers C_1 and C_2 and controlled on register A. To describe this controlled unitary concisely we will need to imagine that there is some total order on the elements $j \in Y$ (any total order will do, one can simply imagine that the j's are indexed by bit strings which encode integers), and we will define $s_{ij} \equiv |\{j' \in Y : j' < j, \text{ and } (i, j') \in E_{X,Y}\}|$. Note that, since every $i \in X$ has degree at most 2^Q, s_{ij} is always an integer between 0 and 2^Q, so it can always be expressed in binary as a Q-bit binary number. We will take this convention in the following argument.

Now to define Alice's controlled unitary: When controlled on $|i\rangle_A$ Alice's unitary moves the state $|0^{\otimes Q}\rangle_{C_1} \otimes |0^{\otimes Q}\rangle_{C_2}$ to the state $|i\text{-controlled}\rangle_{C_1 C_2} \equiv \sum_{j \in Y : (i,j) \in E_{X,Y}} \sqrt{\kappa_j / \tau_i} |s_{ij}\rangle_{C_1} \otimes$

$|s_{ij}\rangle_{C_2}$. Note that since s_{ij} is always a Q-bit binary string, it can always be contained in the Q-qubit registers C_1 and C_2. Further note that, since $\tau_i = \sum_{j \in Y:(i,j) \in E_{X,Y}} \kappa_j$ by assumption, $|i\text{-controlled}\rangle_{C_1C_2}$ is a normalized pure state. Thus there exists a unitary operation that moves $|0^{\otimes Q}\rangle_{C_1} \otimes |0^{\otimes Q}\rangle_{C_2}$ to $|i\text{-controlled}\rangle_{C_1C_2}$ and Alice need only perform this specific unitary when the control register is in state $|i\rangle_A$. So, when Alice applies this controlled unitary to her registers C_1, C_2 and A (where A is the controlling register), the resulting new shared state between Alice and Bob is:

$$|\tau\rangle = \sum_{i \in X} |i\text{-controlled}\rangle_{C_1C_2} \otimes |i\rangle_A \otimes |i\rangle_B = \sum_{i \in X} \sum_{j \in Y:(i,j) \in E_{X,Y}} \sqrt{\tau_i} \cdot \sqrt{\kappa_j / \tau_i} |s_{ij}\rangle_{C_1} \otimes |s_{ij}\rangle_{C_2} \otimes |i\rangle_A \otimes |i\rangle_B \tag{5.1}$$

$$= \sum_{i \in X} \sum_{j \in Y:(i,j) \in E_{X,Y}} \sqrt{\kappa_j} |s_{ij}\rangle_{C_1} \otimes |s_{ij}\rangle_{C_2} \otimes |i\rangle_A \otimes |i\rangle_B \tag{5.2}$$

At this point Alice uses Q-qubits of communication to pass the Q-qubit register C_2 to Bob. The resulting shared state is:

$$\sum_{i \in X} \sum_{j \in Y:(i,j) \in E_{X,Y}} \sqrt{\kappa_j} |s_{ij}\rangle_{C_1} \otimes |i\rangle_A \otimes |i\rangle_B \otimes |s_{ij}\rangle_{C_2}$$

Where Alice owns registers C_1 and A, and Bob owns registers C_2 and B. Now it is not hard to see from the definition of s_{ij} and the fact that every $j \in Y$ has degree exactly 1 in the graph $G_{X,Y}$, that there is a bijection mapping each $j \in Y$ to the tuple (i, s_{ij}). Alice and Bob both know this bijection since they know the description of $G_{X,Y}$, and since bijections are invertible, Alice and Bob can now both apply a local unitary which relabels the basis element $|i\rangle \otimes |s_{ij}\rangle$ to the basis element j. The resulting shared state is:

$$\sum_{i \in X} \sum_{j \in Y:(i,j) \in E_{X,Y}} \sqrt{\kappa_j} |j\rangle_A \otimes |j\rangle_B = \sum_{j \in Y} \sqrt{\kappa_j} |j\rangle_A \otimes |j\rangle_B \equiv |\kappa\rangle$$

Where the first equality follows because each $j \in Y$ appears in the initial sum exactly once (because j has degree exactly one in $G_{X,Y}$).

This completes the protocol.

□

Corollary 91. *Given two states $|\tau\rangle$ and $|\kappa\rangle$ such that there is a Left Index-1 Flow from $|\kappa\rangle$ to $|\tau\rangle$ with degree at most 2^Q, then, for two parties sharing entangled state $|\kappa\rangle$, there exists a two-way quantum communication protocol $\mathcal{P}$, which uses Q qubits of communication (in total, in either direction), and converts the shared state $|\kappa\rangle$ to the shared state $|\tau\rangle$.*

Proof. By definition, if there is a Left Index-1 Flow from $|\kappa\rangle$ to $|\tau\rangle$, then there is a Right Index-1 Flow from $|\tau\rangle$ to $|\kappa\rangle$ (which is the starting assumption of Lemma 90). One can check that, in the proof Lemma 90, every operation performed by Alice and Bob was reversible. Therefore, the proof of this corollary is simple the start at the end of the proof of Lemma 90, and "reverse" every step of the proof in order from end to beginning (including the communication step...now communication goes from Bob to Alice rather than Alice to Bob). The result is the desired quantum communication protocol, which converts the shared state $|\kappa\rangle$ to the shared state $|\tau\rangle$ using Q-qubits of communication. □

Proof of Theorem 83

Proof. The proof follows by applying Lemma 87, followed by Lemma 90 and Corollary 91. □

5.4 Main Result

Lemma 92. *Given two (sub-normalized) quantum states $|\psi\rangle$ and $|\nu\rangle$ on $\mathcal{H}_A \otimes \mathcal{H}_B$ (that is, $\||\psi\rangle\|, \||\nu\rangle\| \leq 1$), such that the Schmidt coefficients of ψ are upper bounded by $\lambda_{\max}$, and those of ν are upper bounded by $\nu_{\max}$, we have:*

$$|\langle\psi|\nu\rangle| \leq rk_{Schmidt}(|\psi\rangle)\sqrt{\lambda_{\max}\nu_{\max}}$$

