Games, Protocols, and Quantum Entanglement

by

Henry Yuen

B.A., University of Southern California (2010)
S.M., Massachusetts Institute of Technology (2013)

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

Doctor of Philosophy

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

September 2016

Signature redacted

Author ....
Department of Electrical Engineering and Computer Science
August 24, 2016

Signature redacted

Certified by. ....
Dana Moshkovitz
Assistant Professor
Thesis Supervisor

Signature redacted

Accepted by..... ....
Leslie A. Kolodziejski
Chair, Department Committee on Graduate Students

Games, Protocols, and Quantum Entanglement

by
Henry Yuen

Submitted to the Department of Electrical Engineering and Computer Science
on August 24, 2016, in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy

Abstract

Quantum entanglement has evolved from being "spooky action at a distance" to being a fundamental information-theoretic resource, extending the frontiers of what is possible in communications, computation, and cryptography. It gives rise to non-local correlations that can be harnessed to perform tasks such as certified randomness generation and classical verification of quantum computation. However, these same non-local correlations also pose a challenge when analyzing complexity-theoretic or cryptographic protocols in a quantum world: the soundness or security of the protocol may no longer hold in the presence of entangled adversaries. This thesis presents several results involving games and protocols with entangled parties; in each result, we introduce new techniques and methods to analyze soundness against adversaries that can manipulate quantum entanglement.

First, we present a protocol wherein a classical verifer interacts with eight non-communicating quantum devices, and for all integer N the verifier can statistically certify that the devices have produced N bits of randomness that is ε-close to uniform, while only using $O(\log^3 \frac{1}{\varepsilon})$ bits of seed randomness. We call this an *infinite randomness expansion* protocol, because the amount N of certified output randomness is independent of the verifier's seed length. Entanglement is both a blessing and a curse for this protocol: on one hand, the devices need entanglement in order to successfully generate randomness to pass the protocol. But on the other hand, the devices may try to use entanglement to cheat and pass the protocol without producing additional randomness. We show that the monogamous nature of entanglement prevents this from happening.

Next, this thesis studies the parallel repetition of games with entangled players. Raz's classical parallel repetition theorem (SICOMP 1998) is an influential result in complexity theory showing that the maximum success probability of *unentangled* players in a two-player game must decrease exponentially when the game is repeated in parallel. Its proof is highly non-trivial, and a major open question is whether it extends to the case of entangled players.

We make progress on this question in several ways. First, we present an efficient transformation on games called "anchoring" that converts any k-player game G into a k-player game $G_\perp$ such that the entangled value of its n-fold parallel repetition, $G_\perp^n$, is exponentially small in n (provided that the entangled value of G is less than 1). Furthermore, the transformation is *completeness preserving*, in that if the entangled value of G is 1, then the entangled value of $G_\perp^n$ is also 1. This yields the first gap amplification procedure for general entangled games that achieves exponential decay.

We also show that parallel repetition of a game causes the entangled value to decrease at a polynomial rate with the number of repetitions. In particular, this gives the first proof that the entangled value of a parallel repeated game converges to 0 for *all* games who entangled value is less than 1.

The third result of this thesis on entangled parallel repetition is an improved analysis of the parallel repetition of *free* games with entangled players. Free games are those where the players' questions are independent of each other. We show how to use the fact that the DISJOINTNESS problem of size N can be solved with $O(\sqrt{N})$ qubits of quantum communication in order to *speed up* the rate of decay for the parallel repetition: given a free game G with entangled value $1 - \varepsilon$, its n-fold parallel repetition G^n has entangled value at most $(1 - \varepsilon^{3/2})^{\Omega(n/s)}$, where s is the length of the players' answers in G. In contrast, the best parallel repetition theorem for free games with unentangled players, due to Barak, et al. (RANDOM 2009), shows that for a free game G with entangled value $1 - \delta$, the classical value of G^n is at most $(1 - \varepsilon^2)^{\Omega(n/s)}$, which is a slower rate of decay. This suggests a separation between the behavior of entangled games and unentangled games under parallel repetition.

In the final part of this thesis, we examine message authentication in a quantum world. Message authentication is a fundamental task in cryptography that ensures data integrity when communicating over an insecure channel. We consider two settings. One is *classical* authentication against quantum attacks. The other is *total quantum* authentication of quantum data.

We give a new class of security definitions for both modes of message authentication. Our definitions capture and strengthen several existing definitions, including that of Boneh-Zhandry (EUROCRYPT 2013), which pertains to superposition attacks on classical authentication schemes, as well as the definition of Barnum, et al. (FOCS 2002), which addresses total authentication of quantum data. Our definitions give strong characterizations for what a quantum adversary is able to do in a message authentication protocol, even when the adversary has quantum side information that is entangled with the message state. We argue that, in the "one time" setting, our definitions are the strongest possible.

We prove that our security definition for total quantum authentication has some surprising implications, such as the ability to reuse the key whenever verification is successful, and a conceptually simple quantum key distribution protocol. We then give several constructions of protocols that satisfy our security definitions: (1) we show that the classical Wegman-Carter scheme with 3-universal hashing is secure against quantum adversaries with quantum side information; (2) we present a protocol based on unitary designs that achieves total quantum authentication, and (3) we show that using the classical Wegman-Carter scheme to authenticate in complementary bases yields a form of total quantum authentication, with bounded key leakage.

Thesis Supervisor: Dana Moshkovitz
Title: Assistant Professor

Acknowledgments

On the surface, the theorems in this thesis appear to be merely a collection of symbols that (hopefully) form true sentences in Zermelo-Fraenkel set theory. That would be completely missing a critical dimension, however: behind each theorem is a rich, complicated, and wonderful story whose most important component is not mathematics, but *people*. Theorems frequently come from spirited effort with collaborators. Just as often, though, they are a product of inspiring interactions – both mathematical and non-mathematical – with mentors, teachers, colleagues, friends, and family. So while the mathematical part of this thesis outweighs the acknowledgments section many times over in terms of page count, no number of pages (and certainly not the next few paragraphs) can properly capture the importance of the people who have shaped the course of my grad school years.

First, deep thanks goes to my adviser Dana Moshkovitz. I am grateful for her support and faith in me as I tried to forge my own research path. She gave me a lot of freedom to explore my own interests, but by no means was Dana an aloof adviser. Her door was always open, and was always willing to chat about anything: research, academia, or life. I greatly appreciate all the encouragement and guidance she has given over the years, as well as the numerous explanations of the intricacies of PCP, derandomized parallel repetition, and games that left me simultaneously bewildered and in awe. It makes me happy that I can count Dana as a colleague and friend, in addition to having her as a wonderful mentor.

Next, I have had many wonderful opportunities to visit various people at institutions around the world. Each visit led to rewarding experiences, both research-wise and otherwise. Thanks go to Aram Harrow and Anup Rao (visit to the University of Washington, summer 2012 and summer 2015), the Simons Institute at Berkeley (spring 2014), Ronald de Wolf (visits to CWI in Amsterdam, summer 2014 and summer 2015), Mark Braverman (Princeton, spring 2015), Thomas Vidick (CalTech, summer 2015 and Stellenbosch Institute of Advanced Study in South Africa, fall 2015), Troy Lee (two workshops at NUS in Singapore, January 2016), Irit Dinur (Weizmann Institute of Science, February 2016), and Cedric Lin (QuICS, Maryland, summer 2016).[1] In particular, it was at Princeton and Singapore, respectively, that the results on anchoring parallel repetition and polynomial decay parallel repetition in this thesis were worked out.

I've had the privilege of working with many brilliant and talented collaborators: Mohammad Bavarian, Kai-Min Chung, Matt Coudron, Sumegha Garg, Ioana Ivan, Troy Lee, Michael Mitzenmacher, Dana Moshkovitz, Govind Ramnarayan, Anupam Prakash, Justin Thaler, Thomas Vidick, Ronald de Wolf, Xiaodi Wu, and Mark Zhandry. Thanks to everyone for making being in theoretical computer science a fun and exciting enterprise.

One of the best things about being a part of the MIT theory group is the convivial atmosphere and the extreme friendliness of the inhabitants of G5 and G6. In addition to the usual academic events – seminars, lectures, talks, and so on – there were many other non-academic events that made being a part of MIT theory so joyful: theory retreats, theory jams (Needs More Cowbell™), NotSoGITCS, theory lunches, theory tea – the list goes on. I will miss the camaraderie and the liveliness of MIT theory.

I have to give thanks to the other branch of the superposition, which is the MIT quantum group. It's been a blast to do learn and do quantum at MIT. Thanks go to Scott Aaron-

[1] Despite all these miles flown, I *still* don't have Silver status with any airline! This goes to show you how pointless airline loyalty is.

son for his inspiring – and entertaining – teaching of quantum complexity theory; to the Friday group meeting which always has wonderful nuggets of gossip and news about quant-ph and beyond; the postdocs and students, too many to list, from whom I've learned much. I especially have to think Scott Aaronson and Aram Harrow for their scientific guidance and mentorship, and of course graciously serving on my thesis committee.

Special acknowledgments go to the wonderful cohort of grad students who started in 2011: Mohammad Bavarian, Adam Bouland, Matt Coudron, Alan Guo, Ioana Ivan, Sepideh Mahabadi, Ludwig Schmidt, Aaron Sidford, Christos Tzamos, Madars Virza, Adrian Vladu. I've learned much from you all, and I'm glad to have "grown up" through grad school with this exceptional group of people.

I thank Govind Ramnarayan for helping me file this thesis; I owe him a few beers for this favor.

I'm grateful for my USC friends in the Boston area: Candice Yip, Karan Gill, Tanay Mehta. During some of the long and dreary Boston winters, it was helpful to reminisce about California sunshine together.

Grad school came with some epic non-academic travel, and I'm fortunate to have had amazing company during these trips. I have to thank Matt Coudron for being so game for so many crazy adventures: getting lost in rural China, windsurfing in Thailand, biking in the Spanish countryside, encountering the Italian Mafia in Rome[2], scuba diving in Puerto Rico, the roadtrip in the Pacific Northwest. I thank Candice Yip for suggesting that we hike the Tour de Mont Blanc trail during the summer of 2014. Those 8 days in the Alps and 4 days in Istanbul were incredible. Next, I'm thankful to Evan Snyder to being a great roadtrip buddy as we drove from California to Yosemite, Glacier National Park, Coeur d'Alene, and Crater Lake. Thanks go to Karan Gill for organizing the aforementioned roadtrip. I'll always look back very fondly and very wistfully on all the stories and memories from these times.

I have to thank Joseph Bebel for his friendship and great company. I've known him for nearly a decade now, and he had a large role in introducing me to all this theoretical computer science stuff. I remember how incredulous I was when, over GChat, Joe claimed that it was possible to determine the correctness of a mathematical proof by only examining 3 random symbols. This was my sophomore year at USC. In the years since then, I've had many inspiring conversations and learning experiences with Joe.

Joe also introduced me to the Mathemagicians, as Len Adleman's research group was known. The three years that I spent working with Len and the Mathemagicians greatly influenced my development as a budding mathematician and scientist. I was heavily inspired by Len's clarity of thought, commitment to rigor, creativity, sense of adventure, and maverick streak, and even today I find myself trying to emulate his style. I learned a lot of mathematics from Len, but more importantly I learned how important it is to have courage to pursue the right questions. The rest of the Mathemagicians were great compatriots: Joe Bebel, Dustin Reishus, Urmila Mahadev, Rolfe Schmidt, and Tanay Mehta.

I also have to thank Pierre de Vries and Aiichiro Nakano, who supervised my first research experiences in undergrad. With Pierre I got a taste of social science research, and with Aiichiro I learned a lot about computational physics. I am grateful that both advisers treated me as an equal. Doing so is probably one of the best things a mentor can do for a young mentee.

Now, for some acknowledgments on the personal end of the spectrum. Easily, my

[2] That's the explanation we came up with, anyways.

best discovery in graduate school is Corinna Li, who I happily call my fiancé now. Thank you, Corinna, for making life in the last year and a half deliciously sweet, and especially for keeping me grounded through the trials and frustrations that come with research and academia. I am so excited for the life we are going to share together.

I have to thank my younger brother, Alan Yuen, for putting up with my antics over the years. I'm grateful for your company, and grateful for the special bond we share. It is stronger than ever now, and I expect it to only get stronger with time. I am very, very proud of you.

Finally, I dedicate this thesis to my parents, King Yuen and Thai Yuen. I cannot even come close to fully expressing how thankful I am for the depths of their unconditional love, patience and support that they have shown me my entire life. They've always put my and Alan's well being ahead of theirs, and I'll never be able to imagine the amount of blood and sweat they've literally put into ensuring that we'll both have better lives than they.

A little bit about my parents, because their story deserves to be told. Both hail from a modest village in Cambodia, and lived through a perilous period of history: my dad and his family gave up everything they had in order to flee Pol Pot's regime; my mom and her family weren't so lucky and endured several years of labor camps. It's something out of a movie. Despite all that, they were able to make it to the United States of America, where through hard work and luck, they were able to carve out a hard-earned life for themselves and for my brother and I. It hasn't always been easy, and they still continue to work far harder than they should have to, but I think they really embody the American Dream. They are, and will continue to be, my heroes.

For my parents.

Contents

Chapter 1

Introduction

The story of quantum entanglement begins as a troubling conundrum about the interpretation of quantum mechanics. The famous 1935 paper of Einstein, Podolsky and Rosen [40] (known as EPR) considered a thought experiment involving quantumly entangled particles separated by interstellar distances, leading to what EPR considered an untenable description of reality. How could the act of measuring one particle instantaneously affect the state of another particle lightyears away? It must be because the quantum mechanical picture of reality, EPR concluded, was incomplete. For nearly thirty years afterwards, however, most physicists were content with ignoring thorny issues of interpretation, so long as quantum physics continued to produce its fantastically accurate predictions.

When John Bell published his monumental 1964 paper "On the Einstein-Podolsky-Rosen paradox" however, quantum entanglement was suddenly elevated from harmless philosophical nuisance to empirical, falsifiable science [14]. In it, he showed that the predictions of quantum theory were inconsistent with "hidden variable" models of physics, which are theories based on the classical principles advocated by EPR. He presented a simple experiment – involving entangled particles – where if the outcomes were consistent with quantum theory, then local hidden variable theories would be ruled out. In one move, Bell's theorem (as his result is known) made the foggy problem of interpretation suddenly very concrete and very real – it was *testable.*

We can distill his experiment into a simple form, in terms of a game. The game consists of three parties: Alice, Bob, and a referee. Before the start of the game, Alice and Bob can perform any amount of collusion. Once the game begins, however, Alice and Bob are not allowed to communicate, and the referee does the following: it picks two bits x, y uniformly and independently at random, and sends x to Alice and y to Bob. The instant that Alice and Bob receive their respective bits, they must perform some physical process as fast as they can in order to produce bits of their own: Alice generates a, Bob generates b, and both bits are sent to the referee. Their strategy for generating answer bits must be quick so they don't have time to signal to each other. The referee then compares whether the parity of their answers (i.e., $a \oplus b$) is equal to the logical AND of their questions (i.e., $x \wedge y$). If so, then Alice and Bob win the game – otherwise they lose. This game is known as the *CHSH game,* named after its inventors Clauser, Horne, Shimony, and Holt [28].

What is the maximum winning probability of Alice and Bob? In a world governed by the classical principles posited by EPR, the answers of Alice and Bob would be generated by hidden variables (called "elements of reality" by EPR). In this model, we can imagine that Alice and Bob's strategy to play this game is as follows: in the collusion phase, Alice and Bob flip a series of coins and each copy down the outcomes. During the game, Alice generates her answer a solely as a deterministic function of the random coin flips from the collusion phase and her question x. Bob does the same thing. It is an easy exercise to see that with such a strategy, the maximum winning probability of Alice and Bob is 75%. Even if Alice and Bob used common randomness (by flipping coins before the game, and using the outcomes of the coins during the game to coordinate their answers), their maximum success probability is still bounded by 75%.[1]

However, quantum mechanical Alice and Bob can do significantly better. Before the game, Alice and Bob generate two entangled particles in the state $|\psi\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$, fittingly known as an EPR pair. Alice takes one particle for herself and Bob takes the other. During the game, Alice and Bob perform measurements on their share of the EPR pair, and they report the measurement outcomes as their answers. By choosing the measurements carefully, Alice and Bob can win this game with probability approximately 85.36%! This also gives another way to formulate Bell's theorem: using quantum resources, Alice and Bob can win the CHSH game more often than if they were governed by hidden variables.

This immediately suggests an experiment: play the CHSH game many times, and check how many times Alice and Bob win. *Any* success rate noticeably greater than 75% would imply that the behavior of Alice and Bob – and hence the laws of physics – is non-classical. Here, "Alice", "Bob", and the "referee" are personifications of measurement apparatuses and a random number generator that a skilled experimenter could set up in a laboratory. Assuming that (a) all the laboratory equipment is ideal, (b) the components corresponding to Alice and Bob are separated far enough to prevent communication, and (c) the experiment is repeatable, then the empirically observed win rate will give a reliable criterion to reject the hidden variable model of physics.

Since 1964, countless implementations of Bell tests (as his experiments and variations of it are called) have been conducted, each time reaffirming the quantum nature of reality. While ideal experimental conditions cannot be achieved exactly, each experiment has come closer in closing all the so-called Bell test "loopholes". These are caveats that prevent one from incontrovertibly concluding that nature is behaving non-classically: Alice and Bob could be too close to each other, and thus in principle they could signal to each other during the game; measurement devices could be imperfect, and thus the runs of the game in which the devices *did* work could artificially inflate the success percentage of Alice and Bob. However, the long history of performing Bell tests recently culminated in a historic milestone: in 2015, the Hanson group of the Netherlands reported the first *loophole-free* Bell test [54]. Eighty years after the EPR paper, we can finally put the classical vision of nature to rest.

1.1 Beyond Bell

Since EPR and Bell, quantum entanglement has grown from a philosophical peculiarity to a fundamental physical phenomenon. We now know that entanglement manifests itself in exotic materials [99], black hole physics [4], and even plant photosynthesis [92]. As quantum information processing – and one day, quantum computing – becomes widespread, we will need precise and exquisite control of complex quantum systems, including the manipulation of entanglement.

[1] This is by averaging: for any strategy involving shared randomness, one can obtain a deterministic strategy that achieves the same success probability by simply fixing the best randomness used by the players.

Quantum entanglement can be regarded as a *resource,* just like time, energy, and space. We've seen how entanglement is useful for games like the CHSH game: it allows Alice and Bob to win the game with higher probability than if they didn't have entanglement. In quantum protocols such as device-independent quantum key distribution, or delegated quantum computation, the use of entanglement is necessary in order for the protocols to work at all. However, entanglement is not always "good"; it can also be a harmful resource used by an adversary to break the security of a cryptographic protocol or the soundness of a proof system.

This thesis focuses òn *constraining* quantum entanglement in games and protocols. Specifically, I will focus on the behavior of quantum entanglement in *infinite randomness expansion protocols* the *parallel repetition of games,* and *classical and quantum message authentication in the presence of entangled adversaries.* In each of these topics, the central problem is that of characterizing the power of an *entangled adversary* who is trying to disrupt the desired functionality of the game or protocol. The main contribution of this thesis are techniques for characterizing and mitigating such adversarial entanglement.

1.2 Infinite randomness expansion with untrusted quantum devices

The first part of this thesis studies how quantum entanglement enables *classical* testing of *quantum* randomness generation.

The fact that Bell's theorem gives an operational method to distinguish between (local) hidden variable models of reality and quantum theory is only the beginning. One of the most startling implications of Bell's theorem, discovered only ten years ago, is that it also gives an operational method for *testing quantum randomness generation.*

Recall the CHSH game. Suppose that Alice and Bob employ a deterministic strategy to play the game. That is, Alice's answer a is a deterministic function of her question x, and Bob's answer b is another deterministic function of his question y. Since this is a hidden variable theory, Alice and Bob's maximum winning probability is 75%, over the choice of questions chosen by the referee. If we take this in the contrapositive, then if we we observe that Alice and Bob were employing a strategy that allowed them to win more than 75% of the time, we must conclude that their outputs a and b must contain some entropy!

It is imperative to emphasize that, while randomness generation is *necessary* to win the CHSH game with better than 75% probability, it is *not* a sufficient condition: as mentioned earlier, if Alice and Bob only employed shared randomness in their strategies, they would not be able to beat the 75% bound. Thus, one should think of the CHSH game as a test for *non-classicality,* which implies randomness generation.

This simple but powerful observation initiated the study of *device-independent randomness expansion.* Here, we can test that an untrusted device (consisting of multiple components that cannot communicate with each other) produces randomness by having it play multiple rounds of the CHSH game. Astoundingly, the amount of initial seed randomness required to run such tests can be much less than the amount of output randomness – hence we have *expanded* the amount of randomness that we started with. Note that, while randomness expansion protocols sound similar to pseudorandom generators, there is nothing "pseudo" about the output: a randomness expansion protocol guarantees that, so long as the device passes the protocol with some minimum probability, the output will contain much more information-theoretic entropy than was contained in the seed!

Without this simple non-communication assumption on the devices, it is easy to see that such black-box randomness testing is impossible. The term "device-independence" means that, other than this, we make no additional assumption on the internal structure of the device. In particular, it could've been manufactured by an adversary.

The first randomness expansion protocol was demonstrated by Roger Colbeck in his Ph.D. thesis in 2006 [31], which expanded m bits of seed randomness to cm bits of close-to-uniform randomness, for some constant $c > 1$. This was followed up by *quadratic* randomness expansion: m bits expanded to $\Theta(m^2)$ bits [84]. Then, two works (one by Vazirani and Vidick [96], and the other by Fehr, et al. [42]) simultaneously demonstrated protocols attaining *exponential* randomness expansion: successfully passing the protocols certifies that the outputs have $2^{\Omega(m)}$ bits of entropy, while only starting with m initial seed bits.

The obvious open question is, "Can we do better?" Are there any fundamental limits to how much randomness expansion one could achieve? In joint work with Matthew Coudron and Thomas Vidick, we showed that a natural class of *non-adaptive* randomness expansion protocols could not achieve unbounded expansion [32]; in fact, doubly-exponential expansion ($m \to 2^{2^{O(m)}}$) is the limit. Here, "non-adaptive" means that the inputs given to the devices only depend on the initial seed, and not on their outputs. This limitation applied to nearly every randomness expansion protocol in the literature at the time. Still, the tantalizing question remainded: could we circumvent this doubly-exponential barrier by designing adaptive randomness expansion protocols?

In joint work with Matthew Coudron, we demonstrated the existence of an adaptive protocol that involves eight non-communicating devices, and starting with m bits of seed randomness, produces a string of length N that is guaranteed to be $\exp(-\text{poly}(m))$-close to uniform in statistical distance [33]. Here, N can be arbitrarily large – to produce a larger random string, you simply run the protocol for more iterations. This settled the "infinite randomness expansion" conjecture.

At the heart of the analysis of our infinite randomness expansion protocol is the construction of a non-adaptive randomness expansion protocol with an especially strong security guarantee about its output: if the protocol succeeds, then the output randomness is unentangled (and hence private) from any external adversary, *even* if the adversary was originally entangled with the devices used in the protocol, *and* also generated the seed used by the classical user of the protocol! Given a randomness expansion protocol with such guarantees, then one can safely combine two instances of these protocols in order to adaptively generate an unbounded amount of private and secure randomness, by treating each instance as the supplier of ever-growing amounts of seed randomness for the other instance.

1.3 Parallel repetition of games in the presence of entanglement

The second part of the thesis studies the parallel repetition of games involving entangled players.

Classical parallel repetition. The parallel repetition theorem is an important tool in classical complexity theory and cryptography for amplifying the hardness of two-player games. We have already seen one example of a two-player game, the CHSH game. More generally, a two-player game G is played as follows: a referee samples a pair of questions (x, y)

from some distribution μ, sends x to the first player (who we call Alice) and y to the second player (who we call Bob). Alice and Bob cannot communicate during the game. Alice responds with an answer a, Bob responds with an answer b, and the referee checks if $V(x,y,a,b) = 1$ for some predicate V. If so, then the players win G.

When the players are *classical* (that is, their answers are a deterministic function of their questions), we call the maximum success probability of the players in the game G as the *classical value* of G, denoted by $\mathrm{val}(G)$. One of the most important results in classical complexity theory is Raz's parallel repetition theorem [88], which states the following:

Theorem 1 (Raz's parallel repetition theorem). *Let G be a two-player game with classical value* $\mathrm{val}(G) = 1 - \varepsilon$. *Then*

$$\mathrm{val}(G^n) \leq (1 - \varepsilon^3)^{\Omega(n)}$$

where the constant in the $\Omega(\cdot)$ depends on the game G.

Here, G^n denotes a two-player game called the *n-fold parallel repetition of G*, denoted by G^n. In this game, the referee plays n independent instances of G in parallel with two players: the referee samples n independent question pairs $(x_1, y_1), \ldots, (x_n, y_n)$ from μ, and sends $(x_1, \ldots, x_n)$ to Alice, and $(y_1, \ldots, y_n)$ to Bob. Alice responds with $(a_1, \ldots, a_n)$, and Bob with $(b_1, \ldots, b_n)$. They win the game G^n only if $V(x_i, y_i, a_i, b_i) = 1$ for all $i = 1, \ldots, n$. Theorem 1 shows that if $\mathrm{val}(G) < 1$, then the players' success probability in the repeated game G^n is exponentially small in n. Though the statement is intuitive, the proof of Theorem 1 is nontrivial, and requires clever information-theoretic arguments.

The main application of Raz's parallel repetition theorem is to the areas of *hardness of approximation* and *probabilistically checkable proofs*. The famous *PCP Theorem* [6] can be formulated in terms of two-player games: it is NP-hard to approximate the (classical) value of a game G within an additive error of, say, 0.001. The parallel repetition theorem gives a blackbox method to amplify this inapproximability: we can then conclude that for any $\varepsilon > 0$ it is NP-hard to approximate the classical value of a game G within an additive error $1 - \varepsilon$. Since the value of a game is a number between 0 and 1, this implies strong inapproximability for games. From this, optimal inapproximability results for various natural optimization problems can be obtained [52, 38].

Games with entangled players. We are primarily interested in the setting of games with *entangled* players: to produce their answers, Alice and Bob make measurements on an entangled state. When Alice and Bob are allowed to use entangled strategies, we call their maximum success probability the *entangled value*, denoted by $\mathrm{val}^*(G)$. There are games for which the entangled value is strictly larger than the classical value; the CHSH game is one example.

The general study of one-round games with entangled players was initiated by Cleve, Høyer, Toner, and Watrous [29]. This study was motivated by the important role that two-player games have in classical complexity theory, as well as the fact that Bell's theorem and Bell inequalities are naturally formulated in the language of entangled games. Since then, the field of entangled games (also called *non-local games* by [29]) has blossomed into a rich area that touches upon quantum complexity theory, Hamiltonian complexity, optimization, and more.

Quantum parallel repetition. Here we are interested in whether there is a *quantum* analogue of Raz's parallel repetition theorem. A natural open question, which we call the

Quantum Parallel Repetition Conjecture, is whether an analogue of Raz's parallel repetition theorem holds when the players are allowed to use shared quantum entanglement as part of their strategy.

We've seen quantum entanglement can be a powerful information theoretic resource (as dramatically demonstrated with the Infinite Randomness Expansion result!). But can it be so powerful as to defeat parallel repetition? In other words, is it possible that there is a game G such that $\text{val}^*(G) < 1$, but for all n,$\text{val}^*(G^n)$ is lower bounded by some constant independent of n? This ludicrous possibility has not been ruled out, prior to the results in this thesis.

The parallel repetition of entangled games has been studied extensively in recent years. A quantum analogue of Raz's parallel repetition theorem has been established for many special classes of games: including free games [24, 61, 27], projection games [39], XOR games [30], and unique games [64], but the general case has resisted attack. This thesis presents three results concerning the Quantum Parallel Repetition Conjecture, in order of increasing generality and scope:

1. Improved parallel repetition theorems for free entangled games
2. Hardness amplification for general entangled games via anchoring
3. A parallel repetition theorem for all entangled games

In Chapter 4, I will give an in-depth survey of the subject of quantum parallel repetition, as well as summaries of the three results above.

1.4 Message authentication in a quantum world

Message authentication is a fundamental task in cryptography. While encryption *hides* the contents of a message from an eavesdropper, authentication *protects* a message from a *tamperer*. With message authentication, Alice can send a message to Bob, and he can verify the *integrity* of his received message to check whether it was manipulated by an active adversary. It is well known that encryption and authentication are orthogonal tasks[2].

A simple message authentication scheme is the following: Alice and Bob share a random secret key k, and also agree on a family of hash functions $\{h_k\}$. To authenticate a message m, Alice sends m along with the hash $h_k(m)$, called the tag. When Bob receives a message/tag pair (m', t), he checks whether $t = h_k(m')$. If so, then he accepts and concludes that m' is the original message m, otherwise he rejects and concludes that some tampering must have happened. This is the classical Wegman-Carter message authentication scheme [101]. The idea is that, if an adversary does not know the secret key k and the hash family is 2-universal, then the adversary has a small chance of successfully changing $(m, h_k(m))$ into another valid message/tag pair.

The last part of this thesis is on message authentication in a quantum world. The main contributions of this work include security definitions for authentication against quantum adversaries that subsume previous ones, as well as authentication schemes instantiating our new definitions. We consider both *classical authentication with quantum adversaries*, and *fully quantum authentication with quantum adversaries*.

[2] The famous one-time pad, while achieving perfect encryption, offers no authentication capabilities whatsoever: an adversary can flip any number of bits of the ciphertext without being detected, and the receiver would consequently decipher a message that may have little to do with the original message. On the other hand, many message authentication schemes do not even attempt to hide the message.

Classical authentication in a quantum world. First, we consider what happens if adversaries try to perform quantum attacks on classical authentication schemes. This is part of the broader subject of *post-quantum cryptography*, where one of the central questions is: which classical cryptographic primitives survive in a world where the adversaries are equipped with quantum computers and are able to mount quantum attacks [15]?

In this setting, we can imagine that message authentication is performed by some physical device, such a smart card. It is ostensibly non-quantum, performing classical authentication on classical inputs, and returning classical outputs. However, an adversary could in principle operate on this device in a quantum manner, by cooling it down to very low temperatures, shielding it from noise and radiation, and access the device in *superposition*: for example, if the device used the Wegman-Carter authentication scheme, then the adversary could submit a superposition of messages $\sum_m \alpha_m |m\rangle$, and the device would return $\sum_m \alpha_m |m, h_k(m)\rangle$. Furthermore, the adversary could submit a superposition of messages that is entangled with some *quantum side information*: $\sum_m \alpha_m |m\rangle |\varphi_m\rangle$, where $\{|\varphi_m\rangle\}$ are arbitrary quantum states held by the adversary. After authentication, the state is $\sum_m \alpha_m |m, h_k(m)\rangle |\varphi_m\rangle$.

We focus on the *one-time setting*. That is, the adversary is only able to use the smart card once. Still, could the adversary take advantage of superposition attacks and quantum side information to produce a *forgery*, i.e., two distinct message/tag pairs $(m_1, h_k(m_1))$ and $(m_2, h_k(m_2))$? Could the adversary extract the secret key k in this way?

In [18], Boneh and Zhandry gave the first security definition for classical authentication against superposition attacks: at minimum, if the adversary is only able to quantumly access the authentication oracle (in this case, the smart card) q times, then it should not be able to produce $q+1$ valid message/tag pairs with non-negligible probability. When the adversary only performs classical attacks, this coincides with the classical definition of security for message authentication. They prove that the Wegman-Carter scheme, when instantiated with a q-wise independent hash family, satisfies this stronger quantum security definition.

However, the Boneh-Zhandry security definition does not constrain the relationship between q message/tag pairs that the adversary could produce, and the q queries made to the authentication oracle. For example, consider the case where the adversary submits one superposition of messages that all start with `bob@gmail.com`. Suppose the adversary were able to manipulate the authenticated superposition (which may be entangled with quantum side information) to produce an authentication of a message that started with `charlie@hotmail.com` instead. This is clearly an undesirable outcome, although the Boneh-Zhandry definition does not rule such an attack out.

Our first contribution is a significantly strengthened security definition for one-time classical authentication schemes. It characterizes, in a strong way, the (effective) actions of a quantum adversary, who may share arbitrary quantum entanglement with the messages being authenticated. At a high level, the security definition says that "all the adversary can do" is, given an authenticated state, measure the message/tag pair, and based on the outcome of its measurement, apply an arbitrary quantum operation on its quantum side information. Since a real adversary can certainly do this in an undetectable way, this means that our security definition is the strongest possible.

From this security definition we are able to easily deduce properties such as unforgeability (and hence recover the Boneh-Zhandry security definition for one-time message authentication), as well as ruling out attacks like the one given above. Then, we show how the Wegman-Carter authentication scheme satisfies this strengthened security definition.

Quantum authentication of quantum data. Next, we consider *total quantum authentication*. If we think of authentication as a general cryptographic primitive to detect tampering of a message, then in the quantum setting we should expect that if a receiver accepts an authenticated quantum state, the state should be indistinguishable from the original authenticated message state. A classical authentication scheme like Wegman-Carter cannot provide such functionality; for example, given the authenticated state $\sum_m \alpha_m |m, h_k(m)\rangle$, the adversary could simply measure the state in the computational basis, producing a mixed state; yet this would go undetected by the receiver.

In [9], Barnum et al. investigate the possibility of authenticating quantum data using a quantum protocol. They present a definition of quantum authentication where, conditioned on the protocol succeeding, the sender has effectively teleported a quantum state to the receiver. They then give a scheme which attains this definition. Interestingly, they show that quantum state authentication necessarily implies quantum state *encryption*.

However, the security definition given by Barnum et al. for quantum authentication does not take entanglement into account; the adversary may have access to quantum side information about the state being authenticated, which could potentially give it more power. Follow up works [53] showed that the Barnum et al. protocol actually has *universal composable security*, which implies that it remains secure in the presence of side information. However, no general definition for authentication with quantum side information was given.

Our second contribution is a strengthened security definition for total quantum authentication that handles quantum side information. Again, our security definition gives a strong characterization of the adversary's actions on the authenticated message state: essentially "all the adversary can do" conditioned on the receiver accepting is to perform an arbitrary quantum operation on its quantum side information, independently of the message state. Since a real adversary could do this without detection, this is the strongest possible security definition.

This security definition subsumes the definition given by Barnum, et al. It also implies surprising consequences: a quantum authentication scheme can be easily turned into a *quantum key distribution* protocol, in which two parties Alice and Bob can generate shared private keys that are secure against an active quantum eavesdropper. Furthermore, our security definition implies a *key reuse property*: whenever the receiver accepts, not only is the message state certified to be untouched by the adversary, the *key* is also guaranteed to be independent of the adversary.[3]

Finally, we present two schemes that perform total quantum authentication: the first one, based on unitary designs, satisfies the security definition outright. The second one is based on applying the Wegman-Carter classical authentication scheme in complementary bases. The caveat with the second scheme is that it potentially leaks certain bits of the key, although we have control over which bits of the key are insecure. It makes up for this caveat by being conceptually very simple.

[3] Hayden, et al. [53] also show that the specific protocol of Barnum, et al. implies quantum key distribution and (partial) key reuse.

Chapter 2

Preliminaries

2.1 Notation

2.1.1 Sets and indices

For an integer n, we let $[n] = \{1, \ldots, n\}$. For an alphabet $\mathcal{X}$, we let $\mathcal{X}^n$ denote the n-fold Cartesian product of $\mathcal{X}$. We denote elements of $\mathcal{X}^n$ by $x^n = (x_1, \ldots, x_n)$. For a subset $C = \{i_1, \ldots, i_t\} \subseteq [n]$, we let x_C denote the ordered tuple $(x_{i_1}, \ldots, x_{i_t})$.

We write $\mathbb{R}$ to denote the field of real numbers, $\mathbb{C}$ to denote the field of complex numbers, $\mathbb{Z}$ to denote the ring of integers, and $\mathbb{N}$ to denote the set of natural numbers $\{1, 2, \ldots\}$.

2.1.2 Linear algebra

We use $\mathbb{I}$ to denote the identity matrix. For Hermitian matrices A, B we write $A \preceq B$ to indicate that $A - B$ is positive semidefinite. For a linear operator X acting on a complex vector space, we let $\mathrm{ad}_X[\cdot]$ to denote the map that takes linear operators $\rho \mapsto X\rho X^\dagger$.

2.1.3 Probability distributions, random variables, and expectations

We let capital letters denote random variables and lower case letters denote specific samples. We will use superscripts to denote tuples, e.g., $X^n := (X_1, \ldots, X_n)$, $x^n = (x_1, \ldots, x_n)$. For a subset $C \subset [n]$ we write X_C to denote the sub-tuple of X^n indexed by C. We use P_X to denote the probability distribution of random variable X, and $\mathsf{P}_X(x)$ to denote the probability that $X = x$ for some value x. For multiple random variables, e.g., X, Y, Z, $\mathsf{P}_{XYZ}(x, y, z)$ denotes their joint distribution with respect to some probability space understood from context.

We use $\mathsf{P}_{Y|X=x}(y)$ to denote the conditional distribution $\mathsf{P}_{YX}(y, x)/\mathsf{P}_X(x)$, which is defined when $\mathsf{P}_X(x) > 0$. When conditioning on many variables, we usually use the shorthand $\mathsf{P}_{X|y,z}$ to denote the distribution $\mathsf{P}_{X|Y=y,Z=z}$. For example, we write $\mathsf{P}_{V|\omega_{-i},x_i,y_i}$ to denote $\mathsf{P}_{V|\Omega_{-i}=\omega_{-i},X_i=x_i,Y_i=y_i}$. For an event W we let $\mathsf{P}_{XY|W}$ denote the distribution conditioned on W. We use the notation $\mathbb{E}_X f(x)$ and $\mathbb{E}_{\mathsf{P}_X} f(x)$ to denote the expectation $\sum_x \mathsf{P}_X(x) f(x)$.

Let P_{X_0} be a distribution of $\mathcal{X}$, and for every x in the support of P_{X_0}, let $\mathsf{P}_{Y|X_1=x}$ be a conditional distribution defined over $\mathcal{Y}$. We define the distribution $\mathsf{P}_{X_0}\mathsf{P}_{Y|X_1}$ over $\mathcal{X} \times \mathcal{Y}$ as

$$(\mathsf{P}_{X_0}\mathsf{P}_{Y|X_1})(x, y) := \mathsf{P}_{X_0}(x) \cdot \mathsf{P}_{Y|X_1=x}(y).$$

Additionally, we write $\mathsf{P}_{X_0Z}\mathsf{P}_{Y|X_1}$ to denote the distribution $(\mathsf{P}_{X_0Z}\mathsf{P}_{Y|X_1})(x,z,y) := \mathsf{P}_{X_0Z}(x,z) \cdot \mathsf{P}_{Y|X_1=x}(y)$.

For two random variables X_0 and X_1 over the same set $\mathcal{X}$, $\mathsf{P}_{X_0} \approx_\varepsilon \mathsf{P}_{X_1}$ indicates that the total variation distance between P_{X_0} and P_{X_1},

$$\|\mathsf{P}_{X_0} - \mathsf{P}_{X_1}\| := \frac{1}{2}\sum_{x\in\mathcal{X}} |\mathsf{P}_{X_0}(x) - \mathsf{P}_{X_1}(x)|,$$

is at most ε.

The following simple lemma will be used repeatedly.

Lemma 2. *Let Q_F and S_F be two probability distributions of some random variable F, and let $\mathsf{R}_{G|F}$ be a conditional probability distribution for some random variable G, conditioned on F. Then*

$$\|\mathsf{Q}_F\mathsf{R}_{G|F} - \mathsf{S}_F\mathsf{R}_{G|F}\| = \|\mathsf{Q}_F - \mathsf{S}_F\|.$$

Proof. Note that $\|\mathsf{Q}_F\mathsf{R}_{G|F} - \mathsf{S}_F\mathsf{R}_{G|F}\|$ is equal to

$$\begin{aligned}\frac{1}{2}\sum_{f,g}|\mathsf{Q}(f)\mathsf{R}(g|f) - \mathsf{S}(f)\mathsf{R}(g|f)| &= \frac{1}{2}\sum_{f}|\mathsf{Q}(f) - \mathsf{S}(f)| \cdot \left(\sum_{g}\mathsf{R}(g|f)\right)\\ &= \frac{1}{2}\sum_{f}|\mathsf{Q}(f) - \mathsf{S}(f)|\\ &= \|\mathsf{Q}_F - \mathsf{S}_F\|.\end{aligned}$$

□

2.2 Quantum states and measurements

For comprehensive references on quantum information we refer the reader to [82, 102].

We use $\mathcal{H}$ to denote a finite dimensional Hilbert space. A d-dimensional quantum pure state is a unit-length vector $|\psi\rangle \in \mathbb{C}^d$. A matrix $\rho \in \mathbb{C}^{d\times d}$ is a *d-dimensional density matrix* if it is positive semidefinite and has trace 1. A *positive operator valued measurement* (POVM) with outcome set $\mathcal{A}$ is a set of positive semidefinite matrices $\{E^a\}$ labeled by $a \in \mathcal{A}$ that sum to the identity. Given a density matrix $\rho \in \mathbb{C}^{d\times d}$ and a POVM $\{E_a\}$ where each E_a acts on $\mathbb{C}^{d\times d}$, each outcome $a \in \mathcal{A}$ occurs with probability $\mathrm{Tr}(\rho E_a)$, and for each outcome the state ρ is transformed into the *post-measurement* state

$$\rho_a = \frac{\sqrt{E_a}\rho\sqrt{E_a}}{Tr(\rho E_a)}$$

where $\sqrt{E_a}$ denotes the matrix square root of E_a. The reader may be aware that the post-measurement states of a POVM have a unitary freedom, but in this thesis we shall restrict ourselves to the canonical post-measurement states just defined.

We will use the convention that, when $|\psi\rangle$ is a pure state, ψ refers to the rank-1 density matrix $|\psi\rangle\langle\psi|$. We use superscripts to denote system labels; so ρ^{AB} will denote the density matrix on the systems A and B. A *classical-quantum* state ρ^{XE} is classical on X and quantum on E if it can be written as $\rho^{XE} = \sum_x p(x)|x\rangle\langle x|_X \otimes \rho_x^E$ for some probability measure $p(\cdot)$.

The state ρ_x^E is by definition the E part of the state ρ_{XE}, conditioned on the classical register $X = x$. We write ρ_x^{XE} to denote the state $|x\rangle\langle x|_X \otimes \rho_x^E$.

We will generally decorate states (both pure states and density matrices) with superscripts to indicate the spaces and registers they reside in.

2.3 Norms and distance measures

For a vector $|\psi\rangle$, we use $\||\psi\rangle\|$ to denote its Euclidean length. For a matrix A, we will use $\|A\|_1$ to denote its *trace norm* $\mathrm{Tr}(\sqrt{AA^\dagger})$. A density matrix is a positive semidefinite matrix with trace 1. The *fidelity* between two density matrices ρ and σ is defined as $F(\rho,\sigma) = \|\sqrt{\rho}\sqrt{\sigma}\|_1$. The Fuchs-van de Graaf inequalities relate fidelity and trace norm as

$$1 - F(\rho,\sigma) \le \frac{1}{2}\|\rho - \sigma\|_1 \le \sqrt{1 - F(\rho,\sigma)^2}. \tag{2.1}$$

2.3.1 Hellinger distance

The fidelity distance measure is not a metric on the space of positive semidefinite operators. For one, it does not satisfy a triangle inequality. However, one can convert fidelity into other measures that are metrics. One such measure is the *Hellinger distance*, defined as $\mathrm{h}(\rho,\sigma) := \sqrt{1 - F(\rho,\sigma)}$. In this paper, we will use the *squared Hellinger metric*, denoted by $\mathrm{h}^2(\rho,\sigma) := 1 - F(\rho,\sigma)$, as the primary distance measure between quantum states. It satisfies many pleasant properties, including the following:

Fact 3 (Triangle inequality). *Let $n \ge 2$ and let $\rho_1, \ldots, \rho_{n+1}$ be density matrices. Then*

$$\mathrm{h}^2(\rho_1, \rho_{n+1}) \le n \sum_i \mathrm{h}^2(\rho_i, \rho_{i+1}).$$

Proof. We adapt the proof from [24]. For $i \in [n]$ let $\alpha_i = \arccos(F(\rho_i, \rho_{i+1}))$. Let $\alpha = \arccos(F(\rho_1, \rho_{n+1}))$. Then, since $\arccos(F(\cdot,\cdot))$ is a distance measure for quantum states, we have $\alpha \le \sum_i \alpha_i$. Then we have

$$\mathrm{h}^2(\rho_1, \rho_{n+1}) = 1 - \cos(\alpha) \le n^2(1 - \cos(\alpha/n)) \le n \sum_i (1 - \cos(\alpha_i)) = n \sum_{i=1}^{n} \mathrm{h}^2(\rho_i, \rho_{i+1}).$$

□

Fact 4 (Contractivity under quantum operations). *Let $\mathcal{E}$ be a quantum operation, and let ρ and σ be density matrices. Then* $\mathrm{h}^2(\mathcal{E}(\rho), \mathcal{E}(\sigma)) \le \mathrm{h}^2(\rho,\sigma)$.

Fact 5 (Unitary invariance). *Let U be unitary, and let ρ and σ be density matrices.Then* $\mathrm{h}^2(U\rho U^\dagger, U\sigma U^\dagger) = \mathrm{h}^2(\rho,\sigma)$.

Fact 6 (Convexity). *Let $\{A_i\}$ and $\{B_i\}$ be finite collections of positive semidefinite operators, and let $\{p_i\}$ be a probability distribution. Then* $\mathrm{h}^2(\sum_i p_i A_i \sum_i p_i B_i) \le \sum_i p_i \mathrm{h}^2(A_i, B_i)$.

Fact 7. *Let $\{A_i\}$ and $\{B_i\}$ be finite collections of positive semidefinite operators, and let $\{p_i\}$ be a probability distribution. Then* $\mathrm{h}^2(\sum_i p_i |i\rangle\langle i| \otimes A_i, \sum_i p_i |i\rangle\langle i| \otimes B_i) = \sum_i p_i \mathrm{h}^2(A_i, B_i)$.

Fact 8 ([58]). *Let ρ and σ be density matrices. Then* $S(\rho\|\sigma) \ge \mathrm{h}^2(\rho,\sigma)$.

2.4 Quantum information theory

For two positive semidefinite operators ρ, σ, the *relative entropy* $S(\rho\|\sigma)$ is defined to be $\mathrm{Tr}(\rho(\log\rho - \log\sigma))$. The *relative min-entropy* $S_\infty(\rho\|\sigma)$ is defined as $\min\{\lambda : \rho \preceq 2^\lambda\sigma\}$.