Proof. For brevity let $r = rk_{Schmidt}(|\psi\rangle)$. Schmidt decompose $|\psi\rangle$ and $|\nu\rangle$ as $|\psi\rangle = \sum_{i=0}^{r-1}\sqrt{\lambda_i}|i\rangle_A \otimes |i\rangle_B$, as $|\nu\rangle = \sum_j \sqrt{\nu_j}|j\rangle_A \otimes |j\rangle_B$. Define the matrix $M_\nu = \sum_j \sqrt{\nu_j}|j\rangle_A \otimes \langle j|_B^*$, and note that

$$\langle\psi|\nu\rangle = \sum_{i=0}^{r-1}\sum_j \sqrt{\lambda_i\nu_j}\langle i_A|j_A\rangle \otimes \langle i_B|j_B\rangle = \sum_{i=0}^{r-1}\sum_j \sqrt{\lambda_i\nu_j}\langle i_A|j_A\rangle \otimes (\langle j_B|i_B\rangle)^*$$
$$= \sum_{i=0}^{r-1}\sum_j \sqrt{\lambda_i\nu_j}\langle i_A|j_A\rangle \otimes \langle j_B^*|i_B^*\rangle = \sum_{i=0}^{r-1}\sqrt{\lambda_i}\langle i_A|\left(\sum_j \sqrt{\nu_j}|j\rangle_A \otimes \langle j|_B\right)|i_B^*\rangle = \sum_{i=0}^{r-1}\sqrt{\lambda_i}\langle i_A|M_\nu|i_B^*\rangle$$

Now, by definition of a Schmidt Decomposition, we know that the maximum singular value of M_ν is ν_{max}. Thus, for all i we have that $|\langle i_A|M_\nu|i_B^*\rangle| \leq \nu_{max}$ (since $|i_A\rangle$ and $|i_B\rangle$ are normalized vectors by definition). It then follows that:

$$|\langle\psi|\nu\rangle| = \left|\sum_{i=0}^{r-1}\sqrt{\lambda_i}\langle i_A|M_\nu|i_B^*\rangle\right| \leq \sqrt{\lambda_{\max}}\sum_{i=0}^{r-1}|\langle i_A|M_\nu|i_B^*\rangle| \leq r\sqrt{\lambda_{\max}\nu_{\max}}$$
$$= rk_{Schmidt}(|\psi\rangle)\sqrt{\lambda_{\max}\nu_{\max}}$$

□

Theorem 93 (Main Result). *Consider a one-way or two-way quantum communication protocol $\mathcal{R}$ whose goal it is to compute a joint function $g(x,y) \in \{0,1\}$. Suppose that $\mathcal{R}$ uses an arbitrary entangled state $|\varphi\rangle^{AB}$ (of unbounded size), as well as Q qubits of communication total, in either direction. Then, for every $\varepsilon > 0$, there exists a communication protocol $\mathcal{R}'$ which simulates $\mathcal{R}$ with error ϵ, while using only EPR pairs as an entangled resource (rather than $|\psi\rangle^{AB}$ or any other state), and using $O(Q/\epsilon)$ qubits of communication . Thus, if $\mathcal{R}$ computes f with error ε' it follows that $\mathcal{R}'$ computes f with error $\epsilon + \varepsilon'$, while using only a maximally entangled state of some dimension, and $O(Q/\epsilon)$ qubits of communication.*

Proof. Schmidt decompose $|\psi\rangle$ as $\sum_i \sqrt{\lambda_i}|i,i\rangle$.

Let N be an integer, which will be specified later. Define a function $f : [0,1] \to \mathbb{N}$ given by

$$f(\lambda) = \left\lceil e^{\left\lceil \frac{\ln(1/\lambda)}{N} \right\rceil N - \ln(1/\lambda)} \right\rceil,$$

and define a new state $|\varphi\rangle \equiv \sum_i \sum_{j \in \{1,\ldots,f(\lambda_i)\}} \nu_{i,j} |(i,j),(i,j)\rangle$, where $\nu_{i,j} \equiv \frac{\lambda_i}{f(\lambda_i)}$. Note that $\sum_{i,j} \nu_{i,j} = 1$, so that $|\varphi\rangle$ is a normalized pure state. Furthermore, every Schmidt coefficient $\nu_{i,j}$ of $|\varphi\rangle$ is within one multiple of e^2 of the integer power $e^{-\left\lceil \frac{\ln(1/\lambda_i)}{N} \right\rceil N}$. This follows because

$$\begin{aligned}
&\left| \ln \left(\frac{\nu_{i,j}}{e^{-\left\lceil \frac{\ln(1/\lambda_i)}{N} \right\rceil N}} \right) \right| = \left| \ln(\lambda_i) - \ln(f(\lambda_i)) + \left\lceil \frac{\ln(1/\lambda_i)}{N} \right\rceil N \right| \\
&\leq \left| \ln \left(e^{\left\lceil \frac{\ln(1/\lambda_i)}{N} \right\rceil N - \ln(1/\lambda_i)} \right) - \ln(f(\lambda_i)) \right| + \left| \ln(\lambda_i) - \ln \left(e^{\left\lceil \frac{\ln(1/\lambda_i)}{N} \right\rceil N - \ln(1/\lambda_i)} \right) + \left\lceil \frac{\ln(1/\lambda_i)}{N} \right\rceil N \right| \\
&\leq 1 + \left| \left\lceil \frac{\ln(1/\lambda_i)}{N} \right\rceil N - \ln(1/\lambda_i) - \left\lceil \left\lceil \frac{\ln(1/\lambda_i)}{N} \right\rceil N - \ln(1/\lambda_i) \right\rceil \right| \leq 2 \qquad (5.3)
\end{aligned}$$

Finally, note that, $\forall \lambda \in [0,1]$, $f(\lambda) \leq e^{2N}$, and it follows that $d_\infty(|\psi\rangle, |\varphi\rangle) \leq 2N$ (since one can move the mass at $\nu_{i,j}$ to λ_i). Therefore, by Theorem 83, there is a protocol $\mathcal{M}$ by which Alice and Bob can prepare $|\varphi\rangle$ from $|\psi\rangle$, using $O(d_\infty(|\chi\rangle, |v\rangle)) = O(N)$ classical communication, and using only EPR pairs as an entangled resource.