Let ρ_{AB} be a bipartite state. The mutual information $I(A:B)_\rho$ is defined as $S(\rho_{AB}\|\rho^A \otimes \rho^B)$. For a classical-quantum state ρ_{XAB} that is classical on X and quantum on AB, we write $I(A;B|x)_\rho$ to indicate $I(A;B)_{\rho_x}$.

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

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

where $\mathrm{D}(\mathcal{H}_B)$ denotes the set of density matrices on register B. Let $\varepsilon > 0$. Then ε-smoothed min-entropy of A conditioned on B is defined as

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

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 [91].

The following propositions and facts will be useful throughout this thesis.

Proposition 9 (Pinsker's inequality). *For all density matrices ρ, σ, $\frac{1}{2}\|\rho - \sigma\|_1^2 \leq S(\rho\|\sigma)$.*

Fact 10 ([61], Fact II.8). *Let $\rho = \sum_z \mathsf{P}_Z(z)|z\rangle\langle z| \otimes \rho_z$, and $\rho' = \sum_z \mathsf{P}_{Z'}(z)|z\rangle\langle z| \otimes \rho'_z$. Then $S(\rho'\|\rho) = S(\mathsf{P}_{Z'}\|\mathsf{P}_Z) + \mathbb{E}_{Z'}\left[S(\rho'_z\|\rho_z)\right]$. In particular, $S(\rho'\|\rho) \geq \mathbb{E}_{Z'}\left[S(\rho'_z\|\rho_z)\right]$.*

Fact 11 ([58]). *Let μ be a probability distribution on $\mathcal{X}$. Let $\rho = \sum_{x\in X} \mu_x |x\rangle\langle\otimes|\rho^A_x$. Then $I(X:A)_\rho = \mathbb{E}_{x\leftarrow\mu}[S(\rho_x\|\rho)]$.*

Fact 12 ([61], Fact II.11). *Let ρ^{XY} and σ^{XY} be quantum states. Then $S(\rho^{XY}\|\sigma^{XY}) \geq S(\rho^X\|\sigma^X)$.*

Fact 13. *Let ρ^{XY} and $\sigma^{XY} = \sigma^X \otimes \sigma^Y$ be quantum states. Then $S(\rho^{XY}\|\sigma^{XY}) \geq S(\rho^X\|\sigma^X) + S(\rho^Y\|\sigma^Y)$.*

Fact 14 ([61], Lemma II.13). *Let $\rho = p\rho_0 + (1-p)\rho_1$. Then $S_\infty(\rho_0\|\rho) \leq \log 1/p$.*

Fact 15. *Let ρ^{AB} and σ^{AB} be density matrices. Then $S_\infty(\rho^{AB}\|\sigma^{AB}) \geq S_\infty(\rho^A\|\sigma^B)$.*

Fact 16. *Let ρ, σ, and τ be density matrices such that $S_\infty(\rho\|\sigma) \leq \lambda_1$ and $S_\infty(\sigma\|\tau) \leq \lambda_2$. Then $S_\infty(\rho\|\tau) \leq \lambda_1 + \lambda_2$.*

Fact 17. *Let ρ, σ, and τ be density matrices such that $S(\rho\|\sigma) \leq \lambda_1$ and $S_\infty(\sigma\|\tau) \leq \lambda_2$. Then $S_\infty(\rho\|\tau) \leq \lambda_1 + \lambda_2$.*

Proof. $S_\infty(\sigma\|\tau) = \lambda_2$ implies that $2^{-\lambda_2}\sigma \preceq \tau$. Then,

$$\begin{aligned}
S(\rho\|\tau) &= \mathrm{Tr}(\rho(\log\rho - \log\tau)) \\
&\leq \mathrm{Tr}(\rho(\log\rho - \log 2^{-\lambda_2}\sigma)) \\
&\leq \mathrm{Tr}(\rho(\log\rho - (-\lambda_2)\mathbb{I} - \log\sigma)) \\
&\leq \lambda_2 + \mathrm{Tr}(\rho(\log\rho - \log\sigma)) \\
&= \lambda_1 + \lambda_2.
\end{aligned}$$

□

2.4.1 Quantum Raz's Lemma

We prove a quantum analogue of Raz's Lemma, which is the central tool behind many information-theoretic proofs of parallel repetition theorems [88, 55, 8]:

Lemma 18 (Quantum Raz's Lemma). *Let ρ and σ be two CQ states with $\rho_{XA} = \rho_{X_1X_2\ldots X_nA}$ and $\sigma = \sigma_{XA} = \sigma_{X_1} \otimes \sigma_{X_2} \otimes \ldots \otimes \sigma_{X_n} \otimes \sigma_A$ with $X = X_1X_2\ldots X_n$ classical in both states. Then*

$$\sum_{i=1}^{n} I(X_i : A)_\rho \leq S(\rho_{XA} \| \sigma_{XA}). \tag{2.2}$$

Proof. By the chain rule (Fact 10) we have

$$S(\rho_{XA}\|\sigma_{XA}) = S(\rho_{X_1}\|\sigma_{X_1}) + \mathop{\mathbb{E}}_{x_1 \leftarrow \rho_{X_1}} S(\rho_{X_2|X_1=x_1}\|\sigma_{X_2}) + \ldots + \mathop{\mathbb{E}}_{x \leftarrow \rho_{X_1\cdots X_n}} S(\rho_{A|X=x}\|\sigma_A), \tag{2.3}$$

where $x_1 \leftarrow \rho_{X_1}$ means sampling x_1 according to the classical distribution ρ_{X_1}, and similarly for $x \leftarrow \rho_{X_1\cdots X_n}$. Consider any of the first n terms in (2.3). We have

$$\mathop{\mathbb{E}}_{x_{<i} \leftarrow \rho_{X_1X_2\ldots X_{i-1}}} S(\rho_{X_i|x_{<i}}\|\sigma_{X_i}) \geq \mathop{\mathbb{E}}_{x_{<i} \leftarrow \rho_{X_1X_2\ldots X_{i-1}}} S(\rho_{X_i|x_{<i}}\|\rho_{X_i}) = I(X_1\ldots X_{i-1} : X_i)_\rho,$$

where $\rho_{X_i|x_{<i}}$ stands for $\rho_{X_i|X_{<i}=x_{<i}}$. Now consider the last term in (2.3):

$$\begin{aligned} \mathop{\mathbb{E}}_{x \leftarrow \rho_X} S(\rho_{A|X=x}\|\sigma_A) &\geq \mathop{\mathbb{E}}_{x \leftarrow \rho_X} S(\rho_{A|X=x}\|\rho_A) = S(\rho_{XA}\|\rho_X \otimes \rho_A) \\ &= I(X : A)_\rho = \sum_{i=1}^{n} I(X_i : A|X_1X_2\ldots X_{i-1})_\rho. \end{aligned}$$

Summing up the last two equations and using $I(X_i : AX_1\ldots X_i) = I(X_i : X_1\ldots X_{i-1}) + I(X_i : A|X_1\ldots X_{i-1})$ implies

$$S(\rho_{XA}\|\sigma_{XA}) \geq \sum_{i=1}^{n} I(X_i : AX_1\ldots X_{i-1})_\rho \geq \sum_{i=1}^{n} I(X_i : A)_\rho,$$

where the last inequality follows from strong subadditivity, i.e., $I(X_i : X_1\ldots X_{i-1}|A)_\rho \geq 0$. □

Chapter 3

Infinite Randomness Expansion

The work presented in this chapter was conducted with Matthew Coudron, and published in the proceedings of Symposium on Theory of Computing in 2014 under the title of "Infinite Randomness Expansion with a Constant Number of Devices" [33].

3.1 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 [14]. 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 [31] in 2006, device-independent randomness expansion has flourished into an active area of research [84, 97, 93, 76]. Its study involves a diverse array of concepts from quantum information theory, theoretical computer science, and quantum cryptography, including the monogamy of entanglement [41], randomness extractors [91, 69, 36], and quantum key distribution [10, 97, 76]. Randomness expansion has even been experimentally realized by [84], who reported the generation of 42 bits of certified randomness[1].

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 [84], 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. Another approach, developed in [96], 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 paper) 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 [76] not only achieves quantum security, but randomness expansion that tolerates a constant level of noise in the devices.

The original protocol of [31] obtained $g(m) = \Theta(m)$, or linear expansion. This was improved by Pironio et al. [84] to achieve quadratic expansion $g(m) = \Theta(m^2)$. The protocols of [96, 42, 76] 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) [32]. There the authors showed that *noise robust*, non-adaptive protocols must have a finite bound on their expansion factor[2]. With the exception of [42], randomness expansion protocols prior to our work were *non-adaptive*, and hence the results of [32] 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

[1] It took over a month to collect these many bits – but they were *quantumly certified*!

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

protocol, this time with much larger expansion factor. Our InfiniteExpansion protocol is the infinite composition of the ClusterExpansion sub-protocol.

In Section 6.1.3, we discuss two relevant and enlightening results about randomness expansion [26, 76], 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. $2^{2^{2^{\cdots^{2N}}}}$): 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 [104], and in [76] 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 (... $\mathrm{much}^{\mathrm{much}^{\cdots}}$) 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.

3.1.1 Barriers to infinite randomness expansion

Here we identify the inherent technical challenges in analyzing any adaptive randomness expansion protocol. In Section 3.2 we discuss how to overcome these challenges. Some of the technical issues discussed here have been identified in previous work (e.g., [42]) 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, [42] 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[3]. 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 exponential randomness expansion protocol that produces an output with high conditional min-entropy[4] – uses, in its analysis, an assumption that the initial seed to the protocol is secure against the eavesdropper [96]. 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 [96] 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 [36, 69]) require that the extractor seed be secure against the quantum eavesdropper. As pointed out by [42], 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} is such that $\rho_{SDE} \approx U_{|S|} \otimes \rho_{DE}$, where $U_{|S|}$ denotes the uniform distribution on $|S|$ bits,

[3] 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.

[4] Recent work by [76] gives another such protocol with quantum security. See Section 6.1.3 for more information.

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)[5].

3.2 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 [96] (which we denote VV)[6], and the sequential CHSH game protocol of Reichardt, et al. [90] (which we denote RUV). See Section 3.4 for more detail on these sub-protocols. We describe the protocol below, both algorithmically and schematically (see Figure 3-1).

The main result of this paper is the following theorem, stated informally here (for the formal version see Theorems 29 and 28):

Theorem 19 (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* $\Pr($*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.

[5] 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 $(S, \text{first bit of } \mathrm{Ext}(D, S))$. 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.

[6] 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.

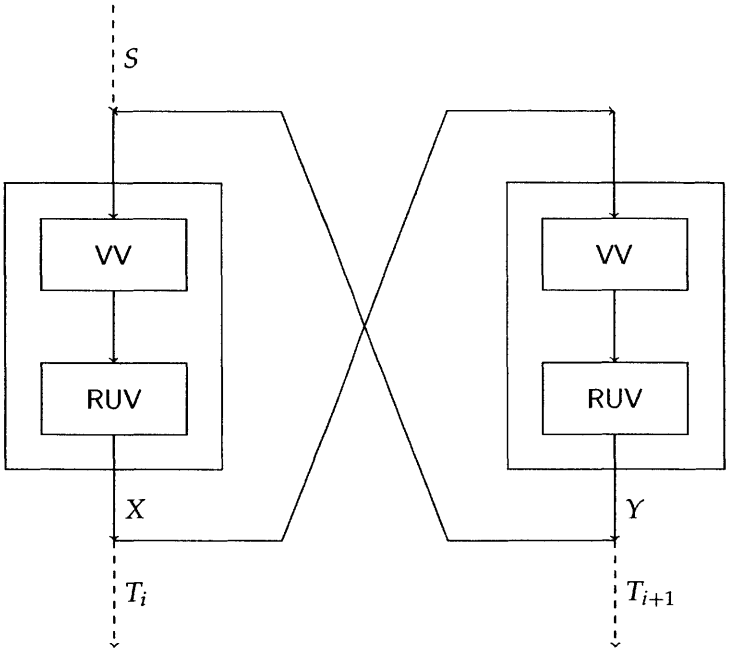

Figure 3-1: The InfiniteExpansion protocol. All arrows indicate classical operations performed by the referee. S denotes the initial seed to the protocol, and T_i denotes the output of the protocol at the ith iteration. Each of the VV and RUV boxes involve two devices, for a total of eight devices used in the protocol.

The analysis of the InfiniteExpansion protocol overcomes the challenges described in the previous section. We now give an overview of how we solve them.

3.2.1 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 [90], which is based on the phenomenon of *CHSH game rigidity*. Recall that, in the CHSH game, classical referee chooses two input bits x and y uniformly at random, and sends x to Alice and y to Bob. Alice and Bob produce binary outputs a and b, and they win the game if $a \oplus b = x \wedge y$. The classical value of the CHSH game is 75%, and the quantum value is $\cos^2(\pi/8) \approx 85\%$. 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 $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. We call this the *ideal*

```
Non-signaling devices: $D_1, \dots, D_8$.
Initial seed randomness: $S \sim U_m$.

  1. Let $X_1 \leftarrow S$.
  2. For $i = 1, 2, 3, \dots$
     (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 3-2: 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 3.4). The X_i, Y_i, Z_i, and W_i registers are all classical, and managed by the referee.

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 [73] and later made robust by [74, 75].

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 [90] Theorem 5.38, or Theorem 2.8 in this paper), which they call *sequential CHSH game rigidity*:

Theorem 20 (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 20 that, with high probability, the outputs of the RUV protocol were generated by a strategy approximating the ideal sequential strategy. The ideal sequential 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.

3.2.2 Comment on the relation between our work and the works of Chung-Shi-Wu and Miller-Shi

Here we mention work that was developed in parallel and independently of our results. In the following description we will occasionally use the terminology of this paper to restate results of these other works, though those papers used different terminology in the original statements.

First, Chung, Shi and Wu [26] studied *physical randomness extractors*, which are device-independent protocols that take in a weak source of randomness as seed (i.e. the seed only has some amount of min-entropy, but is not guaranteed to be uniform), and certifiably produce uniform sources of randomness. This is the device-independent analogue of randomness extractors discussed above. The work of [26] required an Input Secure randomness expansion protocol to use as a building block for their amplification protocol. They prove a powerful result called the Equivalence Lemma, which may be informally summarized as follows (see [26] for a formal statement):

Consider a device-independent randomness expansion protocol P that starts with a seed S, which is uniform and unentangled with the devices D involved in the protocol as well as a quantum adversary E. Suppose that the protocol P produces an output string X that is certifiably close to uniform and in tensor product with E and S (conditioned on the protocol succeeding). 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.

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.

Secondly, another independent work of Miller and Shi [76] gives the first provably robust protocol for randomness expansion (and, in fact, gives robust exponential expansion). Combining the main result of [76] with Equivalence Lemma of [26], allows one to obtain a provably *robust* infinite expansion protocol requiring only four non-communicating devices. Thus the combination of [26] and [76] supersedes our results, and represents (at the current time of writing) the state-of-the-art in randomness expansion.

3.2.3 The minimum seed length required to "jumpstart" infinite randomness expansion

In [50], Gross and Aaronson analyze the minimum amount of randomness necessary to "jumpstart" an infinite randomness expansion protocol. They analyzed the randomness expansion protocol of Miller and Shi [76], combined with the quantum-secure extractor of De, et al [36]. As mentioned before, composing an Input Secure randomness expansion protocol such as Miller Shi with itself, by the Equivalence Lemma, will yield infinite randomness expansion.

The minimum seed size has a dependence on an error parameter ε, which indicates how close to uniform the final output is (conditioned on the protocol succeeding). They showed that an upper bound on the minimum seed length needed to guarantee that the output is within $\varepsilon = 10^{-6}$, the minimum seed length is at most $715,000$ bits of uniform randomness needed. When $\varepsilon = 10^{-1}$, the minimum seed length needs to be at most $225,000$. Thus, one can fancifully say that, as long as there are $225,000$ bits of uniform randomness scattered *somewhere* throughout the universe, in principle one can use these bits to certify the production of an unbounded amount of additional randomness.

3.3 Preliminaries

3.3.1 Notation

Throughout this chapter, we will adopt the notation of using subscripts to denote the registers that a state resides in, e.g., the state ρ_{AB} denotes a bipartite density matrix in registers A and B.

Definition 21 (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*

$$\|\rho_{XE} - U_{|X|} \otimes \rho_E\|_1 \leq \zeta.$$

3.3.2 Modelling protocols and input robustness

In this paper, 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.

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 $\mathcal{F}\mathcal{E}$ to be the composition of the two quantum operations $\mathcal{E}$, followed by $\mathcal{F}$. Throughout this paper, 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., $F = 1$).

[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.

The completeness and soundness of protocol P are statements about the post-measurement state $\mathcal{FE} \otimes \mathbb{I}_E(\rho^i_{FSXDE})$ (where $\mathbb{I}_E$ 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 22 below.

Lemma 22. *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*

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

Let $\delta, \lambda > 0$. Let ρ^i_{FSXDE} be such that $\|\rho^i_{FSXDE} - \sigma_{FSXDE}\|_1 \leq \delta$ 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 $\mathcal{E} \otimes \mathbb{I}_E(\rho^i_{FSXDE})$ is at least λ. Then, there exists a state μ_{XDE} such that $\mu_{XE} = U_{|X|} \otimes \mu_E$ and

$$\|\rho^f_{XDE} - \mu_{XDE}\|_1 \leq \varepsilon + \delta/\lambda,$$

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

The proof of Lemma 22 is deferred to Appendix 3.5.3.

3.3.3 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 [96, Protocol B]. We record a formulation of their result as it will be used by us here:

Theorem 23 (Vazirani-Vidick protocol [96]). *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 $\Pr(\text{Protocol succeeds}) \geq \varepsilon$, 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 24 (Quantum-secure extractor). *A function* 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 25 ([36]). *For all positive integers n, r, there exists a function* 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 $d = O(\log^2(n/\varepsilon)\log r)$.*

3.3.4 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 [90] 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 [90]). The main property of ζ-ideal strategy that we will use is the following:

Lemma 26. *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,*

$$\|\rho_{X_iE|I_i=1} - U_n \otimes \rho_{E|I_i=1}\|_1 \leq \zeta,$$

where $\rho_{X_iE|I_i=1}$ 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 [90, Definitions 5.4, 5.5 and 5.37] for more detail. □

Theorem 27 (Sequential CHSH game rigidity; Theorem 5.38 of [90]). *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 [90], instantiated with the parameter settings used in Theorem 5.39. □

3.4 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 3-3: 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.

$\mathsf{ClusterExpansion}(C, S)$ **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.

3.4.1 The VV sub-protocol

The VV sub-protocol consists of performing Protocol B from [96], 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 23). We give a detailed account of the particular parameter settings we use for Protocol B in Appendix 3.6.

We use the QExt randomness extractor given by Theorem 25. 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 3.6).

3.4.2 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 [90, Theorem 5.7].

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

$\mathsf{VV}(A, B, S)$ **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 [96] 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 3-4: 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 23 on s bits of seed.

3.5 Analysis of the InfiniteExpansion Protocol

We now analyze the InfiniteExpansion protocol. As discussed in the Preliminaries (Section 5.2), 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 3.4). 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 28 establishes that there exists a quantum strategy by which the devices, with high probability, do not abort the InfiniteExpansion protocol. Theorem 29 establishes the soundness of the InfiniteExpansion protocol.

Theorem 28 (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 [96] 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 $\exp(-\Omega(m^{1/3}))$. □

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 $i = 1, \dots, N$, 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.

Theorem 29 (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* $\text{WIN}_{\leq i} = \text{WIN}_1 \wedge \cdots \wedge \text{WIN}_i$. *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 $\Pr(\text{WIN}_{\leq k}) \geq \lambda \geq \exp(-C'm^{1/3})$ for some universal constant C', then*

$$\|\rho^k_{X_kE} - U_{g^{(k)}(m)} \otimes \rho^k_E\|_1 \leq 4\exp(-C''m^{1/3})/\lambda^2,$$

where

- *C'' is the universal constant from Theorem 30, 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 29, 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 29 assumes the correctness of the ClusterExpansion sub-protocol (Theorem 30), 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

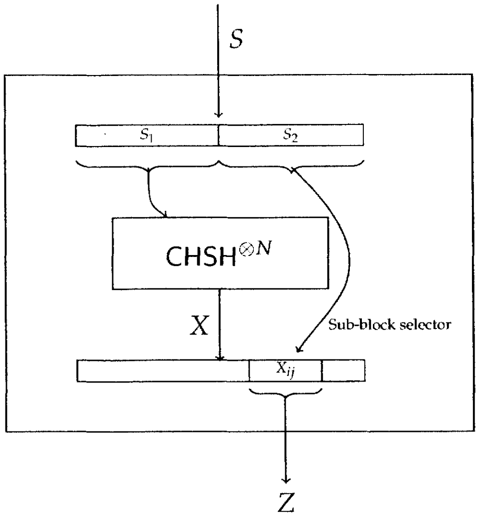

Figure 3-5: The RUV sub-protocol. All arrows indicate classical operations performed by the referee.

$C_{i \bmod 2}$) 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 $C_j := C_{j \bmod 2}$. Divide the overall probability of success, $\Pr(\mathsf{WIN}_{\leq k})$, into conditional probabilities: let $p = \Pr(\mathsf{WIN}_{\leq k})$ and let $p_i = \Pr(\mathsf{WIN}_i | \mathsf{WIN}_{\leq i-1})$. 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 30. 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

$$\|\rho^i_{X_iC_iC_{i+1}E} - \mu^i_{X_iC_iC_{i+1}E}\|_1 \leq \delta(i),$$

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 $\mathsf{WIN}_{\leq i}$.

Let $k = 1$. Then, by invoking Theorem 30 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

$$\|\rho^1_{X_1C_1C_2E} - \mu^1_{X_1C_1C_2E}\|_1 \leq \varepsilon_{\mathsf{EC}}(m, p_1) = \delta(1).$$

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 30 along with Lemma 22 to conclude that there exists a state $\mu^k_{X_kC_kC_{k+1}E}$ such that $\mu^k_{X_kC_{k+1}E} = U_{g^{(k)}}(m) \otimes$

$\mu^k_{C_{k+1}E}$ and

$$\|\rho^k_{X_kC_kC_{k+1}E} - \mu^k_{X_kC_kC_{k+1}E}\|_1 \le \varepsilon_{\mathrm{EC}}(g^{(k-1)}(m), p_k) + \delta(k-1)/p_k := \delta(k).$$

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

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

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

Finally, for every k, we have that

$$\begin{aligned}\|\rho^k_{X_kE} - U_{g^{(k)}(m)} \otimes \rho^k_E\|_1 &\le \|\rho^k_{X_kE} - \mu^k_{X_kE}\|_1 + \|\mu^k_{X_kE} - U_{g^{(k)}(m)} \otimes \rho^k_E\|_1\\ &\le \delta(k) + \|U_{g^{(k)}}(m) \otimes \mu^k_E - U_{g^{(k)}(m)} \otimes \rho^k_E\|_1\\ &= \delta(k) + \|\mu^k_E - \rho^k_E\|_1\\ &\le 2\delta(k).\end{aligned}$$

□

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 31 and 32, respectively).

Theorem 30. *Let C be an Expansion Cluster. Suppose that a classical referee executes the* 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* $\Pr($ClusterExpansion(C,S) *succeeds*$) \ge \lambda \ge \exp(-C'm^{1/3})$ *for some universal constant C', then there exists a state τ_{XCE} such that $\tau_{XE} = U_{g(m)} \otimes \tau_E$ and*

$$\|\rho^f_{XCE} - \tau_{XCE}\|_1 \le \varepsilon_{\mathrm{EC}}(m,\lambda),$$

where $\varepsilon_{\mathrm{EC}}(m,\lambda) := \exp(-C''m^{1/3})/\lambda$ 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 ClusterExpansion(C,S) *succeeding.*

Proof. Let λ_1 denote the probability that Step 1 of ClusterExpansion(C,S) succeeds, and let λ_2 denote the probability that Step 2 of ClusterExpansion(C,S) succeeds, conditioned on Step 1 succeeding, so that $\lambda_1\lambda_2 \ge \lambda$. 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 VV(D_1, D_2, S) (which is Step 1 of ClusterExpansion(C,S)). By definition of the VV protocol, $|Y| = v(m)$. By Lemma 31 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

$$\|\rho^v_{YDGE} - \tau^v_{YDGE}\|_1 \leq \varepsilon_{\mathsf{VV}}(m), \tag{3.1}$$

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 31. 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 32, we would get that there existed a state τ^f_{XDGE} such that $\tau^f_{XE} = U_{g(m)} \otimes \tau^f_E$, and

$$\|\rho^f_{XDGE} - \tau^f_{XDGE}\|_1 \leq \varepsilon_{\mathsf{RUV}}(v(m), \lambda_2),$$

where $\varepsilon_{\mathsf{RUV}}(\cdot, \cdot)$ is the error bound given by Lemma 32. However, we only have the approximate guarantee on Y given by (3.1). So, by Lemma 22, we instead get that there exists a state τ^f_{XDGE} such that $\tau^f_{XE} = U_{g(m)} \otimes \tau^f_E$, and

$$\|\rho^f_{XDGE} - \tau^f_{XDGE}\|_1 \leq \varepsilon_{\mathsf{RUV}}(v(m), \lambda_2) + \frac{\varepsilon_{\mathsf{VV}}(m)}{\lambda_2}.$$

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''. □

3.5.1 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 [96] 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 32, the random seed is not required to be secure against an eavesdropper, yet the output is guaranteed to be! On the other hand, Lemma 31 below requires the assumption that the seed to the VV protocol is secure against the protocol's devices and the eavesdropper simultaneously.

Lemma 31. *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*

$$\|\rho^f_{XDE} - \tau_{XDE}\|_1 \leq \varepsilon_{\mathsf{VV}}(m),$$

[8] See 6.1.3 for more about this issue.

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 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 [96] 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 23, 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 QExt : $\{0,1\}^{|Y|} \times \{0,1\}^{d(m)} \to \{0,1\}^{h(m)/2}$ randomness extractor promised by Theorem 25, 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 a $(h(m), \varepsilon)$-quantum-secure extractor, we have that

$$\|\tilde{\rho}_{XE} - U_{v(m)} \otimes \tilde{\rho}_E\|_1 \leq \varepsilon, \tag{3.2}$$

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 $\rho^f_{\mathsf{QExt}(Y,S_2)}$. Then, by the triangle inequality, we have

$$\begin{aligned}\|\mathcal{E} \otimes \mathbb{I}_E(\rho^v_{YS_2E}) - U_{v(m)} \otimes \rho^f_E\|_1 \leq & \|\mathcal{E} \otimes \mathbb{I}_E(\rho^v_{YS_2E}) - \mathcal{E} \otimes \mathbb{I}_E(\tilde{\rho}_{YS_2E})\|_1 + \\ & \|\mathcal{E} \otimes \mathbb{I}_E(\tilde{\rho}_{YS_2E}) - U_{v(m)} \otimes \tilde{\rho}_E\|_1 + \\ & \|U_{v(m)} \otimes \tilde{\rho}_E - U_{v(m)} \otimes \rho^f_E\|_1.\end{aligned}$$

Since $\mathcal{E}$ is trace-preserving, we can bound the first term by ε. The second term is bounded by ε via equation (3.2). The third term is bounded by ε because the trace distance is non-increasing with respect to the partial trace. Thus,

$$\|\rho^f_{XE} - U_{v(m)} \otimes \rho^f_E\|_1 = \|\mathcal{E} \otimes \mathbb{I}_E(\rho^v_{YS_2E}) - U_{v(m)} \otimes \rho^f_E\|_1 \leq 3\varepsilon.$$

We then apply Lemma 35 to obtain that there exists a state τ_{XDE} such that $\tau_{XE} = U_{v(m)} \otimes \rho^f_E$ and

$$\|\rho^f_{XDE} - \tau_{XDE}\|_1 \leq \sqrt{3\varepsilon}.$$

which proves the claim. □

3.5.2 Analysis of the RUV protocol

In this section, we analyze the RUV protocol. Before stating Lemma 32, it will be necessary to give formal and precise definitions of several (classical) random variables, and how they

[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., [91].

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 5.2 and [90] 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 32, 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 normalization 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 32. *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*

$$\|\rho^f_{ZDE|F=1} - \tau_{ZDE}\|_1 \leq \varepsilon_{\mathsf{RUV}}(m, \lambda),$$

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 $\|\rho^f_{ZE'|F=1} - U_{r(m)} \otimes \rho^f_{E'|F=1}\|_1 \leq \varepsilon$ implies $\|\rho^f_{ZE|F=1} - U_{r(m)} \otimes \rho^f_{E|F=1}\|_1 \leq \varepsilon$, 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
$$\|\rho_{X_{ij}E|F=1} - U_{\sqrt{t}} \otimes \rho_{E|F=1}\|_1 \leq \eta,$$
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.,,

$$\|\rho_{ZE|F=1} - U_{\sqrt{t}} \otimes \rho_{E|F=1}\|_1 \leq \eta + \delta.$$

We then invoke Lemma 35 to argue that there exists a state τ_{ZDE} such that $\tau_{ZE} = U_{\sqrt{t}} \otimes \rho_{E|F=1}$ and

$$\|\rho_{ZDE|F=1} - \tau_{ZDE}\|_1 \leq \sqrt{\eta+\delta},$$

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 26,

$$\|\rho_{X_iE|I_i=1} - U_t \otimes \rho_{E|I_i=1}\|_1 \leq \zeta.$$

It follows by Proposition 33 that, for at least a $1 - t^{-1/4}$ fraction of sub-blocks j of block i we have that

$$\|\rho_{X_{ij}EF|I_i=1} - U_{\sqrt{t}} \otimes \rho_{EF|I_i=1}\|_1 \leq \mu,$$

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

$$\|\rho_{X_{ij}E|I_i=1,F=1} - U_{\sqrt{t}} \otimes \rho_{E|I_i=1,F=1}\|_1 \leq \frac{\mu}{\Pr(F=1)} \leq \frac{\mu}{\lambda} \tag{3.3}$$

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 $\sum_{i\in[M]} \mathcal{E}[I_i = 0|H = 1] \leq \nu M$. 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 27, $\Pr(H = 0, F = 1) \leq t^{-2}$. Thus

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

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,

$$\begin{aligned}\|\rho_{X_iE|F=1} - \rho_{X_iE|I_i=1,F=1}\|_1 &= \|(-\tau)\rho_{X_iE|I_i=1,F=1} + \tau\rho_{X_iE|I_i=0,F=1}\|_1\\ &\leq \tau(\|\rho_{X_iE|I_i=1,F=1}\|_1 + \|\rho_{X_iE|I_i=0,F=1}\|_1)\\ &\leq 2\tau.\end{aligned}$$

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

$$\|\rho_{X_iE|I_i=1,F=1} - \rho_{X_iE|F=1}\|_1 \leq 2\frac{\sqrt{\nu} + \lambda t^{-2}}{\lambda^2}$$

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

$$\|\rho_{X_{ij}E|I_i=1,F=1} - \rho_{X_{ij}E|F=1}\|_1 \leq 2\frac{\sqrt{\nu} + \lambda t^{-2}}{\lambda^2} \tag{3.4}$$

By tracing over the entire X_i register we get

$$\|\rho_{E|I_i=1,F=1} - \rho_{E|F=1}\|_1 \leq 2\frac{\sqrt{\nu} + \lambda t^{-2}}{\lambda^2} \tag{3.5}$$

Thus, at least a $(1 - t^{-1/4})(1 - \sqrt{\nu})$ of all the sub-blocks X_{ij} have the property that equations (3.3), (3.5), and (3.4) all hold. It follows by the triangle inequality that

$$\begin{aligned}\|\rho_{X_{ij}E|F=1} - U_{\sqrt{t}} \otimes \rho_{E|F=1}\|_1 &\leq \|\rho_{X_{ij}E|F=1} - \rho_{X_{ij}E|I_i=1,F=1}\|_1 + \|\rho_{X_{ij}E|I_i=1,F=1} - U_{\sqrt{t}} \otimes \rho_{E|I_i=1,F=1}\|_1\\ &\quad + \|U_{\sqrt{t}} \otimes \rho_{E|I_i=1,F=1} - U_{\sqrt{t}} \otimes \rho_{E|F=1}\|_1\\ &\leq 2\frac{\sqrt{\nu} + \lambda t^{-2}}{\lambda^2} + \frac{\mu}{\lambda} + \|\rho_{E|I_i=1,F=1} - \rho_{E|F=1}\|_1\\ &\leq 4\left(\frac{\sqrt{\nu} + \lambda t^{-2}}{\lambda^2}\right) + \frac{\mu}{\lambda}\\ &\leq \frac{96}{\lambda}t^{-1/8}.\end{aligned} \tag{3.6}$$

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

$$\|\sigma^f_{X_{ij}E'|F=1} - U_{\sqrt{t}} \otimes \sigma^f_{E'|F=1}\|_1 \leq \eta,$$

   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,

$$\begin{aligned}
\|\sigma^f_{X_{ij}E'|F=1} - U_{\sqrt{t}} \otimes \sigma^f_{E'|F=1}\|_1 &= \|\mathrm{Tr}_{\neq(i,j),D}(V\rho^f_{XDE|F=1}V^\dagger) - U_{\sqrt{t}} \otimes \mathrm{Tr}_{XD}(V\rho^f_{XDE|F=1}V^\dagger)\|_1 \\
&= \|V\left(\mathrm{Tr}_{\neq(i,j),D}(\rho^f_{XDE|F=1}) - U_{\sqrt{t}} \otimes \mathrm{Tr}_{XD}(\rho^f_{XDE|F=1})\right)V^\dagger\|_1 \\
&= \|\mathrm{Tr}_{\neq(i,j),D}(\rho^f_{XDE|F=1}) - U_{\sqrt{t}} \otimes \mathrm{Tr}_{XD}(\rho^f_{XDE|F=1})\|_1 \\
&= \|\rho^f_{X_{ij}E|F=1} - U_{\sqrt{t}} \otimes \rho^f_{E|F=1}\|_1,
\end{aligned}$$

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 $\|\sigma^f_{X_{ij}E'|F=1} - U_{\sqrt{t}} \otimes \sigma^f_{E'|F=1}\|_1 \leq \eta$ are exactly those sub-blocks that are η-good in the state ρ^f_{XFDE}.

□

Proposition 33. *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 35, there exists a state σ_{X_iFE} such that $\sigma_{X_iE} = U_t \otimes \rho_{E|I_i=1}$, and $\|\rho_{X_iFE|I_i=1} - \sigma_{X_iFE}\|_1 \leq \sqrt{\zeta}$. 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:

$$\begin{aligned}
\|\rho_{X_{ij}FE|I_i=1} - U_{\sqrt{t}} \otimes \rho_{FE|I_i=1}\|_1 &\leq \|\rho_{X_{ij}FE|I_i=1} - \sigma_{X_{ij}FE}\|_1 + \|\sigma_{X_{ij}FE} - U_{\sqrt{t}} \otimes \sigma_{FE}\|_1 \\
&\quad + \|U_{\sqrt{t}} \otimes \sigma_{FE} - U_{\sqrt{t}} \otimes \rho_{FE|I_i=1}\|_1 \\
&\leq \sqrt{\zeta} + \sqrt{4t^{-1/4}} + \sqrt{\zeta}.
\end{aligned}$$

The bound on the second term in the second inequality is given via Pinsker's Inequality (see Proposition 9), which states that $\|\sigma_{X_{ij}FE} - U_{\sqrt{t}} \otimes \sigma_{FE}\|_1 \leq \sqrt{2I(X_{ij} : FE)_\sigma}$. 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 $\sigma_{X_i FE}$ 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

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

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:

$$\begin{aligned} I(X_i : FE) &= I(X_i : E) + I(F : E|X_i) && (3.7)\\ &= I(F : E|X_i) && (3.8)\\ &\leq 2H(F) && (3.9)\\ &\leq 2. && (3.10) \end{aligned}$$

We used the fact that $\sigma_{X_i E} = \sigma_{X_i} \otimes \sigma_E$, so therefore $I(X_i : E) = 0$. The last inequalities follow from the fact that F is simply one qubit. We now lower bound the individual terms of the expectation $I(X_{ij} : FE|X_{i,<j})$.

$$\begin{aligned} I(X_{ij} : FE|X_{i,<j}) &= H(X_{ij}|X_{i,<j}) - H(X_{ij}|FEX_{i,<j}) && (3.11)\\ &\geq H(X_{ij}) - H(X_{ij}|FE) && (3.12)\\ &= I(X_{ij} : FE). && (3.13) \end{aligned}$$

Equation (3.11) is the definition of conditional mutual information. Equation (3.12) follows 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 (3.13) is again the definition of mutual information.

Thus,

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

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. □

3.5.3 Miscellaneous lemmas

Proof of Lemma 22. 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:

$$\begin{aligned} \|\rho^f_{XDE} - \mu_{XDE}\|_1 \leq &\|\mathcal{FE} \otimes \mathbb{I}_E(\rho^i_{FSXDE}) - \mathcal{FE} \otimes \mathbb{I}_E(\sigma_{FSXDE})\|_1 && (3.14)\\ &+ \|\mathcal{FE} \otimes \mathbb{I}_E(\sigma_{FSXDE}) - \mu_{XDE}\|_1. \end{aligned}$$

We bound the first term on the right hand side:

$$\|\mathcal{FE} \otimes \mathbb{I}_E(\rho^i_{FSXDE}) - \mathcal{FE} \otimes \mathbb{I}_E(\sigma_{FSXDE})\|_1 \leq \frac{1}{\lambda}\|\mathcal{E} \otimes \mathbb{I}_E(\rho^i_{FSXDE}) - \mathcal{E} \otimes \mathbb{I}_E(\sigma_{FSXDE})\|_1$$

$$\leq \frac{1}{\lambda} \| \rho^i_{FSXDE} - \sigma_{FSXDE} \|_1$$
$$\leq \delta / \lambda.$$

Let λ' denote the probability that the F register of the state $\mathcal{E} \otimes \mathbb{I}_E(\sigma_{FSXDE})$, when measured, has outcome $|1\rangle$. Note that $\max\{\lambda, \lambda'\} \geq \lambda$, so the first inequality follows from Lemma 34. 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 (3.14) is bounded by ε from our assumption on the quantum operation $\mathcal{FE}$. □

Lemma 34. *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,*

$$\| \rho_{FQ|E} - \sigma_{FQ|E} \|_1 \leq \frac{\| \rho_{FQ} - \sigma_{FQ} \|_1}{\max\{\Pr_\rho(E), \Pr_\sigma(E)\}},$$

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 $\|\rho - \sigma\|_1 = \max_A \Pr(A(\rho) = 1) - \Pr(A(\sigma) = 1)$, 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 $\Pr(B(\rho_{FQ|E}) = 1) - \Pr(B(\sigma_{FQ|E}) = 1) = \|\rho_{FQ|E} - \sigma_{FQ|E}\|_1$. 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

$$\begin{aligned}
\|\rho_{FQ} - \sigma_{FQ}\|_1 &\geq \Pr(A(\rho_{FQ}) = 1) - \Pr(A(\sigma_{FQ}) = 1) \\
&= \lambda_\rho \Pr(B(\rho_{FQ|E}) = 1) - \lambda_\sigma \Pr(B(\sigma_{FQ|E}) = 1) \\
&= \lambda_\rho \left(\|\rho_{FQ|E} - \sigma_{FQ|E}\|_1 + \Pr(B(\sigma_{FQ|E}) = 1) \right) - \lambda_\sigma \Pr(B(\sigma_{FQ|E}) = 1).
\end{aligned}$$

Solving for $\|\rho_{FQ|E} - \sigma_{FQ|E}\|_1$, we get that

$$\|\rho_{FQ|E} - \sigma_{FQ|E}\|_1 \leq \frac{\|\rho_{FQ} - \sigma_{FQ}\|_1 - \beta(\lambda_\rho - \lambda_\sigma)}{\lambda_\rho} \leq \frac{\|\rho_{FQ} - \sigma_{FQ}\|_1}{\lambda_\rho} \leq \frac{\|\rho_{FQ} - \sigma_{FQ}\|_1}{\max\{\lambda_\rho, \lambda_\sigma\}},$$

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

$$\|\rho_{FQ|E} - \sigma_{FQ|E}\|_1 \leq \frac{\|\rho_{FQ} - \sigma_{FQ}\|_1}{\lambda_\sigma} \leq \frac{\|\rho_{FQ} - \sigma_{FQ}\|_1}{\max\{\lambda_\rho, \lambda_\sigma\}}.$$

□

Lemma 35. *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 $\|\rho_{A_1A_2} - \sigma_{A_1A_2}\|_1 \leq \varepsilon$. 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 $\|\rho_{A_1A_2B} - \tau_{A_1A_2B}\|_1 \leq \sqrt{\varepsilon}$.*

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 $\mathrm{F}(\rho, \sigma)$ 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 $\mathrm{F}(\rho_A, \sigma_A) = |\langle\psi|\phi\rangle|$ [102]. But by the Fuchs-van de Graaf inequalities, we also have that $\mathrm{F}(\rho_A, \sigma_A) \geq 1 - \|\rho_A - \sigma_A\|_1/2 \geq 1 - \varepsilon/2$ [102]. Since $\|\rho_{AQ} - \sigma_{AQ}\|_1 = \sqrt{1 - |\langle\psi|\phi\rangle|^2}$, we have that

$$\|\rho_{AQ} - \sigma_{AQ}\|_1 \leq \sqrt{\varepsilon}.$$

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

$$\begin{aligned} \|\rho_{ABR} - \tau'_{ABR}\|_1 &= \|V\rho_{AQ}V^{\dagger} - V\tau'_{AQ}V^{\dagger}\|_1 \\ &= \|V(\rho_{AQ} - \tau'_{AQ})V^{\dagger}\|_1 \\ &= \|\rho_{AQ} - \tau'_{AQ}\|_1 \\ &\leq \sqrt{\varepsilon}. \end{aligned}$$

Since the trace norm cannot increase when discarding subsystems, we obtain $\|\rho_{AB} - \tau'_{AB}\|_1 \leq \sqrt{\varepsilon}$. $\tau'_{AB} = \tau'_{A_1A_2B}$ 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 $\|\rho_{A_1A_2B} - \tau_{A_1A_2B}\|_1 \leq \sqrt{\varepsilon}$, and we are done. □

3.6 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 [96] in our VV sub-protocol (see Section 3.4). 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 [96, 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 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 25 there exists a function

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 paper, 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 4

Parallel repetition of games with entangled players: an overview

In this portion of the thesis, we investigate many aspects of *parallel repetition for entangled games.*

A *two-player one-round* game is specified by finite question sets $\mathcal{X}, \mathcal{Y}$, finite answer sets $\mathcal{A}, \mathcal{B}$, a probability distribution μ over $\mathcal{X} \times \mathcal{Y}$, and a verification predicate $V : \mathcal{X} \times \mathcal{Y} \times \mathcal{A} \times \mathcal{B} \to \{0,1\}$ that determines the acceptable question and answer combinations. The game is played as follows: a referee samples questions $(x,y) \in \mathcal{X} \times \mathcal{Y}$ according to μ and sends x to the first player and y to the second. Each player replies with an answer, $a \in \mathcal{A}$ and $b \in \mathcal{B}$ respectively. The referee accepts if and only if $V(x,y,a,b) = 1$, in which case we say that the players win the game. The *value* of the game, denoted by $\mathrm{val}(G)$, is the maximum winning probability over all strategies where each player's answer is a function of their respective question. Mathematically, we define it as follows:

$$\mathrm{val}(G) = \sup_{f,g} \sum_{x,y} \mu(x,y) \sum_{a,b} V(x,y,f(x),g(y))$$

where the supremum is over functions $f : \mathcal{X} \to \mathcal{A}$ and $g : \mathcal{Y} \to \mathcal{B}$. These functions constitute the *deterministic strategy* of Alice and Bob.

A natural operation on a game is *parallel repetition*: given a game G, its n-fold parallel repetition G^n is a game where the referee samples $(x_1,y_1),\ldots,(x_n,y_n)$ independently according to G, sends $(x_1,\ldots,x_n)$ to the first player and $(y_1,\ldots,y_n)$ to the second player, who in turn respond with answer tuples $(a_1,\ldots,a_n)$ and $(b_1,\ldots,b_n)$. The players win G^n if $V(x_i,y_i,a_i,b_i) = 1$ for all i. A fundamental question concerns the relationship between $\mathrm{val}(G)$ and $\mathrm{val}(G^n)$. Intuitively, if $\mathrm{val}(G) < 1$, then one would expect that $\mathrm{val}(G^n)$ decays exponentially in n. The starting point of this work is Raz's parallel repetition theorem [88], which confirms this intuition:

Theorem 36 (Raz). *Let G be a two-player game with* $\mathrm{val}(G) = 1 - \varepsilon$. *Then*

$$\mathrm{val}(G^n) \leq \left(1 - \varepsilon^3\right)^{-cn/s}, \tag{4.1}$$

where $s = \log(|\mathcal{A}| \cdot |\mathcal{B}|)$ and $c > 0$ is a universal constant.

If the players treat each instance of G in the repeated game G^n independently (i.e. use a *product strategy*), then clearly their winning probability is at most $\mathrm{val}(G)^n$. However, the players are not constrained to use product strategies, and can use correlated strategies with which they can win G^n with probability strictly greater than $\mathrm{val}(G)^n$ (e.g., as described in [45, 89]). Raz's theorem shows that even though such correlated strategies can offer some advantage compared to product strategies, the players success probability must decay exponentially with the number of repetitions.

The main application of Raz's parallel repetition theorem is to the areas of *hardness of approximation* and *probabilistically checkable proofs*. The famous *PCP Theorem* [6] can be formulated in terms of two-player games: there exists an $\varepsilon_0 > 0$ (think of it as being very tiny, such as smaller than 0.0001) such that it is NP-hard to approximate the (classical) value of a game G within an additive error of ε_0. The parallel repetition theorem gives a blackbox method to amplify this inapproximability: we can then conclude that for any $\varepsilon > 0$ it is NP-hard to approximate the classical value of a game G within an additive error $1 - \varepsilon$. Since the value of a game is a number between 0 and 1, this implies strong inapproximability for games. From this, optimal inapproximability results for various natural optimization problems can be obtained [52, 38]. Furthermore, the information-theoretic techniques used in the proof of the parallel repetition theorem have also been heavily used in *direct sum* and *direct product* results in communication complexity [23, 59].

Entangled games. The study of games where the players share entanglement – which we call *entangled games* – was initiated in a seminal paper of Cleve, et al [29]. This work was motivated by both the importance of games in the context of Bell inequalities and non-locality, as well as the central role of games in complexity theory, a seemingly entirely unrelated field. The intermingling of computational complexity theory and non-locality has proved to be a fascinating line of research (see, e.g., [100, 47, 62, 79]).

Now the important quantity associated with a two-player game is its *entangled value*, denoted by $\mathrm{val}^*(G)$. This is the maximum success probability that non-communicating players can achieve when using an entangled strategy. More precisely, an entangled strategy for Alice and Bob consists of an integer $d > 0$, a shared entangled state $|\psi\rangle \in \mathbb{C}^{d \times d}$, and collections of measurement operations for Alice and Bob individually: Alice has POVMs $\{A_x^a\}_{a \in \mathcal{A}}$ for every $x \in \mathcal{X}$, and Bob has $\{B_y^b\}_{b \in \mathcal{B}}$ for every $y \in \mathcal{Y}$. Since these are POVMs, we have $\sum_a A_x^a = \mathbb{I}$ and $\sum_b \mathcal{B}_y^b = \mathbb{I}$. Then we define the entangled value to be

$$\mathrm{val}^*(G) = \sup_{\substack{d, |\psi\rangle \in \mathbb{C}^{d \times d} \\ \{A_x^a\}, \{B_y^b\}}} \sum_{x,y} \mu(x,y) \sum_{a,b} \langle \psi | A_x^a \otimes \mathcal{B}_y^a | \psi \rangle \cdot V(x,y,a,b)$$

where the supremum is over a dimension d, a shared entangled state $|\psi\rangle$, and measurements for Alice and Bob. From this point on we shall call $\mathrm{val}(G)$ the *classical value* of a game G, to contrast it with the entangled value of G.

For all games G, the relationship $\mathrm{val}(G) \leq \mathrm{val}^*(G)$ is always true: this is because for every deterministic strategy $f : \mathcal{X} \to \mathcal{A}, g : \mathcal{Y} \to \mathcal{B}$ of Alice and Bob, we obtain an "entangled strategy" where the shared "state" is one-dimensional: $|\psi\rangle = 1$. The measurements are defined to be $A_x^a = 1$ iff $f(x) = a$ and $B_y^b = 1$ iff $g(y) = b$. However, for there are games G for which $\mathrm{val}(G)$ is strictly less than $\mathrm{val}^*(G)$; the CHSH game is one famous example.

Parallel repetition of entangled games. Due to the outsized influence of Raz's parallel repetition theorem on the field of classical complexity theory, it became natural to ask whether there is an analogue of his theorem for entangled games. That is, for a game G where $\mathrm{val}^*(G) < 1$, does $\mathrm{val}^*(G^n)$ decay exponentially with n? We call the assertion that this is true the **Quantum Parallel Repetition Conjecture**.

The Quantum Parallel Repetition Conjecture has been studied extensively for many special classes of games, and has been affirmatively established in each of these classes. However, whether an exponential-decay bound holds for *all* two-player games G remains open. In fact, until the work presented in this thesis, it was not known whether $\mathrm{val}^*(G^n)$ tends to 0 with growing n, if $\mathrm{val}^*(G) < 1$.

In this chapter, I will briefly survey the previous results on the parallel repetition of entangled games. Then, I will give an overview of the parallel repetition results in this thesis.

4.1 Previous work

XOR games. The parallel repetition of entangled games was first studied by Cleve, et al [30], who proved that *XOR games* with entangled players satisfy *perfect parallel repetition*. In an XOR game, Alice and Bob output single bits a, b as answers, and the verification predicate depends only on their questions and the parity $a \oplus b$. Though simple, XOR games actually capture difficult problems in classical complexity theory: Håstad showed that approximating the value of an XOR game is NP-hard [52]. By perfect parallel repetition, we mean that for all two-player XOR games G and for all n, we have $\mathrm{val}^*(G^n) = \mathrm{val}^*(G)^n$. Interestingly, this elegant "tensorization" property of the entangled value of XOR games does not hold for the classical value. This tensorization property comes from the fact that the entangled value of an XOR game can be exactly expressed as the value of a semidefinite program (SDP), and the SDP has nice tensorization properties.

Unique games. Next, Kempe, Regev, and Toner studied the parallel repetition of entangled *unique games* [64]. A unique game G is one where for every question pair (x, y) there exists a bijection $\pi_{x,y} : \mathcal{A} \to \mathcal{B}$ such that $V(x, y, a, b) = 1$ if and only if $\pi_{x,y}(a) = b$. The famous Unique Games Conjecture of Khot [66] asserts, roughly speaking, that for every ε and δ it is NP-hard to determine whether a given unique game G is such that $\mathrm{val}(G) \leq \varepsilon$ or $\mathrm{val}(G) \geq 1 - \delta$, promised that one is the case. First, [64] showed that approximating the *entangled value* of a unique game is polynomial-time computable, thus refuting a quantum version of the Unique Games Conjecture (unless P = NP). This is again due to semidefinite programming, although its use is more involved than in [30]. Regarding parallel repetition, [64] are able to leverage their SDP relaxation for the entangled value of unique games to prove that $\mathrm{val}^*(G^n) \leq (1 - \varepsilon^2/16)^n$ if $\mathrm{val}^*(G) = 1 - \varepsilon$ for a unique game G.

The Dinur-Reingold transformation. Kempe and Vidick proved one of the first generally applicable parallel repetition results for entangled games [65]. However, is *not* a parallel repetition theorem for general entangled games. Rather, they give a method that transforms a game G with entangled value $\mathrm{val}^*(G) = 1 - \varepsilon < 1$ into another game $G_{DR(n)}$ – called the n'th "Dinur-Reingold repetition" of G – whose entangled value is polynomially small in n and ε. Thus the transformation $G \mapsto G_{DR(n)}$ behaves analogously to $G \mapsto G^n$; the entangled value of the output game is much smaller than the entangled value of the input game.

This transformation, called the Dinur-Reingold transformation, is simple. First, we assume that the game G is *symmetric*, meaning that the marginal distribution of each players' questions are the same (so in particular, they both receive questions from the same question set). We can view the Dinur-Reingold transformation as a two-step process: first a game G is transformed into G_{DR}, which behaves in the following way:

1. The referee randomly chooses whether to play a "game round", a "consistency round", or a "confuse round", each with some probability.
2. In a game round, the referee will play the original game G; that is, it will choose questions $(x, y) \sim \mu$ and accept or reject using the verification predicate V.
3. In a confuse round, the referee chooses x and y independently from their respectively marginals in μ, and sends them to the players. The referee always accepts in a confuse round.
4. In a consistency round, the referee samples a question x from one of the players' marginals (which, by the symmetry assumption, is the same for both players), and sends x to both players. The referee accepts only if the answers of both players match.

Finally, the final game $G_{DR(n)}$ is simply G_{DR}^n, the n'th parallel repetition of G_{DR}. Clearly, the transformation $G \mapsto G_{DR(n)}$ is polynomial-time computable.

However, this transformation is not a general gap amplification technique. In particular, it isn't *completeness preserving*: if $\text{val}^*(G) = 1$, it is not necessarily the case that $\text{val}^*(G_{DR(n)}) = 1$. This is because of the "consistency rounds": passing the consistency rounds with probability 1 forces the players to have perfectly correlated answers when asked the same question. At a high level, this induces a "global assignment" to all the questions, and thus reduces the players' strategies to being more classical. Indeed, if $\text{val}(G) = 1$, then certainly $\text{val}^*(G_{DR}) = 1$. However, there may be a entangled strategy with value 1 that cannot be shoehorned to pass the consistency rounds with probability 1.

Nonetheless, for many games of interest, the Dinur-Reingold transformation *is* completeness preserving. For example, if the *classical value* $\text{val}(G)$ is equal to 1, then $\text{val}^*(G_{DR(n)}) = 1$. This is useful for multiprover proof systems where, in the "YES" case, the provers can use some deterministic strategy (based on, say, a satisying assignment to a SAT formula) to succeed in the protocol with probability 1, but in the "NO" case, we would like to guarantee soundness against cheating entangled provers.

The analysis of the Dinur-Reingold repetition of a game G in [65] is quite involved. It actually proves something much stronger than just reduction of the entangled value: it shows that any entangled strategy for $G_{DR(n)}$ that performs well must have a *serial structure*, that is, it plays many of the rounds of G_{DR}^n in a sequential fashion. Of course, once the strategy is identified as behaving sequentially, the decrease in game value follows nearly immediately (intuitively speaking).

Kempe and Vidick also analyze the *Feige-Kilian transformation*, which is just like the Dinur-Reingold transformation, except it only has "game rounds" and "confuse rounds". It is easy to see that, unlike the Dinur-Reingold transformation, the Feige-Kilian transformation *is* completeness preserving. However, Kempe and Vidick could only analyze the Feige-Kilian transformation on *projection games*, which are games where for every answer of Alice, there is at most one answer of Bob that would be accepted by the referee. Projection games are the most important types of games considered in hardness of approximation.

The Feige-Kilian and Dinur-Reingold transformations originated in classical complexity theory. The Dinur-Reingold transformation was used to obtain an alternative proof of the PCP Theorem [37]. Before Raz's parallel repetition theorem, Feige and Kilian proved [44] that one could apply the Feige-Kilian transformation to obtain a gap amplification method that achieves *polynomial decay*: the decrease in game value as a function of the number of repetitions n is inverse polynomial, whereas the optimal rate of decrease is inverse exponential. An important conceptual contribution of [44] is that, to obtain gap amplification, one need not stick with the vanilla parallel repetition technique. It was – and still remains – a difficult procedure to analyze. Thus, one can try to shortcut the difficulties by changing the game into a more amenable format first, before using parallel repetition. This foreshadows the core motivation for "anchored games", one of the contributions of this thesis.

Free games. Up to this point, the proofs of parallel repetition for entangled games have bore little resemblance to the proof of Raz's parallel repetition theorem. The analysis used in Raz's proof (and most subsequent proofs of parallel repetition [55, 87, 22]) is information-theoretic, while the previous results used semidefinite programming (in the case of [30, 64]), or proved stronger structural results about the players' strategies (in the case of [65]). However, the SDP techniques appear limited to special classes of games, and the analytical techniques of [65] depend heavily on the extra consistency/confuse questions of the Feige-Kilian/Dinur-Reingold transformations. One would hope that the tools of quantum information theory would be as efficacious in solving the general quantum parallel repetition problem as *classical* information theory was for classical parallel repetition.