Define $\mathcal{C} \equiv \mathcal{R} \circ \mathcal{M}$ to be the composed protocol in which Alice and Bob start with shared state $|\varphi\rangle$, first use protocol $\mathcal{M}$ to convert $|\varphi\rangle$ to $|\psi\rangle$, and then perform protocol $\mathcal{R}$ using shared state $|\psi\rangle$ and inputs x and y, to compute the joint function $g(x,y)$. It is evident that $\mathcal{C}$ has exactly the same success probability as $\mathcal{R}$, and, since $\mathcal{M}$ uses $O(N)$ qubits of communication and $\mathcal{R}$ together uses $O(Q)$ qubits of communication, $\mathcal{C}$ can be performed with $O(Q+N)$ qubits of communication. For the remainder of this proof we will consider protocol $\mathcal{C}$, which uses shared state $|\varphi\rangle$, and how it may be "rounded" to produce

a protocol $\mathcal{R}'$. For simplicity of notation we will continue the proof as if $\mathcal{C}$ uses exactly $Q+N$ qubits of communication, rather than $O(Q+N)$, but the analysis is easy to adapt to the case of $O(Q+N)$.

For j a nonnegative integer, define $I_j := \{i : e^{-jN+2} \geq \lambda_i > e^{-jN-2}\}$. It follows from the calculation in Equation (5.3) that $\cup_j I_j$ contains all of the Schmidt coefficients of $|\varphi\rangle$. So, defining the subnormalized states $|\varphi_j\rangle \equiv \sum_{i \in I_j} \sqrt{\lambda_i}|i,i\rangle$, we have that $|\varphi\rangle = \sum_j |\varphi_j\rangle$. Furthermore, by the definition of I_j, it follows that $|\varphi_j\rangle$ has spread at most 4 (note that the spread of $|\varphi_j\rangle$ does not depend on whether the state is normalized or not).

The idea of the proof is that different $|\varphi_j\rangle$ are not only orthogonal, but must remain approximately orthogonal even after a small amount of quantum communication. In particular, observe that if U is a unitary transform using M qubits of communication, then, for any j, $rk_{Schmidt}(U|\varphi_j\rangle) \leq 2^M rk_{Schmidt}(|\varphi_j\rangle) \leq 2^M e^{jN+2} \||\varphi_j\rangle\|^2$. Also, for all k we have, by definition, that the Schmidt coefficients of $|\varphi_k\rangle$ are bounded above by e^{-kN+2}. It follows by Lemma 92, that $\forall j,k$,

$$|\langle\varphi_k|U|\varphi_j\rangle| \leq 2^M e^{\min(j,k)N+2} \left\||\varphi_{\min(j,k)}\rangle\right\|^2 \sqrt{e^{-jN+2} \cdot e^{-kN+2}} \leq 2^M e^{-N\frac{|j-k|}{2}+4} \left\||\varphi_{\min(j,k)}\rangle\right\|^2 \tag{5.4}$$

To apply this to our problem, we observe that the entire communication protocol can be expressed as performing $\mathcal{C}$ and then measuring the first qubit. Thus, the probability that the protocol outputs $b \in \{0,1\}$ is

$$\Pr[b] = \langle\varphi|\mathcal{C}^\dagger(|b\rangle\langle b| \otimes I)\mathcal{C}|\varphi\rangle,$$

where I acts on all qubits except for the one being measured. Define $\mathcal{P} \equiv \mathcal{C}^\dagger(\sigma_z \otimes I)\mathcal{C} = \mathcal{C}^\dagger(|0\rangle\langle 0| \otimes I)\mathcal{C} - \mathcal{C}^\dagger(|1\rangle\langle 1| \otimes I)\mathcal{C}$. Then

$$\Pr[0] - \Pr[1] = \langle\varphi|\mathcal{P}|\varphi\rangle = \sum_{j,k}\langle\varphi_j|\mathcal{P}|\varphi_k\rangle \tag{5.5}$$

Additionally, observe that $\mathcal{P}$ is a unitary operator that can be constructed using $O(Q+N)$ qubits of communication.

We now seek to replace $\varphi = \sum_{jk}|\varphi_j\rangle\langle\varphi_k|$ with a density matrix ρ that (a) is close to a mixture of states with small spread so that it can be efficiently produced starting from the maximally entangled state, and (b) has the property that the protocol $\mathcal{P}$, when run with shared state ρ, has nearly the same success probability as when it is run with φ. It is clear that if we establish both (a) and (b) then we will be done.

Part (a) Let us first establish part (a). Towards this end, we consider the state $\rho \equiv \sum_{k,l:|k-l|\leq 20+2\left\lceil\frac{\ln(1/\epsilon)}{N}\right\rceil}|\varphi_k\rangle\langle\varphi_l|$. It is not clear whether ρ itself is a mixture of states of small spread, but we can use ρ to determine how to "cut" φ down into a mixture of states of small spread.

The intuition behind this is that we can argue that there is a simple way to project ρ into a block diagonal matrix (a union of submatrices of ρ), with block sizes of $O(N/\epsilon + \ln(1/\epsilon)/\epsilon)$, such that this block diagonal matrix only differs from ρ by ϵ in the trace norm. It will then follow, in the second part of the argument, that projecting φ down into these same blocks produces a state which is a mixture of states with spread at most $O(N/\epsilon + \ln(1/\epsilon)/\epsilon)$, and has the property that the communication protocol $\mathcal{P}$ acting on this new mixture is only ϵ different from $\mathcal{P}$ acting on φ.

The first part proceeds as follows:

Define a nested sequence of projectors P_i, where each P_i is the projection onto the span of $\{|\varphi_l\rangle\}_{l=1}^{2i\cdot(20+2\left\lceil\frac{\ln(1/\epsilon)}{N}\right\rceil)}$ (and $P_i^c \equiv I - P_i$). Consider the matrices $M_i \equiv P_i\rho P_i^c + P_i^c\rho P_i$. Note the following two properties:

Fact 94. *$\rho - M_i = P_i\rho P_i + P_i^c\rho P_i^c$, which is block diagonal, and is a state (PSD and trace 1,*

because it is a union of submatrices of ρ containing the diagonal of ρ).