In 2014, the first information theory-based proofs of parallel repetition for entangled games emerged. Chailloux and Scarpa [24], simultaneously with Jain, Pereszlényi, and Yao [61] proved the Quantum Parallel Repetition Conjecture is true for *free games*. In a free game, the questions to Alice and Bob are independent of each other. Specifically, they prove:

Theorem 37 (Parallel repetition for free entangled games [24, 61]). *Let G be a two-player game with product question distribution $\mu(x,y) = \mu_X(x) \times \mu_Y(y)$ and entangled value* $\mathrm{val}^*(G) = 1 - \varepsilon$. *The entangled value of the n-fold repetition is upper bounded by*

$$\mathrm{val}^*(G^n) \leq (1 - \varepsilon^c)^{\Omega(n/s)},$$

where s is the length of the players' answers in G, and $c \leq 3$ is some universal constant.

The proof of Jain, et al. [61] bears the strongest resemblance to the proof strategy of Holenstein in [55]. In [24], Chailloux and Scarpa adopt an interesting communication-complexity based approach. Ultimately, when viewed in the right way, both [61] and [24] prove Theorem 37 in essentially the same way.

Projection games. An exponential-decay parallel repetition theorem for projection games was proved by Dinur, Steurer, and Vidick [39]. This work is the quantum extension of the work of Dinur and Steurer [38], who develop an analytical framework for proving an improved parallel repetition theorem for projection games, leading to optimal inapproximability for the SET COVER problem. The analytical framework of Dinur and Steurer is very different from the information theoretic approach of Holenstein. They introduce the quantity $\text{val}_+(G)$ of a game, which is a *relaxation* of the game value $\text{val}(G)$, meaning that $\text{val}_+(G) \geq \text{val}(G)$. The benefit of dealing with this relaxation is that it is *multiplicative*, meaning that $\text{val}_+(G^2) = \text{val}_+(G)^2$. The key insight is that $\text{val}_+(G)$ is a good approximation of $\text{val}(G)$, and thus this implies that $\text{val}(G^n) \approx \text{val}(G)^n$, thus proving the parallel repetition bound.

This framework lifts beautifully to the quantum setting: Dinur, Steurer and Vidick define the quantum analogue of $\text{val}_+(G)$, denoted by $\text{val}_+^*(G)$, and show that this too is a good approximation of $\text{val}^*(G)$ with better-behaved multiplicativity properties. Another key contribution of their proof is *quantum correlated sampling technique*. This is the quantum analogue of classical correlated sampling, which is an integral part of Raz's and Holenstein's proofs of parallel repetition.

It is an intriguing question for whether this framework can be used to analyze *general games*, even in the unentangled setting. However, the analytical framework seems quite tailored for projection games.

4.2 Parallel repetition of games without entanglement

Before delving into parallel repetition for games with entangled players, it is useful (and perhaps necessary) to consider how parallel repetition for games with *unentangled* players is proved.

The difficulty of proving that $\text{val}(G^n)$ decreases with n for a game G such that $\text{val}(G) < 1$ is that sometimes $\text{val}(G^n)$ *does not* decrease from $\text{val}(G)$ at all! This phenomenon is succinctly illustrated by the following example, called *Feige's Counterexample* (which is a simplification of Fortnow's counterexample [48]). This is a two-player game G for which $\text{val}(G) = \frac{1}{2}$, but $\text{val}(G^2) = \frac{1}{2}$. This immediately shows that the naive guess that $\text{val}(G^n) = \text{val}(G)^n$ is incorrect.

4.2.1 Feige's Counterexample

In this game, Alice and Bob get uniformly random bits x, y respectively. Alice outputs (i, a) and Bob outputs (j, b). The outputs i and j indicate "Alice" or "Bob". In order to win, it must be that $i = j$, and if $i = j =$ "Alice", then a must be equal to b must be equal to x. Otherwise, if $i = j =$ "Bob", then a must be equal to b must be equal to y. In other words, in this game, the players have to agree on whose input they're talking about, and both players must output a guess for that players' output. The value of this game is equal to $\frac{1}{2}$; this is because at least one player must be guessing the other person's input, and can succeed with probability at most $\frac{1}{2}$. On the other hand, the deterministic strategy where both players output ("Alice", 0) suceeds with probability $\frac{1}{2}$.

In the repeated game G^2, Alice gets two inputs (x_1, x_2), and Bob gets (y_1, y_2). Now consider the following strategy: For the first game, Alice outputs ("Bob", x_2) and Bob outputs ("Bob", y_1), and for the second game, Alice outputs ("Alice", x_2) and Bob outputs ("Alice", y_1). The probability that Alice and Bob win the first game is $\frac{1}{2}$, because we require that $x_2 = y_1$. Conditioned on this event, however, Alice and Bob will win the second game with certainty, and thus $\text{val}(G^2) = \frac{1}{2}$.

Observe that this strategy is a *non-product* strategy: to play the first game, Alice uses her input from the second game, which ostensibly has no business with the first game whatsoever! This non-product structure is necessary, however; any product strategy can succeed with probability at most $\text{val}(G)^2$. The existence of these non-product strategies for games is the confounding difficulty for parallel repetition, because they disrupt the original independence between games.

4.2.2 How to prove parallel repetition

Let us delve more deeply into the difficulty presented by non-product strategies. Let G be an arbitrary two-player game where $\text{val}(G) < 1$, and we have $\text{val}(G^n) \gg \text{val}(G)^n$ for very large n. For now we will be somewhat informal and leave "$\gg$" and "very large" unquantified.

Fix an optimal strategy for G^n. This is a pair of functions $f^{[n]} : \mathcal{X}^n \to \mathcal{A}^n$ and $g^{[n]} : \mathcal{Y}^n \to \mathcal{A}^n$. We will work in the probability space induced by the choices of random choices of questions $(x_1, y_1), \ldots, (x_n, y_n)$, all drawn independently from the question distribution μ. Let W_i denote the event that, using the optimal strategy, the players win the i'th coordinate. Then, via the chain rule:

$$\text{val}(G^n) = \Pr(W_1 \wedge \cdots \wedge W_n) = \Pr(W_1) \cdot \Pr(W_2 | W_1) \cdots \Pr(W_n | W_{n-1} \wedge \cdots \wedge W_1). \quad (4.2)$$

The probability $\Pr(W_1)$ must be bounded above by $\text{val}(G)$: if the players had a strategy for G^n where the first coordinate was won with probability strictly greater than $\text{val}(G)$, then the players could use the following strategy to play single-shot game G: given inputs (x, y), Alice pretends $x_1 = x$, Bob pretends $y_1 = y$, and using public randomness, Alice and Bob sample $(x_2, y_2), \ldots, (x_n, y_n)$ independently from μ. Then, Alice computes $(a_1, \ldots, a_n) = f^{[n]}(x_1, \ldots, x_n)$ and outputs a_1. Bob computes $(b_1, \ldots, b_n) = g^{[n]}(y_1, \ldots, y_n)$ and outputs b_1. It is not difficult to see that the probability Alice and Bob win is precisely equal to $\Pr(W_1)$. But this is a contradiction, since this implies that we have a strategy for G that does better than $\text{val}(G)$.

However, the fact that $\text{val}(G^n) \gg \text{val}(G)^n$ implies that, for an *average* i, the quantity $\Pr(W_i | W_{<i})$ is significantly closer to 1 than it is to $\text{val}(G)$, where $W_{<i} = W_{i-1} \wedge \cdots \wedge W_1$. We cannot use the argument from the previous paragraph to obtain a contradiction, however. In Feige's counterexample, say, we have that $\Pr(W_2 | W_1) = 1$. Now we need to use that the number n of repetitions is large. Essentially, we need to derive a contradiction from the fact that $\Pr(W_i | W_{<i})$ is large for *many* coordinates i.

To obtain a contradiction, we wish to construct a strategy for the single-shot game G that "embeds" it into an average coordinate i in the repeated game G^n, *conditioned* on the event $W_{<i}$. By this, we mean that, on input (x, y), Alice and Bob first pretend that $(x_i, y_i) = (x, y)$. Using a combination of public and private randomness, they sample "fake questions" (x_{-i}, y_{-i}) in such a way that the resulting distribution on $(x_1, y_1), \ldots, (x_n, y_n)$, is close to their distribution in the game G^n conditioned on the event $W_{<i}$. Clearly, if they are able to do this, then using the strategy $(f^{[n]}, g^{[n]})$ on these fake questions and (x_i, y_i), the probability they produce answers that win the ith round will be close to $\Pr(W_i | W_{<i})$.

The main difficulty, now, is that conditioning on the event $W_{<i}$ introduces correlations across coordinates. For example, even though y_i was originally independent of y_{-i}, in the event $W_{<i}$, they may no longer be independent. Thus, Alice and Bob cannot jointly sample (x_{-i}, y_{-i}) conditioned on $W_{<i}$, because otherwise Alice could "know" something about y_i through y_{-i}, which would violate the non-communication property. That is, the event $W_{<i}$ introduces some spurious *dependencies* between the players' questions, as well as across coordinates.

In the actual analysis, the event we will condition on will not be $W_{<i}$ in general, but some event $W_C = \bigwedge_{j \in C} W_j$ for some subset $C \subset [n]$. The subset C will be chosen in a way such that $\Pr(W_i | W_C) \gg \mathrm{val}(G)$ (that is, it is much closer to 1 than it is to $\mathrm{val}(G)$) for most $i \in [n] \backslash C$.

Dependency-breaking variables. The solution by Holenstein is to use so-called *dependency-breaking variables* [55] (though he did not use that name in his paper). Suppose the the players want to embed the game G into the ith coordinate of G^n, conditioned on an event W_C. We shall use $\mathsf{P}_{X^n Y^n A^n B^n}$ to denote the global probability distribution of the players' questions and answers in the game G^n, when they use the strategy $(f^{[n]}, g^{[n]})$. A dependency-breaking variable R is one such that we have the factorization

$$\mathsf{P}_{X_i Y_i A_i B_i R | W_C} = \mathsf{P}_{X_i Y_i | W_C} \times \mathsf{P}_{R | X_i Y_i W_C} \times \mathsf{P}_{A_i | X_i R W_C} \times \mathsf{P}_{B_i | Y_i R W_C}, \tag{4.3}$$

where $\mathsf{P}_{X_i Y_i A_i B_i R | W_C}$ represents the joint probability distribution of the players' questions and answers in the i'th coordinate, as well as the dependency-breaking variable R (to be defined later), conditioned on the event W_C.[1] I call this factorization the **Usefulness** property of the random variable R.

The first important lemma to use is that, for an average i, the distribution $\mathsf{P}_{X_i Y_i | W_C} \approx \mathsf{P}_{X_i Y_i}$, where by "$\approx$" we mean closeness in statistical distance. The intuition behind this is this: since we are assume that $\mathrm{val}(G^n)$ is "too large", this implies that the probability of W_C is also "too large". The following, which we call *Raz's Lemma*, formalizes this: it states that in a probability space where the random variables $U_1, U_2, \ldots, U_n$ are initially independent, after conditioning on a "not-too-small" probability event E, the marginal distribution of a typical $U_i | E$ is close in statistical distance to U_i:

Lemma 38 (Raz's Lemma, basic version [55]). *Let $U_1, \ldots, U_n$ be independent random variables in a probability space. Let E be an event in the probability space. Then*

$$\frac{1}{n} \sum_{i=1}^{n} \|\mathsf{P}_{U_i | E} - \mathsf{P}_{U_i}\|_1 \leq \sqrt{\frac{1}{n} \log \frac{1}{\mathsf{P}(E)}}.$$

Thus in the factorization (4.3), $\mathsf{P}_{X_i Y_i | W_C}$ can be replaced by $\mathsf{P}_{X_i Y_i}$ with small error, but notice that $\mathsf{P}_{X_i Y_i}$ is simply the original game distribution μ.

Now suppose that, upon receiving questions $(x, y) \sim \mu$, Alice and Bob were able to jointly sample r from the distribution $\mathsf{P}_{R | X_i Y_i W_C}$. Then, the factorization (4.3) implies that Alice and Bob would be able to sample from $\mathsf{P}_{A_i B_i | X_i = x, Y_i = y, R = r, W_C} = \mathsf{P}_{A_i | X_i = x, R = r, W_C} \times \mathsf{P}_{B_i | Y_i = y, R = r, W_C}$, because Alice can sample A_i independently of Bob, and Bob can sample B_i independently of Alice.

The joint distribution of their questions and answers is:

$$\begin{aligned} \mathsf{P}_{X_i Y_i} \times \mathsf{P}_{R | X_i Y_i W_C} \times \mathsf{P}_{A_i | X_i R W_C} \times \mathsf{P}_{B_i | Y_i R W_C} &\approx \mathsf{P}_{X_i Y_i | W_C} \times \mathsf{P}_{R | X_i Y_i W_C} \times \mathsf{P}_{A_i B_i | X_i Y_i R W_C} \\ &= \mathsf{P}_{X_i Y_i R A_i B_i | W_C} \end{aligned}$$

where in the first approximation we used Raz's Lemma and the factorization of (4.3). The probability of the event W_i in the the latter distribution, however, is equal to $\Pr(W_i | W_C) > \mathrm{val}(G)$. We have arrived at a contradiction, because we have just described a strategy

[1] The semantics of the P notation are covered in Chapter 2.

(assuming that $\mathsf{P}_{R|X_iY_iW_C}$ is jointly sampleable by Alice and Bob) for the game G that wins with probability greater than $\mathrm{val}(G)$.

The remaining question is how the dependency-breaking variable R is sampled. While it will not be true that $\mathsf{P}_{R|X_iY_iW_C}$ is *exactly* jointly sampleable, it will be *approximately* so. The dependency-breaking variable will satisfy what I call the **Sampleability** property: using the fact that $\Pr(W_C)$ is too large, we will get that $\mathsf{P}_{R|X_iY_iW_C} \approx \mathsf{P}_{R|X_iW_C} \approx \mathsf{P}_{R|Y_iW_C}$. That is, the distribution of R conditioned on the event W_C is independent of one player's question, when conditioned on the other's question. This implies that the players are able to jointly sample a consistent R that's approximately distributed according to $\mathsf{P}_{R|X_iY_iW_C}$, due to the *correlated sampling lemma*, mentioned earlier:

Lemma 39 (Correlated sampling [55]). *Let* P *and* Q *be distributions over a universe* $\mathcal{U}$ *such that* $\mathsf{P} \approx_\varepsilon \mathsf{Q}$. *Then there exists a no-communication protocol where Alice and Bob, using public randomness, output samples* p *and* q *respectively such that the marginal distribution of* p *is* P, *the marginal distribution of* q *is* Q, *and the probability that* $p = q$ *is at least* $1 - O(\varepsilon)$. *Furthermore, Alice's actions only depend on* P, *and Bob's actions only depend on* Q.

Proof. Alice and Bob use an infinite amount of shared random bits, and interpret the randomness as an infinite sequence of $(a_1, u_1), (a_2, u_2), \ldots$, where each (a_j, u_j) is uniformly distributed in $[0,1] \times \mathcal{U}$. Alice outputs the first sample u_j such that $a_j \le \Pr_{\mathsf{P}}(u_j)$. Bob similarly outputs the first u_k such that $a_k \le \Pr_{\mathsf{Q}}(u_k)$. Clearly, Alice's output is distributed according to P, and Bob's output is distributed according to Q. The probability that $j < k$ is if a_j falls in the region where $\Pr_{\mathsf{P}}(u_j) > \Pr_{\mathsf{Q}}(u_j)$; similarly, the probability that $j > k$ is if a_k falls in the region where $\Pr_{\mathsf{Q}}(u_k) > \Pr_{\mathsf{P}}(u_k)$. This probability this happens is at most

$$\sum_{u \in \mathcal{U}} |\Pr_{\mathsf{P}}(u) - \Pr_{\mathsf{Q}}(u)| = 2\|\mathsf{P} - \mathsf{Q}\|_1 \le 2\varepsilon.$$

□

The players can use the correlated sampling protocol from Lemma 39 to jointly sample from $\mathsf{P}_{R|X_iY_iW_C}$: Alice's output will be distributed according to $\mathsf{P}_{R|X_iW_C}$, and with probability $1 - O(\varepsilon)$, Bob's output will be the same as Alice's, where $\varepsilon = \|\mathsf{P}_{R|X_iW_C} - \mathsf{P}_{R|Y_iW_C}\|_1$. But $\mathsf{P}_{R|X_iW_C}$ is close to $\mathsf{P}_{R|X_iY_iW_C}$, so therefore Alice and Bob's sample will be consistent and approximately distributed correctly with high probability.

Thus, given a dependency-breaking variable R satisfying the Usefulness and Sampleability properties, we would obtain a contradiction, therefore implying that $\Pr(W_C)$ (and thus $\mathrm{val}(G^n)$) cannot be too large. All that remains is to exhibit such a variable R.

In words, the variable R is defined as follows: it fixes the questions and answers for Alice and Bob for the coordinates indexed by the subset C. Then, for every other coordinate $j \in [n] \backslash (C \cup \{i\})$, R will fix either X_j or Y_j with equal probability, and leaves the other question unfixed.

Formally, we define $R = (X_C, Y_C, A_C, B_C, \Omega_{-i})$. The variables X_C, Y_C, A_C, B_C correspond to the players' answers and questions in the C-coordinates. The variable Ω_{-i} consists of a sequence of coordinate variables Ω_j for $j \in [n] \backslash (C \cup \{i\})$. Each $\Omega_j = (D_j, M_j)$, where D_j is uniformly distributed in $\{Alice, Bob\}$, and

$$M_j = \begin{cases} X_j & \text{if } D_j = Alice \\ Y_j & \text{if } D_j = Bob. \end{cases}$$

That is, the variable M_j is coupled to either X_j or Y_j, depending on the value of D_j.

Proposition 40. *R satisfies the Usefulness and Sampleability properties.*

Proof. The proof of this can be found in, e.g., [55]. We remark that this proof crucially relies on the fact that (a) there are two players, and (b) the players' strategies are deterministic. □

The idea of defining a dependency-breaking variable in this way (i.e., fixing at least one out of two questions in every coordinate) originates from the seminal work of Bar-Yossef, et al. [7] in their information-theoretic proof of the linear lower bound on the communication complexity of DISJOINTNESS. Since then, this idea of using a dependency-breaking variable has been used in all information-theoretic proofs of the parallel repetition theorem [55, 87, 22].

Astute readers may notice something that I have swept under the rug: what is this index i? All statements I have made above are true for an *average* i. When Alice and Bob try to play this embedding strategy, they will first randomly choose an index $i \in [n] \backslash C$, and proceed from there.

4.3 Parallel repetition of games with entanglement

The preceding discussion on the proof of the (classical) parallel repetition theorem serves as the starting point for the following treatment of parallel repetition of entangled games. While we don't yet have a direct analogue of Raz's parallel repetition theorem for *all* entangled games (at least, not with exponential decay), we will use key ingredients from the classical proof in the results of this thesis.

We record some basic observations. First, we have the trivial inequality $\text{val}^*(G^n) \geq \text{val}^*(G)^n$. Next, Feige's counterexample is still a counter-example even with entangled strategies: $\text{val}^*(G^2_{Feige}) = \text{val}^*(G_{Feige}) = \frac{1}{2}$. Thus, use of non-product strategies in parallel repeated games is still a source of difficulty in the entangled case.

We wish to prove a parallel repetition bound along the same lines: suppose that $\text{val}^*(G^n) \gg \text{val}^*(G)^n$. Fix an optimal entangled strategy for G^n (we call this the "repeated strategy"), which consists of a shared entangled state $|\psi\rangle$ and measurements for Alice and Bob. There exists a set of coordinates $C \subset [n]$ that is not too large such that, for an average i, $\Pr(W_i | W_C) \gg \text{val}^*(G)$, under this optimal strategy. We wish to extract from the repeated strategy a strategy for the single-shot game G where the players attempt to embed their question (x, y) into the i'th coordinate of the game G^n, conditioned on W_C, and thus win with probability greater than $\text{val}^*(G)$, a contradiction.

The issue is this: when Alice and Bob receive x and y respectively, they will try to play the optimal repeated strategy for G^n conditioned on $X_i = x$, $Y_i = y$, and the event W_C as before. However, to play this conditioned repeated strategy, it no longer suffices for the players to sample fake inputs (x_{-i}, y_{-i}). The probability space in the game G^n now involves the results of measurements made by the players on their shared entangled state $|\psi\rangle$, which in general is not a deterministic function of their questions. Thus, conditioning the probability space on the event W_C corresponds to "conditioning" $|\psi\rangle$ on the W_C – it is not clear *a priori* what this means.

Ultimately, though, the players need to have access to *some* sort of shared entanglement $|\Phi_{x,y}\rangle$ that "simulates" the environment in G^n corresponding to the event W_C and $X_i =$

$x, Y_i = y$. We call the $|\Phi_{x,y}\rangle$ *dependency-breaking states*. Each of [61, 24, 39, 27, 11, 105] all explore different ways to define dependency-breaking states, and different methods to analyze them. At a high level, though, they all argue for analogues of the Usefulness and Sampleability properties:

1. **Usefulness**: Given $|\Phi_{x,y}\rangle$ which is shared between Alice and Bob, Alice can perform a measurement depending on x on her part of the state, Bob performs a measurement depending on y on his part of the state, and the joint distribution of their measurement outcomes will be distributed close to $\mathrm{P}_{A_iB_i|X_i=x,Y_i=y,W}$.

2. **Sampleability**: There exists a shared entangled state $|\Phi\rangle$ and unitaries U_x, V_y such that $U_x \otimes V_y|\Phi\rangle$ is close in trace distance to $|\Phi_{x,y}\rangle$.

The Sampleability property implies that, given question pair (x,y), Alice and Bob can start with the shared state $|\Phi\rangle$ and apply local operations to generate an approximation of $|\Phi_{x,y}\rangle$, in analogy with the correlated sampling procedure in the classical case. Once they have the approximation of $|\Phi_{x,y}\rangle$, the Usefulness property implies that Alice and Bob are able to make measurements that produce answers for the i'th game conditioned on $X_i = x, Y_i = y$, and the event W_C. Assuming $\mathrm{val}^*(G^n)$ is too large, this will imply that Alice and Bob can win G with probability better than $\mathrm{val}^*(G)$, a contradiction.

Sampleability is generally the more difficult property to establish. The bulk of the technical work in the chapters to follow will be focused on establishing the Sampleability property for some family of dependency-breaking states.

4.4 Summary of results

4.4.1 Parallel repetition for free entangled games, improved

The first result on quantum parallel repetition that I will present is about "free games" with entangled players. In a free game, the players' questions are chosen independently of each other. In [27], Kai-Min Chung, Xiaodi Wu and I gave improved parallel repetition theorems. We showed that for a free game G with quantum winning probability $1-\varepsilon$, the quantum winning probability of G^n is at most $(1-\varepsilon^{3/2})^{\Omega(n)}$.[2] Interestingly, there is no known classical analogue of this theorem: the best parallel repetition theorem we have for classical free games is that the winning probability of G^n is at most $(1-\varepsilon^2)^{\Omega(n)}$ [8]. This suggests that classical games and quantum games might behave differently under parallel repetition.

We obtain our improvements by exploiting a novel connection between quantum communication protocols and parallel repetition, first explored by [24]. In our analysis, we use the fact that the communication problem of DISJOINTNESS can be solved using quantum communication with only $O(\sqrt{N})$ qubits of communication (while classically it requires $\Omega(N)$ communication). The quadratic speedup in communication is what allows us to improve ε^2 to $\varepsilon^{3/2}$ for our upper bound. More generally, our result unlocks a richer toolbox for the field of hardness amplification, where one can use communication complexity results in a black-box fashion to obtain better theorems.

[2] For simplicity of exposition, I omit the alphabet dependence in the exponent.

4.4.2 Gap amplification for general entangled games via anchoring

Next, this thesis will present work conducted with Mohammad Bavarian and Thomas Vidick, in which we prove a quantum parallel repetition theorem for a new class of games which we call *anchored games* [11]. The significance of this class of games is that they are "universal" in that *any* game G can be easily transformed into an *equivalent* anchored game $G_{\perp}$, but now we can show that $G_{\perp}^n$, the n-fold parallel repetition of $G_{\perp}$, satisfies a parallel repetition theorem. More precisely, we prove the following:

Theorem 41. *There exists a polynomial-time computable transformation, called* **anchoring**, *that transforms any k-game G to a k-player game $G_{\perp}$ with the following properties: if* $\text{val}^*(G) = 1 - \varepsilon$, *then* $\text{val}^*(G_{\perp}) = 1 - \varepsilon/2$. *Furthermore, for all integer $n \geq 1$,*

$$\text{val}^*(G_{\perp}^n) \leq (1 - \varepsilon^8)^{c_k n/s}$$

where c_k is a universal constant depending on k and s is the length of the players' answers in G.

The anchoring transformation is very simple to describe: the referee samples a question tuple for the k players as he would in the game G; but then for each player i, he independently chooses with some probability to erase the player i's question and replace it with a dummy symbol "$\perp$". If at least one player receives a dummy question, then the referee automatically accepts, regardless of the players' answers. Otherwise the referee accepts or rejects based on the verification predicate of the original game G. This transformation is a simplification of the Feige-Kilian/Dinur-Reingold transformation described above. Furthermore, the transformation is completeness-preserving (unlike the Dinur-Reingold transformation used in [65]).

The anchoring transformation, combined with parallel repetition, yields an efficient gap amplification technique for entangled games with exponential decay, and in fact is the first such result for *arbitrary* entangled games – recall that the parallel repetition result of Kempe and Vidick, in addition to not preserving completeness, only obtains polynomial decay.

Although the transformation $G \mapsto G^n$ is the canonical gap amplification procedure, one of the contributions of the classical work of Feige and Kilian is the idea that, for hardness of approximation purposes, the hardness result doesn't require that the output of a gap amplification procedure be G^n *exactly*. Our anchoring parallel repetition result carries this idea over to the entangled games setting. While we still don't know that $G \mapsto G^n$ (i.e., standard parallel repetition) achieves exponential gap amplification (in the next section, we see that it achieves polynomial gap amplification), as far as gap amplification is concerned, it is no longer necessary to prove this: the transformation $G \mapsto G_{\perp} \mapsto G_{\perp}^n$ does the job.

We also prove a *threshold* version of our parallel repetition theorem:

Theorem 42. *Let G be a k-player game with* $\text{val}^*(G) = 1 - \varepsilon$, *and let $G_{\perp}$ be the anchored version of G as in Theorem 41 with* $\text{val}^*(G_{\perp}) = 1 - \varepsilon/2$. *Then for all integer $n \geq 1$ the probability that in the game $G_{\perp}^n$ the players can win more than $(1 - \varepsilon/2 + \gamma)n$ games is at most*

$$\left(1 - \gamma^9/2\right)^{c_k n/s}$$

where c_k is a universal constant depending on k and s is the length of the players' answers in G.

Another feature of our anchoring repetition is that it allows us to analyze games with more than two players. Even in the setting of classical games (i.e. the players are unentangled), it is a major open problem for whether Raz's parallel repetition theorem can be extended to more than two players. Here, the anchoring transformation sidesteps many of the difficulties that occur when studying multiplayer games, and allow us to obtain a universal gap amplification technique for them.

4.4.3 A parallel repetition theorem for general entangled games

While Theorem 41 gives a gap amplification result that works for all entangled games and has exponential decay, the original Quantum Parallel Repetition Conjecture remains as a fascinating scientific question about the limitations of quantum entanglement. As mentioned before, one might have wondered whether there exists a game G such that $\mathrm{val}^*(G) < 1$, but for all n the entangled value of G^n is lower bounded by some constant δ independent of n!

The last result of this thesis argues that this cannot happen. I show that for all nontrivial entangled games G (i.e. $\mathrm{val}^*(G) < 1$), the entangled value of G^n must converge to 0. This resolves a weaker version of the Quantum Parallel Repetition Conjecture for general games. Quantitatively, the result is the following:

Theorem 43. *Let G be a two-player one-round game with $\mathrm{val}^*(G) = 1 - \varepsilon$ and $n > 0$ be an integer. Then,*

$$\mathrm{val}^*(G^n) \lesssim c_G \varepsilon^{-17} n^{-1/4}$$

where c_G is a constant that depends on the game G, and "$\lesssim$" denotes less than, up to logarithmic factors in n.

This shows that the entangled value of G^n must decay at a polynomial rate with n. Improving this result to achieve exponential decay, and thus the full quantum analogue of Raz's Quantum parallel repetition theorem, is still open.

4.5 Application of quantum parallel repetition to the Quantum PCP Conjecture

Just as the the classical parallel repetition theorem was useful for proving hardness of approximation results, one might expect that a *quantum* parallel repetition theorem would be useful for proving *quantum* hardness of approximation results. However, we do not (yet) have a Quantum PCP theorem; as of writing this is an active field of research. Furthermore, while the classical PCP theorem has three equivalent formulations – one in terms of probabilistically checkable proofs, one in terms of hardness of approximation, and one in terms of games – the corresponding formulations of the Quantum PCP Conjecture are not known to be equivalent to one another. Thus parallel repetition may not play the same role in the Quantum PCP setting as it does in classical setting.

The following is the most standard formulation of the Quantum PCP Conjecture:

Conjecture 44 (Quantum PCP Conjecture, constraint satisfaction formulation). Let $k \geq 2$ be an integer. There is a constant $\gamma > 0$ for which the following problem is QMA-hard: Given $a, b \in [0,1]$ such that $a - b \geq \gamma$, and a k-local Hamiltonian $H = H_1 + \cdots + H_m$ acting on n qudits of local dimension d, with each term H_i satisfying $\|H_i\| \leq 1$, decide whether the smallest eigenvalue of H is at least a or at most b, promised that one is the case.

This problem is known as the k-LOCAL HAMILTONIAN problem with *constant promise gap*, where by promise gap we mean the gap γ between the thresholds a and b.[3] When the promise gap is only required to be inverse polynomial in n, then the problem is known to be QMA-complete [67]. This problem is the quantum analogue of the k-CONSTRAINT SATISFACTION problem, where given a collection of k-ary constraints over a set of variables, one has to decide whether the minimum fraction of unsatisfiable constraints is at least some number a or at most some number b. Since the classical PCP theorem can be formulated as establishing the NP-hardness of solving the k-CONSTRAINT SATISFACTION problem with a constant promise gap, it is natural to call Conjecture 44 the Quantum PCP Conjecture.

However one can consider a *games* version of the conjecture:

Conjecture 45 (Quantum PCP Conjecture, games formulation). There exists a constant $\gamma \in (0,1)$ and integers $s \geq 1, k \geq 2$ for which the following problem is QMA-hard: Given $a, b \in [0,1]$ such that $a - b \geq \gamma$, and a k-player game G where each player answers with s many bits, decide whether $\mathrm{val}^*(G) \geq a$ or $\mathrm{val}^*(G) \leq b$, promised that one is the case.

When $\mathrm{val}^*(\cdot)$ is replaced with $\mathrm{val}(\cdot)$, the above conjecture is exactly equivalent to the classical PCP theorem. It was proved by [100] that the problem of approximating the entangled value of a game is at least NP-hard.

For the remainder of this chapter, we shall refer to Conjecture 44 as the "CSP qPCP Conjecture" (or simply CSP qPCP), and Conjecture 45 as the "games qPCP Conjecture" (or simply games qPCP).

It is not known whether CSP qPCP is equivalent to games qPCP, although partial progress has been made to address this question. Fitzsimons and Vidick showed that the k-LOCAL HAMILTONIAN problem with inverse polynomial gap can be polynomial-time reduced to the problem of approximating the value of a game within an inverse polynomial additive error [46]. The type of games they reduce to involve a quantum verifier interacting with entangled players, with the verifier asking classical questions but receiving quantum answers. Later, Ji gave an efficient reduction to games where the verifier and the communication is completely classical [62]. However, none of these reductions are *gap preserving;* even if the starting local Hamiltonian instance had a constant promise gap, the resulting game only has an inverse polynomial gap. Natarajan and Vidick recently gave a gap preserving reduction from the LOCAL HAMILTONIAN problem to the problem of estimating the value of a game [79]. This would show that constraint satisfaction version of the Quantum PCP Conjecture implies games version, except that their reduction is not efficient: the size of the game (as measured by the number of questions) is *exponential* in the original local Hamiltonians instance size. However the pace of progress is rapid, and I expect that researchers will discover an efficient gap-preserving reduction soon.

As for the other direction – whether the games qPCP implies CSP qPCP – very little is known, aside from some restricted results of [49]. One of the barriers to proving this direction is that there is no general upper bound on the amount of entanglement needed to play any game optimally. For instance, it is not known in general whether there is any limit on the size of the entanglement needed to optimally play any particular game G! In fact,

[3] We won't give a formal definition of what a local Hamiltonian is; we point the reader to [3] for more details.

there is evidence that there are games G that require an infinite amount of entanglement in the optimal strategy [72]. Another significant barrier is that we do know if the entangled value of games is (approximately) computable! A reduction (even a horribly inefficient one) from computing the entangled value of a game to approximating the ground energy of a local Hamiltonian would establish the first upper bound on the complexity of games.

Though neither Conjecture 44 nor Conjecture 45 looks anywhere close to being resolved, we can nonetheless explore the consequences if they were true. We end this chapter by giving a simple application of our parallel repetition for anchored games: assuming the truth of Conjecture 45, we can boost its hardness to any desired gap between completeness and soundness:

Proposition 46. *If Conjecture 45 is true, then for all $\delta > 0$ the following problem is* QMA*-hard: given a description of a k-player game G with answer size that depends only on δ, distinguish between whether* $\mathrm{val}^*(G) \geq 1 - \delta$, *or* $\mathrm{val}^*(G) \leq \delta$, *promised that one is the case.*

Proof. Let $0 \leq b < a \leq 1$ be a promise gap satisfying the conditions in the proposition statement. Define $a' = (1+3a)/4$, and $b' = (1+3b)/4$. Consider the following reduction: given a description of a k-player game G, promised that either $\mathrm{val}^*(G) \leq b$ or $\mathrm{val}^*(G) \geq a$, outputs the description of the following *threshold game* $G_\perp^{t,\geq\tau}$: the referee plays $G_\perp^t$, the t-fold repetition of $G_\perp$, the anchored version of G, but instead accepts iff the players win at least $\tau := (a' - \frac{a'-b'}{4})t$ games. We set parameters $\Delta = (a' - b')/4$ and $t = \frac{s}{c_k} \cdot \frac{2}{\Delta^9} \cdot \ln \frac{1}{\delta}$, where s is the length of the players' outputs in G, and c_k is the universal constant from Theorem 42.

We get that if $\mathrm{val}^*(G) \geq a$, then $\mathrm{val}^*(G_\perp) \geq a'$. One strategy for $G_\perp^{t,\geq\tau}$ is for the players to play each coordinately independently using the optimal strategy for $G_\perp$. By a Chernoff-Hoeffding bound, the probability that they win at least τ games is at least

$$\mathrm{val}^*(G_\perp^{t,\geq\tau}) \geq 1 - \exp(-t\Delta^2/2) \geq 1 - \delta.$$

Otherwise, $\mathrm{val}^*(G) \leq b$. Applying Theorem 42, we get that

$$\mathrm{val}^*(G_\perp^{t,\geq\tau}) \leq (1 - \Delta^9/2)^{c_k t/s} \leq \delta.$$

Observe that this reduction is efficient: the size of the description of $G_\perp^{t,\geq\tau}$ is $O(|G|^t)$; since Conjecture 45 is true, this means that $a' - b' = \Omega(a - b) = \Omega(1)$, and thus since δ and s are constant, t is constant. The answer size of the new game is $O(1)$, still. Thus the reduction runs in time polynomial in the input instance size, so if there were an algorithm that could distinguish between $\mathrm{val}^*(G_\perp^{t,\geq\tau}) \geq 1 - \delta$ or $\mathrm{val}^*(G_\perp^{t,\geq\tau}) \leq \delta$, then this would distinguish between whether $\mathrm{val}^*(G) \geq a$ or $\mathrm{val}^*(G) \leq b$, respectively. □

We point out that we used two features of the anchoring transformation: first, that it allows us to analyze the repetition of arbitrary k-player games; second, it yields threshold theorems for parallel repetition.

Finally, we refer the reader to [3] for a more in-depth survey on the Quantum PCP Conjecture.

Chapter 5

Improved parallel repetition for free entangled games

This chapter presents work that was conducted jointly with Kai-Min Chung and Xiaodi Wu, and appeared in the Conference on Computational Complexity in 2015 under the title "Parallel repetition for entangled k-player games via fast quantum search" [27].

5.1 Introduction

The first information-theoretic proofs of parallel repetition for entangled games appeared in the independent works of Chailloux and Scarpa, and Jain, et al. [24, 61], for the class of *free games*. In a free game, the question distribution μ is a product distribution. They prove the following theorem:

Theorem 47 (Parallel repetition for free entangled games [24, 61]). *Let G be a two-player free game with entangled value* $\mathrm{val}^*(G) = 1 - \varepsilon$. *The entangled value of the n-fold repetition is upper bounded by*

$$\mathrm{val}^*(G^n) \leq (1 - \varepsilon^c)^{\Omega(n/s)},$$

where s is the length of the players' answers in G, and $c \leq 3$ is some universal constant.

In [24, 61], the constant c was proved to be at most 3. In [25], Chailloux and Scarpa gave a tighter analysis and showed that $c = 2$, matching the best classical parallel repetition theorem for free games by Barak, et al. [8].

We improve upon Theorem 47, and prove the following:

Theorem 48. *Let G be a two-player free game with entangled value* $\mathrm{val}^*(G) = 1 - \varepsilon$. *Then, for $n = \Omega(s \log(1/\varepsilon)/\varepsilon^{3/2})$,*

$$\mathrm{val}^*(G^n) \leq (1 - \varepsilon^{3/2})^{\Omega(n/s)}$$

where s is the length of the players' answers in G.

The difference between Theorem 48 and Theorem 47 is that the *rate* of parallel repetition for entangled free games is faster: the base of the bound on $\mathrm{val}^*(G^n)$ is $1 - \varepsilon^{3/2}$, which is smaller than $1 - \varepsilon^2$. Thus the rate at which $\mathrm{val}^*(G^n)$ goes to 0 is faster than what is known for the case of classical players!

The proof of Theorem 48 exploits a connection between parallel repetition and communication complexity that was developed in [24].[1] Our analysis uses a quantum communication protocol that performs a version of distributed unstructured search (i.e. searching for a 1 in a bitstring). The improvement of the base from $1 - \varepsilon^2$ to $1 - \varepsilon^{3/2}$ comes from the fact that the unstructured search problem on N bits can be solved by a quantum algorithm using only $O(\sqrt{N})$ queries. We discuss this in more detail in the next section.

5.1.1 Parallel repetition and communication protocols

At a high level, most proofs of parallel repetition proceed via reduction. Let G be a two-player free game with verification predicate $V(x, y, a, b)$. If there were a strategy for the repeated game G^n that wins with too large probability, then one can transform this repeated strategy to a strategy for the single-shot game G with success probability larger than $\mathrm{val}^*(G)$, which would be a contradiction.

As discussed in Chapter 4, the proof strategy is to define an appropriate ensemble of dependency-breaking states $|\Phi_{xy}\rangle$ that are both Useful and Sampleable. Generally, the goal is to create advice states that closely mimick the joint state of the players during an actual execution of the repeated strategy, conditioned on the event of winning a sizable fraction of coordinates.

Consider an optimal entangled strategy for G^n that uses shared entanglement $|\psi\rangle$ and measurement operators $A^{a^n}_{x^n}$ and $B^{b^n}_{y^n}$ for every x^n, y^n, a^n, b^n (question and answer tuples for the n parallel coordinates). In both [61] and [24], the dependency-breaking states $|\Phi_{xy}\rangle$ are defined as the result of an multi-step protocol. Alice and Bob first start with the state

$$\sum_{x^n, y^n} \sqrt{\mu^n(x^n, y^n)} |x^n x^n\rangle^{X^n \widetilde{X}^n} \otimes |\psi\rangle^{E_A E_B} \otimes |y^n y^n\rangle^{Y^n \widetilde{Y}^n}$$

where Alice has registers $X^n \widetilde{X}^n E_A$, and Bob has registers $E_B Y^n \widetilde{Y}^n$. This represents the state of Alice and Bob before the start of the game G^n, where their questions are given in superposition. Alice and Bob then apply the measurements from the optimal strategy, recording their measurement outcomes coherently:

$$\sum_{x^n, y^n, a^n, b^n} \sqrt{\mu^n(x^n, y^n)} |x^n x^n\rangle^{X^n \widetilde{X}^n} \otimes |\psi_{x^n y^n a^n b^n}\rangle^{E_A E_B} \otimes |y^n y^n\rangle^{Y^n \widetilde{Y}^n} \otimes |a^n b^n\rangle^{A^n B^n} \tag{5.1}$$

where $|\psi_{x^n y^n a^n b^n}\rangle = \sqrt{A^{a^n}_{x^n}} \otimes \sqrt{B^{b^n}_{y^n}} |\psi\rangle$ is the (subnormalized) post-measurement state of $|\psi\rangle$.

In both [61] and [24], the dependency-breaking state $|\Phi_{xy}\rangle$ is defined to be (5.1) conditioned on the event W_C of winning all the coordinates in a subset $C \subset [n]$, and $X_i = x, Y_i = y$ for some i.

However, [24] view this as the result of a *communication protocol* between Alice and Bob, where Alice sends her questions and answers for the coordinates in C to Bob so that Bob can compute the indicator for whether they succeeded in those games (i.e., they compute the event W_C). They define the dependency-breaking state $|\Phi_{xy}\rangle$ to be the final state of Alice and Bob after this communication protocol, *conditioned* on Bob's computation of the

[1] This connection was also presented in greater generality by Parnafes, Raz, and Wigderson in [83] for *classical* parallel repetition.

indicator for the event W_C, and Alice's i'th question is x, and Bob's i'th question is y.

If C is small, then the communication cost is small. Chailloux and Scarpa use this fact to argue that the dependency-breaking states are Sampleable: since the communication from Alice to Bob was small, and we're assuming that the probability of the event W_C is too large (because $\mathrm{val}(G^n)$ is too large), the amount of information that Bob has about Alice's question in an average coordinate i is very small. Similarly, Alice's information about Bob's i'th question is very small. We fix an i such that this is the case. This implies the existence of unitaries U_x, V_y and an initial state $|\Phi\rangle$ such that $U_x \otimes V_y|\Phi\rangle \approx |\Phi_{xy}\rangle$. The error in the approximation, which affects the final parameters of the parallel repetition theorem, is ultimately determined by the communication cost of this protocol.

Although the proof of [61] shows that this communication complexity perspective is not necessary to achieve the parameters of Theorem 47, we take this communication paradigm further to obtain a quantitative improvement: we show that if Alice and Bob engage in a *two-way* communication protocol, they can *approximately* compute the indicator for W_C using less communication than the simple protocol given above. Conditioning the final state of the protocol on this approximation of W_C yields dependency-breaking states $|\Phi_{xy}\rangle$ that can be better approximated by $U_x \otimes V_y|\Phi\rangle$ for some unitaries U_x and V_y – and hence yield better parameters for the parallel repetition.

The idea for the communication protocol is simple: Alice and Bob run a distributed version of Grover's search algorithm to search for an index $j \in C$ such that $V(x_j, y_j, a_j, b_j) = 0$. If any such index exists, then Alice and Bob conclude that W_C did not occur. Otherwise, they conclude that W_C did occur. Roughly speaking, the communication complexity of this protocol is $O(\sqrt{|C|})$, whereas the communication complexity of the simple protocol in [24] is $\Theta(|C|)$. This quadratic savings in communication is precisely what allows us to improve the base of the repeated game value from $1 - \varepsilon^2$ to $1 - \varepsilon^{3/2}$.

At the moment, we do not see a way to generalize the proof strategy of [61] to get this quantitative improvement.

Our use of quantum search in the protocol to generate the advice states gives a generic way to improve the reduction for arbitrary free games. However, one could also use this technique to prove *game-specific* parallel repetition theorems. That is, one could try to leverage special properties of a particular game to design a succinct communication protocol for generating advice states, and in turn, obtain a parallel repetition theorem with better parameters. Indeed, one can see this idea in the result of [24] for free projection games: by using the projection property of the game, their communication protocol avoids sending whole input and output symbols. This allows them to prove a repeated game value of $(1 - \varepsilon)^{\Omega(n)}$ – note that this does not depend on the output alphabet!

Finally, we note that this connection between communication complexity and parallel repetition was first explored by Parnafes, Raz and Wigderson in the context of *classical* parallel repetition [83]. They showed that for an arbitrary game G with verification predicate V,

$$\mathrm{val}(G^n) \leq \mathrm{val}(G)^{\Omega(n/c(V))}$$

where $c(V)$ is the deterministic communication complexity of computing the function $V(x, y, a, b)$, where both Alice receives as input a, Bob receives b, and both parties know (x, y). Thus, if communication complexity of *checking* whether the Alice and Bob have won game G or not is small, then the rate of decay in the repeated game is faster.

Our results is similar in spirit, except we relate the communication complexity of *searching* for a lost coordinate in a set of coordinates to the rate of decay. It would be interesting if one could establish a quantum analogue of the Parnafes-Raz-Wigderson result, even for a restricted class of games such as free games.

5.2 Preliminaries

The following lemma is due to [8]:

Lemma 49 ([8], Lemma 3.3). *Let $P = (p, 1-p)$ and $Q = (q, 1-q)$ be binary distributions. If $S(P\|Q) \leq \delta$, and $p < \delta$, then $q \leq 4\delta$.*

The following adapts Lemma 49 to use the distance measure K instead:

Lemma 50. *Let $P = (p, 1-p)$ and $Q = (q, 1-q)$ be binary distributions. If $\mathrm{h}^2(P,Q) \leq \delta$, and $p < \delta$, then $q \leq 9\delta$.*

Proof. If $q \leq p$, then we are done. Assume otherwise. We have that $\delta \geq \mathrm{h}^2(P,Q) = 1 - F(P,Q) \geq (1 - F(P,Q)^2)/2$, because $0 \leq F(P,Q) \leq 1$. $F(P,Q)^2 = (\sqrt{pq} + \sqrt{(1-p)(1-q)})^2 = pq + 1 - p - q + pq + 2\sqrt{pq(1-p)(1-q)}$, and thus

$$\begin{aligned}
2\delta &\geq p + q - 2pq - 2\sqrt{pq(1-p)(1-q)} \\
&\geq p + q - 2pq - 2\sqrt{pq} \\
&= (\sqrt{p} - \sqrt{q})^2 - 2pq \\
&\geq (\sqrt{p} - \sqrt{q})^2 - 2\delta,
\end{aligned}$$

where in the last line we used the assumption that $p \leq \delta$. Then $2\sqrt{\delta} \geq |\sqrt{p} - \sqrt{q}|$. Either $q \leq p$, in which case $q \leq \delta$, or $q \geq p$, in which case $\sqrt{q} \leq 2\sqrt{\delta} + \sqrt{p} \leq 3\sqrt{\delta}$, so $q \leq 9\delta$. □

5.3 Quantum strategy rounding

Lemma 51 ([61]). *Let μ be a probability distribution on $\mathcal{X}$. Let*

$$|\varphi\rangle := \sum_{x \in \mathcal{X}} \sqrt{\mu(x)} |xx\rangle^{XX'} \otimes |\psi_x\rangle^{AB}$$

for some set of states $\{|\psi_x\rangle\}$. Let $|\varphi_x\rangle := |xx\rangle^{XX'} \otimes |\psi_x\rangle^{AB}$. Then there exists unitary operators $\{U_x\}_{x\in\mathcal{X}}$ acting on $XX'A$ such that

$$\mathop{\mathbb{E}}_{x\sim\mu}\left[\mathrm{h}^2(\varphi_x, \mathrm{ad}_{U_x}[\varphi])\right] \leq I(X:B)_\varphi.$$

Proof. We follow the proof in [61]. Let $\rho_x := \mathrm{Tr}_{XX'A}(\varphi_x)$ and $\rho := \mathrm{Tr}_{XX'A}(\varphi)$. By Facts 8 and 11, we get that

$$I(X:B)_\varphi = \mathop{\mathbb{E}}_{x\sim\mu}[S(\rho_x\|\rho)] \geq \mathop{\mathbb{E}}_{x\sim\mu}[\mathrm{h}^2(\rho_x, \rho)].$$

By Uhlmann's Theorem, for each $x \in \mathcal{X}$ there exists U_x such that $|\langle\varphi_x|(U_x \otimes \mathbb{I}_B)|\varphi\rangle| = F(\rho_x, \rho)$. Furthermore, $|\langle\varphi_x|(U_x \otimes \mathbb{I}_B)|\varphi\rangle|$ is also equal to $F(\varphi_x, (U_x \otimes \mathbb{I}_B)\, \varphi\, (U_x^\dagger \otimes \mathbb{I}_B))$. We thus obtain the claim. □

Lemma 52. *Let $\{|\varphi_a\rangle\}_{a\in\mathcal{A}}$ be a finite collection of pure states. Let μ and τ be probability distributions over $\mathcal{A}$. Then*

$$\mathrm{h}^2(\mathop{\mathbb{E}}_{a\sim\mu}\varphi_a, \mathop{\mathbb{E}}_{a\sim\tau}\varphi_a) \leq S(\mu\|\tau).$$

Proof. Consider the states

$$|\psi^{\mu}\rangle = \sum_{a\in\mathcal{A}}\sqrt{\mu_a}|aa\rangle^{AA'}\otimes|\varphi_a\rangle$$

and

$$|\psi^{\tau}\rangle = \sum_{a\in\mathcal{A}}\sqrt{\tau_a}|aa\rangle^{AA'}\otimes|\varphi_a\rangle.$$

Let $\rho^{\mu} = \mathrm{Tr}_{A'}(\psi^{\mu})$ and $\rho^{\tau} = \mathrm{Tr}_{A'}(\psi^{\tau})$. Then notice that $\mathbb{E}_{a\sim\mu}\varphi_a = \mathrm{Tr}_{AA'}(\rho^{\mu})$ and $\mathbb{E}_{a\sim\tau}\varphi_a = \mathrm{Tr}_{AA'}(\rho^{\tau})$, respectively. We then have that, considering the partial trace as a quantum operation,

$$\mathrm{h}^2(\mathop{\mathbb{E}}_{a\sim\mu}\varphi_a, \mathop{\mathbb{E}}_{a\sim\tau}\varphi_a) \leq \mathrm{h}^2(\rho^{\mu},\rho^{\tau}).$$

By Uhlmann's Theorem, this is at most $1 - |\langle\psi^{\mu}|\psi^{\tau}\rangle| = 1 - \sum_{a\in A}\sqrt{\mu_a\tau_a} = \mathrm{h}^2(\mu,\tau)$. By Fact 8, this is at most $S(\mu\|\tau)$. □

Lemma 53 (Quantum strategy rounding). *Let $\mu = \mu_X\otimes\mu_Y$ be a product probability distribution over $\mathcal{X}\times\mathcal{Y}$. Let*

$$|\varphi\rangle := \sum_{(x,y)\in\mathcal{X}\times\mathcal{Y}}\sqrt{\mu(x,y)}|xxyy\rangle^{X\tilde{X}Y\tilde{Y}}\otimes|\varphi_{xy}\rangle^{E_AE_B}$$

Then there exist unitary operators $\{U_x\}_{x\in\mathcal{X}}$ acting on $X\tilde{X}E_A$ and $\{V_y\}_{y\in\mathcal{Y}}$ acting on $Y\tilde{Y}E_B$ such that

$$\mathop{\mathbb{E}}_{(x,y)\sim\mu}\left[\mathrm{h}^2\left(\varphi_{xy}, \mathrm{ad}_{U_x\otimes V_y}[\varphi]\right)\right] \leq 2\left[I(X:Y\tilde{Y}E_B)_{\varphi} + I(Y:X\tilde{X}E_A)_{\varphi}\right],$$

where for all $(x,y)\in\mathcal{X}\times\mathcal{Y}$, $|\varphi_{xy}\rangle := |xxyy\rangle\otimes|\varphi_x\rangle$.

Proof. Follows the same proof as in [61], except instead of using trace distance, we use the (squared) Hellinger distance. Let $|\varphi_x\rangle$ and $|\varphi_y\rangle$ denote $|\varphi\rangle$ conditioned on $X = x$ and $Y = y$, respectively. Then by Lemma 51, there exist unitaries U_x and V_y such that

$$\mathop{\mathbb{E}}_{x\sim\mu_X}\mathrm{h}^2(\varphi_x, \mathrm{ad}_{U_x}[\varphi]) \leq I(X:Y\tilde{Y}E_B)_{\varphi}$$

and

$$\mathop{\mathbb{E}}_{y\sim\mu_Y}\mathrm{h}^2(\varphi_y, \mathrm{ad}_{V_y}[\varphi]) \leq I(Y:X\tilde{X}E_A)_{\varphi}.$$

Then,

$$\begin{aligned}&\mathrm{h}^2\left(\mathop{\mathbb{E}}_{(x,y)\sim\mu}[|xy\rangle\langle xy|\otimes\varphi_{xy}], \mathop{\mathbb{E}}_{(x,y)\sim\mu_X\otimes\mu_Y}[|xy\rangle\langle xy|\otimes\mathrm{ad}_{U_x\otimes V_y}[\varphi]]\right)\\ &\leq 2\,\mathrm{h}^2\left(\mathop{\mathbb{E}}_{(x,y)\sim\mu}[|xy\rangle\langle xy|\otimes\varphi_{xy'}], \mathop{\mathbb{E}}_{(x,y)\sim\mu_X\otimes\mu_Y}[|xy\rangle\langle xy|\otimes\mathrm{ad}_{U_x\otimes\mathbb{I}}[\varphi_y]]\right) +\\ &\qquad 2\,\mathrm{h}^2\left(\mathop{\mathbb{E}}_{(x,y)\sim\mu_X\otimes\mu_Y}[|xy\rangle\langle xy|\otimes\mathrm{ad}_{U_x\otimes\mathbb{I}}[\varphi_y]], \mathop{\mathbb{E}}_{(x,y)\sim\mu_X\otimes\mu_Y}[|xy\rangle\langle xy|\otimes\mathrm{ad}_{U_x\otimes V_y}[\varphi]]\right)\end{aligned}$$

$$
\begin{aligned}
&\leq 2\,\mathrm{h}^2\left(\mathop{\mathbb{E}}_{x\sim\mu_X}[|x\rangle\langle x|\otimes\varphi_x], \mathop{\mathbb{E}}_{x\sim\mu_X}[|x\rangle\langle x|\otimes \mathrm{ad}_{U_x\otimes\mathbb{I}}[\varphi]]\right)+\\
&\qquad 2\,\mathrm{h}^2\left(\mathop{\mathbb{E}}_{(x,y)\sim\mu_X\otimes\mu_Y}[|xy\rangle\langle xy|\otimes\varphi_y], \mathop{\mathbb{E}}_{(x,y)\sim\mu_X\otimes\mu_Y}[|xy\rangle\langle xy|\otimes \mathrm{ad}_{\mathbb{I}\otimes V_y}[\varphi]]\right)\\
&= 2\mathop{\mathbb{E}}_{x\sim\mu_X}\mathrm{h}^2\left(\varphi_x, \mathrm{ad}_{U_x\otimes\mathbb{I}}[\varphi]\right)+2\mathop{\mathbb{E}}_{y\sim\mu_Y}\mathrm{h}^2\left(\varphi_y, \mathrm{ad}_{\mathbb{I}\otimes V_y}[\varphi]\right)\\
&\leq 2(I(X:Y\widetilde{Y}E_B)_\varphi + I(Y:X\widetilde{X}E_A)_\varphi).
\end{aligned}
$$

But notice that

$$
\mathrm{h}^2\left(\mathop{\mathbb{E}}_{(x,y)\sim\mu}[|xy\rangle\langle xy|\otimes\varphi_{xy}], \mathop{\mathbb{E}}_{(x,y)\sim\mu_X\otimes\mu_Y}[|xy\rangle\langle xy|\otimes \mathrm{ad}_{U_x\otimes V_y}[\varphi]]\right) = \mathop{\mathbb{E}}_{(x,y)\sim\mu}\mathrm{h}^2\left(\varphi_{xy}, \mathrm{ad}_{U_x\otimes V_y}[\varphi]\right)
$$

where we use the fact that $\mu = \mu_X \otimes \mu_Y$. This completes the proof. □

5.4 Parallel repetition using fast quantum search

We make the following observation, which will be useful for us in our analysis: without loss of generality, we can restrict our attention to free games whose input distribution is the uniform distribution over some alphabet. Let $G = (\mathcal{X}\times\mathcal{Y}, \mathcal{A}\times\mathcal{B}, \mu, V)$ be a two-player free game. Write $\mu = \mu_X \times \mu_Y$. Fix an $\gamma > 0$. There exists alphabets $\mathcal{X}'$ and $\mathcal{Y}'$ and maps $f_X : \mathcal{X}' \to \mathcal{X}, f_Y : \mathcal{Y}' \to \mathcal{Y}$ such that

$$
f_X(U_{\mathcal{X}'}) \approx_{\gamma/2} \mu_X \qquad\qquad f_Y(U_{\mathcal{Y}'}) \approx_{\gamma/2} \mu_Y
$$

where $f_X(U_{\mathcal{X}'})$ and $f_Y(U_{\mathcal{Y}'})$ denote the outputs of f_X and f_Y on the uniform distribution over $\mathcal{X}'$ and $\mathcal{Y}'$, respectively, and "$\approx_{\gamma/2}$" denotes $\gamma/2$-closeness in statistical distance. Thus the random variable $(f_X(U_{\mathcal{X}'}), f_Y(U_{\mathcal{Y}'}))$ is at most γ-far from μ. Thus, we can "simulate" the game G with another game $G' = (\mathcal{X}'\times\mathcal{Y}', \mathcal{A}\times\mathcal{B}, U_{\mathcal{X}'}\times U_{\mathcal{Y}'}, V')$, where $V' : \mathcal{X}'\times\mathcal{Y}'\times\mathcal{A}\times\mathcal{B} \to \{0,1\}$ is the map $(x', y', a, b) \to V(f_X(x'), f_Y(y'), a, b)$.

Claim 54. $\mathrm{val}^*(G') = \mathrm{val}^*(G) \pm \gamma$.

Proof. Consider the optimal strategy for G. Then a strategy for G' is the following: Alice and Bob receive $(x', y') \in (\mathcal{X}', Y')$. Alice computes $x = f_X(x')$ and Bob computes $y = f_Y(y')$. They now apply the optimal strategy for G using input pair (x, y). The input distribution, from the point of view of the strategy for G, is at most γ-far from the original input distribution μ. Thus the winning probability is at least $\mathrm{val}^*(G) - \gamma$.

Now consider the optimal strategy for G'. The strategy for G is the following: Alice and Bob receive (x, y) sampled from μ. Alice and Bob compute uniformly random preimages $x' \in f_X^{-1}(x)$ and $y' \in f_Y^{-1}(y)$, respectively, and they perform the strategy they would've used in G'. The input distribution, from the point of view of the strategy for G', is at most γ-far from the uniform distribution U. Thus the winning probability is at least $\mathrm{val}^*(G') - \gamma$. □

Furthermore, this simulation "commutes" with parallel repetition, in that $\mathrm{val}^*((G')^n) = \mathrm{val}^*(G^n) \pm \gamma n$. We can make γ arbitrarily small, at the cost of (potentially) increasing the input alphabet size, so that the behavior of the simulation G' is essentially the same as the original game G. However, since our theorems do not depend on the input alphabet size, we will treat γ as infinitesimally small, and hence neglect it.

Theorem 55. *Let G be a two-player free game. Suppose that* $\mathrm{val}^*(G) = 1 - \varepsilon$. *Then for all integer n,*

$$\mathrm{val}^*(G^n) \le (1 - \varepsilon^{3/2})^{\Omega(n/s)}.$$

where $s = \log |\mathcal{A}| \cdot |\mathcal{B}|$.

Proof. Because of Claim 54, it is without loss of generality to assume that the input distribution μ is the uniform distribution – the following analysis can be performed on a simulation of G, which will still bound the repeated game value of G.

Let n be an integer. Consider an optimal entangled strategy for G^n, and let 2^{-t} denote its winning probability. Suppose for contradiction that $t \le c\varepsilon^{3/2}n/s$ for some universal constant c. Using this strategy, we will construct the following state

$$|\rho\rangle^{X^n\tilde{X}^nEA^nB^nY^n\tilde{Y}^n} := \sum_{x^n,y^n} \sqrt{\mathsf{Q}_{X^nY^n}(x^n,y^n)}|x^nx^n\rangle^{X^n\tilde{X}^n} \otimes |\rho_{x^ny^n}\rangle^{EA^nB^n} \otimes |y^ny^n\rangle^{Y^n\tilde{Y}^n}$$

where $\mathsf{Q}_{X^nY^n}(x^n,y^n)$ is some probability distribution over $\mathcal{X}^n \times \mathcal{Y}^n$, and $\{|\rho_{x^ny^n}\rangle^{EA^nB^n}\}$ is some collection of pure states.

Probability distributions. Before continuing, we will establish some notation regarding probability distributions. We will use Q to denote the joint distribution on classical random variables associated with the state $|\rho\rangle^{X^n\tilde{X}^nEA^nB^nY^n\tilde{Y}^n}$. For example, $\mathsf{Q}_{X_iY_iA_iB_i}(x_i,y_i,a_i,b_i)$ denotes the distribution of outcomes if the $X_iY_iA_iB_i$ registers of $|\rho\rangle$ are measured in the standard basis, and $\mathsf{Q}_{A_iB_i|X_i=x_i,Y_i=y_i}(a_i,b_i)$ denotes the distribution of A_iB_i conditioned on $(X_i,Y_i) = (x_i,y_i)$ in $|\rho\rangle$. Intuitively, the state $|\rho\rangle$ will represent the state of Alice and Bob in the game G^n conditioned on winning some set of coordinates, so the distribution Q will be a "conditioned" distribution. We will also use P to denote the distribution of the same variables *without* conditioning. For example, P_{XY} is exactly the question distribution μ. The distribution $\mathsf{P}_{X_iY_i}$ represents the question distribution of the i'th coordinate of G^n, which again is exactly μ. The distribution $\mathsf{P}_{X^nY^n}$ is exactly the product distribution $\mathsf{P}_{X_1Y_1} \times \cdots \times \mathsf{P}_{X_nY_n}$.

Continuing with the proof, we will show that exists a coordinate $i \in [n]$, and $\delta < \varepsilon/128$ satisfying the following properties:

1. **(Winning answers)** Measuring the $X_iY_iA_iB_i$ registers of ρ yields a tuple (x_i,y_i,a_i,b_i) satisfying $V(x_i,y_i,a_i,b_i) = 1$ with probability at least $1 - \delta$;
2. **(Unaffected Question Distribution)** $S(\mathsf{Q}_{X_iY_i}\|\mathsf{P}_{XY}) \le \delta$.
3. **(Small mutual information)** $I(X_i : Y^n\tilde{Y}^nE_BB^n)_\rho \le \delta$ and $I(Y_i : X^n\tilde{X}^nE_AA^n)_\rho \le \delta$.

For now, we assume the existence of such a state $|\rho\rangle$; we will construct it in Lemma 56. We use Lemma 53 on the state ρ to obtain unitaries $\{U_x\}_{x\in\mathcal{X}}$ and $\{V_y\}_{y\in\mathcal{Y}}$ acting on $X^n\tilde{X}^nE_AA^n$ and $Y^n\tilde{Y}^nE_BB^n$ respectively such that

$$\mathop{\mathbb{E}}_{(x_i,y_i)\sim\mathsf{Q}_{X_iY_i}} \left[K\left(\rho_{x_i,y_i}, \mathrm{ad}_{U_{x_i}\otimes V_{y_i}}[\rho]\right)\right] \le 8(I(X_i : Y^n\tilde{Y}^nE_BB^n)_\rho + I(Y_i : X^n\tilde{X}^nE_AA^n)_\rho) \le 16\delta, \tag{5.2}$$

where recall that for an operator X, $\mathrm{ad}_X[\cdot] = X(\cdot)X^\dagger$, and the state ρ_{x_i,y_i} denotes ρ conditioned on $(X_i, Y_i) = (x_i, y_i)$.

We now describe a protocol for game G. The players share the ρ entangled state, where Alice has the registers $X^n\widetilde{X}^n E_A A^n$ and Bob has the registers $Y^n\widetilde{Y}^n E_B B^n$.

Protocol A

Input: $(x, y) \sim \mu$
Preshared entanglement: $\rho \in \mathrm{D}(X^n\widetilde{X}^n E A^n B^n Y^n \widetilde{Y}^n)$

1. Alice applies U_x on $\mathrm{X}^n\widetilde{X}^n E_A A^n$ and Bob applies V_y on $Y^n\widetilde{Y}^n E_B B^n$ registers of ρ.
2. Alice measures the A_i register and outputs outcome a_i, Bob measures the B_i register and outputs outcome b_i.

Slightly overloading notation, for all $(x, y) \in \mathcal{X} \times \mathcal{Y}$ we let $V^i_{x,y}$ denote the projector $\sum_{(a,b)\in\mathcal{A}\times\mathcal{B}:V(x,y,a,b)=1} |ab\rangle\langle ab|$ that acts on the A_iB_i registers. Let κ denote the winning probability of Protocol A. This is equal to

$$\begin{aligned}\kappa &= \mathop{\mathbb{E}}_{(x,y)\sim \mathrm{P}_{XY}} \left\| V^i_{x,y}\, U_x \otimes V_y \,|\rho\rangle \right\|^2 \\ &\geq \mathop{\mathbb{E}}_{(x,y)\sim \mathrm{Q}_{X_iY_i}} \left\| V^i_{x,y}\, U_x \otimes V_y \,|\rho\rangle \right\|^2 - 4\delta.\end{aligned}$$

where we used the Unaffected Question Distribution Property and appealed to Lemma 49. Let

$$\tau = \mathop{\mathbb{E}}_{(x,y)\sim \mathrm{Q}_{X_iY_i}} \left\| V^i_{x,y}\, U_x \otimes V_y \,|\rho\rangle \right\|^2 .$$

For every $i \in [n]$, $(x, y) \in \mathcal{X} \times \mathcal{Y}$, define the quantum operation $\mathcal{E}_{i,x,y}$ that, given a state ρ, measures the A_iB_i registers using $V^i_{x,y}$ measurement, and outputs a classical binary random variable F indicating the verification measurement outcome (outcome 1 corresponds to "accept" and outcome 0 corresponds to "reject"). Let

$$F_0 = \mathop{\mathbb{E}}_{(x_i,y_i)\sim \mathrm{Q}_{X_iY_i}} \mathcal{E}_{i,x,y}\left(\rho_{x_i,y_i}\right) \qquad \text{and} \qquad F_1 = \mathop{\mathbb{E}}_{(x_i,y_i)\sim \mathrm{Q}_{X_iY_i}} \mathcal{E}_{i,x,y}\left(\mathrm{ad}_{U_{x_i}\otimes V_{y_i}}[\rho]\right).$$

The random variables F_0 and F_1 correspond to two different experiments:

Experiment 0. F_0 is a random variable corresponding to the experiment in which, upon receiving questions (x_i, y_i) drawn from $\mathrm{Q}_{X_iY_i}$, the players are gifted with the advice state $\rho_{x_iy_i}$, they measure the answer registers A_iB_i, and the referee checks whether $V(x_i, y_i, a_i, b_i) = 1$.

Experiment 1. The random variable F_1 corresponds to the experiment where the players preshare ρ as entanglement, and upon receiving questions (x_i, y_i) drawn from $\mathrm{Q}_{X_iY_i}$, the players apply the local unitares U_{x_i} and V_{y_i} respectively to their share of the entanglement. Then they measure $A_i B_i$, and the referee checks whether $V(x_i, y_i, a_i, b_i) = 1$.

Since ρ satisfies the Winning Answers property, we have that $\Pr(F_0 = 1) \geq 1 - \varepsilon/8$. Furthermore, $\Pr(F_1 = 1) = \tau$ by definition. Then,

$$\begin{aligned} \mathrm{h}^2(F_0, F_1) &\leq \mathop{\mathbb{E}}_{(x_i,y_i) \sim \mathrm{Q}_{X_i Y_i}} \mathrm{h}^2\left(\mathcal{E}_{i,x,y}\left(\rho_{x_i,y_i}\right), \mathcal{E}_{i,x,y}\left(\mathrm{ad}_{U_{x_i} \otimes V_{y_i}}[\rho]\right)\right) && \text{(Fact 6)} \\ &\leq \mathop{\mathbb{E}}_{(x_i,y_i) \sim \mathrm{Q}_{X_i Y_i}} \mathrm{h}^2\left(\rho_{x_i,y_i}, \mathrm{ad}_{U_{x_i} \otimes V_{y_i}}[\rho]\right) && \text{(Fact 4)} \\ &\leq 16\delta. \end{aligned}$$

where in the last line we used line (5.2). By our assumption on δ, this is at most $\mathrm{h}^2(F_0, F_1) \leq \varepsilon/8$. By Lemma 50, $\Pr(F_1 = 1) \geq \Pr(F_0 = 1) - \varepsilon/8 \geq 1 - \varepsilon/8 - \varepsilon/2$. Thus $\kappa \geq 1 - 3\varepsilon/4$. But notice that Protocol A is a valid strategy for the game G; thus we have produced a strategy for game G that wins with probability strictly greater than $1 - \varepsilon$, a contradiction. Thus, it must be at $t = \Omega(\varepsilon^{3/2} n/s)$, which establishes the theorem. □

5.4.1 Construction of ρ

Lemma 56. *There exists a state $|\rho\rangle$, and a coordinate $i \in [n]$ satisfying the Winning Answers, Unaffected Question Distribution, and Small Mutual Information properties.*

Proof. Suppose there was a strategy to win the repeated game G^n with probability 2^{-t}, involving a shared state $|\psi\rangle^{E_A E_B}$ and measurements $\{A^{a^n}_{x^n}\}$ and $\{B^{b^n}_{y^n}\}$ for the players, respectively. Recall we assume that $t \leq c\varepsilon^{3/2} n/s$ for some constant c, and that $n \geq c''' \varepsilon^{-3/2} \log(128/\varepsilon) s$ for some constant c'''.

We will build the state ρ in steps. Consider the initial state

$$|\rho^0\rangle = \sum_{x^n, y^n} \sqrt{\mathsf{P}_{X^n Y^n}(x^n, y^n)} |x^n x^n\rangle^{X^n \tilde{X}^n} \otimes |\varphi_{x^n y^n}\rangle^{EA^n B^n} \otimes |y^n y^n\rangle^{Y^n \tilde{Y}^n}.$$

where

$$|\varphi_{x^n y^n}\rangle^{EA^n B^n} = \sum_{a^n, b^n} \sqrt{A^{a^n}_{x^n}} \otimes \sqrt{B^{b^n}_{y^n}} |\psi\rangle^{E_A E_B} \otimes |a^n b^n\rangle^{A^n B^n}$$

is a subnormalized state. For every set $C \subset [n]$, and every fixing of the inputs (x_C, y_C) to the coordinates indexed by C, define the state $|\rho^0_{x_C, y_C}\rangle$ to be $|\rho^0\rangle$ conditioned on $(X_C, Y_C) = (x_C, y_C)$. The states $|\rho^0_{x_C, y_C}\rangle$ also depend on C, but for notational simplicity we shall omit this dependence because it is clear from context.

Now consider the following two-player communication protocol: for every set $C \subset [n]$ and every $(x_C, y_C) \in \mathcal{X}^C \otimes \mathcal{Y}^C$, the players share a copy of the entangled state $|\rho^0_{x_C, y_C}\rangle$. Then, using shared randomness, the players sample h independent and uniformly random coordinates $C = \{i_1, \ldots, i_h\} \subset [n]$, and sample (x_C, y_C) from $\mathsf{P}_{X_C Y_C}$. We will determine what h is later. For the remainder of the protocol, the players perform all their operations on the shared state $|\rho^0_{x_C, y_C}\rangle$.

In the next phase of the protocol, the players communicate qubits to each other to determine whether they have won or lost the parallel repeated game G^n. In particular, they run a protocol to search for a coordinate $i \in C$ such that $V(x_i, y_i, a_i, b_i) = 0$, if it exists

– call such a coordinate a losing coordinate. The state $|\rho^0_{x_C,y_C}\rangle$ becomes transformed to

$$
\begin{aligned}
&|\rho^{pre}_{x_C,y_C}\rangle^{X^n\widetilde{X}^nE'A^nB^nY^n\widetilde{Y}^nR} \\
&= \sum_{x^n,y^n} \sqrt{\mu^n(x^n,y^n|x_C,y_C)}|x^nx^n\rangle^{X^n\widetilde{X}^n} \otimes \sum_{a^n,b^n} |\varphi'_{Cx^ny^na^nb^n}\rangle^{E'} \otimes |a^nb^n\rangle^{A^nB^n} \otimes |y^ny^n\rangle^{Y^n\widetilde{Y}^n} \\
&\qquad \otimes (\alpha_{Cx^ny^na^nb^n}|\mathrm{ACC}\rangle + \beta_{Cx^ny^na^nb^n}|\mathrm{REJ}\rangle)^R
\end{aligned}
$$

where $\mu^n(x^n,y^n|x_C,y_C)$ is probability of (x^n,y^n) conditioned on x_C, y_C, and $|\varphi'_{Cx^ny^na^nb^n}\rangle = |\varphi_{x^ny^na^nb^n}\rangle \otimes |w_{Cx^ny^na^nb^n}\rangle$ with $|w_{Cx^ny^na^nb^n}\rangle$ denoting the workspace qubits that are used during the protocol. The coefficients $\alpha_{Cx^ny^na^nb^n}$ and $\beta_{Cx^ny^na^nb^n}$ denote the amplitude that the search protocol places on the flags "No losing coordinates" and "Exists a losing coordinate" respectively.

For now, we will abstract away from the particulars of this communication protocol and defer the details of it until later. The only things we will use about this search protocol is the following Lemma:

Lemma 57. *The state $|\rho^{pre}_{x_C,y_C}\rangle$ is generated by a quantum communication protocol between Alice and Bob, who preshare entanglement. The communication protocol is a search protocol satisfying the following properties:*

1. *The search protocol is run conditioned on C, and the $X^nY^nA^nB^n$ registers;*

2. *At most $T = O(\sqrt{1/\varepsilon'}\log(1/\eta)s)$ qubits in total are exchanged.*

3. *For every fixing of (x^n, y^n, a^n, b^n), if there are no coordinates $i \in [n]$ such that $V(x_i, y_i, a_i, b_i) = 0$, then the search procedure reports "No losing coordinates" with probability 1; and*

4. *If there are at least an $\varepsilon' n$ bad coordinates, then the search procedure reports "No losing coordinates" with probability at most η (over the quantum randomness of the protocol, as well as over the choice of C). In other words, for tuples (x^n, y^n, a^n, b^n) such that $\mathbb{E}_i[V(x_i, y_i, a_i, b_i)] < 1 - \varepsilon'$,*

$$\sum_C \mathsf{P}(C)\,|\alpha_{Cx^ny^na^nb^n}|^2 \leq \eta,$$

where $\mathsf{P}(C)$ is the distribution that samples h independent and uniformly random coordinates from $[n]$.

We will defer the proof of this Lemma until later.

For all C, x_C, y_C define $|\rho_{x_C,y_C}\rangle$ to be

$$\frac{1}{\sqrt{\lambda_{C,x_C,y_C}}}(\mathbb{I} \otimes |\mathrm{ACC}\rangle\langle\mathrm{ACC}|)|\rho^{pre}_{x_C,y_C}\rangle$$

where λ_{C,x_C,y_C} is for normalization, and the projector $|\mathrm{ACC}\rangle\langle\mathrm{ACC}|$ acts on the R register. In the case that $\lambda_{x_C,y_C} = 0$ (meaning that we were trying to normalize the 0 state), we leave the state undefined.

Define the joint probability distribution

$$\mathsf{P}(C, x_C, y_C) = \mathsf{P}(C) \cdot \mathsf{P}_{X_CY_C}(x_C, y_C)$$

and

$$\mathsf{Q}(C, x_C, y_C) = \frac{1}{\lambda}\mathsf{P}(C) \cdot \mathsf{P}_{X_C Y_C}(x_C, y_C) \cdot \lambda_{C, x_C, y_C}$$

where $\lambda = \sum_{C, x_C, y_C} \lambda_{C, x_C, y_C}$. The distribution $\mathsf{P}(C, x_C, y_C)$ denotes the marginal distribution of C and (x_C, y_C) before conditioning, and $\mathsf{Q}(C, x_C, y_C)$ denotes the marginal distribution *after* conditioning on $R = \text{ACC}$.

Define the global state

$$\rho = \mathop{\mathbb{E}}_{(C, x_C, y_C) \sim \mathsf{Q}} |C\rangle\langle C| \otimes |x_C y_C\rangle\langle x_C y_C| \otimes \rho_{x_C, y_C}.$$

Proposition 58. *The probability that measuring CX_CY_C registers, choosing a random index $i \notin C$, and measuring the $X_iY_iA_iB_i$ register of $\rho_{x_C y_C}$ yields a tuple (x_i, y_i, a_i, b_i) such that $V(x_i, y_i, a_i, b_i) = 0$ is at most $2^t \eta + \frac{\varepsilon n}{2048(n-h)}$.*

Proof. Let $\mathcal{E}$ denote the quantum operation that (1) measures the CX_CY_C registers, (2) chooses a uniformly random $i \notin C$, (3) measures X_iY_i register to obtain outcome (x_i, y_i), and (4) then performs the binary verification measurement $V^i_{x_i, y_i}$ defined in the previous section, setting an auxiliary register Q to $|\text{ACC}\rangle$ if the measurement accepts, $|\text{REJ}\rangle$ if it rejects.

We wish to argue that the probability that a measurement of the Q register of $\mathcal{E}(\rho)$ yields ACC with high probability. This probability is equivalent to the probability the following process succeeds: first, measure the $X^nY^nA^nB^n$ registers of ρ to obtain a tuple (x^n, y^n, a^n, b^n). Then, measure the C register. Finally, select a random index $i \notin C$, and we succeed if $V(x_i, y_i, a_i, b_i) = 1$. This is an equivalent process because the C, X_C, Y_C registers are disjoint from the $X_iY_iA_iB_i$ registers.

Define $\varepsilon' = \varepsilon/2048$. In this alternative process, the probability that we measure (x^n, y^n, a^n, b^n) such that $\mathbb{E}_{i \in [n]} V(x_i, y_i, a_i, b_i) < 1 - \varepsilon'$ (call such (x^n, y^n, a^n, b^n) tuples "bad") is equal to

$$\frac{1}{\lambda} \sum_{(x^n, y^n, a^n, b^n) \text{ bad}} \mathsf{Q}(x^n, y^n, a^n, b^n) \sum_C \mathsf{P}(C) |\alpha_{Cx^n y^n a^n b^n}|^2 \leq \eta/\lambda$$

where in the inequality we used Assumption 4 above. Since the players' strategy wins the repeated game G^n with probability 2^{-t}, we have that $\lambda \geq 2^{-t}$. Thus the probability of measuring a bad (x^n, y^n, a^n, b^n) is at most $2^t \eta$.

Now suppose we measure (x^n, y^n, a^n, b^n) such that $\mathbb{E}_{i \in [n]} V(x_i, y_i, a_i, b_i) \geq 1 - \varepsilon'$. Then, for any C, a random $i \notin C$ loses with probability at most

$$\varepsilon' n/(n - |C|) \leq \varepsilon' n/(n - h)$$

Thus, the probability that the $\mathcal{E}(\rho)$ yields REJ is at most $2^t \eta + \varepsilon' n/(n - h)$. □

Proposition 59. $\mathbb{E}_{(C, x_C, y_C) \sim \mathsf{Q}} \mathbb{E}_{i \notin C} S(\rho^{X_iY_i}_{x_C, y_C} \| \mathsf{P}_{X_iY_i}) \leq \frac{1}{n-h} \log \frac{1}{\lambda}$.

Proof. Define

$$\rho^{pre} = \mathop{\mathbb{E}}_{(C, x_C, y_C) \sim \mathsf{P}(C, x_C, y_C)} |C\rangle\langle C| \otimes |x_C y_C\rangle\langle x_C y_C| \otimes \rho^{pre}_{x_C, y_C}$$

This state corresponds to the joint state of C, X_C, Y_C, and state of the players after the communication protocol, but *before* conditioning.

By Fact 14, since $\rho \preceq 2^{\lambda}\rho^{pre}$, we have

$$\begin{aligned}
\log 1/\lambda &\geq S_{\infty}(\rho \| \rho^{pre}) \\
&\geq S(\rho \| \rho^{pre}) \\
&\geq \mathop{\mathbb{E}}_{(C,x_C,y_C)\sim \mathsf{Q}} S(\rho_{x_C,y_C} \| \rho^{pre}_{x_C,y_C}) \tag{5.3} \\
&\geq \mathop{\mathbb{E}}_{(C,x_C,y_C)\sim \mathsf{Q}} S(\rho^{X^nY^n}_{x_C,y_C} \| (\rho^{pre}_{x_C,y_C})^{X^nY^n}) \tag{5.4} \\
&\geq \mathop{\mathbb{E}}_{(C,x_C,y_C)\sim \mathsf{Q}} \sum_{i\notin C} S(\rho^{X_iY_i}_{x_C,y_C} \| (\rho^{pre}_{x_C,y_C})^{X_iY_i}) \tag{5.5} \\
&= \mathop{\mathbb{E}}_{(C,x_C,y_C)\sim \mathsf{Q}} \sum_{i\notin C} S(\rho^{X_iY_i}_{x_C,y_C} \| \mathsf{P}_{X_iY_i})
\end{aligned}$$

where we used Fact 10 to get (5.3), Fact 12 to get (5.4), and Fact 13 to get (5.5).

□

Proposition 60.

$$\mathop{\mathbb{E}}_{(C,x_C,y_C)\sim \mathsf{Q}} \mathop{\mathbb{E}}_{i\notin C} I(X_i : Y^n\tilde{Y}^nE_BB^n)_{\rho_{x_Cy_C}} + I(Y_i : X^n\tilde{X}^nE_AA^n)_{\rho_{x_Cy_C}} \leq 2(\log 1/\lambda + 2T)/(n-h).$$

Proof. First we need the following Claim.

Claim 61. *Fix C, x_C, y_C. There exists a state $\sigma^{Y^n\tilde{Y}^nE_BB^n}_{x_Cy_C}$ such that*

$$S_{\infty}((\rho^{pre}_{x_Cy_C})^{X^nY^n\tilde{Y}^nE_BB^n} \| (\rho^{pre}_{x_Cy_C})^{X^n} \otimes \sigma^{Y^n\tilde{Y}^nE_BB^n}_{x_Cy_C}) \leq 2T,$$

and a state $\tau^{X^n\tilde{X}^nE_AA^n}_{x_Cy_C}$ such that

$$S_{\infty}((\rho^{pre}_{x_Cy_C})^{Y^nX^n\tilde{X}^nE_AA^n} \| (\rho^{pre}_{x_Cy_C})^{Y^n} \otimes \tau^{X^n\tilde{X}^nE_AA^n}_{x_Cy_C}) \leq 2T.$$

We defer the proof of this claim for later, and will assume it for now. We have that

$$\begin{aligned}
&\mathop{\mathbb{E}}_{(C,x_C,y_C)\sim \mathsf{Q}} S(\rho^{X^nY^n\tilde{Y}^nE_BB^n}_{x_Cy_C} \| (\rho^{pre}_{x_Cy_C})^{X^n} \otimes \sigma^{Y^n\tilde{Y}^nE_BB^n}_{x_Cy_C}) \\
&\leq \mathop{\mathbb{E}}_{(C,x_C,y_C)\sim \mathsf{Q}} S(\rho^{X^nY^n\tilde{Y}^nE_BB^n}_{x_Cy_C} \| (\rho^{pre}_{x_Cy_C})^{X^nY^n\tilde{Y}^nE_BB^n}) \\
&\qquad\qquad + S_{\infty}((\rho^{pre}_{x_Cy_C})^{X^nY^n\tilde{Y}^nE_BB^n} \| (\rho^{pre}_{x_Cy_C})^{X^n} \otimes \sigma^{Y^n\tilde{Y}^nE_BB^n}_{x_Cy_C}) \\
&\leq \log 1/\lambda + 2T
\end{aligned}$$

where the first inequality uses Fact 17, and the second inequality comes from line (5.3) and the bound from Claim 61. Using Quantum Raz's Lemma, we get

$$\mathop{\mathbb{E}}_{(C,x_C,y_C)\sim \mathsf{Q}} \mathop{\mathbb{E}}_{i\in[n]} I(X_i : Y^n\tilde{Y}^nE_BB^n)_{\rho_{x_Cy_C}} \leq (\log 1/\lambda + 2T)/n.$$

Similarly, we also have

$$\mathop{\mathbb{E}}_{(C,x_C,y_C)\sim \mathsf{Q}} \mathop{\mathbb{E}}_{i\in[n]} I(Y_i : X^n\tilde{X}^nE_AA^n)_{\rho_{x_Cy_C}} \leq (\log 1/\lambda + 2T)/n.$$

Combining both statements, and multiplying both sides by $n/(n-h)$ (recall that $|C| \leq h$), we obtain the Proposition. □

Combining Propositions 58, 59, and 60, we get that

$$\begin{aligned}
\mathop{\mathbb{E}}_{(C,x_C,y_C)\sim Q} \mathop{\mathbb{E}}_{i \notin C} & \mathrm{Tr}\big(\mathcal{E}_i(\rho_{x_C y_C}) \, |\mathrm{REJ}\rangle\langle\mathrm{REJ}|\big) + S(\rho^{X_i Y_i}_{x_C, y_C} \| \mathsf{P}_{X_i Y_i}) \\
& + I(X_i : Y^n \widetilde{Y}^n E_B B^n)_{\rho_{x_C y_C}} + I(Y_i : X^n \widetilde{X}^n E_A A^n)_{\rho_{x_C y_C}} \\
& \leq 2^t \eta + \frac{\varepsilon n/2048}{n-h} + \frac{1}{n-h} \log \frac{1}{\lambda} + \frac{2}{n-h} (\log \frac{1}{\lambda} + 2T) \\
& \leq 2^t \eta + \frac{(\varepsilon/2048)n + 3t + 4T}{n-h}
\end{aligned}$$

where $\mathcal{E}_i$ corresponds to the quantum operation of measuring $X_i Y_i A_i B_i$ registers of the input state, and then checking whether $V(x_i, y_i, a_i, b_i) = 1$. The projector $|\mathrm{REJ}\rangle\langle\mathrm{REJ}|$ acts on the Q register output by the operation $\mathcal{E}_i$. In the last inequality, we used that $\lambda \geq 2^{-t}$. Use the following setting of parameters:

- $\eta = 2^{-t} \varepsilon / 2048$
- $h = c' \log(1/\eta)/\varepsilon$ for some large enough constant c'

Recall we assume that $t \leq c\varepsilon^{3/2} n/s$ for some constant c, and that $n \geq c''' \varepsilon^{-3/2} \log(2048/\varepsilon) s$ for some constant c'''. By our choices of parameters, we have ensured that $2^t \eta \leq \varepsilon/1024$, and $((\varepsilon/2048)n + 3t + 4T)/(n-h) \leq \varepsilon/1024$, and thus by averaging there exists a setting of C, x_C, y_C, and $i \notin C$ such that

1. $\mathrm{Tr}\big(\mathcal{E}_i(\rho_{x_C y_C}) \, |\mathrm{REJ}\rangle\langle\mathrm{REJ}|\big) \leq \varepsilon/128$,
2. $S(\rho^{X_i Y_i}_{x_C, y_C} \| \mathsf{P}_{X_i Y_i}) \leq \varepsilon/128$,
3. $I(X_i : Y^n \widetilde{Y}^n E_B B^n)_{\rho_{x_C y_C}} + I(Y_i : X^n \widetilde{X}^n E_A A^n)_{\rho_{x_C y_C}} \leq \varepsilon/128$

which correspond to the desired Winning Answers, Unaffected Question Distribution, and Small Mutual Information properties.

□

5.4.2 The search protocol

Proof of Lemma 57. Next, we detail the search protocol used to construct $|\rho^{pre}\rangle$. Let $G = (\mathcal{X} \times \mathcal{Y}, \mathcal{A} \times \mathcal{B}, \mu, V)$ be a two-player free game, where $\mathcal{X}$ and $\mathcal{Y}$ are Alice and Bob's input alphabets, respectively, and $\mathcal{A}$ and $\mathcal{B}$ are their output alphabets. Consider the optimal strategy for G^n, where there is a shared state $|\psi\rangle^{E_A E_B}$ where on input $(x^n, y^n) \in \mathcal{X}^n \times \mathcal{Y}^n$, Alice and Bob apply measurements $\{A^{a^n}_{x^n}\}_{a^n \in \mathcal{A}^n}$ and $\{B^{b^n}_{y^n}\}_{b^n \in \mathcal{B}^n}$ respectively on their share of $|\psi\rangle$.

At the start of the search protocol, a multiset $C = \{i_1, \ldots, i_h\}$, $x_C \in \mathcal{X}^C$, and $y_C \in \mathcal{Y}^C$ are publicly visible to Alice and Bob. They are also given access to the shared state

$$|\theta^0_{C,x_C,y_C}\rangle^{X^n \widetilde{X}^n Y^n \widetilde{Y}^n E_A E_B R} = \sum_{x^n, y^n} \sqrt{\mathsf{P}_{X^n Y^n | x_C, y_C}(x^n, y^n)} |x^n x^n y^n y^n\rangle^{X^n \widetilde{X}^n Y^n \widetilde{Y}^n} \otimes |\psi\rangle^{E_A E_B} \otimes |0\rangle^R$$

Alice has access to registers $X^n \widetilde{X}^n E_A R$, and Bob has access to registers $E_B Y^n \widetilde{Y}^n$.

Then, Alice and Bob apply their measurements from the optimal strategy, controlled on the X^n and Y^n registers, respectively, to obtain

$$|\theta^1_{C,x_C,y_C}\rangle^{X^n\widetilde{X}^nY^n\widetilde{Y}^nE_AE_BA^nB^nR} = \sum_{x^n,y^n} \sqrt{\mathsf{P}_{X^nY^n|x_C,y_C}(x^n,y^n)}|x^nx^ny^ny^n\rangle^{X^n\widetilde{X}^nY^n\widetilde{Y}^n} \otimes \sum_{a^n,b^n} |\zeta_{x^ny^na^nb^n}\rangle^{E_AE_B} \otimes |a^nb^n\rangle^{A^nB^n} \otimes |0\rangle^R$$

where $|\zeta_{x^ny^na^nb^n}\rangle = \sqrt{A^{a^n}_{x^n}} \otimes \sqrt{B^{b^n}_{y^n}}|\psi\rangle$.

Alice and Bob then run a distributed search protocol controlled on the $X^nY^nA^nB^n$ registers. Consider the (x^n, y^n, a^n, b^n) branch of the superposition in the $X^nY^nA^nB^N$ registers of $|\theta^1\rangle$. Let $\varepsilon' = \varepsilon/2048$. The protocol proceeds as follows: Alice and Bob divide the multiset C into groups $D_1, \dots, D_q$, each of size $m = \lceil 1/\varepsilon' \rceil$. Thus $q = \lceil h/m \rceil$. For each $\ell = 1, \dots, q$, Alice and Bob perform a distributed version of the Aaronson-Ambainis 3-dimensional search algorithm [1] to determine whether D_ℓ contains a losing coordinate – i.e., if there is a coordinate $i \in D_\ell$ such that $V(x_i, y_i, a_i, b_i) = 0$.

The search protocol for a group D_ℓ works as follows. Whenever the Aaronson-Ambainis algorithm is in the state $\sum_i \gamma_{i,z}|i,z\rangle$, where $|i\rangle$ corresponds to an index in $D_\ell \subset C$, and $|z\rangle$ is a qubit indicating whether a marked item has been found, the joint state between Alice and Bob will be $\sum_i \gamma_{i,z}|i\rangle \otimes |z\rangle \otimes |i\rangle$, where Alice holds the first $|i\rangle$ and $|z\rangle$, and Bob holds the second $|i\rangle$. Thus, Alice and Bob query locations are "synchronized". When Aaronson-Ambainis algorithm has to perform a query controlled on $|i\rangle$, Bob sends the qubit containing $|b_i\rangle$. Alice, controlled on $|b_i\rangle$, performs $|z\rangle \mapsto |z \oplus V(x_i, y_i, a_i, b_i) \oplus 1\rangle$ – note that Alice can perform this, because in addition to x_i, a_i, and b_i, she also has access to y_i because y_C is public. We perform an additional XOR with 1 because a "marked item" for the search algorithm corresponds to a *losing* coordinate. Alice then sends back $|b_i\rangle$ to Bob. The other non-query transformations of the Aaronson-Ambainis algorithm are handled as in the the protocol described in [1]. Each step of the algorithm incurs at most $O(\log|\mathcal{B}|)$ qubits of communication, and there are $O(\sqrt{m})$ steps, resulting in $O(\sqrt{m}\log|\mathcal{B}|)$ qubits of total communication. If D_ℓ contains a losing coordinate, then this protocol will succeed in finding one with probability at least $2/3$.

If for at least one ℓ, Alice and Bob find a losing coordinate in G_ℓ, Alice sets the R register to REJ; otherwise, Alice sets it to ACC. Thus the total amount of communication of this protocol is $T = O(q\sqrt{m}\log|\mathcal{B}|) = O(\sqrt{1/\varepsilon'}\log 1/\eta \log|\mathcal{B}|)$. The final state of the protocol looks like

$$|\theta^2_{C,x_C,y_C}\rangle^{X^n\widetilde{X}^nY^n\widetilde{Y}^nE_AE_BA^nB^nR} = \sum_{x^n,y^n} \sqrt{\mathsf{P}_{X^nY^n|x_C,y_C}(x^n,y^n)}|x^nx^ny^ny^n\rangle^{X^n\widetilde{X}^nY^n\widetilde{Y}^n} \otimes \sum_{a^n,b^n} |\zeta'_{x^ny^na^nb^n}\rangle^{E_AE_BW_AW_B} \otimes |a^nb^n\rangle^{A^nB^n} \otimes (\alpha_{Cx^ny^na^nb^n}|\mathrm{ACC}\rangle^R + \beta_{Cx^ny^na^nb^n}|\mathrm{REJ}\rangle^R)$$

where $|\zeta'_{x^ny^na^nb^n}\rangle^{E_AE_BW_AW_B} = |\zeta_{x^ny^na^nb^n}\rangle^{E_AE_B} \otimes |w_{Cx^ny^na^nb^n}\rangle^{W_AW_B}$ with $|w_{Cx^ny^na^nb^n}\rangle$ denoting the workspace qubits of the two players that arise from running the Aaronson-Ambainis protocol.

Fix a setting of the registers $X^nY^nA^nB^n = (x^n, y^n, a^n, b^n)$. Suppose there was no $i \in [n]$ such that $V(x_i, y_i, a_i, b_i) = 0$. Then the search algorithm will never find a losing coordinate in any of the G_ℓ's, so for all C, the we have $\beta_{Cx^ny^na^nb^n} = 0$.

On the other hand, suppose there were at least $\varepsilon' n$ losing coordinates in (x^n, y^n, a^n, b^n). We analyze, for a fixed (x^n, y^n, a^n, b^n), the error quantity $\sum_C \mathsf{P}(C)\,|\alpha_{Cx^ny^na^nb^n}|^2$ – this is the probability that measuring the R register yields $|\mathrm{ACC}\rangle$, even though there many losing coordinates. We can write $\mathsf{P}(C) = \prod_\ell \mathsf{P}(D_\ell)$, because each index in C is chosen uniformly and independently at random. Furthermore, we can decompose $|\alpha_{Cx^ny^na^nb^n}|^2 = \prod_\ell |\alpha_{D_\ell x^ny^na^nb^n}|^2$, where $\alpha_{D_\ell x^ny^na^nb^n}$ is the probability amplitude that the Aaronson-Ambainis protocol does not find a losing coordinate in D_ℓ. Thus the error quantity can be written as

$$\begin{aligned}\sum_C \mathsf{P}(C)\,|\alpha_{Cx^ny^na^nb^n}|^2 &= \sum_{D_1,\ldots,D_q} \prod_\ell \mathsf{P}(D_\ell) \prod_\ell |\alpha_{D_\ell x^ny^na^nb^n}|^2 \\ &= \prod_\ell \left(\sum_{D_\ell} \mathsf{P}(D_\ell) |\alpha_{D_\ell x^ny^na^nb^n}|^2 \right) \\ &= \left(\sum_D \mathsf{P}(D) |\alpha_{Dx^ny^na^nb^n}|^2 \right)^q\end{aligned}$$

Since C is chosen independently of $X^nY^nA^nB^n$, each D_ℓ independently has at least $1-(1-\varepsilon')^m \geq 1-1/e$ probability of containing a losing coordinate. When D_ℓ has a losing coordinate, the Aaronson-Ambainis search protocol will succeed in finding it with probability at least $2/3$. Thus, for a fixed D, we have

$$\begin{aligned}&|\alpha_{Dx^ny^na^nb^n}|^2 \\ &= \Pr(D \text{ contains losing coordinate}) \cdot \frac{1}{3} + \Pr(D \text{ does not have losing coordinate}) \cdot (1) \\ &\leq \frac{1}{3} + \frac{1}{e}.\end{aligned}$$

Thus $\left(\sum_D \mathsf{P}(D) |\alpha_{Dx^ny^na^nb^n}|^2\right)^q \leq (1/3 + 1/e)^q \leq \eta$.

Thus by letting $|\rho^{pre}_{x_C,y_C}\rangle = |\theta^2_{C,x_C,y_C}\rangle$, we obtain the desired state promised by the Lemma statement. □