Fact 95. *The matrix $M = \sum_{i=1}^{\infty} M_i$ is block diagonal with each M_i lying in a different block. This is because ρ is a banded matrix by definition, and the support of the projectors P_i increases in increments of $2 \cdot (20 + 2\left\lceil \frac{\ln(1/\epsilon)}{N} \right\rceil)$, which is twice the width of the bandwidth of ρ.*

Now, for $k \in [1, ..., \lceil 1/\varepsilon \rceil]$ define $S_k = \sum_{i=0}^{\infty} M_{i \cdot \lceil 1/\varepsilon \rceil + k}$. It follows from Fact 94 and from the fact that P_i are strictly nested projectors (so $(P_i - P_{i-1}) = P_i P_{i-1}^c$ is a projector), that $\sum_{i=1}^{\infty} P_i P_{i-1}^c \rho P_i P_{i-1}^c = \rho - \sum_{i=1}^{\infty} M_i = \rho - M = \rho - \sum_{k=1}^{\lceil 1/\varepsilon \rceil} S_k$.

So, we have that :

$$\left\| \sum_{k=1}^{\lceil 1/\varepsilon \rceil} S_k \right\|_1 = \|\rho - \sum_{i=1}^{\infty} P_i P_{i-1}^c \rho P_i P_{i-1}^c\|_1 \leq \|\rho\|_1 + \| \sum_{i=1}^{\infty} P_i P_{i-1}^c \rho P_i P_{i-1}^c \|_1$$
$$= \|\rho\|_1 + \sum_{i=1}^{\infty} \|P_i P_{i-1}^c \rho P_i P_{i-1}^c\|_1 = 2$$

Where the first inequality follows from trace inequality, and the last equality follows from the fact that the set of projectors $\{P_i P_{i-1}^c\}_{i=1}^{\infty}$ is an orthonormal set of measurements spanning the support of ρ.

Now, by Fact 95 we know that $\left\| \sum_{k=1}^{\lceil 1/\varepsilon \rceil} S_k \right\|_1 = \sum_{k=1}^{\lceil 1/\varepsilon \rceil} \|S_k\|_1$, so combining this with our bound on $\left\| \sum_{k=1}^{\lceil 1/\varepsilon \rceil} S_k \right\|_1$, gives

$$\sum_{k=1}^{\lceil 1/\varepsilon \rceil} \|S_k\|_1 \leq 2$$

Thus, there must exist a k such that $\|S_k\|_1 \leq 2/\lceil 1/\varepsilon \rceil \leq 2\epsilon$. Fix k' to be the particular k with this property. Consider the matrix $\rho - S_{k'}$.

First note that, by Facts 94 and 95 above, we have that

$$\rho - S_{k'} = \sum_{i=1}^{\infty} P^c_{(i-1+k')\lceil 1/\varepsilon \rceil} P_{(i+k')\lceil 1/\varepsilon \rceil} \rho P^c_{(i-1+k')\lceil 1/\varepsilon \rceil} P_{(i+k')\lceil 1/\varepsilon \rceil}$$

Recall that $P^c_{(i-1+k')\lceil 1/\varepsilon\rceil} P_{(i+k')\lceil 1/\varepsilon\rceil}$ is a projector (since the P_i are strictly nested projectors). Thus, we know that

$$\rho'_i \equiv P^c_{(i-1+k')\lceil 1/\varepsilon\rceil} P_{(i+k')\lceil 1/\varepsilon\rceil} \varphi P^c_{(i-1+k')\lceil 1/\varepsilon\rceil} P_{(i+k')\lceil 1/\varepsilon\rceil}$$

is an un-normalized state, for every i, and the new state

$$\rho' \equiv \sum_{i=1}^{\infty} \rho'_i \equiv \sum_{i=1}^{\infty} P^c_{(i-1+k')\lceil 1/\varepsilon\rceil} P_{(i+k')\lceil 1/\varepsilon\rceil} \varphi P^c_{(i-1+k')\lceil 1/\varepsilon\rceil} P_{(i+k')\lceil 1/\varepsilon\rceil}$$

is a normalized mixture of these states (since $\{P_i P^c_{i-1}\}_{i=1}^{\infty}$ is an orthonormal set of measurements spanning the support of φ). Note that we are now defining ρ' as a projection of φ, not of ρ. The purpose of studying ρ was to obtain the projectors $P^c_{(i-1+k')\lceil 1/\varepsilon\rceil} P_{(i+k')\lceil 1/\varepsilon\rceil}$, and the matrix $S_{k'}$, which will play a role in establishing part (b) below.

For now we note that the states ρ_i are pure states since:

$$\rho'_i \equiv P^c_{(i-1+k')\lceil 1/\varepsilon\rceil} P_{(i+k')\lceil 1/\varepsilon\rceil} \varphi P^c_{(i-1+k')\lceil 1/\varepsilon\rceil} P_{(i+k')\lceil 1/\varepsilon\rceil}$$

$$= P^c_{(i-1+k')\lceil 1/\varepsilon\rceil} P_{(i+k')\lceil 1/\varepsilon\rceil} |\varphi\rangle\langle\varphi| P^c_{(i-1+k')\lceil 1/\varepsilon\rceil} P_{(i+k')\lceil 1/\varepsilon\rceil}$$

and, defining index limits $B_s \equiv 2((i+k'-1)\lceil 1/\varepsilon\rceil)(20 + 2\left\lceil \frac{\ln(1/\epsilon)}{N} \right\rceil)$ and $B_b \equiv 2((i+k')\lceil 1/\varepsilon\rceil)(20 + 2\left\lceil \frac{\ln(1/\epsilon)}{N} \right\rceil)$, we have

$$P^c_{(i-1+k')\lceil 1/\varepsilon\rceil} P_{(i+k')\lceil 1/\varepsilon\rceil} |\varphi\rangle = \sum_{B_s < l \leq B_b} |\varphi_l\rangle$$

We know by definition that the $|\varphi_l\rangle$ are orthogonal to each other, and that each $|\varphi_l\rangle$ has Schmidt coefficients bounded by $e^{-jN+2} \geq \lambda_i > e^{-jN-2}$. Thus, it is immediate that ρ'_i (and the pure state $P^c_{(i-1+k')\lceil 1/\varepsilon\rceil} P_{(i+k')\lceil 1/\varepsilon\rceil} |\varphi\rangle$) have spread at most $(B_b - B_s)N + 4 = 2\lceil 1/\varepsilon\rceil(20 + 2\left\lceil \frac{\ln(1/\epsilon)}{N} \right\rceil)N + 4 = O(N/\epsilon + \ln(1/\epsilon)/\epsilon)$. It follows that ρ' is a normalized

mixture of states with spread at most $O(N/\epsilon + \ln(1/\epsilon)/\epsilon)$.

Consider the normalized version of ρ'_i, which is still a pure state of spread at most $O(N/\epsilon + \ln(1/\epsilon)/\epsilon)$ it is clear that this state has Earthmover distance at most $O(N/\epsilon + \ln(1/\epsilon)/\epsilon)$ from the nearest maximally entangled state (simply move all of the weight onto Schmidt coefficients of the size of the smallest Schmidt coefficient, which can be done by moving all the weight a distance less than or equal to the spread). It follows easily, by using Theorem 83 that there is a protocol which prepares the normalized version of ρ'_i from EPR pairs, with only $O(N/\epsilon + \ln(1/\epsilon)/\epsilon)$ bits of communication. Now the state $\rho' \equiv \sum_i \rho'_i$ can be prepared by applying this same protocol in superposition over i (with the probability $tr(\rho'_i)$ assigned to each i), and then tracing out over the i register. Thus ρ' can be prepared starting from EPR pairs with $O(N/\epsilon + \ln(1/\epsilon)/\epsilon)$ bits of communication (exactly because it is a mixture of states with spread at most $O(N/\epsilon + \ln(1/\epsilon)/\epsilon)$).

This establishes part (a).

Part (b) We will now establish property (b), that the difference between the success bias for protocol $\mathcal{P}$ when run with shared state ρ' and the success bias when run with shared state φ is $O(\epsilon)$. To prove this we will consider the intermediate matrix $\rho' + S_{k'}$, where $S_{k'}$ is defined above in the argument for part (a). We already know from part (a) that $\|S_{k'}\|_1 \leq 2\epsilon$. Furthermore, we know that the non-zero elements of the matrices ρ' and $S_{k'}$ are disjoint. More precisely, for a matrix θ, define $T_\theta = \{(l,k) : \langle\varphi_k|\theta|\varphi_l\rangle \neq 0\}$. It follows from the argument in part (a) that the sets $T_{\rho'}$, and $T_{S_{k'}}$ are disjoint. Moreover, again according to the construction in part (a), we have that for every $(l,k) \in T_{\rho'+S_{k'}}$, $\langle\varphi_k|(\rho' + S_{k'})|\varphi_l\rangle = \langle\varphi_k|\varphi|\varphi_l\rangle$. Finally, recalling the original definition $\rho \equiv \sum_{k,l:|k-l|\leq 20+2\left\lceil\frac{\ln(1/\epsilon)}{N}\right\rceil} |\varphi_k\rangle\langle\varphi_l|$, we have from part (a) that $\{(l,k) : |k-l| \leq 20 + 2\left\lceil\frac{\ln(1/\epsilon)}{N}\right\rceil\} = T_\rho \subseteq T_{\rho'+S_{k'}}$.

We can now bound the difference between the protocol $\mathcal{P}$ acting on φ versus the protocol acting on ρ', following equation 5.5 as follows:

$$\left|(\Pr_{\varphi}[0]-\Pr_{\varphi}[1])-(\Pr_{\rho'}[0]-\Pr_{\rho'}[1])\right| = \left|\mathrm{Tr}(\mathcal{P}(\varphi-\rho'))\right| \leq \left|\mathrm{Tr}(\mathcal{P}(\varphi-(\rho'+S_{k'})))\right|+2\epsilon$$

$$= \left|\sum_{(k,l)\notin T_{(\rho'+S_{k'})}} \langle\varphi_k|\mathcal{P}|\varphi_l\rangle\right| + 2\epsilon \leq \sum_{(k,l)\notin T_{(\rho'+S_{k'})}} |\langle\varphi_k|\mathcal{P}|\varphi_l\rangle| + 2\epsilon \leq \sum_{(k,l)\notin T_{\rho}} |\langle\varphi_k|\mathcal{P}|\varphi_l\rangle| + 2\epsilon$$

$$= \sum_{k,l:|k-l|>20+2\left\lceil\frac{\ln(1/\epsilon)}{N}\right\rceil} |\langle\varphi_k|\mathcal{P}|\varphi_l\rangle| + 2\epsilon$$

The first inequality follows because $\|S_{k'}\|_1 \leq 2\epsilon$. The rest of the above follows because $\langle\varphi_k|(\rho'+S_{k'})|\varphi_l\rangle = \langle\varphi_k|\varphi|\varphi_l\rangle$ for $(l,k) \in T_{\rho'+S_{k'}}$ and $\langle\varphi_k|(\rho'+S_{k'})|\varphi_l\rangle = 0$ elsewhere, and finally because $T_\rho \subseteq T_{\rho'+S_{k'}}$.

Now, by using equation 5.4, we have that:

$$\left|(\Pr_{\varphi}[0]-\Pr_{\varphi}[1])-(\Pr_{\rho'}[0]-\Pr_{\rho'}[1])\right| - 2\epsilon$$

$$\leq \sum_{k,l:|k-l|>20+2\left\lceil\frac{\ln(1/\epsilon)}{N}\right\rceil} \min(1, 2^{2(Q+N)}e^{-N\frac{|k-l|}{2}+4}) \left\| |\varphi_{\min(k,l)}\rangle \right\|^2$$

$$= 2\sum_{l} \| |\varphi_l\rangle \|^2 \sum_{k>l+20+2\left\lceil\frac{\ln(1/\epsilon)}{N}\right\rceil} \min(1, 2^{2(Q+N)}e^{-N\frac{|k-l|}{2}+4})$$

$$= 2 \sum_{n>20+2\left\lceil\frac{\ln(1/\epsilon)}{N}\right\rceil} \min(1, 2^{2(Q+N)}e^{-N\frac{n}{2}+4})$$

$$= 2 \sum_{n>20+2\left\lceil\frac{\ln(1/\epsilon)}{N}\right\rceil} \min(1, 2^{2(Q+N)}e^{-N\frac{n}{2}+4}) \leq 2\cdot 2^{2(Q+N)}e^{-10N+4-\ln(1/\epsilon)} \sum_{n=1}^{\infty} e^{-N\frac{n}{2}}$$

$$= 2\cdot 2^{2(Q+N)}e^{-10N+4-\ln(1/\epsilon)} \left(\frac{e^{-\frac{1}{2}}}{1-e^{-\frac{1}{2}}}\right) \leq 4\cdot 2^{2(Q+N)}e^{-10N+4-\ln(1/\epsilon)}$$