Proof of Claim 61. Fix C, x_C, y_C. Take the start state $\rho^0_{x_C,y_C}$ defined above, and trace out the $\tilde{X}^n$ register: define $\tau^0_{x_C,y_C} = \mathrm{Tr}_{\tilde{X}^n}(\rho^0_{x_C,y_C})$. Since G is a free game, this means that μ^n is a product distribution across players and also across game coordinates, so we have that

$$\tau^0_{x_C,y_C} = |x_C\rangle\langle x_C|^{X_C} \otimes \Phi^{X_{-C}} \otimes |\varphi^0_{x_C,y_C}\rangle\langle \varphi^0_{x_C,y_C}|^{Y^n\tilde{Y}^nE_AE_B}$$

where $\Phi^{X_{-C}}$ is the maximally mixed state for the register X_{-C} (that is, X^n without the X_C coordinates), and

$$|\varphi^0_{x_C,y_C}\rangle^{Y^n\tilde{Y}^nE_AE_B} = \sum_{y^n} \sqrt{\mathsf{P}_{Y^n|Y_C=y_C}(y^n)}\,|y^ny^n\rangle^{Y^n\tilde{Y}^n} \otimes |\psi\rangle^{E_AE_B}$$

Here, we used the simplifying assumption that μ is the uniform distribution. The sequence of quantum operations used to construct the state $|\rho^{pre}\rangle$ – the game strategy and the search protocol described in Lemma 57 – never touches the $\tilde{X}^n$ register. Thus, we can view the protocol as between Alice and Bob, who preshare an entangled state $\varphi^0_{x_Cy_C}$ where E_A belongs to Alice, and the $Y^n\tilde{Y}^n E_B$ registers belong to Bob. Alice receives a uniformly random input X^n conditioned on $X_C = x_C$. Then, as described above, Alice and Bob first apply the optimal game strategy. Afterwards, they run the search protocol. The only communication comes from the search protocol phase. The final state is $(\rho^{pre}_{x_C,y_C})^{X^n Y^n \tilde{Y}^n E_A E_B A^n B^n R}$.

We now wish to analyze the min-entropy of Bob's input register Y^n, conditioned on Alice's registers (which are $X^n E_A A^n R$), within the final state $\rho^{pre}_{x_C,y_C}$. We appeal to the beautiful result of Nayak and Salzman [81], whose theorem statement we reproduce here:

Theorem 62 ([81]). *Consider a communication protocol, without prior entanglement, where Alice receives a uniformly random n-bit input X, and interacts with Bob over a quantum communication channel. Let ψ^{XB} be the final joint state of Alice's input X and Bob's state in the protocol. Then, for any measurement strategy $\{M_x\}_x$ that Bob applies to his own state, the probability that Bob guesses Alice's input X correct is at most $2^{2m_A}/2^n$, where m_A is the number of qubits sent from Alice to Bob over the course of the protocol.*

We give a simplified proof of their theorem in Appendix A.

We now rephrase their theorem to use relative min-entropy instead of guessing probabilities. Let α be the optimal guessing probability for Bob. Then, the *quantum conditional min-entropy* $H_{\min}(X|B)_\psi$ is defined to be $-\log \alpha$. However, by SDP duality [68], we have the alternative characterization that

$$H_{\min}(X|B)_\psi = -\inf_{\sigma^B} S_\infty(\psi^{XB} \| \mathbb{I}^X \otimes \sigma^B).$$

Let σ^B be a state achieving this infimum. Then $\log \alpha = S_\infty(\psi^{XB} \| \mathbb{I}^X \otimes \sigma^B) = S_\infty(\psi^{XB} \| \frac{1}{2^n}\mathbb{I}^X \otimes \sigma^B) - n$. By the theorem of Nayak and Salzman, $\log \alpha \leq 2m_A - n$, so

$$S_\infty(\psi^{XB} \| \frac{1}{2^n}\mathbb{I}^X \otimes \sigma^B) = S_\infty(\psi^{XB} \| \psi^X \otimes \sigma^B) \leq 2m_A,$$

where we used the fact that ψ^X is the uniform distribution.

We now apply this theorem to our setting. At first it may seem that the Nayak-Salzman theorem does not apply, because Alice and Bob preshare the entanglement $|\varphi^0_{x_C y_C}\rangle$, whereas the theorem statement requires that Alice and Bob do not share prior entanglement. However, observe that the Nayak-Salzman theorem does not depend on the number of qubits sent from Bob to Alice! Thus, we can imagine that at the beginning of the protocol, instead of sharing $|\varphi^0_{x_C y_C}\rangle$ with Alice, Bob possesses all of $|\varphi^0_{x_C y_C}\rangle^{Y^n \tilde{Y}^n E_A E_B}$, and then sends over the E_A part to Alice. From this point Alice and Bob proceed as usual – they play the optimal repeated game strategy, followed by the search protocol. Alice exchanges at most T qubits with Bob.

Thus the Nayak-Salzman theorem and our alternative characterization, we have that there exists a state $\sigma^{Y^n \tilde{Y}^n E_B B^n}$ such that

$$S_\infty((\rho^{pre}_{x_C y_C})^{X^n Y^n \tilde{Y}^n E_B B^n} \| (\rho^{pre}_{x_C y_C})^{X^n} \otimes \sigma^{Y^n \tilde{Y}^n E_B B^n}_{x_C y_C}) \leq 2T.$$

Similarly, we can interchange the roles of Alice and Bob to conclude that there exists a state $\tau^{X^n \tilde{X}^n E_A A^n}_{x_C y_C}$ such that

$$S_\infty((\rho^{pre}_{x_C y_C})^{Y^n X^n \tilde{X}^n E_A A^n} \| (\rho^{pre}_{x_C y_C})^{Y^n} \otimes \tau^{X^n \tilde{X}^n E_A A^n}_{x_C y_C}) \leq 2T.$$

□

Chapter 6

Parallel repetition for anchored games

This chapter presents work conducted with Mohammad Bavarian and Thomas Vidick, and appears on the arXiv under the title "Anchoring games for parallel repetition" [11].

6.1 Introduction

We study the problem of parallel repetition in both the multiplayer classical and quantum settings. We prove, by introducing and analyzing a simple variant of parallel repetition, exponential-decay parallel repetition theorems that apply to *arbitrary* games with multiple players or with entangled players. In particular, we obtain the first general gap amplification technique for games in the multiplayer and quantum settings.

Our main results can be summarized as follows; see Theorems 68 and 74 for precise statements.

Theorem 63 (Main theorem, informal). *There exists a polynomial-time transformation (called* anchoring*) that takes the description of an arbitrary k-player game G and returns a k-player game $G_\perp$ with the following properties:*

1. $\mathrm{val}(G_\perp) = \frac{1}{4} + \frac{3}{4}\mathrm{val}(G)$.
2. $\mathrm{val}^*(G_\perp) = \frac{1}{4} + \frac{3}{4}\mathrm{val}^*(G)$.
3. *If* $\mathrm{val}(G) = 1 - \varepsilon$*, then* $\mathrm{val}(G_\perp^n) \leq \exp(-\Omega(\varepsilon^3 \cdot n))$.
4. *If* $\mathrm{val}^*(G) = 1 - \delta$*, then* $\mathrm{val}^*(G_\perp^n) \leq \exp(-\Omega(\delta^8 \cdot n))$,

where the implied constants in the $\Omega(\cdot)$ only depend on the number of players and the cardinality of the answer sets.

The idea of modifying the game to facilitate its analysis under parallel repetition originates from the work of Feige and Kilian [44] which predates Raz's parallel repetition theorem. Feige and Kilian introduce a transformation that converts an arbitrary game G to a so-called *miss-match* game G^{FK}. The transformation is *value-preserving* in the sense that there is a precise affine relationship $\mathrm{val}(G^{FK}) = (2 + \mathrm{val}(G))/3$. Furthermore Feige and Kilian show that the value of the n-fold repetition of G^{FK} decays *polynomially* in n whenever $\mathrm{val}(G) < 1$. This enables them to establish a general gap amplification result without having to prove a parallel repetition theorem for arbitrary games. This is sufficient for many applications, including to hardness of approximation, for which it is enough that the gap amplification procedure be efficient and value-preserving.

Theorem 63 adopts a similar approach to that of Feige and Kilian by providing an arguably even simpler transformation, *anchoring*, which *preserves both the classical and entangled value* of a game and for which we are able to prove an exponential decay under parallel repetition. In contrast, the transformation considered by Feige and Kilian does not in general preserve the entangled value, as discussed in Chapter 4. We proceed to describe our transformation and then discuss the role it plays in facilitating the proof of our parallel repetition theorem.

6.1.1 The anchoring transformation

Our parallel repetition results apply to a class of games we call *anchored*. The anchoring transformation of Theorem 63 produces games of this type; however, anchored games can be more general. We give a full definition of anchored games in Section 6.2. First we describe the anchoring transformation.

Definition 64 (Basic anchoring). *Let G be a two player game with question distribution μ on $\mathcal{X} \times \mathcal{Y}$, and verification predicate V. In the α-anchored game $G_\perp$ the referee chooses a question pair $(x,y) \in \mathcal{X} \times \mathcal{Y}$ according to μ, and independently and with probability α replaces each of x and y with an auxiliary "anchor" symbol $\perp$ to obtain the pair $(x',y') \in (\mathcal{X} \cup \{\perp\}) \times (\mathcal{Y} \cup \{\perp\})$ which is sent to the players as their respective questions. If any of x', y' is $\perp$ the referee accepts regardless of the players' answers; otherwise, the referee checks the players' answers according to the predicate V.*

For a choice of $\alpha = 1 - \frac{\sqrt{3}}{2}$ it holds that both $\mathrm{val}(G_\perp) = \frac{3}{4}\mathrm{val}(G) + \frac{1}{4}$ and $\mathrm{val}^*(G_\perp) = \frac{3}{4}\mathrm{val}^*(G) + \frac{1}{4}$. One can think of $G_\perp$ as playing the original game G with probability $3/4$, and a trivial game with probability $1/4$. The term "anchored" refers to the fact that question pairs chosen according to μ are all "anchored" by a common question $(\perp, \perp)$. Though the existence of this anchor question makes the game $G_\perp$ *easier* to play than the game G, it facilitates showing that the repeated game $G_\perp^n$ is *hard*. At a high level, the anchor questions provide a convenient way to handle the complicated correlations that may arise when the players use non-product strategies in the repeated game, as we explain in the next section.

6.1.2 Proving parallel repetition by breaking correlations

In virtually all known (information theoretic) proofs of parallel repetition theorems, the key step consists in arguing that the players' success probability in most instances of G individually cannot be substantially larger than the value of G itself, *even when conditioned on the players winning a significant fraction of the instances.* Coupled with the possibility of using non-product strategies this conditioning introduces correlations between the player's questions which make the task of bounding their success probability in the remaining instances of G non-trivial.

In the proof of his parallel repetition theorem, Raz [88] introduced a technique, further refined in subsequent work of Holenstein [56], to *break* such correlations. The idea consists of introducing a *dependency-breaking random variable* Ω satisfying two properties: (1) Ω can be sampled jointly, using shared randomness, by all players, and (2) conditioned on Ω and a pair of questions distributed according to μ, the players are able to locally generate questions and answers from the same distribution as they would in the repeated game, *conditioned on winning* a (not too large) subset of instances. These two requirements are at odds with each other, and the main difficulty is to design an Ω that satisfies both simultaneously.

Extending this approach to more players, or quantum strategies, remains a challenge. Rather than solving the general problem directly, we sidestep it and instead analyze the parallel repetition of anchored games, for which designing an appropriate dependency-breaking variable (or, in the case of entangled players, a dependency-breaking quantum state) is easier, though by no means trivial. Combined with the anchoring operation this yields a simple and efficient method to achieve hardness amplification for arbitrary games in the multiplayer and entangled-player settings. We give a more detailed explanation of how this is achieved in Section 6.2 below.

6.1.3 Related work

The transformation from general games into anchored games that we introduce is inspired by the work of Feige and Kilian [44]. This alternative approach to achieving gap amplification is also used by Moshkovitz [78], who shows how projection games can be "fortified", and gives a simple and elegant proof that the classical value of fortified games decays exponentially under parallel repetition (see also the follow-up work by Bhangle et al. [16]). In a separate work, we prove a parallel repetition theorem for the entangled value of fortified games [12], giving an alternative general gap amplification method for entangled and multiplayer games.

6.2 Technical overview

We give a technical overview of anchored games and their parallel repetition. For concreteness we focus on the case of two-player games. For the full definition of k-player anchored games, see Section 6.3.

Definition 65 (Two-player anchored games). *Let G be a two-player game with question alphabet $\mathcal{X} \times \mathcal{Y}$ and distribution μ. For any $0 < \alpha \leq 1$ we say that G is α-anchored if there exists subsets $\mathcal{X}_\perp \subseteq \mathcal{X}$ and $\mathcal{Y}_\perp \subseteq \mathcal{Y}$ such that, denoting by μ the respective marginals of μ on both coordinates,*

1. *Both $\mu(\mathcal{X}_\perp), \mu(Y_\perp) \geq \alpha$,*
2. *Whenever $x \in \mathcal{X}_\perp$ or $y \in \mathcal{Y}_\perp$ it holds that $\mu(x,y) = \mu(x) \cdot \mu(y)$.*

Informally, a game is *anchored* if each player independently has a significant probability of receiving a question from the set of "anchor questions" $\mathcal{X}_\perp$ and $\mathcal{Y}_\perp$. An alternative way of thinking about the class of anchored games is to consider the case where μ is uniform over a set of edges in a bipartite graph on vertex set $\mathcal{X} \times \mathcal{Y}$; then the condition is that the induced subgraph on $\mathcal{X}_\perp \times \mathcal{Y}_\perp$ is a complete bipartite graph that is connected to the rest of $\mathcal{X} \times \mathcal{Y}$ and has weight at least α. In other words, a game G is anchored if it contains a free game that is connected to the entire game.

It is easy to see that the games $G_\perp$ output by the anchoring transformation given in Definition 64 are α-anchored. Free games are automatically 1-anchored (set $\mathcal{X}_\perp = \mathcal{X}$ and $\mathcal{Y}_\perp = \mathcal{Y}$), but the class of anchored games is much broader; indeed assuming the Exponential Time Hypothesis it is unlikely that there exists a similar (efficient) reduction from general games to free games [2]. Additionally, since free games are anchored games, our parallel repetition theorems automatically reproduce the quantum and multiplayer parallel repetition of free games results of [61, 24, 27], albeit with worse parameters.

Breaking correlations in repeated anchored games. Rather than providing a complete extension of the framework of Raz and Holenstein to the multiplayer and quantum settings, we interpolate between the case of free games and the general setting by showing how the same framework of dependency-breaking variables and states can be extended to anchored games – without using correlated sampling. We introduce dependency-breaking variables Ω and states $|\Phi_{x,y}\rangle$, and show that together they satisfy both Usefulness and Sampleability (properties discussed in Chapter 4).

The analysis for anchored games is more intricate than for free games. Proofs of the analogous statements for free games in [60, 24, 27] make crucial use of the fact that all possible question tuples are possible. An anchored game can be far from having this property. Instead, we use the anchors as a "home base" that is connected to all questions. Intuitively, no matter what question tuple $(x, y, z, \ldots)$ we are considering, it is only a few replacements away from the set of anchor questions. Thus the dependency of the variable Ω or state $|\Phi_{x,y}\rangle$ on the questions can be iteratively removed by "switching" each players' question to an anchor as

$$\mathsf{P}_{\Omega|X_i=x,Y_i=y,Z_i=z,W} \approx \mathsf{P}_{\Omega|X_i=x,Y_i=y,Z_i\in\perp,W} \approx \mathsf{P}_{\Omega|X_i=x,Y_i\in\perp,Z_i\in\perp,W} \approx \mathsf{P}_{\Omega|X_i\in\perp,Y_i\in\perp,Z_i\in\perp,W},$$

where "$X_i \in \perp$" is shorthand for the event that $X_i \in \mathcal{X}_\perp$.

Dealing with quantum strategies adds another layer of complexity to the argument. The local unitaries U_x and V_y such that $U_x \otimes V_y|\Phi\rangle \approx |\Phi_{xy}\rangle$ are quite important in the arguments of [61, 24, 27]. The difficulty in extending the argument for free games to the case of general games is to show that these local unitaries each only depend on the input to a single player. In fact with the definition of $|\Omega_{x,y}\rangle$ used in these works it appears likely that this statement does not hold, thus a different approach must be found.

When the game is anchored, however, we are able to use the anchor question in order to show the existence of requisite local unitaries U_x and V_y that depend only on a single player's question each. Achieving this requires us to introduce dependency-breaking states $|\Omega_{x,y}\rangle$ that are more complicated than those used in the free games case; in particular they include information about the *classical* dependency-breaking variables of Raz and Holenstein.

To do this, we prove a sequence of approximate equalities: first we show that for most x there exists U_x such that $(U_x \otimes \mathbb{I})|\Omega_{\perp,\perp}\rangle \approx |\Omega_{x,\perp}\rangle$, where $|\Omega_{\perp,\perp}\rangle$ denotes the dependency-breaking state in the case that both Alice and Bob receive the anchor question "$\perp$", and $|\Omega_{x,\perp}\rangle$ denotes the state when Alice receives x and Bob receives "$\perp$". Then we show that for all y such that $\mu(y|x) > 0$ there exists a unitary V_y such that $(\mathbb{I} \otimes V_y)|\Omega_{x,\perp}\rangle \approx |\Omega_{x,y}\rangle$. Accomplishing this step requires ideas and techniques going beyond those in the free games case. Interestingly, a crucial component of our proof is to argue the existence of a local unitary $R_{x,y}$ that depends on *both* inputs x and y. The unitary $R_{x,y}$ is not implemented by Alice or Bob in the simulation, but it is needed to show that V_y maps $|\Omega_{x,\perp}\rangle$ onto $|\Omega_{x,y}\rangle$.

6.3 Games, parallel repetition, and anchoring

We formally define k-player one-round games, their parallel repetition, and anchored games.

Multiplayer games. A k-player game $G = (\mathcal{X}, \mathcal{A}, \mu, V)$ is specified by a question set $\mathcal{X} = \mathcal{X}^1 \times \mathcal{X}^2 \times \cdots \times \mathcal{X}^k$, answer set $\mathcal{A} = \mathcal{A}^1 \times \mathcal{A}^2 \times \cdots \times \mathcal{A}^k$, a probability measure μ on $\mathcal{X}$, and a verification predicate $V : \mathcal{X} \times \mathcal{A} \to \{0,1\}$. Throughout this paper, we use superscripts in order to denote which player an input/output symbol is associated with. For example, we write x^1 to denote the input to the first player, and a^t to denote the output of the t-th player. Finally, to denote the tuple of questions/answers to all k players we write $x = (x^1, \ldots, x^k)$ and $a = (a^1, \ldots, a^k)$ respectively.

The *classical value* of a game G is denoted by $\mathrm{val}(G)$ and defined as

$$\mathrm{val}(G) := \sup_{f^1,\ldots,f^k} \mathop{\mathbb{E}}_{(x^1,\ldots,x^k)\sim\mu} \left[V\left((x^1, \ldots, x^k), (f^1(x^1), \ldots, f^k(x^k)) \right) \right]$$

where the supremum is over all functions $f_i : \mathcal{X}_i \to \mathcal{A}_i$; these correspond to deterministic strategies used by the players. It is easy to see that the classical value of a game is unchanged if we allow the strategies to take advantage of public or private randomness.

The *entangled value* of G is denoted by $\mathrm{val}^*(G)$ and defined as

$$\mathrm{val}^*(G) := \sup_{\substack{|\psi\rangle \in (\mathbb{C}^d)^{\otimes k} \\ M^1,\ldots,M^k}} \mathop{\mathbb{E}}_{(x^1,\ldots,x^k)\sim\mu} \sum_{\substack{(a^1,\ldots,a^k): \\ V((x^1,\ldots,x^k),(a^1,\ldots,a^k))=1}} \langle \psi | M^1(x^1, a^1) \otimes \cdots \otimes M^k(x^k, a^k) | \psi \rangle$$

where the supremum is over all integer $d \geq 2$, k-partite pure states $|\psi\rangle$ in $(\mathbb{C}^d)^{\otimes k}$, and $M^1, \ldots, M^k$ for each player. Each M^t is a set of POVM measurements $\{M(x^t, a^t)\}_{a^t \in \mathcal{A}^t}$ acting on $\mathbb{C}^d$, one for each question $x^t \in \mathcal{X}^t$.

Repeated games. Let $G = (\mathcal{X}, \mathcal{A}, \mu, V)$ be a k-player game, with $\mathcal{X} = \mathcal{X}^1 \times \cdots \times \mathcal{X}^k$ and $\mathcal{A} = \mathcal{A}^1 \times \cdots \times \mathcal{A}^k$. Let $\mu^{\otimes n}$ denote the product probability distribution over $\mathcal{X}^{\otimes n} = \bigotimes_{i=1}^n \mathcal{X}_i$, where each $\mathcal{X}_i$ is a copy of $\mathcal{X}$. Similarly let $\mathcal{A}^{\otimes n} = \bigotimes_{i=1}^n \mathcal{A}_i$ where each $\mathcal{A}_i$ is a copy of $\mathcal{A}$. [1] Let $V^{\otimes n} : \mathcal{X}^{\otimes n} \times \mathcal{A}^{\otimes n} \to \{0,1\}$ denote the verification predicate that is 1 on question tuple $(x_1, \ldots, x_n) \in \mathcal{X}^{\otimes n}$ and answer tuple $(a_1, \ldots, a_n) \in \mathcal{A}^{\otimes n}$ iff for all i, $V(x_i, a_i) = 1$. We define the n-fold parallel repetition of G to be the k-player game $G^n = (\mathcal{X}^{\otimes n}, \mathcal{A}^{\otimes n}, \mu^{\otimes n}, V^{\otimes n})$.

When working with games with more than 2 players, we use subscripts to denote which game round/coordinate a question/answer symbol is associated with. For example, by x_i^t we mean the question to the t-th player in the i-th round. While this is overloading notation slightly (because superscripts are meant to indicate tuples), we use this convention for the sake of readability. When x^n refers to a tuple $(x_1, \ldots, x_n)$ and when x_i^t refers to the t-th player's question in the i-th coordinate should be clear from context.

Anchored games. We give the general definition of an anchored game.

[1] We will use the tensor product notation ("$\otimes$") to denote product across coordinates in a repeated game, and the traditional product notation ("$\times$") to denote product across players.

Definition 66 (Multiplayer Anchored Games). *A game $G = (\mathcal{X}, \mathcal{A}, \mu, V)$ is called α-anchored if there exists $\mathcal{X}^t_\perp \subseteq \mathcal{X}^t$ for all $t \in [k]$ where*

1. *$\mu(\mathcal{X}^t_\perp) \geq \alpha$ for all $t \in [k]$, and*
2. *for all $x \in \mathcal{X}$,*
$$\mu(x) = \mu(x|_{\overline{F}_x}) \cdot \prod_{t \in F_x} \mu(x^t) \tag{6.1}$$

where for all question tuples $x = (x^1, x^2, \ldots, x^k) \in \mathcal{X}$, $F_x \subseteq [n]$ denotes the set of coordinates of x that lie in the anchor, i.e.
$$F_x = \{t \in [k] : x^t \in \mathcal{X}^t_\perp\}$$
and $\overline{F}_x$ denotes the complement, i.e., $[n] - F_x$.

Here for a set $S \subseteq [n]$, $\mu(x|_S)$ denotes the marginal probability of the question tuple x restricted to the coordinates in S, i.e.
$$\mu(x|_S) = \sum_{x'|_S = x|_S} \mu(x').$$

When $k = 2$ this definition coincides with the definition of two-player anchored games in Definition 65. Additionally, just like the two-player case, one can easily extend the anchoring transformation given in Definition 64 to arbitrary k-player games:

Proposition 67. *Let $G = (\mathcal{X}, \mathcal{A}, \mu, V)$ be a k-player game. Let $G_\perp$ be the k-player game where the referee samples $(x^1, x^2, \ldots, x^k)$ according to μ, replaces each x^t with an auxiliary symbol $\perp$ independently with probability α, and checks the players' answers according to V if all $x^t \neq \perp$, and otherwise the referee accepts. Then $G_\perp$ is an α-anchored game satisfying*
$$\mathrm{val}(G_\perp) = 1 - (1-\alpha)^k \cdot (1 - \mathrm{val}(G)), \qquad \mathrm{val}^*(G_\perp) = 1 - (1-\alpha)^k \cdot (1 - \mathrm{val}^*(G)). \tag{6.2}$$

Proof. We give the proof for the classical value; the same argument carries over to the entangled value. First, it is clear that $\mathrm{val}(G_\perp) \geq (1 - (1 - \alpha^k)) + (1-\alpha)^k \cdot \mathrm{val}(G)$. For the other direction, consider an optimal strategy for $G_\perp$. Under this strategy, we can express the entangled value as
$$\mathrm{val}(G_\perp) = (1-\alpha)^k \cdot \Pr(W | \forall t,\, x^t \neq \perp) + (1 - (1-\alpha^k)) \cdot \Pr(W | \exists\, t \text{ s.t. } x^t = \perp)$$
where W is the event that the players win. The optimal strategy for $G_\perp$ yields a strategy for G that wins with probability $\Pr(W | \forall t,\, x^t \neq \perp)$, which can be at most $\mathrm{val}(G)$. Since $\Pr(W | \exists\, t \text{ s.t. } x^t = \perp) = 1$, we obtain the desired equality. □

6.4 Classical multiplayer games

Perhaps the most well-known open problem about the classical parallel repetition of games is whether an analogue of Raz's theorem holds for games with more than two players. While the two-player case already presented a number of non-trivial difficulties, proving a parallel repetition theorem for three or more players is believed to require substantially new ideas.[2]

[2] This is mainly because the Raz/Holenstein framework, if extended to a multiplayer parallel repetition theorem in full generality, would likely also yield new lower bound techniques for multiparty communi-

In this section we make some progress on the multiplayer parallel repetition question: we prove a parallel repetition theorem for anchored games involving any number of players.

Theorem 68. *Let* $G = (\mathcal{X}, \mathcal{A}, \mu, V)$ *be a k-player* α*-anchored game such that* $\mathrm{val}(G) \leq 1 - \varepsilon$. *Then*

$$\mathrm{val}(G^n) \leq \exp\left(-\frac{\alpha^{2k} \cdot \varepsilon^3 \cdot n}{384 \cdot s \cdot k^2}\right), \tag{6.3}$$

where $s = \log |\mathcal{A}|$.

Combined with the anchoring operation described in Proposition 67, we obtain a gap amplification transformation that can be applied to any k-player game, yielding a decay of the value that matches, at least qualitatively, what one would expect from a general parallel repetition theorem.

From a more quantitative point of view, even in the two-player setting the optimal exponent of ε in (6.3) remains unknown. Perhaps more importantly, it is unclear whether the exponential dependence in k, due to the term α^k, in the bound is necessary; known lower bounds [43, 27] only show the need for a polynomial dependence on k in the exponent.

For the remainder of this section we fix a k-player α-anchored game $G = (\mathcal{X}, \mathcal{A}, \mu, V)$, an integer n, and a deterministic strategy for the k players in the repeated game G^n that achieves success probability $\mathrm{val}(G^n)$. In Section 6.4.1 we introduce the notation, random variables and basic lemmas for the proof. The proof of Theorem 68 itself is given in Section 6.4.2.

6.4.1 Breaking classical multipartite correlations

We refer to Section 6.3 for basic notation related to multiplayer games.

Let $C \subseteq [n]$ a fixed set of coordinates for the repeated game G^n of size $|C| = n - m$. It will be convenient to fix $C = \{m+1, m+2, \ldots, n\}$; the symmetry of the problem will make it clear that this is without loss of generality. Let $Z = A_C = (A_C^1, A_C^2, \ldots, A_C^k)$ denote the players' answers associated with the coordinates indexed by C.

For $t \in [k]$ let $\mathcal{Y}^t = (\mathcal{X}^t \setminus \mathcal{X}_\perp^t) \cup \{\perp\}$, and define a random variable

$$Y^t = \begin{cases} X^t, & X^t \in \mathcal{X}^t \setminus \mathcal{X}_\perp^t \\ \perp, & X^t \in \mathcal{X}_\perp^t \end{cases}. \tag{6.4}$$

Let $\mathcal{Y} = \mathcal{Y}^1 \times \mathcal{Y}^2 \times \ldots \times \mathcal{Y}^k$ and $Y = (Y^1, Y^2, \ldots, Y^k)$. For G^n we write

$$Y^{\otimes n} = (Y_1, Y_2, \ldots, Y_n) = \left(\left(Y_1^1, \ldots, Y_1^k\right), \left(Y_2^1, \ldots, Y_2^k\right), \ldots, \left(Y_n^1, \ldots, Y_n^k\right)\right).$$

Note that each k-tuple Y_i is a deterministic function of X_i. Furthermore, we will write Y_i^{-t} to denote Y_i with the t-th coordinate Y_i^t omitted.

For $i \in [n]$ let D_i be a subset of $[k]$ of size $k-1$ chosen uniformly at random, and $\overline{D}_i \in [k]$ its complement in $[k]$. Let $M_i = Y_i^{D_i}$ denote the coordinates of Y associated to

cation complexity, an area that has long resisted progress (especially for the important multiparty direct sum/product problems).

indices in D_i. Define the *dependence-breaking random variable* Ω_i as

$$\Omega_i = \begin{cases} (D_i, M_i) & i \in \overline{C} \\ X_i & i \in C \end{cases}. \tag{6.5}$$

The importance of Ω is captured in the following lemma.

Lemma 69. *(Local Sampling) Let X, Z, Ω be as above. Then $\mathsf{P}_{X_{-i}|X_i\Omega_{-i}Z}$ is a product distribution across the players:*

$$\mathsf{P}_{X_{-i}|X_i\Omega_{-i}Z} = \prod_{t=1}^{k} \mathsf{P}_{X^t_{-i}|\Omega^t_{-i}Z^tX^t_i}.$$

Proof. Conditioned on $M_i = Y_i^{D_i}$ each $X_i = (X_i^1, X_i^2, \dots, X_i^k)$ is a product distribution, hence $\mathsf{P}_{X_{-i}|\Omega_{-i}X_i}$ is product. Since for $t \in [k]$ Z^t is a deterministic function of X^t the same holds of $\mathsf{P}_{X_{-i}|\Omega_{-i}ZX_i}$. □

Lemma 69 crucially relies on the sets D_j being of size $k-1$: if two or more of the players' questions are unconstrained in a coordinate it is no longer necessarily true that $\mathsf{P}_{X_{-i}|\Omega_{-i}ZX_i}$ is product across all players.

Let $W = W_C = \bigwedge_{i=1}^{C} W_i$ denote the event that the players' answers Z to questions in the coordinates indexed by C satisfy the predicate V. Let

$$\delta = \frac{|C| \log |\mathcal{A}| + \log \frac{1}{\Pr(W_C)}}{m}. \tag{6.6}$$

The following lemma and its corollary are direct consequences of analogous lemmas used in the analysis of repeated two-player games, as stated in e.g. [56, Lem. 5] and [56, Cor. 6]. They do not depend on the structure of the game, and only rely on W being an event defined only on (X_C, Z).

Lemma 70. *We have*

$$\begin{aligned} &(i) && \mathop{\mathbb{E}}_{i\in[m]} \|\mathsf{P}_{X_iY_i\Omega_i|W} - \mathsf{P}_{X_iY_i\Omega_i}\| \le \sqrt{\delta}. \\ &(ii) && \mathop{\mathbb{E}}_{i\in[m]} \|\mathsf{P}_{X_iY_iZ\Omega_{-i}|W} - \mathsf{P}_{X_i|Y_i}\mathsf{P}_{Y_iZ\Omega_{-i}|W}\| \le \sqrt{\delta} \\ &(iii) && \mathop{\mathbb{E}}_{i\in[m]} \|\mathsf{P}_{Y_iZ\Omega|W} - \mathsf{P}_{Y_i|\Omega_i}\mathsf{P}_{Z\Omega|W}\| \le \sqrt{\delta}. \end{aligned}$$

Proof. Item (i) follows directly from [56, Lem. 5] by taking $U_i = X_iY_i\Omega_i$. For (ii) apply [56, Cor. 6] with $U_i = X_i$ and $T = (Y_1, Y_2, \dots, Y_m, X_C)$ to get

$$\mathop{\mathbb{E}}_{i\in[m]} \|\mathsf{P}_{X_iZY_{[m]}X_C|W} - \mathsf{P}_{X_i|Y_i}\mathsf{P}_{Y_iZY_{[m]\setminus\{i\}}X_C|W}\| \le \sqrt{\delta}, \tag{6.7}$$

which is stronger than (ii); (ii) follows by marginalizing $Y_i^{\overline{D}_i}$ in each term. Finally, the same corollary applied with $U_i = Y_i$ and $T = \Omega$ shows (iii). □

Corollary 71.

$$\mathop{\mathbb{E}}_{i\in[m]} \sum_{t=1}^{k} \|\mathsf{P}_{Y_i}\mathsf{P}_{Z\Omega_{-i}|WY_i} - \mathsf{P}_{Y_i}\mathsf{P}_{Z\Omega_{-i}|WY_i^{-t}}\| \le 3k \cdot \sqrt{\delta}.$$

Proof. We have $\mathsf{P}_{Y_i|\Omega_i}\mathsf{P}_{Z\Omega|W} = \mathsf{P}_{Y_i|\Omega_i}\mathsf{P}_{\Omega_i|W}\mathsf{P}_{Z\Omega_{-i}|W\Omega_i}$. Applying Lemma 2 with $\mathsf{Q}_F = \mathsf{P}_{\Omega_i|W}$, $\mathsf{S}_F = \mathsf{P}_{\Omega_i}$, and $\mathsf{R}_{G|F} = \mathsf{P}_{Y_i|\Omega_i}\mathsf{P}_{Z\Omega_{-i}|W\Omega_i}$, we see that

$$\mathop{\mathbb{E}}_{i\in[m]} \|\mathsf{P}_{Y_i|\Omega_i}\mathsf{P}_{Z\Omega|W} - \mathsf{P}_{Y_i\Omega_i}\mathsf{P}_{Z\Omega_{-i}|W\Omega_i}\| = \mathop{\mathbb{E}}_{i\in[m]} \|\mathsf{P}_{\Omega_i|W} - \mathsf{P}_{\Omega_i}\| \le \sqrt{\delta},$$

where the last inequality follows from Lemma 70, item (i). Combining the above with item (iii) of the same Lemma, we have

$$\mathop{\mathbb{E}}_{i\in[m]} \|\mathsf{P}_{Y_iZ\Omega|W} - \mathsf{P}_{Y_i\Omega_i}\mathsf{P}_{Z\Omega_{-i}|W\Omega_i}\| \le 2\sqrt{\delta}. \tag{6.8}$$

Noting that Ω_i is determined by Y_i (the D_i are completely independent of everything else), (6.8) implies

$$\begin{aligned}\mathop{\mathbb{E}}_{i\in[m]}\mathop{\mathbb{E}}_{t\in[k]} \|\mathsf{P}_{Y_iZ\Omega_{-i}|W} - \mathsf{P}_{Y_i}\mathsf{P}_{Z\Omega_{-i}|WY_i^{-t}}\| &= \mathop{\mathbb{E}}_{i\in[m]} \|\mathsf{P}_{Y_iZ\Omega_{-i}|W} - \mathsf{P}_{Y_i}\mathsf{P}_{Z\Omega_{-i}|W\Omega_i}\| \\ &\le 2\sqrt{\delta}.\end{aligned}$$

Finally, notice that Lemmas 2 and 70 imply $\mathbb{E}_{i\in[m]} \|\mathsf{P}_{Y_iZ\Omega_{-i}|W} - \mathsf{P}_{Y_i}\mathsf{P}_{Z\Omega_{-i}|WY_i}\| = \mathbb{E}_{i\in[m]} \|\mathsf{P}_{Y_i} - \mathsf{P}_{Y_i|W}\| \le \sqrt{\delta}$; the desired result follows. □

6.4.2 Proof of the parallel repetition theorem

This section is devoted to the proof of Theorem 68. The main ingredient of the proof is given in the next proposition.

Proposition 72. *Let $C \subseteq [n]$ and X, Z, Ω_{-i} be defined as in Section 6.4.1. Then*

$$\mathop{\mathbb{E}}_{i\in[m]} \|\mathsf{P}_{X_i\Omega_{-i}Z|W} - \mathsf{P}_{X_i}\mathsf{P}_{\Omega_{-i}Z|W,Y_i=\perp^k}\| \le (6k\alpha^{-k}+1)\sqrt{\delta}, \tag{6.9}$$

where δ is defined in (6.6).

Theorem 68 follows from this proposition in a relatively standard fashion; this is done at the end of this section. Let us now prove Proposition 72 assuming a certain technical statement, Lemma 73. This lemma is proved immediately after.

Proof of Proposition 72. First observe that

$$\|\mathsf{P}_{X_i\Omega_{-i}Z|W} - \mathsf{P}_{X_i}\mathsf{P}_{\Omega_{-i}Z|W,Y_i=\perp^k}\| = \|\mathsf{P}_{X_iY_i\Omega_{-i}Z|W} - \mathsf{P}_{X_iY_i}\mathsf{P}_{\Omega_{-i}Z|W,Y_i=\perp^k}\|$$

as Y_i is a deterministic function of X_i. Applying Lemma 70, item (ii) we get

$$\mathop{\mathbb{E}}_{i\in[m]} \|\mathsf{P}_{X_iY_i\Omega_{-i}Z|W} - \mathsf{P}_{X_i|Y_i}\mathsf{P}_{Y_i\Omega_{-i}Z|W}\| \le \sqrt{\delta}.$$

The latter distribution can be written as $\mathsf{P}_{Y_i|W}\mathsf{P}_{X_i|Y_i}\mathsf{P}_{\Omega_{-i}Z|WY_i}$. Applying Lemma 2 with $\mathsf{Q}_F = \mathsf{P}_{Y_i|W}$ and $\mathsf{S}_F = \mathsf{P}_{Y_i}$ we see that

$$\|\mathsf{P}_{X_i|Y_i}\mathsf{P}_{Y_i\Omega_{-i}Z|W} - \mathsf{P}_{X_iY_i}\mathsf{P}_{\Omega_{-i}Z|WY_i}\| = \|\mathsf{P}_{Y_i|W} - \mathsf{P}_{Y_i}\|,$$

which is bounded by $\sqrt{\delta}$ on average over i by Lemma 70, item (i). Hence

$$\begin{aligned}\mathop{\mathbb{E}}_{i\in[m]} \left\|\mathsf{P}_{X_i\Omega_{-i}Z|W} - \mathsf{P}_{X_i}\mathsf{P}_{\Omega_{-i}Z|W,Y_i=\perp^k}\right\| &\le 2\sqrt{\delta} + \mathop{\mathbb{E}}_{i\in[m]} \left\|\mathsf{P}_{X_iY_i}\mathsf{P}_{\Omega_{-i}Z|WY_i} - \mathsf{P}_{X_iY_i}\mathsf{P}_{\Omega_{-i}Z|W,Y_i=\perp^k}\right\| \\ &= 2\sqrt{\delta} + \mathop{\mathbb{E}}_{i\in[m]} \left\|\mathsf{P}_{Y_i}\mathsf{P}_{\Omega_{-i}Z|WY_i} - \mathsf{P}_{Y_i}\mathsf{P}_{\Omega_{-i}Z|W,Y_i=\perp^k}\right\|,\end{aligned}$$

where the equality follows from Lemma 2 applied with $\mathsf{R}_{G|F} = \mathsf{P}_{X_i|Y_i}$. Applying the triangle inequality,

$$\begin{aligned}&\mathop{\mathbb{E}}_{i\in[m]} \left\|\mathsf{P}_{X_iY_i}\mathsf{P}_{\Omega_{-i}Z|WY_i} - \mathsf{P}_{X_iY_i}\mathsf{P}_{\Omega_{-i}Z|W,Y_i=\perp^k}\right\| \\ &\qquad = \mathop{\mathbb{E}}_{i\in[m]} \left\|\mathsf{P}_{Y_i}\mathsf{P}_{\Omega_{-i}Z|WY_i} - \mathsf{P}_{Y_i}\mathsf{P}_{\Omega_{-i}Z|W,Y_i=\perp^k}\right\| \\ &\qquad \le \mathop{\mathbb{E}}_{i\in[m]} \sum_{t=1}^{k} \left\|\mathsf{P}_{Y_i}\mathsf{P}_{\Omega_{-i}Z|WY_i^{<t}=\perp^{t-1},Y_i^{\ge t}} - \mathsf{P}_{Y_i}\mathsf{P}_{\Omega_{-i}Z|WY_i^{\le t}=\perp^{t},Y_i^{>t}}\right\| \qquad (6.10) \\ &\qquad \le 6k\alpha^{-k}\cdot\sqrt{\delta}, \qquad (6.11)\end{aligned}$$

where (6.10) is proved by Lemma 73 below and (6.11) follows from Corollary 71. □

Lemma 73. *Let $S \subset [k]$ and $t \in \overline{S}$. Then*

$$\begin{aligned}&\left\|\mathsf{P}_{Y_i}\mathsf{P}_{\Omega_{-i}Z|WY_i^{S}=\perp^{S},Y_i^{\overline{S}}} - \mathsf{P}_{Y_i}\mathsf{P}_{\Omega_{-i}Z|WY_i^{S\cup\{t\}}=\perp^{S\cup\{t\}},Y_i^{\overline{S}\setminus\{t\}}}\right\| \\ &\qquad \le 2\alpha^{-(|S|+1)}\cdot\left\|\mathsf{P}_{Y_i}\mathsf{P}_{Z\Omega_{-i}|WY_i} - \mathsf{P}_{Y_i}\mathsf{P}_{Z\Omega_{-i}|WY_i^{-t}}\right\|. \qquad (6.12)\end{aligned}$$

Proof. In the proof for ease of notation we omit the subscript i and write Y instead of Y_i. After relabeling we may assume $S = \{1,2,\ldots,r-1\}$ and $t = r$ where $1 \le r < k$. Expanding the expectation over Y explicitly we can rewrite the left-hand side of (6.12) as

$$\left\|\mathsf{P}_{Y}\cdot\left(\mathsf{P}_{\Omega_{-i}Z|W,y^{\ge r},y^{<r}=\perp^{r-1}} - \mathsf{P}_{\Omega_{-i}Z|W,y^{>r},y^{\le r}=\perp^{r}}\right)\right\|. \qquad (6.13)$$

Next we use a symmetrization argument to bound the above expression. Consider a random variable $\hat{Y}$ that is a copy of Y, and is coupled to Y in the following way: $\hat{Y}^{-r} = Y^{-r}$, and conditioned on any setting of $Y^r = y^r$, $\hat{Y}^r$ and Y^r are independent. Using the fact that $\Pr[\hat{Y}^r = \perp] \ge \alpha$ conditioned on any value of $Y^{-r} = U^{-r} = y^{-r}$, we get that the expression in (6.13) is at most

$$\alpha^{-1}\left\|\mathsf{P}_{Y^{-r}}\mathsf{P}_{Y^r|Y^{-r}}\mathsf{P}_{\hat{Y}^r|Y^{-r}}\cdot\left(\mathsf{P}_{\Omega_{-i}Z|W,y^{>r},y^{r},y^{<r}=\perp^{r-1}} - \mathsf{P}_{\Omega_{-i}Z|W,y^{>r},\hat{y}^{r},y^{<r}=\perp^{r-1}}\right)\right\|.$$

Using the triangle inequality and symmetry of Y and $\hat{Y}$, this expression can be bounded by

$$2\alpha^{-1}\cdot\left\|\mathsf{P}_{Y}\cdot\left(\mathsf{P}_{\Omega_{-i}Z|W,y^{>r},y^{r},y^{<r}=\perp^{r-1}} - \mathsf{P}_{\Omega_{-i}Z|W,y^{>r},y^{<r}=\perp^{r-1}}\right)\right\|,$$

which after noting that the quantity $\|\mathsf{P}_{\Omega_{-i}Z|W,y^{>r},y^{r},y^{<r}=\perp^{r-1}} - \mathsf{P}_{\Omega_{-i}Z|W,y^{>r},y^{\le r}=\perp^{r}}\|$ is independent of the variable $Y^{<r}$, can be rewritten as

$$2\alpha^{-1}\cdot\left\|\mathsf{P}_{Y^{\ge r}}\cdot\left(\mathsf{P}_{\Omega_{-i}Z|W,y^{>r},y^{r},y^{<r}=\perp^{r-1}} - \mathsf{P}_{\Omega_{-i}Z|W,y^{>r},y^{<r}=\perp^{r-1}}\right)\right\|.$$

Using that the event that $Y^{<r} = \perp^{r-1}$ occurs with probability at least α^{r-1} and $\mathsf{P}_{Y^{\geq r}|Y^{<r}=\perp^{r-1}} = \mathsf{P}_{Y^{\geq r}}$ by the anchor property, we can finally bound (6.13) by

$$2\alpha^{-r} \cdot \|\mathsf{P}_Y \mathsf{P}_{Z\Omega_{-i}|WY} - \mathsf{P}_Y \mathsf{P}_{Z\Omega_{-i}|WY^{-r}}\|,$$

which is the desired result. □

We prove Theorem 68 by iteratively applying Proposition 72 as follows.

Proof of Theorem 68. Let $C_0 = \emptyset$ and $\delta_0 = 0$. While $(6k\alpha^{-k}+1)\sqrt{\delta_s} \leq \varepsilon/2$, by Proposition 72, we can choose $i \in \overline{C}_s$ with $\left\|\mathsf{P}_{X_i\Omega_{-i}Z|W} - \mathsf{P}_{X_i}\mathsf{P}_{\Omega_{-i}Z|W,Y_i=\perp^k}\right\| \leq \varepsilon/2$. Set $C_{s+1} = C_s \cup \{i\}$ and $\delta_{s+1} = (|C_{s+1}|\log|\mathcal{A}| + \log 1/\Pr(W_{C_{s+1}}))/m$. First we show that throughout this process the bound

$$\Pr[W_{C_s}] \leq (1-\varepsilon/2)^{|C_s|} \tag{6.14}$$

holds. Since by the choice of i one has $\|\mathsf{P}_{X_i\Omega_{-i}Z|W_C} - \mathsf{P}_{X_i}\mathsf{P}_{\Omega_{-i}Z|W_C,Y_i=\perp^k}\| \leq \varepsilon/2$, to establish (6.14) it will suffice to show that

$$\Pr(W_i|W_C) \leq \mathrm{val}(G) + \|\mathsf{P}_{X_i\Omega_{-i}Z|W_C} - \mathsf{P}_{X_i}\mathsf{P}_{\Omega_{-i}Z|W_C,Y_i=\perp^k}\|. \tag{6.15}$$

The proof of (6.15) is based on a rounding argument. Consider the following strategy for G: First, the players use shared randomness to obtain a common sample from $\mathsf{P}_{\Omega_{-i}Z|W_C,Y_i=\perp^k}$. After receiving her question x_t^*, player $t \in [k]$ samples questions for the remaining coordinates according to $\mathsf{P}_{X^t_{-i}|\Omega^t_{-i}Z^tX^t_i}$, forming the tuple $X^t = (X^t_{-i}, x_t^*)$. She determines her answer $a_i^t \in \mathcal{A}_i^t$ according to the strategy for G^n. The distribution over questions X implemented by players following this strategy is

$$\mathsf{P}_{X_i}\mathsf{P}_{\Omega_{-i}Z|W_CY_i=\perp^k}\prod_{t=1}^{k}\mathsf{P}_{X^t_{-i}|\Omega^t_{-i}Z^tX^t_i},$$

which by Lemma 69 is equal to

$$\mathsf{P}_{X_i}\mathsf{P}_{\Omega_{-i}Z|W_CY_i=\perp^k}\mathsf{P}_{X_{-i}|\Omega_{-i}Z}.$$

On the other hand from the definition of Ω_{-i} we have

$$\mathsf{P}_{X\Omega_{-i}Z|W_C} = \mathsf{P}_{X_i\Omega_{-i}Z|W_C}\mathsf{P}_{X_{-i}|\Omega_{-i}ZW_C} = \mathsf{P}_{X_i\Omega_{-i}Z|W_C}\mathsf{P}_{X_{-i}|\Omega_{-i}Z}.$$

Applying Lemma 2 with $R = \mathsf{P}_{X_{-i}|\Omega_{-i}Z}$ it follows that

$$\left\|\mathsf{P}_{XZ\Omega_{-i}|W_C} - \mathsf{P}_{X_i}\mathsf{P}_{\Omega_{-i}Z|W_CY_i=\perp^k}\mathsf{P}_{X_{-i}|\Omega_{-i}Z}\right\| = \left\|\mathsf{P}_{X_i\Omega_{-i}Z|W_C} - \mathsf{P}_{X_i}\mathsf{P}_{\Omega_{-i}Z|W_C,Y_i=\perp^k}\right\|.$$

Now by definition the winning probability of the extracted strategy for G is at most $\mathrm{val}(G)$, and (6.15) follows.

Let now C be the final set of coordinates when the above-described process stops; at this point we must have

$$\delta = \frac{|C|\log|\mathcal{A}| + \log\frac{1}{\Pr(W_C)}}{n-|C|} > \frac{\alpha^{2k}\varepsilon^2}{48\cdot k^2}.$$

If $|C| \geq n/2$ we are already done by (6.14). Suppose $\frac{|C|\log|\mathcal{A}|+\log(\frac{1}{\Pr[W_C]})}{n} > \frac{\alpha^{2k}\epsilon^2}{96\cdot k^2}$. If $\log(\frac{1}{\Pr(W_C)}) \geq \frac{n\cdot\alpha^{2k}\epsilon^2}{192\cdot k^2}$ we are again done; hence, we can assume

$$\frac{|C|\log|\mathcal{A}|}{n} > \frac{\alpha^{2k}\epsilon^2}{192\cdot k^2}.$$

Now plugging the lower bound on the size of C in (6.14) we get

$$\mathrm{val}(G^n) \leq \Pr(W_C) \leq \exp\left(-\frac{\alpha^{2k}\cdot\varepsilon^3\cdot n}{384\cdot k^2\cdot s}\right)$$

where $s = \log|\mathcal{A}|$, which completes the proof. □

Some remarks on multiplayer parallel repetition for general games. We conclude this section with some remarks about Theorem 68 and the more general problem of multiplayer parallel repetition. Our analysis of repeated anchored games follows the information-theoretic approach of Raz and Holenstein. It is a natural question, predating this work by many years, whether one can extend this framework to prove parallel repetition for general multiplayer games?

At first sight the Raz/Holenstein framework may seem quite suitable for multiplayer parallel repetition. For instance, it is folklore that classically the approach extends to the case of free games with any number of players, and furthermore, many of the other technical components of the proof readily carry over in much generality. Despite these positive signs, attempts to extend Raz's original argument to the general multiplayer setting have so far failed for different and rather interesting *technical reasons*. Embarrassingly, to our knowledge, it is not even known how to extend the information-theoretic approach to prove that the value of a repeated k-player game decays at all![3]