So, setting $N = Q$ (and assuming $Q \geq 1$ to avoid the trivial case), we have that:

$$\left|(\Pr_{\varphi}[0]-\Pr_{\varphi}[1])-(\Pr_{\rho'}[0]-\Pr_{\rho'}[1])\right|-2\epsilon \leq 4\cdot 2^{2(Q+N)}e^{-10N+4-\ln(1/\epsilon)} \leq 4\cdot 2^{4N}e^{-6N-\ln(1/\epsilon)}$$
$$\leq 4e^{-2N-\ln(1/\epsilon)} \leq \epsilon$$

So,

$$\left|(\Pr_{\varphi}[0]-\Pr_{\varphi}[1])-(\Pr_{\rho'}[0]-\Pr_{\rho'}[1])\right| \leq 3\epsilon = O(\epsilon)$$

This establishes property (b), that the protocol $\mathcal{P}$, when run with shared state ρ', has nearly the same success probability as when it is run with φ (up to error ϵ).

Since we have already shown, in part (a), that ρ' can be produced from EPR pairs using $O(N/\epsilon+\ln(1/\epsilon)/\epsilon = O(Q/\epsilon+\ln(1/\epsilon)/\epsilon)$ communication, it follows that we can define a communication protocol $\mathcal{R}'$, in which the two parties start with shared EPR pairs, use $O(Q/\epsilon+\ln(1/\epsilon)/\epsilon)$ communication to produce ρ' (Note that this preparation is exact. The ϵ in this part comes from the definition of ρ'.), and then use $O(Q+N) = O(Q)$ communication to apply $\mathcal{P}$ to ρ', which we have shown, in part (b), approximates the output of applying $\mathcal{P}$ to φ, up to error ϵ. This gives a protocol $\mathcal{R}'$ which uses only shared EPR pairs, and $O(Q/\epsilon+\ln(1/\epsilon)/\epsilon)$ communication, and approximates the original protocol $\mathcal{R}$ up to $O(\epsilon)$. This is the desired result.

□

Bibliography

[1] Antonio Acín, Serge Massar, and Stefano Pironio. Randomness versus nonlocality and entanglement. *Physical review letters*, 108(10):100402, 2012.

[2] Dorit Aharonov, Aram W. Harrow, Zeph Landau, Daniel Nagaj, Mario Szegedy, and Umesh Vazirani. Local tests of global entanglement and a counterexample to the generalized area law. In *Foundations of Computer Science (FOCS), 2014 IEEE 55th Annual Symposium on*, pages 246–255, Oct 2014.

[3] Leandro Aolita, Rodrigo Gallego, Adán Cabello, and Antonio Acín. Fully nonlocal, monogamous, and random genuinely multipartite quantum correlations. *Physical Review Letters*, 108(10):100401, 2012.

[4] P. K. Aravind. The magic squares and Bell's theorem. Technical report, arXiv:quant-ph/0206070, 2002.

[5] Sanjeev Arora, Carsten Lund, Rajeev Motwani, Madhu Sudan, and Mario Szegedy. Proof verification and the hardness of approximation problems. *J. ACM*, 45(3):501–555, 1998.

[6] Sanjeev Arora and Shmuel Safra. Probabilistic checking of proofs: A new characterization of NP. *J. ACM*, 45(1):70–122, 1998.

[7] László Babai, Lance Fortnow, and Carsten Lund. Non-deterministic exponential time has two-prover interactive protocols. *Comput. Complexity*, 1:3–40, 1991.

[8] Jean-Daniel Bancal, Lana Sheridan, and Valerio Scarani. More randomness from the same data. *New Journal of Physics*, 16(3):033011, 2014.

[9] Jonathan Barrett, Lucien Hardy, and Adrian Kent. No signaling and quantum key distribution. *Physical review letters*, 95(1):010503, 2005.

[10] John S. Bell. On the Einstein Podolsky Rosen paradox. *Physics*, 1:195–200, 1964.

[11] Michael Ben-Or, Shafi Goldwasser, Joe Kilian, and Avi Wigderson. Multi-prover interactive proofs: How to remove intractability assumptions. In *Proceedings of the 20th Annual ACM Symposium on Theory of Computing (STOC)*, pages 113–131, 1988.

[12] C. H. Bennett, I. Devetak, A. W. Harrow, P. W. Shor, and A. Winter. The quantum reverse Shannon theorem and resource tradeoffs for simulating quantum channels. *IEEE Trans. Inf. Theory*, 60(5):2926–2959, May 2014.

[13] R. Bhatia. *Matrix Analysis*. Number 169 in Graduate Texts in Mathematics. Springer-Verlag, New York, 1997.

[14] Fernando GSL Brandao, Ravishankar Ramanathan, Andrzej Grudka, Karol Horodecki, Michal Horodecki, and Pawel Horodecki. Robust device-independent randomness amplification with few devices. *arXiv preprint arXiv:1310.4544*, 2013.

[15] R. Chao, B. W. Reichardt, C. Sutherland, and T. Vidick. Overlapping qubits. Manuscript in preparation, 2016.

[16] Kai-Min Chung, Yaoyun Shi, and Xiaodi Wu. Physical randomness extractors. arXiv:1402.4797, 2014.

[17] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23:880–884, Oct 1969.

[18] 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, 1969.

[19] Richard Cleve, Peter Høyer, Ben Toner, and John Watrous. Consequences and limits of nonlocal strategies. In *Proc. 19th IEEE Conf. on Computational Complexity (CCC'04)*, pages 236–249. IEEE Computer Society, 2004.

[20] Andrea W. Coladangelo. Parallel self-testing of (tilted) EPR pairs via copies of (tilted) CHSH. Technical report, arXiv:1609.03687, 2016.

[21] Roger Colbeck. Quantum and relativistic protocols for secure multi-party computation. *arXiv preprint arXiv:0911.3814*, (December), 2009.

[22] Roger Colbeck and Adrian Kent. Private randomness expansion with untrusted devices. *Journal of Physics A: Mathematical and ...*, pages 1–11, 2011.

[23] A. Connes. Classification of injective factors cases ii_1, ii_∞, iii_λ, $\lambda \neq 1$. *Annals of Mathematics*, 104(1):pp. 73–115, 1976.

[24] Matthew Coudron and Anand Natarajan. The parallel-repeated magic square game is rigid. Technical report, https://arxiv.org/abs/1609.06306, 2016.

[25] Matthew Coudron and Thomas Vidick. Interactive proofs with approximately commuting provers.

[26] Matthew Coudron, Thomas Vidick, and Henry Yuen. Robust randomness amplifiers: Upper and lower bounds. In Raghavendra et al. [80], pages 468–483.

[27] Matthew Coudron, Thomas Vidick, and Henry Yuen. Robust Randomness Amplifiers: Upper and Lower Bounds. *arXiv preprint arXiv:1305.6626*, (0844626):1–28, 2013.

[28] Matthew Coudron, Thomas Vidick, and Henry Yuen. Robust randomness amplifiers: Upper and lower bounds. In Raghavendra et al. [80], pages 468–483.

[29] Matthew Coudron and Henry Yuen. Infinite randomness expansion with a constant number of devices. In *Proceedings of the 46th Annual ACM Symposium on Theory of Computing (STOC '14)*, pages 427–436,, 2014.

[30] Anindya De, Christopher Portmann, Thomas Vidick, and Renato Renner. Trevisan's extractor in the presence of quantum side information. *SIAM Journal on Computing*, 41(4):915–940, 2012.

[31] Andrew C. Doherty, Yeong-Cherng Liang, Benjamin Toner, and Stephanie Wehner. The quantum moment problem and bounds on entangled multi-prover games. In *Proc. 23rd IEEE Conf. on Computational Complexity (CCC'08)*, pages 199–210, 2008.

[32] Albert Einstein, Boris Podolsky, and Nathan Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 47:777–780, 1935.

[33] Ruy Exel and Terry Loring. Almost commuting unitary matrices. *Proceedings of the American Mathematical Society*, 106(4):913–915, 1989.

[34] Serge Fehr, R Gelles, and C Schaffner. Security and composability of randomness expansion from Bell inequalities. *Physical Review A*, pages 1–12, 2013.

[35] 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.

[36] Rodrigo Gallego López et al. Device-independent information protocols: measuring dimensionality, randomness and nonlocality. 2013.

[37] Esther Hänggi, Renato Renner, and Stefan Wolf. Efficient device-independent quantum key distribution. In *Advances in Cryptology–EUROCRYPT 2010*, pages 216–234. Springer, 2010.

[38] A. W. Harrow and D. W. Leung. A communication-efficient nonlocal measurement with application to communication complexity and bipartite gate capacities. *IEEE Trans. Inf. Theory*, 57(8):5504–5508, 2011.

[39] B. Hensen et al. Experimental loophole-free violation of a bell inequality using entangled electron spins separated by 1.3 km. *Nature (London) 526, 682*, (2015).

[40] Thomas Holenstein. Parallel repetition: simplifications and the no-signaling case. In *Proceedings of the thirty-ninth annual ACM symposium on Theory of computing*, pages 411–419. ACM, 2007.

[41] Tsuyoshi Ito, Hirotada Kobayashi, and Keiji Matsumoto. Oracularization and two-prover one-round interactive proofs against nonlocal strategies. In *Proc. 24th IEEE Conf. on Computational Complexity (CCC'09)*, pages 217–228. IEEE Computer Society, 2009.

[42] Tsuyoshi Ito and Thomas Vidick. A multi-prover interactive proof for NEXP sound against entangled provers. *Proc. 53rd FOCS*, pages 243–252, 2012.

[43] Tsuyoshi Ito and Thomas Vidick. A multi-prover interactive proof for NEXP sound against entangled provers. Technical report, arXiv:1207.0550, 2012.

[44] Rahul Jain, Jaikumar Radhakrishnan, and Pranab Sen. Optimal direct sum and privacy trade-off results for quantum and classical communication complexity, 2008.

[45] Zhengfeng Ji. Classical verification of quantum proofs. Technical report, arXiv:1505.07432, 2015.

[46] M. Junge and C. Palazuelos. Large violation of bell inequalities with low entanglement. *Communications in Mathematical Physics*, 306(3):695–746, 2011.

[47] Marius Junge, Miguel Navascues, Carlos Palazuelos, David Perez-Garcia, Volkher B. Scholz, and Reinhard F. Werner. Connes' embedding problem and tsirelson's problem. *J. Math. Physics*, 52(1):–, 2011.

[48] Julia Kempe, Oded Regev, and Ben Toner. Unique games with entangled provers are easy. *SIAM J. Comput.*, 39(7):3207–3229, 2010.

[49] Eberhard Kirchberg. On non-semisplit extensions, tensor products and exactness of group C^*-algebras. *Inventiones mathematicae*, 112(1):449–489, 1993.

[50] Hirotada Kobayashi and Keiji Matsumoto. Quantum multi-prover interactive proof systems with limited prior entanglement. *Journal of Computer and System Sciences*, 66(3):429–450, 2003.

[51] Robert König, Renato Renner, Andor Bariska, and Ueli Maurer. Small accessible quantum information does not imply security. *Physical Review Letters*, 98(14):140502, 2007.

[52] RT Konig and Barbara M Terhal. The bounded-storage model in the presence of a quantum adversary. *Information Theory, IEEE Transactions on*, 54(2):749–762, 2008.

[53] Monique Laurent. A comparison of the Sherali-Adams, Lovász-Schrijver, and Lasserre relaxations for 0-1 Programming. *Mathematics of Operations Research*, 28(3):470–496, 2003.

[54] Debbie Leung, Ben Toner, and John Watrous. Coherent state exchange in multi-prover quantum interactive proof systems. *Chicago Journal of Theoretical Computer Science*, 11:1–18, 2013.

[55] Hong-Wei Li, Marcin Pawłowski, Zhen-Qiang Yin, Guang-Can Guo, and Zheng-Fu Han. Semi-device-independent randomness certification using n? 1 quantum random access codes. *Physical Review A*, 85(5):052308, 2012.