We give an example of one of the difficulties in proving a multiplayer parallel repetition theorem for general games. Consider the problem of defining an appropriate dependency-breaking variable Ω in the multiplayer setting. There are two competing demands on Ω: on one hand the breaking of dependencies between the players' respective questions seems to require it to contain as many of the players' questions as possible for each coordinate $i \in \overline{C}$. In fact, if the correlations between the players inputs' are generic, it seems hard to avoid the need to keep at least $k-1$ inputs in each Ω_i, as we do in Lemma 69. On the other hand, for correlated sampling to be possible, it seems necessary for Ω to specify very few of the questions per coordinate, or in fact in the generic case, at most 1; as soon as $k \geq 3$ both requirements are in direct contradiction.

An insight behind our result is that it is sometimes possible to decouple the above two competing demands on Ω (i.e. the *dependency-breaking* and the *correlated sampling* components). More precisely, when the base game is anchored, we show how to define a useful dependency-breaking variable (or quantum state, in the entangled players setting) that can be sampled *without* correlated sampling. With correlated sampling out of the way, the aforementioned conflict between correlated sampling and dependency-breaking disappears, allowing us to proceed with the argument.

[3] One can modify a Ramsey-theoretic argument of Verbitsky to show that if $\mathrm{val}(G) < 1$, then $\mathrm{val}(G^n)$ must go to 0 eventually as n grows [98], but the bound on the rate of decay is extremely poor.

6.5 Parallel repetition of anchored games with entangled players

This section is devoted to the analysis of the entangled value of repeated anchored games. The main theorem we prove is the following:

Theorem 74. *Let G be a k-player α-anchored game satisfying* $\mathrm{val}^*(G) = 1 - \varepsilon$. *Then*

$$\mathrm{val}^*(G^n) \leq \exp\left(-\Omega\left(\frac{\mathrm{poly}(\alpha^k) \cdot \varepsilon^8 \cdot n}{\mathrm{poly}(k) \cdot s}\right)\right),$$

where s is the total length of the answers output by the players.

Thus as in the classical multiplayer case, the anchoring operation described in Proposition 67 provides a general gap amplification transformation for the entangled value of any multiplayer game.

For clarity we will focus on the $k = 2$ (two-player) case; we will describe how to extend the proof to arbitrary k at the end. We fix an α-anchored two-player game $G = (\mathcal{X} \times \mathcal{Y}, \mathcal{A} \times \mathcal{B}, \mu, V)$ with entangled value $\mathrm{val}^*(G) = 1 - \varepsilon$ and anchor sets $\mathcal{X}_\perp \subseteq \mathcal{X}$, $\mathcal{Y}_\perp \subseteq \mathcal{Y}$ for Alice and Bob, respectively. We also fix an optimal strategy for G^n, consisting of a shared entangled state $|\psi\rangle^{E_A E_B}$ and POVMs $\{A^{a^n}_{x^n}\}$ and $\{B^{b^n}_{y^n}\}$ for Alice and Bob respectively. Without loss of generality we assume that $|\psi\rangle$ is invariant under permutation of the two registers, i.e. there exist basis vectors $\{|v_j\rangle\}_j$ such that $|\psi\rangle = \sum_j \sqrt{\lambda_j}|v_j\rangle|v_j\rangle$.

6.5.1 Setup

We introduce the random variables, entangled states and operators that play an important role in the proof of Theorem 74. The section is divided into three parts: first we define the dependency-breaking variable Ω, with a slightly modified definition from the one introduced for the classical multiplayer setting in Section 6.4. Then we state useful lemmas about conditioned distributions. Finally we describe the states and operators used in the proof.

Dependency-breaking variables. Let $C \subseteq [n]$ a fixed set of coordinates for the repeated game G^n. We will assume that $C = \{m+1, m+2, \ldots, n\}$, where $m = n - |C|$, as this will easily be seen to hold without loss of generality. Let (X^n, Y^n) be distributed according to μ^n and (A^n, B^n) be defined from X^n and Y^n as follows:

$$\mathrm{P}_{A^n B^n | X^n = x^n, Y^n = y^n}(a^n, b^n) = \langle\psi| A^{a^n}_{x^n} \otimes B^{b^n}_{y^n} |\psi\rangle.$$

Let (X_C, Y_C) and $Z = (A_C, B_C)$ denote the players' questions and answers respectively associated with the coordinates indexed by C. For $i \in [n]$ let W_i denote the event that the players win round i while playing G^n. Let $W_C = \bigwedge_{i \in C} W_i$.

We use the same dependency-breaking variable Ω that is used in Holenstein's proof of parallel repetition. In those works, for all $i \in [n]$, Ω_i fixes at least one of X_i or Y_i (and sometimes both, if $i \in C$). Thus, conditioned on Ω, X^n and Y^n are independent of each other.

In more detail, let $D_1, \ldots, D_m$ be independent and uniformly distributed over $\{A, B\}$. Let $M_1, \ldots, M_m$ be independent random variables defined in the following way. If $D_i = A$, then M_i is coupled to X_i (that is, takes the same value as X_i). Otherwise, if $D_i = B$, then M_i is coupled to Y_i. Then $\Omega_i = (D_i, M_i)$, and $\Omega = (\Omega_1, \ldots, \Omega_m, X_C, Y_C)$.

Conditioned distributions. Define $\delta_C := \frac{1}{m}(\log 1/\Pr(W_C) + |C| \log |\mathcal{A}||\mathcal{B}|)$. For notational convenience we often use the shorthand $X_i \in \perp$ and $Y_i \in \perp$ to stand for $X_i \in \mathcal{X}_\perp$ and $Y_i \in \mathcal{Y}_\perp$, respectively. The following lemma essentially follows from lemmas in [56] and the arguments used in the proof of Lemma 73 in Section 6.4.

Lemma 75. *The following statements hold on, average over i chosen uniformly in* $[m]$*:*

1. $\mathbb{E}_i \|\mathsf{P}_{D_i M_i X_i Y_i | W_C} - \mathsf{P}_{D_i M_i X_i Y_i}\| \leq O(\sqrt{\delta_C})$
2. $\mathbb{E}_i \|\mathsf{P}_{\Omega Z X_i Y_i | W_C} - \mathsf{P}_{\Omega Z | W_C} \mathsf{P}_{X_i Y_i | \Omega}\| \leq O(\sqrt{\delta_C})$
3. $\mathbb{E}_i \|\mathsf{P}_{X_i Y_i} \mathsf{P}_{\Omega_{-i} Z | X_i \in \perp, Y_i \in \perp, W_C} - \mathsf{P}_{X_i Y_i} \mathsf{P}_{\Omega_{-i} Z | X_i Y_i W_C}\| \leq O(\sqrt{\delta_C}/\alpha^2)$
4. $\mathbb{E}_i \left\|\mathsf{P}_{X_i Y_i} \mathsf{P}_{\Omega_{-i} Z | X_i Y_i W_C} - \mathsf{P}_{X_i Y_i \Omega_{-i} Z | W}\right\| \leq O(\sqrt{\delta_C}/\alpha^2)$

Quantum states and operators. Recall that we have fixed an optimal strategy for Alice and Bob in the game G^n. This specifies a shared entangled state $|\psi\rangle$, and measurement operators $\{A_{x^n}^{a^n}\}$ for Alice and $\{B_{y^n}^{b^n}\}$ for Bob.

Operators. Define, for all a_C, b_C, x^n, y^n:

$$A_{x^n}^{a_C} := \sum_{a^n | a_C} A_{x^n}^{a^n} \qquad\qquad B_{y^n}^{b_C} := \sum_{b^n | b_C} B_{y^n}^{b^n}$$

where $a^n | a_C$ (resp. $b^n | b_C$) indicates summing over all tuples a^n consistent with the suffix a_C (resp. b^n consistent with suffix b_C). For all i, ω_{-i}, x_i, and y_i define:

$$A_{\omega_{-i}, x_i}^{a_C} = \mathop{\mathbb{E}}_{X^n | \omega_{-i}, x_i} A_{x^n}^{a_C} \qquad\qquad B_{\omega_{-i}, y_i}^{b_C} = \mathop{\mathbb{E}}_{Y^n | \omega_{-i}, y_i} B_{y^n}^{b_C}$$

where recall that $\mathbb{E}_{X^n | \omega_{-i}, x_i}$ is shorthand for $\mathbb{E}_{X^n | \Omega_{-i} = \omega_{-i}, X_i = x_i}$. Intuitively, these operators represent the "average" measurement that Alice and Bob apply, conditioned on $\Omega_{-i} = \omega_{-i}$, and $X_i = x_i$ and $Y_i = y_i$. Next, define

$$A_{\omega_{-i}, \perp}^{a_C} := \mathop{\mathbb{E}}_{X^n | \Omega_{-i} = \omega_{-i} \wedge X_i \in \perp} A_{x^n}^{a_C} \qquad\qquad B_{\omega_{-i}, \perp}^{b_C} := \mathop{\mathbb{E}}_{Y^n | \Omega_{-i} = \omega_{-i} \wedge Y_i \in \perp} B_{y^n}^{b_C}.$$

These operators represent the "average" measurement performed by Alice and Bob, conditioned on $\Omega_{-i} = \omega_{-i}$ and $M_i = \perp$. Finally, for all $x_i \in \mathcal{X}$ and $y_i \in \mathcal{Y}$, define

$$A_{\omega_{-i}, \perp / x_i}^{a_C} := \frac{1}{2} A_{\omega_{-i}, \perp}^{a_C} + \frac{1}{2} A_{\omega_{-i}, x_i}^{a_C} \qquad\qquad B_{\omega_{-i}, \perp / y_i}^{b_C} := \frac{1}{2} B_{\omega_{-i}, \perp}^{b_C} + \frac{1}{2} B_{\omega_{-i}, y_i}^{b_C}.$$

Intuitively, these operators represent the "average" measurements conditioned on $\Omega_{-i} = \omega_{-i}$ and when X_i is x_i with probability $1/2$ and $\perp$ with probability $1/2$ (or when $Y_i = y_i$ with probability $1/2$ and $\perp$ with probability $1/2$).

For notational convenience we often suppress the dependence on $(i, \omega_{-i}, z = (a_C, b_C))$ when it is clea from context. Thus, when we refer to an operator such as $A_{\perp / x}$, we really mean the operator $A_{\omega_{-i}, \perp / x_i}^{a_C}$.

States. For all $x \in \mathcal{X}$ and $y \in \mathcal{Y}$, define the following (unnormalized) states:

$$|\Phi_{x,y}\rangle := \sqrt{A_x} \otimes \sqrt{B_y} |\psi\rangle \qquad\qquad |\Phi_{x,\perp}\rangle := \sqrt{A_x} \otimes \sqrt{B_\perp} |\psi\rangle$$

$$|\Phi_{\perp/x,\perp}\rangle := \sqrt{A_{\perp/x}} \otimes \sqrt{B_\perp}|\psi\rangle \qquad |\Phi_{\perp/x,y}\rangle := \sqrt{A_{\perp/x}} \otimes \sqrt{B_y}|\psi\rangle \tag{6.16}$$

$$|\Phi_{\perp,\perp}\rangle := \sqrt{A_\perp} \otimes \sqrt{B_\perp}|\psi\rangle$$

together with the normalization factors

$$\gamma_{x,y} := \||\Phi_{x,y}\rangle\| \qquad \gamma_{x,\perp} := \||\Phi_{x,\perp}\rangle\|$$

$$\gamma_{\perp/x,\perp} := \||\Phi_{\perp/x,\perp}\rangle\| \qquad \gamma_{\perp/x,y} := \||\Phi_{\perp/x,y}\rangle\|$$

$$\gamma_{\perp,\perp} := \||\Phi_{\perp,\perp}\rangle\|$$

Note that these normalization factors are the square-roots of the probabilities that a certain pair of answers $z = (a_C, b_C)$ occurred, given the specified inputs and the dependency-breaking variables. For example, revealing the depencies on ω_{-i} and z, we have

$$\gamma_{\substack{\omega_{-i},z \\ x_i,y_i}} = \sqrt{\mathsf{P}_{Z|\omega_{-i},x_i,y_i}(z)}.$$

We denote the normalized states by $|\widetilde{\Phi}_{x,y}\rangle = |\Phi_{x,y}\rangle/\gamma_{x,y}$, $|\widetilde{\Phi}_{x,\perp}\rangle = |\Phi_{x,\perp}\rangle/\gamma_{x,\perp}$, $|\widetilde{\Phi}_{\perp/x,\perp}\rangle = |\Phi_{\perp,\perp}\rangle/\gamma_{\perp/x,\perp}$, $|\widetilde{\Phi}_{\perp/x,\perp/y}\rangle = |\Phi_{\perp/x,y}\rangle/\gamma_{\perp/x,y}$, and $|\widetilde{\Phi}_{\perp,\perp}\rangle = |\Phi_{\perp,\perp}\rangle/\gamma_{\perp,\perp}$.

6.5.2 Proof of the parallel repetition theorem

Lemma 76. *Let G be an α-anchored two-player game. Let $C \subset [n]$ be a set of coordinates. Then*

$$\mathop{\mathbb{E}}_{i \notin C} \Pr(W_i|W_C) \leq \mathrm{val}^*(G) + O(\delta_C^{1/8}/\alpha^2)$$

where the expectation is over a uniformly chosen $i \in [n]\backslash C$ and $\delta_C = \frac{1}{m}(\log 1/\Pr(W_C) + |C| \log |\mathcal{A}||\mathcal{B}|)$.

Proof. The proof is based on a similar rounding argument to the multiplayer case, but it now involves entangled strategies. For every ω_{-i}, $z = (a_C, b_C)$, $x_i \in \mathcal{X}$, $y_i \in \mathcal{Y}$, $a_i \in \mathcal{A}$ and $b_i \in \mathcal{B}$, define

$$\hat{A}^{a_i}_{\omega_{-i},x_i} := \sum_{a^n|a_i,a_C} (A^{a_C}_{\omega_{-i},x_i})^{-1/2} A^{a^n}_{\omega_{-i},x_i} (A^{a_C}_{\omega_{-i},x_i})^{-1/2}$$

$$\hat{B}^{b_i}_{\omega_{-i},y_i} := \sum_{b^n|b_i,b_C} (B^{b_C}_{\omega_{-i},y_i})^{-1/2} B^{b^n}_{\omega_{-i},y_i} (B^{b_C}_{\omega_{-i},y_i})^{-1/2}$$

where $a^n|a_i, a_C$ (resp. $b^n|b_i, b_C$) denotes summing over tuples a^n that are consistent with a_C and a_i (resp. b^n that are consistent with b_C and b_i). Note that the $\{\hat{A}^{a_i}_{\omega_{-i},x_i}\}_{a_i}$ and $\{\hat{B}^{b_i}_{\omega_{-i},y_i}\}_{b_i}$ are positive semidefinite operators that sum to identity, so form valid POVMs.

Consider the following strategy to play game G. Alice and Bob share classical public randomness, and for every setting of i, ω_{-i}, z, the bipartite state $|\widetilde{\Phi}_{\substack{\omega_{-i},z \\ \perp,\perp}}\rangle$. Upon receiving questions $x \in \mathcal{X}$ and $y \in \mathcal{Y}$ respectively they perform the following:

1. Alice and Bob use public randomness to sample (i, ω_{-i}, z) conditioned on W_C.
2. Alice applies $U_{\omega_{-i},z,x}$ to her register of $|\widetilde{\Phi}_{\substack{\omega_{-i},z \\ \perp,\perp}}\rangle$.
3. Bob applies $V_{\omega_{-i},z,y}$ to his register of $|\widetilde{\Phi}_{\substack{\omega_{-i},z \\ \perp,\perp}}\rangle$.

4. Alice measures with POVM operators $\{\hat{A}^{a_i}_{\omega_{-i},x}\}$ and returns the outcome as her answer.

5. Bob measures with POVM operators $\{\hat{B}^{b_i}_{\omega_{-i},y}\}$ and returns the outcome as his answer.

Suppose that, upon receiving questions (x,y) and after jointly picking a uniformly random $i \in [m]$, Alice and Bob could jointly sample ω_{-i}, z from $\mathsf{P}_{\Omega_{-i}Z|W_C}$ and locally prepare the state $|\underset{x,y}{\widetilde{\Phi}_{\omega_{-i},z}}\rangle$. For a fixed (x,y), ω_{-i} and z, the distribution of outcomes (a_i,b_i) after measuring $\{\hat{A}^{a_i}_{\omega_{-i},x} \otimes \hat{B}^{b_i}_{\omega_{-i},y}\}_{a_i,b_i}$ will be identical to $\mathsf{P}_{A_iB_i|\omega_{-i},z,x,y}$ (where we mean conditioning on $X_i = x$ and $Y_i = y$). Averaging over $(x,y) \sim \mu$, i, ω_{-i}, and z, the above-defined strategy will win game G with probability at least $\mathbb{E}_i \Pr(W_i|W_C)$.

Next we show that Alice and Bob are able to *approximately* prepare $|\underset{x,y}{\widetilde{\Phi}_{\omega_{-i},z}}\rangle$ with high probability, and thus produce answers that are approximately distributed according to $\mathsf{P}_{A_iB_i|\omega_{-i},z,x,y}$, allowing them to win game G with probability greater than $1-\varepsilon$ — a contradiction.

For the remainder of the proof, we will fix C and implicitly carry it around. Let $\delta = \delta_C$. We use the following lemma:

Lemma 77. *For every C, i, ω_{-i}, $z = (a_C, b_C)$, x_i and y_i there exists unitaries U_{ω_{-i},z,x_i} acting on E_A and V_{ω_{-i},z,y_i} acting on E_B such that*

$$\frac{1}{m}\sum_i \mathop{\mathbb{E}}_{X_iY_i} \mathop{\mathbb{E}}_{\Omega_{-i}Z|W} \left\|(U_{\omega_{-i},z,x_i} \otimes V_{\omega_{-i},z,y_i})\left|\underset{\perp,\perp}{\widetilde{\Phi}_{\omega_{-i},z}}\right\rangle - \left|\underset{x_i,y_i}{\widetilde{\Phi}_{\omega_{-i},z}}\right\rangle\right\|^2 = O(\delta^{1/4}/\alpha^4).$$

The proof of Lemma 77 is given in Section 6.5.2, and we assume it for now. Using the fact that for two pure states $|\psi\rangle$ and $|\phi\rangle$, $\|\psi - \phi\|_1 \leq \sqrt{2}\| \, |\psi\rangle - |\phi\rangle \, \|$, as well as Jensen's inequality,

$$\mathop{\mathbb{E}}_i \mathop{\mathbb{E}}_{XY} \mathop{\mathbb{E}}_{\Omega_{-i}Z|W_C} \left\|(U_{\omega_{-i},z,x} \otimes V_{\omega_{-i},z,y})\left[\underset{\perp,\perp}{\widetilde{\Phi}_{\omega_{-i},z}}\right] - \underset{x,y}{\widetilde{\Phi}_{\omega_{-i},z}}\right\|_1 = O\Big(\frac{\delta^{1/8}}{\alpha^2}\Big), \tag{6.17}$$

where the second expectation is over (x,y) drawn from μ, and $(U \otimes V)[\widetilde{\Phi}]$ denotes $(U \otimes V)\widetilde{\Phi}(U \otimes V)^\dagger$. Conditioned on a given pair of questions (x,y) and the players sampling (i, ω_{-i}, z) in Step 1., the state that the players prepare after Step 3. in the protocol is precisely $(U_{\omega_{-i},z,x} \otimes V_{\omega_{-i},z,y})[\underset{\perp,\perp}{\widetilde{\Phi}_{\omega_{-i},z}}]$. Let $\underset{x,y}{\mathcal{E}_{\omega_{-i},z}}$ denote the quantum-classical channel on density matrices that performs the measurement $\{\hat{A}^{a_i}_{\omega_{-i},x} \otimes \hat{B}^{b_i}_{\omega_{-i},y}\}_{a_i,b_i}$, and outputs a classical register with the measurement outcome (a_i,b_i). Applying $\underset{x,y}{\mathcal{E}_{\omega_{-i},z}}$ to the expression inside the trace norm in (6.17), using that the trace norm is non-increasing under quantum operations,

$$\mathop{\mathbb{E}}_i \mathop{\mathbb{E}}_{XY} \mathop{\mathbb{E}}_{\Omega_{-i}Z|W_C} \left\|\widetilde{\mathsf{P}}_{A_iB_i|\omega_{-i},v,x,y} - \mathsf{P}_{A_iB_i|\omega_{-i},v,x,y}\right\| \leq O(\delta^{1/8}/\alpha^2).$$

where $\widetilde{\mathsf{P}}_{A_iB_i|\omega_i,z,x,y}(a_i,b_i)$ deontes the probability of outcome (a_i,b_i) in the above strategy, conditioned on questions (x,y) and the players sampling (i, ω_{-i}, z) in Step 1. Thus

$$\begin{aligned}\mathsf{P}_I \cdot \mathsf{P}_{\Omega_{-i}Z|W_C} \cdot \mathsf{P}_{XY} \cdot \widetilde{\mathsf{P}}_{A_iB_i|\Omega_{-i}ZX_iY_i} &\approx_{O(\delta^{1/8}/\alpha^2)} \mathsf{P}_I \cdot \mathsf{P}_{\Omega_{-i}Z|W_C} \cdot \mathsf{P}_{XY} \cdot \mathsf{P}_{A_iB_i|\Omega_{-i}ZX_iY_i} \\ &\approx_{O(\delta^{1/8}/\alpha^2)} \mathsf{P}_I \cdot \mathsf{P}_{\Omega_{-i}ZX_iY_i|W_C} \cdot \mathsf{P}_{A_iB_i|\Omega_{-i}ZX_iY_i}\end{aligned}$$

where the X_iY_i in the conditionals is shorthand for $X_i = x, Y_i = y$. The last approximate equality follows from classical correlated sampling lemma (see Chapter 4). Marginalizing $\Omega_{-i}Z$, we get

$$\mathsf{P}_I \cdot \mathsf{P}_{XY} \cdot \widetilde{\mathsf{P}}_{A_iB_i|X_iY_i} \approx_{O(\delta^{1/8}/\alpha^2)} \mathsf{P}_I \cdot \mathsf{P}_{X_iY_iA_iB_i|W_C}. \tag{6.18}$$

Under the distribution $\mathsf{P}_{X_iY_iA_iB_i|W_C}$, the probability that $V(x_i, y_i, a_i, b_i) = 1$ is precisely $\Pr(W_i|W_C)$. On the other hand, (6.18) implies that using the protocol described above the players win G with probability at least $\mathbb{E}_i \Pr(W_i|W_C) - O(\delta^{1/8}/\alpha^2)$. This concludes the proof of the lemma. □

Given Lemma 76, the proof of Theorem 74 (at least the two player case) follows from the same outlint as that of Theorem 68 given in Section 6.4. Later, in Section 6.5.3, we sketch the changes necessary to adapt the proof to handle an arbitrary number of players.

Proof of the main lemma

This section is devoted to the proof of Lemma 77. The proof is based on two lemmas. The first defines the required unitaries.

Lemma 78. *For all i, ω_{-i}, z, $x \in \mathcal{X}$ and $y \in \mathcal{Y}$ there exists unitaries $U_{\omega_{-i}zx}$ acting on E_A and $V_{\omega_{-i}zy}$, $V_{\substack{\omega_{-i},z\\x,y}}$ acting on E_B such that*

$$\frac{1}{m}\sum_i \mathop{\mathbb{E}}_{\Omega_{-i}Z|W} \mathop{\mathbb{E}}_{X} \left\| \left|\widetilde{\Phi}_{x,\perp}\right\rangle - U_{\omega_{-i}zx}\left|\widetilde{\Phi}_{\perp,\perp}\right\rangle \right\|^2 = O(\delta^{1/4}/\alpha^2), \tag{6.19}$$

$$\frac{1}{m}\sum_i \mathop{\mathbb{E}}_{\Omega_{-i}Z|W} \mathop{\mathbb{E}}_{Y} \left\| V_{\omega_{-i}zy}\left|\widetilde{\Phi}_{\perp,\perp}\right\rangle - \left|\widetilde{\Phi}_{\perp,y}\right\rangle \right\|^2 = O(\delta^{1/4}/\alpha^2), \tag{6.20}$$

$$\frac{1}{m}\sum_i \mathop{\mathbb{E}}_{\Omega_{-i}Z|W} \mathop{\mathbb{E}}_{XY} \left\| V_{\substack{\omega_{-i},z\\x,y}}\left|\widetilde{\Phi}_{\perp/x,y}\right\rangle - \left|\widetilde{\Phi}_{\perp/x,\perp}\right\rangle \right\|^2 = O(\delta^{1/4}/\alpha^4). \tag{6.21}$$

where $\mathbb{E}_X$, $\mathbb{E}_Y$, and $\mathbb{E}_{XY}$ denote averaging over $\mu(x)$, $\mu(y)$, and $\mu(x,y)$ respectively.

The proof of Lemma 78 is given in Section 6.5.2. The second lemma relates the normalization factors $\gamma_{x,y}$, $\gamma_{x,\perp}$, $\gamma_{\perp,y}$, $\gamma_{\perp/x,y}$, $\gamma_{\perp/x,\perp}$, $\gamma_{\perp,\perp}$ that appear in the definition of the corresponding normalized states $|\widetilde{\Phi}\rangle$.

Lemma 79. *There exists a set S of triples (i, ω_{-i}, z) that has probability $1 - \delta^{1/4}$ under $\mathsf{P}_I \cdot \mathsf{P}_{\Omega_{-i}Z|W}$ such that*

$$\frac{1}{m} \sum_{\substack{x,y \\ (i,\omega_{-i},z)\in S}} \mathsf{P}_{XY}(x,y) \cdot \mathsf{P}_{\Omega_{-i}Z|W}(\omega_{-i}, v) \left| \gamma^2_{\substack{\omega_{-i},z\\x,y}} - \gamma^2_{\substack{\omega_{-i},z\\\perp,\perp}} \right| = O(\delta^{1/4}/\alpha^2)\gamma^2, \tag{6.22}$$

where

$$\gamma = \Big(\frac{1}{m}\sum_i \sum_{x,y,\omega_{-i},z} \mathsf{P}_{XY}(x,y) \cdot \mathsf{P}_{\Omega_{-i}Z|W}(\omega_{-i}, z) \cdot \gamma^2_{\substack{\omega_{-i},z\\x,y}}\Big)^{1/2}.$$

Furthermore, similar bounds as (6.22) hold where $\gamma_{\substack{\omega_{-i},z\\x,y}}$ is replaced by any of $\gamma_{\substack{\omega_{-i},z\\x,\perp}}$, $\gamma_{\substack{\omega_{-i},z\\\perp,y}}$, $\gamma_{\substack{\omega_{-i},z\\\perp/x,y}}$, $\gamma_{\substack{\omega_{-i},z\\\perp/x,\perp}}$.

The proof of Lemma 79 uses the following claim.

Claim 80.

$$\frac{1}{m}\sum_i \sum_{x,y,(\omega_{-i},z)\in W} \mathsf{P}_{XY}(x,y) \left\| \mathsf{P}_{\Omega_{-i}Z|X_i=x,Y_i=y}(\omega_{-i},z) - \mathsf{P}_{\Omega_{-i}Z|X_i\in\perp,Y_i\in\perp}(\omega_{-i},z) \right\| = O\left(\frac{\sqrt{\delta}}{\alpha^2}\right)\Pr(W).$$

Proof. First note that

$$\begin{aligned}\frac{1}{m}\sum_i\sum_{x,y}\mathsf{P}_{XY}(x,y)\left|\Pr(W|X_i=x,Y_i=y)-\Pr(W)\right| &= \frac{\Pr(W)}{m}\sum_i \|\mathsf{P}_{X_iY_i|W}-\mathsf{P}_{X_iY_i}\| \\ &= O(\sqrt{\delta})\Pr(W), \qquad (6.23)\end{aligned}$$

where the second equality follows from Lemma 89. Using the triangle inequality and $\Pr(X_i\in\perp, Y_i\in\perp)\geq\alpha^2$ we also get

$$\frac{1}{m}\sum_i\sum_{x,y}\mathsf{P}_{XY}(x,y)\left|\Pr(W|X_i=x,Y_i=y)-\Pr(W|X_i\in\perp,Y_i\in\perp)\right| = O(\sqrt{\delta}/\alpha^2)\Pr(W). \qquad (6.24)$$

Using (6.23) and letting $\mathsf{P}_{\Omega_{-i}Z|x,y,W}$ denote $\mathsf{P}_{\Omega_{-i}Z|X_i=x,Y_i=y,W}$,

$$\begin{aligned}&\frac{1}{m}\sum_i\sum_{x,y}\mathsf{P}_{XY}(x,y)\sum_{(\omega_{-i},z)\in W}\left\|\Pr(W)\cdot\mathsf{P}_{\Omega_{-i}Z|x,y,W}(\omega_{-i},z)-\mathsf{P}_{\Omega_{-i}Z|x,y}(\omega_{-i},z)\right\| \\ &\approx_{O(\sqrt{\delta})\Pr(W)}\frac{1}{m}\sum_i\sum_{x,y}\mathsf{P}_{XY}(x,y)\sum_{(\omega_{-i},z)\in W}\left\|\mathsf{P}_{\Omega_{-i}Z\wedge W|x,y}(\omega_{-i},z)-\mathsf{P}_{\Omega_{-i}Z|x,y}(\omega_{-i},z)\right\| \\ &= 0.\end{aligned}$$

A similar derivation proves

$$\frac{1}{m}\sum_i\sum_{(\omega_{-i},z)\in W}\|\Pr(W)\cdot\mathsf{P}_{\Omega_{-i}Z|X_i\in\perp,Y_i\in\perp,W}(\omega_{-i},z)-\mathsf{P}_{\Omega_{-i}Z|X_i\in\perp,Y_i\in\perp}(\omega_{-i},z)\| = O(\sqrt{\delta})\Pr(W).$$

Combining the previous two bounds with the bound

$$\frac{1}{m}\sum_i\Pr(W)\|\mathsf{P}_{X_iY_i}\mathsf{P}_{\Omega_{-i}Z|X_i\in\perp,Y_i\in\perp,W}-\mathsf{P}_{X_iY_i}\mathsf{P}_{\Omega_{-i}Z|X_iY_iW}\| \leq O(\sqrt{\delta}/\alpha^2)\Pr(W)$$

from Lemma 89 with the triangle inequality proves the claim. □

Proof of Lemma 79. For any i, x, y and $(\omega_{-i}, z)\in W$ write

$$\begin{aligned}\mathsf{P}_{XY}(x,y)\cdot\mathsf{P}_{\Omega_{-i}Z|W}(\omega_{-i},z)\cdot\gamma^2_{\substack{\omega_{-i},z\\x,y}} &= \frac{1}{\Pr(W)}\mathsf{P}_{XY}(x,y)\cdot\mathsf{P}_{\Omega_{-i}Z}(\omega_{-i},z)\cdot\gamma^2_{\substack{\omega_{-i},z\\x,y}} \\ &= \frac{1}{\Pr(W)}\mathsf{P}_{XY}(x,y)\cdot\mathsf{P}_{\Omega_{-i}|x,y}(\omega_{-i})\cdot\mathsf{P}_{Z|\omega_{-i}}(z)\cdot\gamma^2_{\substack{\omega_{-i},z\\x,y}},\end{aligned}$$

where for the last equality we used $\mathsf{P}_{\Omega_{-i}|X_iY_i} = \cdot\mathsf{P}_{\Omega_{-i}}$. From the definition, $\gamma^2_{\substack{\omega_{-i},z\\x,y}} = \mathsf{P}_{Z|\omega_{-i},x,y}(z)$,

$$\cdot \quad = \frac{1}{\Pr(W)} \mathsf{P}_{XY}(x,y) \cdot \mathsf{P}_{Z|\omega_{-i}}(z) \cdot \mathsf{P}_{\Omega_{-i}Z|x,y}(\omega_{-i},z), \quad (6.25)$$

where $\mathsf{P}_{\Omega_{-i}Z|x,y}(\omega_{-i},z)$ denotes $\mathsf{P}_{\Omega_{-i}Z|X_i=x,Y_i=y}(\omega_{-i},z)$. Similarly, we have

$$\mathsf{P}_{XY}(x,y) \cdot \mathsf{P}_{\Omega_{-i}Z|W}(\omega_{-i},z) \cdot \gamma^2_{\substack{\omega_{-i},z\\\perp,\perp}} = \frac{1}{\Pr(W)} \mathsf{P}_{XY}(x,y) \cdot \mathsf{P}_{Z|\omega_{-i}}(z) \cdot \mathsf{P}_{\Omega_{-i}Z|\perp,\perp}(\omega_{-i},z). \quad (6.26)$$

By definition

$$\gamma^2 = \frac{1}{m} \sum_{i,\omega_{-i},z} \mathsf{P}_{\Omega_{-i}Z|W}(\omega_{-i},z) \cdot \mathsf{P}_{V|\omega_{-i}}(z),$$

thus for any $\eta > 0$ applying Markov's inequality a fraction at least $1-\eta$ of (i,ω_{-i},z) distributed according to $\mathsf{P}_I \cdot \mathsf{P}_{\Omega_{-i}Z|W}$ are such that $\mathsf{P}_{Z|\omega_{-i}}(z) \leq \gamma^2/\eta$. Let S be the set of such triples, and consider summing the difference

$$\mathsf{P}_{XY}(x,y) \cdot \mathsf{P}_{Z|\omega_{-i}}(z) \cdot \left| \mathsf{P}_{\Omega_{-i}Z|x,y}(\omega_{-i},z) - \mathsf{P}_{\Omega_{-i}Z|\perp,\perp}(\omega_{-i},z) \right|$$

over all (x,y) and $(i,\omega_{-i},z) \in S$. By lines (6.25) and (6.26), and applying Claim 80 we obtain

$$\frac{1}{m} \sum_{\substack{x,y\\(i,\omega_{-i},z)\in S}} \mathsf{P}_{XY}(x,y) \cdot \mathsf{P}_{\Omega_{-i}Z|W}(\omega_{-i},z) \cdot \left| \gamma^2_{\substack{\omega_{-i},z\\x,y}} - \gamma^2_{\substack{\omega_{-i},z\\\perp,\perp}} \right| \leq \frac{\gamma^2}{\eta} O\Big(\frac{\sqrt{\delta}}{\alpha^2}\Big).$$

Choosing $\eta = \delta^{1/4}$ proves the lemma. □

Proof of Lemma 77. For every (i,ω_{-i},z), $x \in \mathcal{X}$ and $y \in \mathcal{Y}$ let unitaries $U_{\omega_{-i}zx}$, $V_{\omega_{-i}zy}$ and $V_{\substack{\omega_{-i},z\\x,y}}$ be as in Lemma 78. For notational convenience we suppress the dependence on (i,ω_{-i},z) when it is clear from context. Call triples (i,ω_{-i},z) that satisfy the conclusion of Lemma 79 for $\gamma_{\substack{\omega_{-i},z\\x,y}}$, $\gamma_{\substack{\omega_{-i},z\\x,\perp}}$, $\gamma_{\substack{\omega_{-i},z\\\perp,y}}$, $\gamma_{\substack{\omega_{-i},z\\\perp/x,y}}$, and $\gamma_{\substack{\omega_{-i},z\\\perp/x,\perp}}$ simutaneously *good triples*, and let S denote the set of good triples. Fix $(i,\omega_{-i},z) \in S$. Using $|a-b|^2 \leq |a^2-b^2|$ for $a,b \geq 0$,

$$\begin{aligned} \sum_{x,y} \mathsf{P}_{XY}(x,y) \cdot \Big\| |\widetilde{\Phi}_{x,y}\rangle - \gamma^{-1}|\Phi_{x,y}\rangle \Big\|^2 &= \sum_{x,y} \mathsf{P}_{XY}(x,y) \cdot \left| \frac{\gamma - \gamma_{\substack{\omega_{-i},z\\x,y}}}{\gamma} \right|^2 \\ &\leq \sum_{x,y} \mathsf{P}_{XY}(x,y) \cdot \left| \frac{\gamma^2 - \gamma^2_{\substack{\omega_{-i},z\\x,y}}}{\gamma^2} \right| \\ &= O(\delta^{1/4}/\alpha^2), \end{aligned} \quad (6.27)$$

and similar bounds hold for $|\widetilde{\Phi}_{x,\perp}\rangle$, $|\widetilde{\Phi}_{\perp,y}\rangle$ and $|\widetilde{\Phi}_{\perp,\perp}\rangle$. Thus to prove the theorem it will be sufficient to establish that

$$\frac{1}{m}\sum_{\substack{x,y\\(i,\omega_{-i},z)\in S}} \mathsf{P}_{XY}(x,y)\cdot \mathsf{P}_{\Omega_{-i},Z|W}(\omega_{-i},z)\cdot \left\|(U_x\otimes V_y)|\Phi_{\perp,\perp}\rangle - |\Phi_{x,y}\rangle\right\|^2 = O\Big(\frac{\delta^{1/4}}{\alpha^2}\Big)\gamma^2. \tag{6.28}$$

Using the lower bound on the measure of S,

$$\begin{aligned}&\frac{1}{m}\sum_{\substack{x,y\\ i,\omega_{-i},v}} \mathsf{P}_{XY}(x,y)\cdot \mathsf{P}_{\Omega_{-i},V|W}(\omega_{-i},v)\cdot \left\|(U_x\otimes V_y)\big|\tilde{\Phi}_{\perp,\perp}\big\rangle - \big|\tilde{\Phi}_{x,y}\big\rangle\right\|^2\\ &\leq \frac{1}{m}\sum_{\substack{x,y\\(i,\omega_{-i},v)\in S}} \mathsf{P}_{XY}(x,y)\cdot \mathsf{P}_{\Omega_{-i},V|W}(\omega_{-i},v)\cdot \left\|(U_x\otimes V_y)\big|\tilde{\Phi}_{\perp,\perp}\big\rangle - \big|\tilde{\Phi}_{x,y}\big\rangle\right\|^2 + O(\delta^{1/4})\end{aligned}$$

For each good triple (i,ω_{-i},z), by the triangle inequality

$$\begin{aligned}\left\|(U_x\otimes V_y)\big|\tilde{\Phi}_{\perp,\perp}\big\rangle - \big|\tilde{\Phi}_{x,y}\big\rangle\right\|^2 &\leq 3\left\|\big|\tilde{\Phi}_{\perp,\perp}\big\rangle - \gamma^{-1}|\Phi_{\perp,\perp}\rangle\right\|^2 + 3\left\|\big|\tilde{\Phi}_{x,y}\big\rangle - \gamma^{-1}|\Phi_{x,y}\rangle\right\|^2\\ &\quad + 3\gamma^{-2}\left\|(U_x\otimes V_y)|\Phi_{\perp,\perp}\rangle - |\Phi_{x,y}\rangle\right\|^2\\ &\leq 3\gamma^{-2}\left\|(U_x\otimes V_y)|\Phi_{\perp,\perp}\rangle - |\Phi_{x,y}\rangle\right\|^2 + O(\delta^{1/4}/\alpha^2).\end{aligned}$$

Using (6.27), the bounds stated in Lemma 78 imply the following bounds on the unnormalized vectors:

$$\frac{1}{m}\sum_{\substack{x\\(i,\omega_{-i},z)\in S}} \mathsf{P}_{X}(x)\cdot \mathsf{P}_{\Omega_{-i}Z|W}(\omega_{-i},z)\cdot \left\||\Phi_{x,\perp}\rangle - U_{\omega_{-i}zx}|\Phi_{\perp,\perp}\rangle\right\|^2 = O\Big(\frac{\delta^{1/4}}{\alpha^2}\Big)\gamma^2, \tag{6.29}$$

$$\frac{1}{m}\sum_{\substack{y\\(i,\omega_{-i},z)\in S}} \mathsf{P}_{Y}(y)\cdot \mathsf{P}_{\Omega_{-i}Z|W}(\omega_{-i},z)\cdot \left\|V_{\omega_{-i}zy}|\Phi_{\perp,\perp}\rangle - |\Phi_{\perp,y}\rangle\right\|^2 = O\Big(\frac{\delta^{1/4}}{\alpha^2}\Big)\gamma^2, \tag{6.30}$$

$$\frac{1}{m}\sum_{\substack{x,y\\(i,\omega_{-i},z)\in S}} \mathsf{P}_{XY}(x,y)\cdot \mathsf{P}_{\Omega_{-i}Z|W}(\omega_{-i},z)\cdot \left\|V_{\substack{\omega_{-i},z\\x,y}}|\Phi_{\perp/x,y}\rangle - |\Phi_{\perp/x,\perp}\rangle\right\|^2 = O\Big(\frac{\delta^{1/4}}{\alpha^4}\Big)\gamma^2. \tag{6.31}$$

We show how to combine these bounds to establish (6.28). We have

$$\begin{aligned}\left\|U_x|\Phi_{\perp,y}\rangle - |\Phi_{x,y}\rangle\right\|^2 &= \left\|U_xA_{\perp}^{1/2}A_{\perp/x}^{-1/2}|\Phi_{\perp/x,y}\rangle - A_{x}^{1/2}A_{\perp/x}^{-1/2}|\Phi_{\perp/x,y}\rangle\right\|^2\\ &= \left\|U_xA_{\perp}^{1/2}A_{\perp/x}^{-1/2}\otimes V_{xy}|\Phi_{\perp/x,y}\rangle - A_{x}^{1/2}A_{\perp/x}^{-1/2}\otimes V_{xy}|\Phi_{\perp/x,y}\rangle\right\|^2.\end{aligned}$$

Using the triangle inequality again,

$$\leq 3\left\|\left(U_xA_{\perp}^{1/2}A_{\perp/x}^{-1/2}\right)\otimes V_{xy}|\Phi_{\perp/x,y}\rangle - \left(U_xA_{\perp}^{1/2}A_{\perp/x}^{-1/2}\right)|\Phi_{\perp/x,\perp}\rangle\right\|^2 \tag{6.32}$$

$$+3\left\|\left(U_xA_\perp^{1/2}A_{\perp/x}^{-1/2}\right)|\Phi_{\perp/x,\perp}\rangle - A_x^{1/2}A_{\perp/x}^{-1/2}|\Phi_{\perp/x,\perp}\rangle\right\|^2 \tag{6.33}$$

$$+3\left\|A_x^{1/2}A_{\perp/x}^{-1/2}|\Phi_{\perp/x,\perp}\rangle - A_x^{1/2}A_{\perp/x}^{-1/2}\otimes V_{xy}|\Phi_{\perp/x,y}\rangle\right\|^2. \tag{6.34}$$

Using $\|U_xA_\perp^{1/2}A_{\perp/x}^{-1/2}\| \leq \sqrt{2}$ the term (6.32) can be bounded as

$$\left\|\left(U_xA_\perp^{1/2}A_{\perp/x}^{-1/2}\right)\otimes V_{xy}\,|\Phi_{\perp/x,y}\rangle - \left(U_xA_\perp^{1/2}A_{\perp/x}^{-1/2}\right)|\Phi_{\perp/x,\perp}\rangle\right\|^2 \leq 2\,\left\|V_{xy}|\Phi_{\perp/x,y}\rangle - |\Phi_{\perp/x,\perp}\rangle\right\|^2.$$

The term (6.33) can be re-written as

$$\left\|\left(U_xA_\perp^{1/2}A_{\perp/x}^{-1/2}\right)|\Phi_{\perp/x,\perp}\rangle - A_x^{1/2}A_{\perp/x}^{-1/2}|\Phi_{\perp/x,\perp}\rangle\right\|^2 = \left\|U_x|\Phi_{\perp,\perp}\rangle - |\Phi_{x,\perp}\rangle\right\|^2.$$

Finally, using $\|A_x^{1/2}A_{\perp/x}^{-1/2}\| \leq \sqrt{2}$ the term (6.34) can be bounded as

$$\left\|A_x^{1/2}A_{\perp/x}^{-1/2}|\Phi_{\perp/x,\perp}\rangle - A_x^{1/2}A_{\perp/x}^{-1/2}\otimes V_{xy}\,|\Phi_{\perp/x,y}\rangle\right\|^2 \leq 2\left\||\Phi_{\perp/x,\perp}\rangle - V_{xy}\,|\Phi_{\perp/x,y}\rangle\right\|^2.$$

Putting the three bounds together, from (6.34) we get

$$\left\|U_x|\Phi_{\perp,y}\rangle - |\Phi_{x,y}\rangle\right\|^2 \leq 3\left\|V_{xy}|\Phi\rangle_{\perp/x,y} - |\Phi_{\perp/x,\perp}\rangle\right\|^2 + 3\left\|U_x|\Phi_{\perp,\perp}\rangle - |\Phi_{x,\perp}\rangle\right\|^2. \tag{6.35}$$

Using that U_x is unitary,

$$\begin{aligned}\left\|(U_x\otimes V_y)|\Phi_{\perp,\perp}\rangle - |\Phi_{x,y}\rangle\right\|^2 &\leq 2\left\|V_y|\Phi_{\perp,\perp}\rangle - |\Phi_{\perp,y}\rangle\right\|^2 + 2\left\|U_x|\Phi_{\perp,y}\rangle - |\Phi_{x,y}\rangle\right\|^2\\ &\leq 18\left\|V_{xy}|\Phi_{\perp/x,y}\rangle - |\Phi_{\perp/x,\perp}\rangle\right\|^2 + 6\left\|U_x|\Phi_{\perp,\perp}\rangle - |\Phi_{x,\perp}\rangle\right\|^2\\ &\quad + 2\left\|V_y|\Phi_{\perp,\perp}\rangle - |\Phi_{\perp,y}\rangle\right\|^2,\end{aligned}$$

where the last inequality is (6.35). Eqs. (6.29), (6.30) and (6.31) bound the three terms above by $O(\delta^{1/4}/\alpha^4)\gamma^2$ on average over (x,y) weighted by P_{XY}, and $(i,\omega_{-i},z)\in S$, weighted by $\mathsf{P}_I\cdot\mathsf{P}_{\Omega_{-i}Z|W}$. This proves (6.28), and the theorem follows. □

Obtaining local unitaries

In this section we give the proof of Lemma 78, which states the existence of the local unitary transformations needed for the proof of Theorem 74.

Proof of Lemma 78. Recall that we let the entangled state $|\psi\rangle$ and POVMs $\{A_{x^n}^{a^n}\}$ and $\{B_{x^n}^{b^n}\}$ constitute an optimal strategy for G^n. We refer the reader to Section 6.5.1 for the definitions of operators $A_\omega^{a_C}$, etc. We will let ρ denote the reduced density matrix of $|\psi\rangle$ on either system (this is well-defined because we've assumed $|\psi\rangle$ is symmetric).

We first prove (6.20), that is, the existence of the unitary $V_{\omega_{-i}zy_i}$. Recall the notation $\psi = |\psi\rangle\langle\psi|$ and $X[\rho] = X\rho X^\dagger$. Introduce the following states:

$$\Xi_{\Omega Y^m E_A E_B Z} = \sum_{\omega,y^m,a_C,b_C} \mathsf{P}_{\Omega Y^m}(\omega,y^m)\,|\omega\, y^m\rangle\langle\omega\, y^m| \otimes \left(\sqrt{A_\omega^{a_C}}\otimes\sqrt{B_{y^m}^{b_C}}\right)[\psi]\otimes|a_Cb_C\rangle\langle a_Cb_C|,$$

$$\zeta_{\Omega Y^m E_A E_B Z} = \Xi_{\Omega Y^m E_A E_B Z|W}, \tag{6.36}$$

$$\zeta^{E_A}_{\substack{\omega_{-i},z\\ \perp,y_i}} = \zeta_{E_A|\Omega_{-i}=\omega_{-i},Y_i=y_i,\omega_i=(A,\perp)}. \tag{6.37}$$

The state Ξ is defined so that tracing out the entanglement registers E_A and E_B the resulting state $\Xi_{\Omega Y^m A_C B_C}$ is a classical state that is equivalent to the probability distribution $\mathsf{P}_{\Omega Y^m A_C B_C}$. In (6.36) the conditioning on W is well-defined since the event only involves classical random variables in Ω and Z. In (6.37) only the reduced density on E_A is considered, all other registers being traced out.

The following claim provides the main step of the proof by relating the reduced densities on Alice's registers of states (6.37) associated with different choices for y_i.

Claim 81.

$$\frac{1}{m}\sum_i \mathop{\mathbb{E}}_{\Omega_{-i}Z|W} \mathop{\mathbb{E}}_{Y_i} \left\| \zeta^{E_A}_{\substack{\omega_{-i},z\\ \perp,y_i}} - \zeta^{E_A}_{\substack{\omega_{-i},z\\ \perp,\perp}} \right\|_1^2 = O\big(\sqrt{\delta}/\alpha^2\big) \tag{6.38}$$

Proof. First we observe that $\Pr(W)\zeta \preceq \Xi$, thus by definition $S(\zeta\|\Xi) \leq S_\infty(\zeta\|\Xi) \leq \log 1/\Pr(W)$. Using the chain rule for the relative entropy (Fact 10),

$$\mathop{\mathbb{E}}_{\Omega V|W} S(\zeta^{Y^m E_A}_{\omega,z} \| \Xi^{Y^m E_A}_{\omega,z}) \leq \log\frac{1}{\Pr(W)}. \tag{6.39}$$

Next we note that for any ω, using Ando's identity

$$\langle\psi|X\otimes Y|\psi\rangle = \mathrm{Tr}(X\sqrt{\rho}Y^\top\sqrt{\rho}),$$

where $|\psi\rangle = \sum\sqrt{\lambda_j}|v_j\rangle|v_j\rangle$, $\rho = \sum\lambda_j|v_j\rangle\langle v_j|$, X, Y are any linear operators and the transpose is taken with respect to the orthonormal basis $\{|v_j\rangle\}$,

$$\begin{aligned}
\Xi^{Y^m E_A A_C B_C}_{\omega} &= \sum_{y^m,a_C,b_C} \mathsf{P}_{Y^m|\omega}(y^m)\ |y^m\rangle\langle y^m| \otimes \sqrt{A^{a_C}_\omega}\sqrt{\rho}\overline{B}^{b_C}_{y^n}\sqrt{\rho}\sqrt{A^{a_C}_\omega} \otimes |a_C b_C\rangle\langle a_C b_C| \\
&\preceq \sum_{y^m,a_C,b_C} \mathsf{P}_{Y^n|\omega}(y^m)\ |y^m\rangle\langle y^m| \otimes \sqrt{A^{a_C}_\omega}\sqrt{\rho}\overline{B}^{b_C}_{x^n}\sqrt{\rho}\sqrt{A^{a_C}_\omega} \otimes \mathbb{I} \\
&= \sum_{y^m,a_C} \mathsf{P}_{Y^m|\omega}(y^m)\ |y^m\rangle\langle y^m| \otimes \sqrt{A^{a_C}_\omega}\rho\sqrt{A^{a_C}_\omega} \otimes \mathbb{I},
\end{aligned} \tag{6.40}$$

where the last equality uses $\sum_{b_C} B^{b_C}_{y^n} = \mathbb{I}$. From (6.40) and the definition of S_∞ it follows that $S_\infty(\Xi^{Y^n E_A}_\omega \| \Xi^{Y^n}_\omega \otimes \Xi^{E_A}_\omega) \leq |C| \cdot \log|\mathcal{A}||\mathcal{B}|$. Applying Lemma 18,

$$\begin{aligned}
\frac{1}{m}\sum_i \mathop{\mathbb{E}}_{\Omega Z|W} I(Y_i;E_A|\omega,z)_\zeta &\leq \frac{1}{m} \mathop{\mathbb{E}}_{\Omega Z|W} S(\zeta^{Y^m E_A}_{\omega,z} \| \Xi^{Y^m}_{\omega,z} \otimes \Xi^{E_A}_{\omega,z}) \\
&\leq \frac{1}{m}\Big(\mathop{\mathbb{E}}_{\Omega Z|W} S(\zeta^{Y^m E_A}_{\omega,z} \| \Xi^{Y^m E_A}_{\omega,z}) + \mathop{\mathbb{E}}_{\Omega Z|W} S_\infty(\Xi^{Y^m E_A}_{\omega,z} \| \Xi^{Y^m}_{\omega,z} \otimes \Xi^{E_A}_{\omega,z})\Big) \\
&\leq \frac{1}{m}\Big(\log\frac{1}{\Pr(W)} + |C| \cdot \log|\mathcal{A}||\mathcal{B}|\Big) = \delta
\end{aligned} \tag{6.41}$$

where in the last line the first term is bounded using (6.39) and the second using (6.40).

Applying Lemma 89,

$$\mathop{\mathbb{E}}_{i} \mathsf{P}_{D_iM_i|W}(A,\perp) \approx_{O(\sqrt{\delta})} \mathop{\mathbb{E}}_{i} \mathsf{P}_{D_iM_i}(A,\perp) = \frac{\alpha}{2},$$

thus from (7.2) by conditioning on $\Omega_i = (A,\perp)$ we deduce

$$\frac{1}{m}\sum_i \mathop{\mathbb{E}}_{\Omega Z|\Omega_i=(A,\perp),W} I\big(Y_i;E_A|\omega,z\big)_{\xi} = O(\delta/\alpha), \tag{6.42}$$

as long as $\alpha = \Omega(\sqrt{\delta})$. Next we apply Pinsker's inequality (Lemma 9) and use that Y_i is classical in ξ to write

$$\begin{aligned}\frac{1}{m}\sum_i \mathop{\mathbb{E}}_{\Omega Z|\Omega_i=(A,\perp),W} \mathop{\mathbb{E}}_{Y_i|\omega,z} \Big\|\xi^{E_A}_{\substack{\omega_{-i},z\\ \perp,y_i}} - \xi^{E_A}_{\omega,z}\Big\|_1^2 &\leq \frac{1}{m}\sum_i \mathop{\mathbb{E}}_{\Omega Z|\Omega_i=(A,\perp),W} \mathop{\mathbb{E}}_{Y_i|\omega,z} S\Big(\xi^{E_A}_{\substack{\omega_{-i},z\\ \perp,y_i}} \,\Big\|\, \xi^{E_B}_{\omega,z}\Big)\\ &= \frac{1}{m}\sum_i \mathop{\mathbb{E}}_{\Omega Z|\Omega_i=(A,\perp),W} I(Y_i;E_A|\omega,z)_{\xi}\\ &= O(\delta/\alpha)\end{aligned}$$

by (6.42). To conclude note that Lemma 89 and the classical correlated sampling lemma imply

$$\mathsf{P}_I \cdot \mathsf{P}_{\Omega Z Y_i|\Omega_i=(A,\perp),W} \approx_{O(\sqrt{\delta}/\alpha^2)} \mathsf{P}_I \cdot \mathsf{P}_{\Omega_{-i}Z|W} \cdot \mathsf{P}_{Y_i}.$$

□

The proof of (6.19) essentially follows from Claim 81 and Uhlmann's theorem. We give the details. First write $\xi^{E_B}_{\substack{\omega_{-i},z\\ \perp,y_i}}$ and $\xi^{E_A}_{\substack{\omega_{-i},z\\ \perp,\perp}}$ explicitly as

$$\begin{aligned}\xi^{E_A}_{\substack{\omega_{-i},z\\ \perp,y_i}} &\propto (A^{a_C}_{\omega_{-i},\perp})^{1/2}\sqrt{\rho}\;\overline{B}^{b_C}_{\omega_{-i},y_i}\;\sqrt{\rho}\;(A^{a_C}_{\omega_{-i},\perp})^{1/2},\\ \xi^{E_A}_{\substack{\omega_{-i},z\\ \perp,\perp}} &\propto (A^{a_C}_{\omega_{-i},\perp})^{1/2}\sqrt{\rho}\;\overline{B}^{b_C}_{\omega_{-i},\perp}\;\sqrt{\rho}\;(A^{a_C}_{\omega_{-i},\perp})^{1/2},\end{aligned}$$

which makes it apparent that the states $\Big|\widetilde{\Phi}_{\substack{\omega_{-i},z\\ \perp,y_i}}\Big\rangle$ and $\Big|\widetilde{\Phi}_{\substack{\omega_{-i},z\\ \perp,\perp}}\Big\rangle$ introduced in (6.16) purify $\xi^{E_A}_{\substack{\omega_{-i},z\\ \perp,y_i}}$ and $\xi^{E_A}_{\substack{\omega_{-i},z\\ \perp,\perp}}$ respectively. Applying Uhlmann's Theorem, there exists a unitary V_{ω_{-i},z,y_i} acting on E_B such that

$$\begin{aligned}\frac{1}{m}\sum_i \mathop{\mathbb{E}}_{\Omega_{-i}Z|W} \mathop{\mathbb{E}}_{Y_i} \Big|\Big\langle \widetilde{\Phi}_{\substack{\omega_{-i},z\\ \perp,y_i}}\Big|V_{\omega_{-i},z,y_i}\Big|\widetilde{\Phi}_{\substack{\omega_{-i},z\\ \perp,\perp}}\Big\rangle\Big| &\geq 1 - \frac{1}{m}\sum_i \mathop{\mathbb{E}}_{\Omega_{-i}Z|W} \mathop{\mathbb{E}}_{Y_i} \Big\|\xi^{E_A}_{\substack{\omega_{-i},z\\ \perp,y_i}} - \xi^{E_A}_{\substack{\omega_{-i},z\\ \perp,\perp}}\Big\|_1\\ &\geq 1 - O(\delta^{1/4}/\alpha), \qquad (6.43)\end{aligned}$$

where the first inequality follows from the Fuchs-van de Graaf inequality (2.1) and the second uses Jensen's inequality and (6.38) from Claim 81. Expanding out the squared Euclidean norm and making sure that V_{ω_{-i},z,y_i} is chosen so as to ensure that the inner product $\langle\widetilde{\Phi}_{\substack{\omega_{-i},z\\ \perp,y_i}}|V_{\omega_{-i},z,y_i}|\widetilde{\Phi}_{\substack{\omega_{-i},z\\ \perp,\perp}}\rangle$ is positive real, (6.43) proves (6.20).

A nearly identical argument yields (6.19). It remains to show (6.21). Define

$$\zeta^{E_A}_{\substack{\omega_{-i},z \\ \perp/x_i,y_i}} = \frac{1}{2}\zeta^{E_A}_{\substack{\omega_{-i},z \\ \perp,y_i}} + \frac{1}{2}\zeta^{E_A}_{\substack{\omega_{-i},z \\ x_i,y_i}} \qquad \text{and} \qquad \zeta^{E_A}_{\substack{\omega_{-i},z \\ \perp/x_i,\perp}} = \frac{1}{2}\zeta^{E_A}_{\substack{\omega_{-i},z \\ \perp,\perp}} + \frac{1}{2}\zeta^{E_A}_{\substack{\omega_{-i},z \\ x_i,\perp}}$$

For notational clarity, we will suppress mention of ω_{-i} and z; it will be implicitly carried around.

The density matrices $\zeta^{E_A}_{\perp/x_i,y_i}$ and $\zeta^{E_A}_{\perp/x_i,\perp}$ are purified by $|\widetilde{\Phi}_{\perp/x_i,y_i}\rangle$ and $|\widetilde{\Phi}_{\perp/x_i,\perp}\rangle$ respectively. We will show that these two density matrices are close to together, on average, and hence by Uhlmann's Theorem implies that there exists a unitary V_{x_i,y_i} acting on E_B that moves $|\widetilde{\Phi}_{\perp/x_i,y_i}\rangle$ close to $|\widetilde{\Phi}_{\perp/x_i,\perp}\rangle$. Consider:

$$\begin{aligned}
\mathop{\mathbb{E}}_{I}\ \mathop{\mathbb{E}}_{\Omega_{-i}Z|W}\ \mathop{\mathbb{E}}_{X_iY_i} \left\| \zeta^{E_A}_{\perp/x_i,y_i} - \zeta^{E_A}_{\perp,\perp} \right\|_1 &= \mathop{\mathbb{E}}_{I}\ \mathop{\mathbb{E}}_{\Omega_{-i}Z|W}\ \mathop{\mathbb{E}}_{X_iY_i} \left\| \frac{1}{2}\zeta^{E_A}_{\perp,y_i} + \frac{1}{2}\zeta^{E_A}_{x_i,y_i} - \zeta^{E_A}_{\perp,\perp} \right\|_1 \\
&\leq \mathop{\mathbb{E}}_{I}\ \mathop{\mathbb{E}}_{\Omega_{-i}Z|W}\ \mathop{\mathbb{E}}_{X_iY_i} \left[\frac{1}{2} \left\| \zeta^{E_A}_{\perp,y_i} - \zeta^{E_A}_{\perp,\perp} \right\|_1 + \frac{1}{2} \left\| \zeta^{E_A}_{x_i,y_i} - \zeta^{E_A}_{\perp,\perp} \right\|_1 \right].
\end{aligned}$$

We obtained a bound on the first term in the calculations above. It remains to bound the second term. Again Lemma 89 implies

$$\mathsf{P}_I \cdot \mathsf{P}_{\Omega Z Y_i | D_i = A, W} \cong_{O(\sqrt{\delta}/\alpha^2)} \mathsf{P}_I \cdot \mathsf{P}_{\Omega_{-i} Z | W} \cdot \mathsf{P}_{X_i Y_i}$$

where "$\cong$" indicates approximate equality, up to relabeling the random variable M_i with X_i, whose marginals are identical conditioned on $D_i = A$. Thus using the same approach as earlier in the proof, we can obtain the bound

$$\mathop{\mathbb{E}}_{I}\ \mathop{\mathbb{E}}_{\Omega_{-i}Z|W}\ \mathop{\mathbb{E}}_{X_iY_i} \left\| \zeta^{E_A}_{x_i,y_i} - \zeta^{E_A}_{\perp,\perp} \right\|_1 \leq O(\sqrt{\delta}/\alpha^4).$$

Thus there exists the desired unitary V_{x_i,y_i} such that

$$\frac{1}{m}\sum_i \mathop{\mathbb{E}}_{\Omega_{-i}Z|W}\ \mathop{\mathbb{E}}_{X_iY_i} \left\| \left|\widetilde{\Phi}_{\perp/x_i,\perp}\right\rangle - V_{x_i,y_i}\left|\widetilde{\Phi}_{\perp/x_i,y_i}\right\rangle \right\|^2 \leq O(\delta^{1/4}/\alpha^4) \tag{6.44}$$

proving (6.21). □

6.5.3 Extending the argument to more than two players

Here we extend the argument above to the case when $k > 2$; that is, when the game involves more than two entangled players. For clarity, we won't redo the entire argument, but instead describe the modifications to the two player proof. Furthermore, we will make the following simplifications: we restrict ourselves to the $k = 3$ player case, and we will analyze the repetition of $G_\perp$ that is the result of applying the anchor transformation to the game G; that is, the anchor questions are literally the "$\perp$". Extending the argument for arbitrary k and arbitrary anchored games is straightforward.