[56] Hong-Wei Li, Zhen-Qiang Yin, Yu-Chun Wu, Xu-Bo Zou, Shuang Wang, Wei Chen, Guang-Can Guo, and Zheng-Fu Han. Semi-device-independent random-number expansion without entanglement. *Physical Review A*, 84(3):034301, 2011.

[57] Ll. Masanes. Extremal quantum correlations for n parties with two dichotomic observables per site. Technical report, arXiv:quant-ph/0512100, 2005.

[58] Lluís Masanes, Stefano Pironio, and Antonio Acín. Secure device-independent quantum key distribution with causally independent measurement devices. *Nature communications*, 2:238, 2011.

[59] 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.

[60] Dominic Mayers and Andrew Yao. Self testing quantum apparatus. *arXiv preprint quant-ph/0307205*, 2003.

[61] 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.

[62] 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.

[63] Matthew McKague. Self-testing graph states. Technical report, arXiv:1010.1989, 2010.

[64] Matthew McKague. Self-testing in parallel. Technical report, arXiv:1511.04194, 2015.

[65] Matthew McKague. Interactive proofs for BQP via self-tested graph states. *Theory of Computing*, 12(3):1–42, 2016.

[66] Matthew McKague. Self-testing high dimensional states using the generalized magic square game. Technical report, arXiv:1605.09435, 2016.

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

[68] Carl A. Miller and Yaoyun Shi. Optimal robust quantum self-testing by binary nonlocal XOR games. arXiv:1207.1819, v4, 2013.

[69] Carl A. Miller and Yaoyun Shi. Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices. In *Proc. 46th STOC*, New York, NY, USA, 2014. ACM.

[70] Anand Natarajan and Thomas Vidick. Constant-soundness interactive proofs for local hamiltonians. Technical report, arXiv:1512.02090, 2015.

[71] Miguel Navascués, Stefano Pironio, and Antonio Acín. Bounding the set of quantum correlations. *Phys. Rev. Lett.*, 98:010401, Jan 2007.

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

[73] Miguel Navascués, Stefano Pironio, and Antonio Acín. A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. Technical report, arXiv:0803.4290v1 [quant-ph], 2008.

[74] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010.

[75] Narutaka Ozawa. Tsirelson's problem and asymptotically commuting unitary matrices. *Journal of Mathematical Physics*, 54(3):–, 2013.

[76] Károly F. Pál and Tamás Vértesi. Maximal violation of a bipartite three-setting, two-outcome Bell inequality using infinite-dimensional quantum systems. *Phys. Rev. A*, 82:022116, Aug 2010.

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

[78] S Pironio, A Acín, and S Massar. Random numbers certified by Bell's theorem. *Nature*, pages 1–26, 2010.

[79] Stefano Pironio and Serge Massar. Security of practical private randomness generation. *Physical Review A*, 87(1):012336, 2013.

[80] Prasad Raghavendra, Sofya Raskhodnikova, Klaus Jansen, and José D. P. Rolim, editors. *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques - 16th International Workshop, APPROX 2013, and 17th International Workshop, RANDOM 2013, Berkeley, CA, USA, August 21-23, 2013. Proceedings*, volume 8096 of *Lecture Notes in Computer Science*. Springer, 2013.

[81] Oded Regev. Bell violations through independent bases games. *Quantum Info. Comput.*, 12(1-2):9–20, January 2012.

[82] 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.

[83] 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.

[84] BW Reichardt, F Unger, and U Vazirani. A classical leash for a quantum system: Command of quantum systems via rigidity of CHSH games. *arXiv preprint arXiv:1209.0448*, 2012.

[85] Renato Renner. Security of quantum key distribution. *International Journal of Quantum Information*, 6(01):1–127, 2008.

[86] Volkher B. Scholz and Reinhard F. Werner. Tsirelson's problem. Technical report, arXiv:0812.4305v1 [math-ph], 2008.

[87] Lana Sheridan, Valerio Scarani, et al. Bell tests with min-entropy sources. *Physical Review A*, 87(6):062121, 2013.

[88] O Nieto Silleras, S Pironio, and J Silman. Using complete measurement statistic for optimal device-independent randomness evaluation. *arXiv preprint arXiv:1309.3930*, 2013.

[89] J. Silman, S. Pironio, and S. Massar. Device-independent randomness generation in the presence of weak cross-talk. *Phys. Rev. Lett.*, 110:100504, Mar 2013.

[90] Jonathan Silman, Stefano Pironio, and Serge Massar. Device-independent randomness generation in the presence of weak cross-talk. *Physical review letters*, 110(10):100504, 2013.

[91] Boris S. Tsirelson. Quantum generalizations of Bell's inequality. *Letters in Mathematical Physics*, 4(2):93–100, 1980.

[92] Mark Um, Xiang Zhang, Junhua Zhang, Ye Wang, Shen Yangchao, D-L Deng, Lu-Ming Duan, and Kihwan Kim. Experimental certification of random numbers via quantum contextuality. *Scientific reports*, 3, 2013.

[93] Umesh Vazirani and Thomas Vidick. Certifiable quantum dice. *Phil. Trans. R. Soc. A*, 2012.

[94] Umesh Vazirani and Thomas Vidick. Fully device independent quantum key distribution. *arXiv preprint arXiv:1210.1810*, 2012.

[95] Thomas Vidick. Three-player entangled XOR games are NP-hard to approximate. In *Proc. 54th FOCS*, 2013.

[96] Thomas Vidick and Stephanie Wehner. More nonlocality with less entanglement. *Phys. Rev. A*, 83:052310, May 2011.

[97] D. Voiculescu. Asymptotically commuting finite rank unitary operators without commuting approximants. *Acta Sci. Math. (Szeged)*, 45:429–431, 1983.

[98] Mark M Wilde. *Quantum Information Theory*. Cambridge University Press, 2013.

[99] 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.

[100] Tzyh Haur Yang, Tamas Vertesi, Jean-Daniel Bancal, Valerio Scarani, and Miguel Navascues. Robust and Versatile Black-Box Certification of Quantum Devices. *Phys. Rev. Lett.*, 113(4), JUL 22 2014.

[101] Henry Yuen. Quantum randomness expansion: Upper and lower bounds. *MIT Department of Electrical Engineering and Computer Science, Master's Thesis*, 2013.