We start with an arbitrary game G involving three players Alice, Bob and Charlie. The players' questions are denoted by X, Y, Z, and their outputs are denoted as A, B, C. We will let $\mu(x, y, z)$ denote the question distribution of the game G. Let $G_\perp$ be the anchoring transformation applied to G (for some α), and let $\mu_\perp(x, y, z)$ denote the question distribution of $G_{\perp}$. We will analyze the behavior of $\mathrm{val}^*(G_{\perp}^n)$. Consider an optimal strategy for $G_{\perp}^n$, involving a tripartite state $|\psi\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d \otimes \mathbb{C}^d$, and measurement POVMs for each of the players: $\{A_{x^n}^{a^n}\}$ for Alice, $\{B_{y^n}^{b^n}\}$ for Bob, and $\{C_{z^n}^{c^n}\}$ for Charlie. The entanglement $|\psi\rangle$ is shared between registers E_A, E_B, and E_C.

The subset of coordinates that we condition on winning (formerly called C) will be denoted by S. The answers to rounds in S that we condition on will be denoted together as $Q = (A_S, B_S, C_S)$ (formerly called $Z = (A_C, B_C)$).

The idea behind the multiplayer extension is that we will reduce to the two-player case by "bundling" two of the three players and treating them as a single player.

Dependency-breaking variable. The dependency-breaking variable Ω is constructed so that for each coordinate $i \notin S$, Ω_i will fix 2 out of 3 questions. That is, D_i will choose uniformly from $\{\{A, B\}, \{A, C\}, \{B, C\}\}$. The variable D_i indicates which questions M_i is coupled to. For example, if $D_i = \{A, B\}$, then M_i will be coupled to the pair (X_i, Y_i). The dependency breaking variable satisfies the following properties:

1. For all $(x, y, z) \in (\mathcal{X} \cup \{\perp\}) \times (\mathcal{Y} \cup \{\perp\}) \times (\mathcal{Z} \cup \{\perp\})$, $\mathrm{P}_{X_i Y_i Z_i}(x, y, z) = \mu_{\perp}(x, y, z)$.
2. For all ω, for all i, $\mathrm{P}_{X_i Y_i Z_i|\Omega=\omega}(x, y, z) = \mathrm{P}_{X_i|\Omega=\omega}(x) \cdot \mathrm{P}_{Y_i|\Omega=\omega}(y) \cdot \mathrm{P}_{Z_i|\Omega=\omega}(z)$.

Operators and states. We define the states and operators in nearly an identical way to the two-player case. We also introduce operators corresponding to the third player, Charlie. His operators $C_{\omega_{-i}, z_i}^{c_S}$, $C_{\omega_{-i}, \perp}^{c_S}$, $C_{\omega_{-i}, \perp/(x_i, y_i)}^{c_S}$, etc. are defined in the analogous manner.

The states are also defined in a similar way:

$$|\Phi_{x,y,z}\rangle = \sqrt{A_x} \otimes \sqrt{B_y} \otimes \sqrt{C_z}|\psi\rangle$$

where x, y, and z can be "normal" questions from $\mathcal{X}$, $\mathcal{Y}$, or $\mathcal{Z}$, or they can be $\perp$ or a hybrid such as $\perp/x$.

The analogue of Lemma 77 in the three-player setting is the following. We use simplified notation to maximize clarity, so we will suppress mention of i, ω_{-i}, and $q = (a_S, b_S, c_S)$, and treat them as implicit. Furthermore, we will ignore issues of normalization.

Lemma 82. *For all $(x, y, z) \in \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$, there exist unitaries U_x, V_y, and W_z acting on E_A, E_B, and E_C respectively such that*

$$\mathop{\mathbb{E}}_{XYZ} \left\| (U_x \otimes V_y \otimes W_z)|\Phi_{\perp,\perp,\perp}\rangle - |\Phi_{x,y,z}\rangle \right\|^2 = O(\delta^{1/4}/\alpha^{2k}).$$

Lemma 82, like in the two-player case, is proved in two steps. The first step is to establish the existence of unitaries U_x, V_y, and W_z such that $U_x|\Phi_{\perp,\perp,\perp}\rangle \approx |\Phi_{x,\perp,\perp}\rangle$, $V_x|\Phi_{\perp,\perp,\perp}\rangle \approx |\Phi_{\perp,y,\perp}\rangle$, and $W_z|\Phi_{\perp,\perp,\perp}\rangle \approx |\Phi_{\perp,\perp,z}\rangle$, with the unitaries acting on the appropriate spaces.

To prove, say, the existence of U_x, we first treat Bob and Charlie as one player – call him "SuperBob" – and use the analysis from the two-player case where the game G is a two player game involving Alice and SuperBob.

Now, using the same reasoning as in the two-player case, we get that

$$\mathop{\mathbb{E}}_{XY} \left\| (U_x \otimes V_y \otimes \mathbb{I})|\Phi_{\perp,\perp,\perp}\rangle - |\Phi_{x,y,\perp}\rangle \right\|^2 = O(\delta^{1/4}/\alpha^{2k}).$$

Now we just have to show that, on average over (x, y, z), $(\mathbb{I} \otimes \mathbb{I} \otimes W_z)|\Phi_{x,y,\perp}\rangle$ is close to $|\Phi_{x,y,z}\rangle$:

$$\begin{aligned}
&\left\|W_z|\Phi_{x,y,\perp}\rangle - |\Phi_{x,y,z}\rangle\right\| \\
&= \left\|W_z C_\perp C_{\perp/z}^{-1/2}|\Phi_{x,y,\perp/z}\rangle - C_z C_{\perp/z}^{-1/2}|\Phi_{x,y,\perp/z}\rangle\right\| \\
&= \left\|H_{x,y,z} \otimes W_z C_\perp C_{\perp/z}^{-1/2}|\Phi_{x,y,\perp/z}\rangle - H_{x,y,z} \otimes C_z C_{\perp/z}^{-1/2}|\Phi_{x,y,\perp/z}\rangle\right\| \\
&\approx \left\|W_z C_\perp C_{\perp/z}^{-1/2}|\Phi_{\perp,\perp,\perp/z}\rangle - C_z C_{\perp/z}^{-1/2}|\Phi_{\perp,\perp,\perp/z}\rangle\right\| \\
&= \left\|W_z|\Phi_{\perp,\perp,\perp}\rangle - |\Phi_{\perp,\perp,z}\rangle\right\| \\
&\approx 0.
\end{aligned}$$

where $H_{x,y,z}$ is a unitary acting on $E_A E_B$ jointly such that $H_{x,y,z}|\Phi_{x,y,\perp/z}\rangle \approx |\Phi_{\perp,\perp,\perp/z}\rangle$. Such a unitary is analogous to that in (6.21).

Once all the normalization factors are added back in to this calculation, we get Lemma 82, and from there, the main multiplayer theorem. The details of normalization are tedious and uninteresting, but essentially follow the same steps as in the two-player case.

6.5.4 A threshold theorem

We also observe that our proof nearly immediately yields a *threshold* version of our parallel repetition theorem: we can give an exponentially small bound on the probability that the players are able to win significantly more than a $(1 - \varepsilon)n$ coordinates in the repeated game $G_\perp^n$, where $\mathrm{val}^*(G_\perp) = 1 - \varepsilon$. In [87], Rao shows how a Lemma of the form 76 yields not only a parallel repetition theorem, but also gives a concentration bound. Using essentially the same argument, we get the following theorem:

Theorem 83. *Let G be an α-anchored k-player game with* $\mathrm{val}^*(G) \leq 1 - \varepsilon$. *Then for all integer $n \geq 1$ the probability that in the game G^n the players can win more than $(1 - \varepsilon + \gamma)n$ games is at most*

$$(1 - \gamma^9/2)^{c\alpha^{8k} n/s}$$

where c is a universal constant and s is the length of the players' answers.

Chapter 7

Parallel repetition for all entangled games

The work presented in this chapter was published in the proceedings of the International Colloquium on Automata, Languages, and Programming (ICALP 2016) under the title of "A parallel repetition theorem for all entangled games" [105].

7.1 Introduction

In this chapter we prove a weaker version of Quantum Parallel Repetition Conjecture. The strongest form of the Quantum Parallel Repetition Conjecture states that for a game G such that $\mathrm{val}^*(G) < 1$, $\mathrm{val}^*(G^{\otimes n})$ decays exponentially with n, analogously to Raz's classical parallel repetition theorem. All previous results have established special cases of this, and the previous chapter shows that, as far as gap amplification is concerned, the Quantum Parallel Repetition Conjecture is effectively solved.

However, the scientific question of how general entangled games behave under parallel repetition still remains: not only did we not know of a quantum analogue of Raz's Parallel Repetition Theorem, it hasn't even been shown that if $\mathrm{val}^*(G) < 1$, then $\mathrm{val}^*(G^n)$ goes to 0 as n goes to infinity! Could quantum entanglement allow players to counteract the value-decreasing effect of parallel repetition?

Here we prove that for all nontrivial entangled games G (i.e. $\mathrm{val}^*(G) < 1$), the entangled value of G^n must converge to 0. This resolves a weaker version of the Quantum Parallel Repetition Conjecture for general games. Quantitatively, we will show:

Theorem 84 (Main Theorem). *Let G be a game involving two entangled players with* $\mathrm{val}^*(G) = 1 - \varepsilon$. *Then for all integer $n > 0$,*

$$\mathrm{val}^*(G^n) \leq c \cdot \frac{s_G \log n}{\varepsilon^{17} n^{1/4}}$$

where c is a universal constant and s_G is the bit-length of the players' answers in G.

This shows that the entangled value of G^n must decay at a polynomial rate with n. The full Quantum Parallel Repetition Conjecture states that the rate of decay is in fact exponential, and this remains an important open problem.

7.1.1 Proof overview

7.1.2 Classical and quantum correlated sampling

Correlated sampling is a key component of Holenstein's proof of the classical parallel repetition theorem.

Lemma 85 (Classical correlated sampling [56]). *Let* P *and* Q *be two probability distributions over a universe* $\mathcal{U}$ *such that* $\|\mathsf{P}-\mathsf{Q}\|_1 \leq \varepsilon < 1$. *Then there exists a zero communication two-player protocol using shared randomness where the first player outputs an element* $p \in \mathcal{U}$ *distributed according to* P, *the second player samples an element* $q \in \mathcal{U}$ *distributed according to* Q, *and with probability at least* $1 - O(\varepsilon)$, *the two elements are identical (i.e.* $p = q$*).*

We call the protocol in the Lemma above the *classical correlated sampling procedure*. The next lemma is the quantum extension of the correlated sampling lemma, proved by [39] in order to obtain a parallel repetition theorem for entangled projection games, a class of two-player games. Their lemma is a robust version of the quantum state embezzlement procedure of [95].

Lemma 86 (Quantum correlated sampling [39]). *Let* d *be an integer and* $\alpha > 0$. *Then there exists an integer* d' *depending on* d *and* α, *and a collection of unitaries* V_ψ, W_ψ *acting on* $\mathbb{C}^{dd'}$ *for every state* $|\psi\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d$, *such that the following holds: for any two states* $|\varphi\rangle, |\theta\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d$,

$$\|\overline{V}_\varphi \otimes W_\theta |E_{dd'}\rangle - |\varphi\rangle|E_{d'}\rangle\| \leq O(\max\{\alpha^{1/12}, \| \, |\varphi\rangle - |\theta\rangle \, \|^{1/6}\})$$

where $|E_d\rangle \propto \sum_{j=1}^d \frac{1}{\sqrt{j}}|j\rangle|j\rangle$ *is the d-dimensional embezzlement state.*

We shall call the protocol in the Lemma above the *quantum correlated sampling procedure*.

7.2 Proof of the Main Theorem

Let G be a two-player one-round game with question distribution μ and referee predicate $V(x,y,a,b)$. Let $\mathcal{A}$ and $\mathcal{B}$ denote the alphabets of Alice's and Bob's answers, respectively. Let $\mathrm{val}^*(G) = 1 - \varepsilon$.

Consider an optimal entangled strategy for G^n, which consists of a shared entangled state $|\psi\rangle^{E_A E_B} \in \mathbb{C}^d \otimes \mathbb{C}^d$ and measurement POVMs for Alice and Bob, $\{A_{x_{[n]}}^{a_{[n]}}\}$ and $\{B_{y_{[n]}}^{b_{[n]}}\}$ respectively. We will assume that $|\psi\rangle$ is symmetric; i.e., $|\psi\rangle = \sum_i \sqrt{\lambda_i}|v_i\rangle|v_i\rangle$ for some orthonormal basis $\{|v_i\rangle\}$. This is without loss of generality, as we can always rotate (say) Bob's basis vectors to match Alice's basis vectors, and fold the unitary rotation into Bob's measurements. For $i \in [n]$, let W_i denote the event that the players win coordinate i using this optimal strategy. Let $W = W_1 \wedge \cdots \wedge W_n$ denote the event that the players win all coordinates. For a set $C \subseteq [n]$, let $W_C = \wedge_{i \in C} W_i$.

Proposition 87. *Suppose that* $\log 1/\Pr(W) \leq \varepsilon n/16 - \log 4/\varepsilon$. *Then there exists a set* $C \subseteq [n]$ *of size at most* $t = \frac{8}{\varepsilon}(\log 4/\varepsilon + \log 1/\Pr(W))$ *such that*

$$\Pr_{i \notin C}(W_i | W_C) \geq 1 - \varepsilon/2.$$

where i *is chosen uniformly from* $[n] - C$.

Proof. Set $\delta = \varepsilon/8$. Let $W_{>1-\delta}$ denote the event that the players won more than $(1-\delta)n$ rounds. To show existence of such a set C, we will show that $\mathbb{E}_C \Pr(\neg W_i | W_C) \leq \varepsilon/2$, where C is a (multi)set of t independently chosen indices in $[n]$. This implies that there exists a particular set C such that $\Pr(\neg W_i | W_C) \leq \varepsilon/2$, which concludes the claim.

First we write, for a fixed C,

$$\begin{aligned}\Pr(\neg W_i | W_C) = \Pr(\neg W_i | W_C, W_{>1-\delta}) \Pr(W_{>1-\delta} | W_C) + \\ \Pr(\neg W_i | W_C, \neg W_{>1-\delta}) \Pr(\neg W_{>1-\delta} | W_C).\end{aligned}$$

Observe that $\Pr(\neg W_i | W_C \wedge W_{>1-\delta})$ is the probability that, conditioned on winning all rounds in C, the randomly selected coordinate $i \in [n] - C$ happens to be one of the (at most) δn lost rounds. This is at most $\delta n/(n-t) \leq \varepsilon/4$, where we use our assumption on t from the Proposition statement. Now observe that

$$\begin{aligned}\mathop{\mathbb{E}}_{C} \Pr(\neg W_{>1-\delta} | W_C) &\leq \mathop{\mathbb{E}}_{C} \frac{\Pr(W_C | \neg W_{>1-\delta})}{\Pr(W_C)} \\ &\leq \frac{1}{\Pr(W)} (1-\delta)^t \\ &\leq \varepsilon/4\end{aligned}$$

where in the second line we used the fact that $\Pr(W_C) \geq \Pr(W)$. □

For the rest of the proof we will fix a set C given by Proposition 87.

7.2.1 Dependency-breaking variables

We introduce the random variables that play an important role in the proof of Theorem 84. Let $C \subseteq [n]$ be as given by Proposition 87. We fix $C = \{m+1, m+2, \ldots, n\}$, where $m = n - |C|$, as this will easily be seen to hold without loss of generality. Let $(X_{[n]}, Y_{[n]})$ be distributed according to $\mu_{[n]}$ and $(A_{[n]}, B_{[n]})$ be defined from $X_{[n]}$ and $Y_{[n]}$ as follows:

$$\mathsf{P}_{A_{[n]}B_{[n]}|x_{[n]},y_{[n]}}(a_{[n]}, b_{[n]}) = \langle \psi | A^{a_{[n]}}_{x_{[n]}} \otimes B^{b_{[n]}}_{y_{[n]}} | \psi \rangle.$$

Let (X_C, Y_C) and $Z = (A_C, B_C)$ be random variables that denote the players' questions and answers respectively associated with the coordinates indexed by C.

We use the random variables Ω and R that are crucially used in Holenstein's proof of Raz's parallel repetition theorem. Let $D_1, \ldots, D_m$ be independent and uniformly distributed in $\{Alice, Bob\}$. Let $M_1, \ldots, M_m$ be independent random variables defined in the following way: for each $i \in [m]$,

$$M_i = \begin{cases} X_i & \text{if } D_i = Alice \\ Y_i & \text{if } D_i = Bob \end{cases}$$

Now for $i \in [m]$, we define $\Omega_i := (D_i, M_i)$. We say that Ω_i *fixes Alice's input* if $D_i = Alice$, and otherwise Ω_i fixes Bob's input. We write Ω to denote the random variable $(\Omega_1, \ldots, \Omega_m, X_C, Y_C)$, where $X_C Y_C$ are Alice and Bob's questions in the coordinates indexed by C. For $i \in [m]$ we write Ω_{-i} to denote the random variable Ω with Ω_i omitted.

Proposition 88. *Conditioned on Ω, $X_{[n]}$ and $Y_{[n]}$ are independent.*

Finally, we will define a *dependency-breaking variable* $R := (\Omega, A_C, B_C)$, where A_C and B_C are the players' answers in the coordinates indexed by C. For $i \notin C$, we let $R_{-i} := (\Omega_{-i}, A_C, B_C)$. R_i will refer to Ω_i. We will use lowercase letters to denote instantiations of these random variables: e.g., r_{-i}, x_i, and y_i refer to specific values of R_{-i}, X_i, and Y_i.

Throughout our proofs, all expectations are implicitly over the measure defined by P. For example, the expectation $\mathbb{E}_{\Omega_{-i}Z|x_i,y_i}$ indicates $\sum_{\omega_{-i},a_C,b_C} \mathsf{P}_{\Omega_{-i}A_CB_C|x_i,y_i}(\omega_{-i}, a_C, b_C)$. Given an event such as W (winning all the coordinates) or W_C (winning all the coordinates in C), $\mathsf{P}(W)$ and $\mathsf{P}(W_C)$ will mean the probability of these events with respect to the distribution P.

The following Lemma expresses the idea that, because W_C is an event that occurs with not-too-small probability, conditioning on it cannot skew the distribution of variables corresponding to an average coordinate by too much. This Lemma follows in a straightforward manner from the [56].

Lemma 89. *The following statements hold on, average over i chosen uniformly in* $[m]$*:*

1. $\mathbb{E}_i \, \|\mathsf{P}_{R_iX_iY_i|W_C} - \mathsf{P}_{R_iX_iY_i}\|_1 \leq O(\sqrt{\delta})$
2. $\mathbb{E}_i \left\|\mathsf{P}_{X_iY_iR_{-i}|W_C} - \mathsf{P}_{X_iY_i} \cdot \mathsf{P}_{R_{-i}|X_iW_C}\right\|_1 \leq O(\sqrt{\delta})$
3. $\mathbb{E}_i \left\|\mathsf{P}_{X_iY_iR_{-i}|W_C} - \mathsf{P}_{X_iY_i} \cdot \mathsf{P}_{R_{-i}|Y_iW_C}\right\|_1 \leq O(\sqrt{\delta})$

where $\delta := \frac{1}{m}\left(\log 1/\mathsf{P}(W_C) + |C| \log |\mathcal{A}||\mathcal{B}|\right)$.

7.2.2 Two key Lemmas, and proof of the Main Theorem

For every $i \in [n] - C$, we will construct a collection of bipartite states $\{|\Psi_{r_{-i},x_i,y_i}\rangle\} \subseteq \mathbb{C}^d \otimes \mathbb{C}^d$, which we call dependency-breaking states, that are indexed by the dependency-breaking variable r_{-i} defined above, and questions (x_i, y_i). The following lemmas state the important properties of this collection of states:

Lemma 90 (Usefulness Lemma). *For all* r_{-i}, x_i, y_i*, there exist POVMs* $\{\hat{A}^{a_i}_{r_{-i},x_i}\}$ *and* $\{\hat{B}^{b_i}_{r_{-i},y_i}\}$ *acting on* $\mathbb{C}^d$ *such that*

$$\mathsf{P}_{A_iB_i|r_{-i},x_i,y_i}(a_i, b_i) = \mathrm{Tr}\left(\hat{A}^{a_i}_{r_{-i},x_i} \otimes \hat{B}^{b_i}_{r_{-i},y_i} \Psi_{r_{-i},x_i,y_i}\right).$$

Lemma 91 (Sampleability Lemma). *For every* i, r_{-i}, x_i, y_i*, there exist an integer* $d' \geq d$ *and local unitaries* U_{r_{-i},x_i}, V_{r_{-i},y_i} *acting on* $\mathbb{C}^{d'}$ *such that*

$$\mathop{\mathbb{E}}_{i} \mathop{\mathbb{E}}_{X_iY_i} \left[\mathop{\mathbb{E}}_{R_{-i}|x_i,y_i,W_C} \left\|U_{r_{-i},x_i} \otimes V_{r_{-i},y_i} |E_{d'}\rangle - |\Psi_{r_{-i},x_i,y_i}\rangle \otimes |\Lambda_{r_{-i},x_i,y_i}\rangle\right\| \right] \leq O((\delta^{1/4}/\mathsf{P}(W_C))^{1/12})$$

where $|E_{d'}\rangle \propto \sum_{j=1}^{d'} \frac{1}{\sqrt{j}} |j\rangle|j\rangle$ *is the* d'*-dimensional embezzlement state, and* $|\Lambda_{r_{-i},x_i,y_i}\rangle$ *is an arbitrary state.*

Lemma 90 shows that the states $|\Psi_{r_{-i},x_i,y_i}\rangle$ are *useful* to have; they allow Alice and Bob to produce answers in the i'th coordinate whose statistics are consistent with the dependency-breaking variable r_{-i} and their inputs (x_i, y_i). Lemma 91 shows that these states are *locally generatable* by Alice and Bob, when given joint access to preshared entanglement, the dependency-breaking variable r_{-i} and their own inputs x_i and y_i respectively.

Using these two Lemmas we can prove the Main Theorem.

Proof of the Main Theorem. Consider the following strategy for the game G. Alice and Bob share beforehand the embezzlement state $|E_{dd'}\rangle$ of dimension dd' given by Lemma 91, and they also have access to shared randomness. Given inputs (x, y) distributed according to $\mathsf{P}_{XY} = \mu$:

1. Alice and Bob jointly sample a uniformly random $i \in [n] - C$. Alice sets $x_i = x$ and Bob sets $y_i = y$.
2. Alice and Bob jointly, approximately sample R_{-i} from $\mathsf{P}_{R_{-i}|x_i,y_i,W_C}$ using the classical correlated sampling procedure.
3. Alice applies U_{r_{-i},x_i} to her side of $|E_{dd'}\rangle$
4. Bob applies V_{r_{-i},y_i} to his side of $|E_{dd'}\rangle$
5. Alice measures her side of the entanglement using $\{\hat{A}^{a_i}_{r_{-i},x_i}\}$ and outputs the outcome a_i
6. Bob measures his side of the entanglement using $\{\hat{B}^{b_i}_{r_{-i},y_i}\}$ and outputs the outcome b_i

We now analyze the success probability of this strategy. We will use $\widetilde{\mathsf{P}}$ to denote the distribution of variables in the probability space associated with an execution of this strategy. For example, we will write $\widetilde{\mathsf{P}}_{R_{-i}|X_iY_i}$ to denote the distribution of R_{-i} conditioned on X_iY_i that is sampled in Step 2. From Lemma 89 we have that on average over i, $\mathsf{P}_{X_iY_iR_{-i}|W_C} \approx \mathsf{P}_{X_iY_i} \cdot \mathsf{P}_{R_{-i}|X_iW_C} \approx \mathsf{P}_{X_iY_i} \cdot \mathsf{P}_{R_{-i}|Y_iW_C}$, where "$\approx$" means closeness in statistical distance. By invoking the classical correlated sampling procedure of Lemma 85, we get

$$\mathop{\mathbb{E}}_{i} \|\mathsf{P}_{X_iY_i} \cdot \widetilde{\mathsf{P}}_{R_{-i}|X_iY_i} - \mathsf{P}_{X_iY_iR_{-i}|W_C}\|_1 \leq O(\sqrt{\delta}).$$

After Step 4, Alice and Bob will possess a state $|\Lambda_{r_{-i},x_i,y_i}\rangle$ such that

$$\mathop{\mathbb{E}}_{i} \mathop{\mathbb{E}}_{X_iY_i} \left[\mathop{\mathbb{E}}_{R_{-i}|x_i,y_i,W_C} \|\Lambda_{r_{-i},x_i,y_i} - \Psi_{r_{-i},x_i,y_i}\|_1 \right] \leq \eta$$

where $\eta = O((\delta^{1/4}/\mathsf{P}(W_C))^{1/12})$. Consider the measurement process in Steps 5 and 6. Let $\widetilde{\mathsf{P}}_{A_iB_i|r_{-i},x_i,y_i}$ denote the distribution of measurement outcomes in this strategy, conditioned on their inputs and a sampled value of r_{-i}. By Lemma 90 and the fact that the trace norm is nonincreasing under quantum operations, we have that

$$\mathop{\mathbb{E}}_{i} \mathop{\mathbb{E}}_{X_iY_i} \left[\mathop{\mathbb{E}}_{R_{-i}|x_i,y_i,W_C} \|\widetilde{\mathsf{P}}_{A_iB_i|x_i,y_i,r_{-i}} - \mathsf{P}_{A_iB_i|x_i,y_i,r_{-i}}\|_1 \right] \leq \eta$$

or equivalently

$$\mathop{\mathbb{E}}_{i} \|\mathsf{P}_{X_iY_i} \cdot \widetilde{\mathsf{P}}_{R_{-i}|X_iY_iW_C} \cdot \widetilde{\mathsf{P}}_{A_iB_i|x_i,y_i,r_{-i}} - \mathsf{P}_{X_iY_i} \cdot \mathsf{P}_{R_{-i}|X_iY_iW_C} \cdot \mathsf{P}_{A_iB_iR_{-i}|X_iY_iW_C}\|_1 \leq \eta.$$

By Lemma 89 we have $\mathbb{E}_i \|\mathsf{P}_{X_iY_i|W_C} - \mathsf{P}_{X_iY_i}\| \le \sqrt{\delta}$. By triangle inequality and that $\widetilde{\mathsf{P}}_{X_iY_i} = \mathsf{P}_{X_iY_i}$, we have

$$\mathop{\mathbb{E}}_i \|\widetilde{\mathsf{P}}_{X_iY_iR_{-i}A_iB_i} - \mathsf{P}_{X_iY_iR_{-i}A_iB_i|W_C}\|_1 \le O(\eta).$$

Note that $\widetilde{\mathsf{P}}_{X_iY_iR_{-i}A_iB_i}$ represents the probability distribution of all the variables present in the strategy above. Let W_i denote the probability the players win the ith coordinate. Thus we get

$$\mathop{\mathbb{E}}_i |\widetilde{\mathsf{P}}(W_i) - \mathsf{P}(W_i|W_C)| \le O(\eta). \tag{7.1}$$

Assume that

$$\mathsf{P}(W) \ge \frac{cs \log n}{\varepsilon^{17} n^{1/4}}$$

where $c > 0$ is a universal constant, and s is the bit-length of the players' answers. Since $\mathsf{P}(W_C) \ge \mathsf{P}(W)$, and using our bound on $|C|$ (from Proposition 87) and our bound on δ (from Lemma 89), this implies that the right hand side of (7.1) is at most $\varepsilon/4$ (for an appropriate choice of c). This implies that

$$\begin{aligned}\mathop{\mathbb{E}}_i \widetilde{\mathsf{P}}(W_i) &\ge \mathop{\mathbb{E}}_i \mathsf{P}(W_i|W_C) - \varepsilon/4\\ &\ge 1 - \varepsilon/2 - \varepsilon/4\\ &> \mathrm{val}^*(G)\end{aligned}$$

where in the second line we used the bound from Proposition 87. However, this is a contradiction, as $\mathbb{E}_i \widetilde{\mathsf{P}}(W_i)$ is the probability that this strategy wins the game G, which cannot be larger than $\mathrm{val}^*(G)$. Therefore $\mathsf{P}(W) \le \frac{cs \log n}{\varepsilon^{17} n^{1/4}}$.

□

7.3 Proofs of the two Key Lemmas

Now we turn to proving the two key lemmas above, the Usefulness Lemma and the Sampleability Lemma.

7.3.1 Quantum states and operators

In this subsection we define the states $|\Psi_{r_{-i},x_i,y_i}\rangle$ and measurement operators $\{\hat{A}^{a_i}_{r_{-i},x_i}\}$ and $\{\hat{B}^{b_i}_{r_{-i},y_i}\}$. Recall that the dependency-breaking variable R consists of the set of fixed questions $\Omega = (X_C, Y_C, \Omega_1, \dots, \Omega_m)$ and fixed answers $Z = (A_C, B_C)$ for the coordinates in C.

Coarse-grained measurements. We first *coarsen* the measurement POVMs $\{A^{a_{[n]}}_{x_{[n]}}\}$ and $\{B^{b_{[n]}}_{y_{[n]}}\}$ that constitute Alice and Bob's strategy in G^n to construct a set of *intermediate measurements*, which essentially produce answers for the games in set C, conditioned on a setting of Ω.

Fix i, ω, a_C, b_C, x_i, y_i. Define

$$A^{a_C}_{\omega_{-i},x_i} = \sum_{a_{[n]}|a_C} \mathop{\mathbb{E}}_{X_{[n]}|\omega_{-i},x_i} A^{a_{[n]}}_{x_{[n]}} \qquad\qquad B^{b_C}_{\omega_{-i},y_i} = \sum_{b_{[n]}|b_C} \mathop{\mathbb{E}}_{Y_{[n]}|\omega_{-i},y_i} B^{b_{[n]}}_{y_{[n]}}$$

where $a_{[n]}|a_C$ (resp. $b_{[n]}|b_C$) indicates summing over all tuples $a_{[n]}$ consistent with the suffix a_C (resp. $b_{[n]}$ consistent with suffix b_C) and recall that $\mathbb{E}_{X_{[n]}|\omega_{-i},x_i}$ is shorthand for $\sum_{x_{[n]}} \mathsf{P}_{X_{[n]}|\Omega_{-i}=\omega_{-i},X_i=x_i}(x_{[n]})$. We also define

$$A^{a_C}_{\omega} = \mathop{\mathbb{E}}_{X_{[n]}|\omega} A^{a_C}_{x_{[n]}} \qquad\qquad B^{b_C}_{\omega} = \mathop{\mathbb{E}}_{Y_{[n]}|\omega} B^{b_C}_{y_{[n]}}.$$

Let ρ denote the reduced density matrix of $|\psi\rangle$ on Alice's side. Since we have assumed that $|\psi\rangle$ is symmetric, ρ is also the reduced density matrix on Bob's side. For all i, ω, x_i, y_i, a_C, b_C, let U_{ω_{-i},x_i,a_C}, U_{ω,a_C}, V_{ω_{-i},y_i,b_C}, and V_{ω,b_C} be unitaries such that

$$U_{\omega_{-i},x_i,a_C}(A^{a_C}_{\omega_{-i},x_i})^{1/2}\sqrt{\rho} \qquad\qquad V_{\omega_{-i},y_i,b_C}(B^{b_C}_{\omega_{-i},y_i})^{1/2}\sqrt{\rho}$$
$$U_{\omega,a_C}(A^{a_C}_{\omega})^{1/2}\sqrt{\rho} \qquad\qquad V_{\omega,b_C}(B^{b_C}_{\omega})^{1/2}\sqrt{\rho}$$

are positive semidefinite. Such unitaries can be found via singular value decompositions. For notational convenience, let

$$S_{\omega_{-i},x_i,a_C} = U_{\omega_{-i},x_i,a_C}(A^{a_C}_{\omega_{-i},x_i})^{1/2} \qquad\qquad T_{\omega_{-i},y_i,b_C} = V_{\omega_{-i},y_i,b_C}(B^{b_C}_{\omega_{-i},y_i})^{1/2}$$
$$S_{\omega,a_C} = U_{\omega,a_C}(A^{a_C}_{\omega})^{1/2} \qquad\qquad T_{\omega,b_C} = V_{\omega,b_C}(B^{b_C}_{\omega})^{1/2}$$

Fine-grained measurements. Now we can define the *fine-grained measurements* that Alice and Bob can apply to obtain answers for the i'th game. Define

$$\hat{A}^{a_i}_{r_{-i},x_i} = S^{-1}_{\omega_{-i},x_i,a_C} A^{a_C,a_i}_{\omega_{-i},x_i} S^{-1}_{\omega_{-i},x_i,a_C} \qquad\qquad \hat{B}^{b_i}_{r_{-i},y_i} = T^{-1}_{\omega_{-i},y_i,b_C} B^{b_C,b_i}_{\omega_{-i},y_i} T^{-1}_{\omega_{-i},y_i,b_C}$$

where

$$A^{a_C,a_i}_{\omega_{-i},x_i} = \sum_{a_{[n]}|a_C,a_i} \mathop{\mathbb{E}}_{X_{[n]}|\omega_{-i},x_i} A^{a_{[n]}}_{x_{[n]}} \qquad\qquad B^{b_C,b_i}_{\omega_{-i},y_i} = \sum_{b_{[n]}|b_C,b_i} \mathop{\mathbb{E}}_{Y_{[n]}|\omega_{-i},y_i} B^{b_{[n]}}_{y_{[n]}}$$

and $a_{[n]}|a_C, a_i$ (resp. $b_{[n]}|b_C, b_i$) denotes summing over all $a_{[n]}$ consistent with a_C and a_i (resp. all $b_{[n]}$ consistent with b_C and b_i). It is easy to verify that the sets $\{\hat{A}^{a_i}_{r_{-i},x_i}\}_{a_i\in\mathcal{A}}$ and $\{\hat{B}^{b_i}_{r_{-i},y_i}\}_{b_i\in\mathcal{B}}$ form POVMs. Here, for a square matrix A, A^{-1} denotes its generalized inverse.

States. Now we are ready to define the states. Fix $i, r_{-i} = (\omega_{-i}, a_C, b_C)$, and x_i, y_i. Then let

$$|\Psi_{r_{-i},x_i,y_i}\rangle = \frac{S_{\omega_{-i},a_C,x_i} \otimes T_{\omega_{-i},b_C,y_i}|\psi\rangle}{\left\| S_{\omega_{-i},a_C,x_i} \otimes T_{\omega_{-i},b_C,y_i}|\psi\rangle \right\|}.$$

Observe that the normalization $\left\| S_{\omega_{-i},a_C,x_i} \otimes T_{\omega_{-i},b_C,y_i}|\psi\rangle \right\|^2$ is equal to $\mathsf{P}_{A_C B_C|\omega_{-i},x_i,y_i}(a_C, b_C)$.

7.3.2 Proof of Usefulness Lemma (Lemma 90)

This Lemma follows from a simple calculation: for every $x_i, y_i, a_i, b_i, r_{-i}$:

$$\mathrm{Tr}\left(\hat{A}^{a_i}_{r_{-i},x_i} \otimes \hat{B}^{b_i}_{r_{-i},y_i}\, \Psi_{r_{-i},x_i,y_i}\right)$$

$$
\begin{aligned}
&= \frac{1}{\left\| S_{\omega_{-i},a_C,x_i} \otimes T_{\omega_{-i},b_C,y_i} |\psi\rangle \right\|^2} \mathrm{Tr}\left(A^{a_C,a_i}_{\omega_{-i},x_i} \otimes B^{b_C,b_i}_{\omega_{-i},y_i} |\psi\rangle\langle\psi| \right) \\
&= \frac{1}{\mathsf{P}_{A_C B_C|\omega_{-i},x_i,y_i}(a_C,b_C)} \sum_{a_{[n]}|a_C,a_i} \sum_{b_{[n]}|b_C,b_i} \mathop{\mathbb{E}}_{X_{[n]}Y_{[n]}|\omega_{-i},x_i,y_i} \mathrm{Tr}\left(A^{a_{[n]}}_{x_{[n]}} \otimes B^{b_{[n]}}_{y_{[n]}} |\psi\rangle\langle\psi| \right) \\
&= \frac{\mathsf{P}_{A_i B_i A_C B_C|\omega_{-i},x_i,y_i}(a_i,b_i,a_C,b_C)}{\mathsf{P}_{A_C B_C|\omega_{-i},x_i,y_i}(a_C,b_C)} \\
&= \mathsf{P}_{A_i B_i|r_{-i},x_i,y_i}(a_i,b_i).
\end{aligned}
$$

In the second equality we used that conditioned on Ω, $X_{[n]}$ and $Y_{[n]}$ are independent, so therefore $\mathbb{E}_{X_{[n]}|\omega_{-i},x_i} \mathbb{E}_{Y_{[n]}|\omega_{-i},y_i} = \mathbb{E}_{X_{[n]}Y_{[n]}|\omega_{-i},x_i,y_i}$. In the last equality we used that $r_{-i} = (\omega_{-i}, a_C, b_C)$. This concludes the Usefulness Lemma.

7.3.3 Proof of the Sampleability Lemma (Lemma 91)

Overview. Here we give some intuition. We first analyze an ensemble of states $\{|\Gamma_{x_i,x_C,a_C}\rangle\}$ (for now we omit mention of the dependency-breaking variable R for simplicity). These are indexed by Alice's questions in the i'th coordinate, her questions in the C coordinates, as well as her answers in the C coordinates. The state $|\Gamma_{x_i,x_C,a_C}\rangle$ roughly represents the state of the players where only Alice has applied her measurements – Bob hasn't done anything yet.

Fix a y_i, x_C, a_C. For average x_i, x_i' that are independently sampled from the marginal distribution $\mathsf{P}_{X_i|Y_i=y_i}$, we will show that

$$
\left\| |\Gamma_{x_i,x_C,a_C}\rangle - |\Gamma_{x_i',x_C,a_C}\rangle \right\| \sim \frac{1}{n}.
$$

To handle issues such as Alice "printing" her input onto the state $|\psi\rangle$ (as discussed in the introduction), the definition of $|\Gamma_{x_i,x_C,a_C}\rangle$ requires local unitaries that "undo" such overt actions of Alice and Bob – this is accomplished by the unitaries U and V defined in Section 7.3.1.

Then, we consider what happens when we apply Bob's measurement to both states $|\Gamma_{x_i,x_C,a_C}\rangle$ and $|\Gamma_{x_i',x_C,a_C}\rangle$, and condition on obtaining answers b_C for the C coordinates. His measurement will depend on the questions y_i and y_C. The post-measurement states will be precisely $|\Psi_{x_i,y_i,x_C,y_C,a_C,b_C}\rangle$ and $|\Psi_{x_i',y_i,x_C,y_C,a_C,b_C}\rangle$. The distance between these states will be, roughly speaking, the distance between $|\Gamma_{x_i,x_C,a_C}\rangle$ and $|\Gamma_{x_i',x_C,a_C}\rangle$ divided by the probability of Bob obtaining outcome b_C conditioned on Alice obtaining a_C. If we average this distance over all choices of x_C, y_C, a_C, b_C that imply the event W_C, we get that the average distance between $|\Psi_{x_i,y_i,x_C,y_C,a_C,b_C}\rangle$ and $|\Psi_{x_i',y_i,x_C,y_C,a_C,b_C}\rangle$ is approximately $\frac{1}{n\mathsf{P}(W_C)}$. If $\mathsf{P}(W)$ is much greater than $1/n$, then this distance is small. We then invoke quantum correlated sampling (Lemma 86), and that proves the Sampleability Lemma.

Proof. We introduce the following state:

$$
\xi_{\Omega X_{[n]} E_A E_B A_C} = \sum_{\omega, x_{[n]}, a_C} \mathsf{P}_{\Omega X_{[n]}}(\omega, x_{[n]}) \, |\omega \, x_{[n]}\rangle\langle\omega \, x_{[n]}| \otimes \sqrt{A^{a_C}_{x_{[n]}}} |\psi\rangle\langle\psi| \sqrt{A^{a_C}_{x_{[n]}}} \otimes |a_C\rangle\langle a_C|.
$$

If we trace out the E_A register, we have that

$$\begin{aligned}
\xi_{\Omega X_{[n]} E_B A_C} &= \sum_{\omega, x_{[n]}, a_C} \mathsf{P}_{\Omega X_{[n]}}(\omega, x_{[n]})\, |\omega\, x_{[n]}\rangle\langle \omega\, x_{[n]}| \otimes \sqrt{\rho}\,\overline{A^{a_C}_{x_{[n]}}}\sqrt{\rho} \otimes |a_C\rangle\langle a_C| \\
&\preceq \sum_{\omega, x_{[n]}, a_C} \mathsf{P}_{\Omega X_{[n]}}(\omega, x_{[n]})\, |\omega\, x_{[n]}\rangle\langle \omega\, x_{[n]}| \otimes \sqrt{\rho}\,\overline{A^{a_C}_{x_{[n]}}}\sqrt{\rho} \otimes \mathbb{I} \\
&= \sum_{\omega, x_{[n]}} \mathsf{P}_{\Omega X_{[n]}}(\omega, x_{[n]})\, |\omega\, x_{[n]}\rangle\langle \omega\, x_{[n]}| \otimes \rho \otimes \mathbb{I},
\end{aligned}$$

where ρ is the reduced density matrix of $|\psi\rangle = \sum_j \sqrt{\lambda_j}|v_j\rangle|v_j\rangle$ on E_B, $\overline{A^{a_C}_{x_{[n]}}}$ denotes the entry-wise complex conjugate of $A^{a_C}_{x_{[n]}}$ with respect to the basis $\{|v_j\rangle\}$, and the last equality uses $\sum_{a_C} \overline{A^{a_C}_{x_{[n]}}} = \mathbb{I}$. From the definition of S_∞ we have

$$\begin{aligned}
|C| \cdot \log |\mathcal{A}| &\geq S_\infty\left(\xi_{\Omega X_{[n]} E_B A_C} \middle\| \xi_{\Omega X_{[n]}} \otimes \xi_{E_B} \otimes \frac{\mathbb{I}}{\mathrm{Tr}(\mathbb{I})}\right) \\
&\geq S\left(\xi_{\Omega X_{[n]} E_B A_C} \middle\| \xi_{\Omega X_{[n]}} \otimes \xi_{E_B} \otimes \frac{\mathbb{I}}{\mathrm{Tr}(\mathbb{I})}\right) && (S(\cdot\|\cdot) \leq S_\infty(\cdot\|\cdot)) \\
&\geq \mathop{\mathbb{E}}_{\Omega, A_C} S\left(\xi_{X_{[n]} E_B|\omega, a_C} \middle\| \xi_{X_{[n]}|\omega} \otimes \xi_{E_B}\right) && \text{(Fact 10)}
\end{aligned}$$

Now we apply Quantum Raz's Lemma:

$$\mathop{\mathbb{E}}_{\Omega, A_C} \mathop{\mathbb{E}}_{i} I(X_i; E_B|\omega, a_C)_\xi \leq \frac{|C| \cdot \log |\mathcal{A}|}{m} \leq \delta \tag{7.2}$$

where recall that we defined $\delta = (|C| \log |\mathcal{A}| \cdot |B|)/m$. Applying the inequalities of Pinsker and Jensen, we obtain

$$\mathop{\mathbb{E}}_{\Omega, A_C} \mathop{\mathbb{E}}_{i} \mathop{\mathbb{E}}_{X_i|\omega, a_C} \left\| \xi_{E_B|\omega, x_i, a_C} - \xi_{E_B|\omega, a_C} \right\|_1 \leq \sqrt{\delta}. \tag{7.3}$$

These marginal density matrices have a nice description. Fix i, ω, x_i, a_C. First we note that the state $\xi_{E_B|\omega, x_i, a_C}$ does not depend on ω_i, because we are already conditioning on x_i. Thus we can write it as $\xi_{E_B|\omega_{-i}, x_i, a_C}$. Then

$$\begin{aligned}
\xi_{E_B|\omega_{-i}, a_C, x_i} &= \frac{1}{\mathsf{P}_{A_C|\omega_{-i}, x_i}(a_C)} \sum_{x_{[n]}} \mathsf{P}_{X_{[n]}|\omega_{-i}, x_i}(x_{[n]})\, \sqrt{\rho}\,\overline{A^{a_C}_{x_{[n]}}}\sqrt{\rho} \\
&= \frac{1}{\mathsf{P}_{A_C|\omega_{-i}, x_i}(a_C)} \sqrt{\rho} \left(\sum_{x_{[n]}} \mathsf{P}_{X_{[n]}|\omega_{-i}, x_i}(x_{[n]}) \overline{A^{a_C}_{x_{[n]}}}\right) \sqrt{\rho} \\
&= \frac{1}{\mathsf{P}_{A_C|\omega_{-i}, x_i}(a_C)} \sqrt{\rho}\,\overline{A^{a_C}_{\omega_{-i}, x_i}}\sqrt{\rho}.
\end{aligned}$$

Similarly,

$$\xi_{E_B|\omega, a_C} = \frac{1}{\mathsf{P}_{A_C|\omega}(a_C)} \sqrt{\rho}\,\overline{A^{a_C}_{\omega}}\sqrt{\rho}.$$

For all ω, x_i, a_C, define the following (unnormalized) states:

$$|\Gamma_{\omega_{-i},x_i,a_C}\rangle = S_{\omega_{-i},x_i,a_C} \otimes \mathbb{I}\,|\psi\rangle \qquad\qquad |\Gamma_{\omega,a_C}\rangle = S_{\omega,a_C} \otimes \mathbb{I}\,|\psi\rangle \tag{7.4}$$

where the S operators were defined in Section 7.3.1. Let $\gamma_{\omega_{-i},x_i,a_C} = (\mathsf{P}_{A_C|\omega_{-i},x_i}(a_C))^{1/2} = \| |\Gamma_{\omega_{-i},x_i,a_C}\rangle \|$ and $\gamma_{\omega,a_C} = (\mathsf{P}_{A_C|\omega}(a_C))^{1/2} = \| |\Gamma_{\omega,a_C}\rangle \|$ denote their norms. We will write

$$|\widetilde{\Gamma}_{\omega_{-i},x_i,a_C}\rangle = \gamma^{-1}_{\omega_{-i},x_i,a_C} |\Gamma_{\omega_{-i},x_i,a_C}\rangle \qquad\qquad |\widetilde{\Gamma}_{\omega,a_C}\rangle = \gamma^{-1}_{\omega,a_C} |\Gamma_{\omega,a_C}\rangle$$

to denote the normalized states.

For notational convenience we will suppress mention of ω_{-i} and $z = (a_C, b_C)$, and implicitly carry them around. Thus, for example, when we write $|\Gamma_{x_i}\rangle$ and $|\Gamma_{\omega_i}\rangle$, we implicitly mean $|\Gamma_{\omega_{-i},x_i,a_C}\rangle$ and $|\Gamma_{\omega,a_C}\rangle$, respectively.

Fix x_i, and consider the following:

$$\begin{aligned}
&\| |\widetilde{\Gamma}_{x_i}\rangle - |\widetilde{\Gamma}_{\omega_i}\rangle \|^2 \\
&= \left(\langle\widetilde{\Gamma}_{x_i}| - \langle\widetilde{\Gamma}_{\omega_i}|\right)\left(|\widetilde{\Gamma}_{x_i}\rangle - |\widetilde{\Gamma}_{\omega_i}\rangle\right) \\
&= \langle\psi|(\gamma_{x_i}^{-1} S_{x_i} - \gamma_{\omega_i}^{-1} S_{\omega_i})^\dagger(\gamma_{x_i}^{-1} S_{x_i} - \gamma_{\omega_i}^{-1} S_{\omega_i}) \otimes \mathbb{I}|\psi\rangle \\
&= \mathrm{Tr}\left(\sqrt{\rho}(\gamma_{x_i}^{-1} S_{x_i} - \gamma_{\omega_i}^{-1} S_{\omega_i})^\dagger(\gamma_{x_i}^{-1} S_{x_i} - \gamma_{\omega_i}^{-1} S_{\omega_i})\sqrt{\rho}\right) \qquad \text{(Ando's Identity)} \\
&= \|\gamma_{x_i}^{-1} S_{x_i}\sqrt{\rho} - \gamma_{\omega_i}^{-1} S_{\omega_i}\sqrt{\rho}\|_F^2.
\end{aligned}$$

Next we use the Powers-Størmer inequality [86], which states that for positive semidefinite operators A, B, we have $\|A - B\|_F^2 \leq \|A^2 - B^2\|_1$. Since $S_{x_i}\sqrt{\rho}$ and $S_{\omega_i}\sqrt{\rho}$ are by construction are positive semidefinite, the above is bounded by

$$\leq \|\gamma_{x_i}^{-2} S_{x_i}\rho S_{x_i}^\dagger - \gamma_{\omega_i}^{-2} S_{\omega_i}\rho S_{\omega_i}^\dagger\|_1. \tag{7.5}$$

We can write $S_{x_i}\rho S_{x_i}^\dagger = U_{x_i}(A_{x_i})^{1/2}\rho(A_{x_i})^{1/2}U_{x_i}^\dagger = \sqrt{\rho}A_{x_i}\sqrt{\rho}$ and $S_{\omega_i}\rho S_{\omega_i}^\dagger = \sqrt{\rho}A_{\omega_i}\sqrt{\rho}$. Next we observe that for any square matrix A, $\|A\|_1 = \|\overline{A}\|_1$, where $\overline{A}$ denotes the entrywise complex conjugate in some basis. By taking the complex conjugate with respect to the basis that diagonalizes ρ, we have that (7.5) is equal to

$$\|\gamma_{x_i}^{-2}\sqrt{\rho}\overline{A_{x_i}}\sqrt{\rho} - \gamma_{\omega_i}^{-2}\sqrt{\rho}\overline{A_{\omega_{-i}}}\sqrt{\rho}\|_1. \tag{7.6}$$

We see that (7.6), averaged over i, ω, a_C and x_i is exactly the quantity bounded in (7.3). Applying Jensen's inequality, we have

$$\begin{aligned}
\delta^{1/4} &\geq \mathop{\mathbb{E}}_{i}\mathop{\mathbb{E}}_{\Omega A_C X_i} \| |\widetilde{\Gamma}_{\omega_{-i},x_i,a_C}\rangle - |\widetilde{\Gamma}_{\omega,a_C}\rangle \| && (7.7) \\
&\geq \mathop{\mathbb{E}}_{i}\mathop{\mathbb{E}}_{\Omega A_C X_i} \| |\widetilde{\Gamma}\rangle\langle\widetilde{\Gamma}|_{\omega_{-i},x_i,a_C} - |\widetilde{\Gamma}\rangle\langle\widetilde{\Gamma}|_{\omega,a_C} \|_1 && (7.8)
\end{aligned}$$

where we write $|\widetilde{\Gamma}\rangle\langle\widetilde{\Gamma}|_{\omega_{-i},x_i,a_C}$ instead of
$|\widetilde{\Gamma}_{\omega_{-i},x_i,a_C}\rangle\langle\widetilde{\Gamma}_{\omega_{-i},x_i,a_C}|$ to save space.

Define the cq-states

$$\Phi^i_{\Omega X_i E_A E_B A_C} = \sum_{\omega, a_C, x_i} \mathsf{P}_{\Omega A_C X_i}(\omega, a_C, x_i)\ |\omega x_i\rangle\langle \omega x_i| \otimes |\widetilde{\Gamma}\rangle\langle\widetilde{\Gamma}|_{\omega_{-i}, x_i, a_C} \otimes |a_C\rangle\langle a_C|$$

and

$$\hat{\Phi}^i_{\Omega X_i E_A E_B A_C} = \sum_{\omega, a_C, x_i} \mathsf{P}_{\Omega A_C X_i}(\omega, a_C, x_i)\ |\omega x_i\rangle\langle \omega x_i| \otimes |\widetilde{\Gamma}\rangle\langle\widetilde{\Gamma}|_{\omega, a_C} \otimes |a_C\rangle\langle a_C|$$

so that the bound in (7.8) is equivalent to

$$\mathop{\mathbb{E}}_{i} \left\| \Phi^i_{\Omega X_i E_A E_B A_C} - \hat{\Phi}^i_{\Omega X_i E_A E_B A_C} \right\|_1 \leq \delta^{1/4} \tag{7.9}$$

We define the quantum operation $\mathcal{E}$ acting on registers ΩE_B as follows: for all ω and density matrices τ,

$$\mathcal{E} : |\omega\rangle\langle\omega| \otimes \tau \mapsto |\omega\rangle\langle\omega| \otimes \sum_{b_C} T_{\omega, b_C} \tau T^\dagger_{\omega, b_C} \otimes |b_C\rangle\langle b_C|.$$

In other words, the quantum operation $\mathcal{E}$ will, controlled on Ω, apply the measurement corresponding to the T_{ω, b_C} operators (defined in Section 7.3.1) to the E_B part of the state, and save the measurement outcomes in an ancilla register.

The operation $\mathcal{E}$ is an isometry, so we have that

$$\mathop{\mathbb{E}}_{i} \left\| \mathcal{E}\left(\Phi^i_{\Omega X_i E_A E_B A_C}\right) - \mathcal{E}\left(\hat{\Phi}^i_{\Omega X_i E_A E_B A_C}\right) \right\|_1 \leq \delta^{1/4}. \tag{7.10}$$

Let us examine what happens when we apply $\mathcal{E}$ to $\Phi^i_{\Omega X_i E_A E_B A_C}$:

$$\begin{aligned}
&\mathcal{E}\left(\Phi^i_{\Omega X_i E_A E_B A_C}\right) \\
&= \mathop{\mathbb{E}}_{\Omega A_C X_i} |\omega x_i\rangle\langle\omega x_i| \otimes \sum_{b_C} T_{\omega, b_C} |\widetilde{\Gamma}_{\omega_{-i}, x_i, a_C}\rangle\langle\widetilde{\Gamma}_{\omega_{-i}, x_i, a_C}| T^\dagger_{\omega, b_C} \otimes |a_C b_C\rangle\langle a_C b_C| \\
&= \mathop{\mathbb{E}}_{\Omega X_i} \sum_{a_C} \mathsf{P}_{A_C|\omega, x_i}(a_C) |\omega x_i\rangle\langle\omega x_i| \otimes \sum_{b_C} \frac{T_{\omega, b_C} |\Gamma_{\omega_{-i}, x_i, a_C}\rangle\langle\Gamma_{\omega_{-i}, x_i, a_C}| T^\dagger_{\omega, b_C}}{\mathsf{P}_{A_C|\omega_{-i}, x_i}(a_C)} \otimes |a_C b_C\rangle\langle a_C b_C| \\
&= \mathop{\mathbb{E}}_{\Omega X_i} |\omega x_i\rangle\langle\omega x_i| \otimes \sum_{a_C, b_C} T_{\omega, b_C} |\Gamma_{\omega_{-i}, x_i, a_C}\rangle\langle\Gamma_{\omega_{-i}, x_i, a_C}| T^\dagger_{\omega, b_C} \otimes |a_C b_C\rangle\langle a_C b_C|
\end{aligned}$$

where in the second equality we used that the normalization of $|\widetilde{\Gamma}\rangle\langle\widetilde{\Gamma}|$ is equal to $\mathsf{P}_{A_C|\omega_{-i}, x_i}(a_C)$, and that $\mathsf{P}_{A_C|\omega, x_i}(a_C) = \mathsf{P}_{A_C|\omega_{-i}, x_i}(a_C)$. Similarly, we have that

$$\mathcal{E}\left(\hat{\Phi}^i_{\Omega X_i E_A E_B A_C}\right) = \mathop{\mathbb{E}}_{\Omega X_i} |\omega x_i\rangle\langle\omega x_i| \otimes \sum_{a_C, b_C} T_{\omega, b_C} |\Gamma_{\omega, a_C}\rangle\langle\Gamma_{\omega, a_C}| T^\dagger_{\omega, b_C} \otimes |a_C b_C\rangle\langle a_C b_C|.$$

Define $\Lambda^i_{\Omega X_i E_A E_B A_C B_C} = \mathcal{E}\left(\Phi^i_{\Omega X_i E_A E_B A_C}\right)$ and $\hat{\Lambda}^i_{\Omega X_i E_A E_B A_C B_C} = \mathcal{E}\left(\hat{\Phi}^i_{\Omega X_i E_A E_B A_C}\right)$. In both these states, the event of W_C is well defined: the registers $X_C Y_C$ (which are part of the dependency-breaking variable Ω) and $A_C B_C$ are classical. Furthermore, we claim that the probability of the event W_C in Λ^i and $\hat{\Lambda}^i$ are equal to the probability of W_C in the actual repeated strategy. Let

$$\Pi = \sum_{\substack{x_C,y_C,a_C,b_C: \\ V(x_C,y_C,a_C,b_C)=1}} |x_C y_C a_C b_C\rangle\langle x_C y_C a_C b_C|$$

be the projector onto the subspace corresponding to the event W_C. Then for all i

$$\begin{aligned}
&\operatorname{Tr}\left(\Pi\Lambda^i\right) \\
&= \sum_{\omega,x_i} \mathsf{P}_{\Omega X_i}(\omega x_i) \sum_{\substack{a_C,b_C: \\ V(x_C,y_C,a_C,b_C)=1}} \langle \Gamma_{\omega_{-i},x_i,a_C} | T^{\dagger}_{\omega,b_C} T_{\omega,b_C} | \Gamma_{\omega_{-i},x_i,a_C}\rangle \\
&= \sum_{\omega,x_i} \mathsf{P}_{\Omega X_i}(\omega x_i) \sum_{\substack{a_C,b_C: \\ V(x_C,y_C,a_C,b_C)=1}} \langle\psi| \left(S_{\omega_{-i},x_i,a_C} \otimes T_{\omega,b_C}\right)^{\dagger} \left(S_{\omega_{-i},x_i,a_C} \otimes T_{\omega,b_C}\right) |\psi\rangle \\
&= \sum_{\omega,x_i} \mathsf{P}_{\Omega X_i}(\omega x_i) \sum_{\substack{a_C,b_C: \\ V(x_C,y_C,a_C,b_C)=1}} \langle\psi| \left(\sqrt{A^{a_C}_{\omega_{-i},x_i}} \otimes \sqrt{B^{b_C}_{\omega}}\right)^{\dagger} \left(\sqrt{A^{a_C}_{\omega_{-i},x_i}} \otimes \sqrt{B^{b_C}_{\omega}}\right) |\psi\rangle.
\end{aligned}$$

Using the definitions of $A^{a_C}_{\omega_{-i},x_i}$ and $B^{b_C}_{\omega}$ we see that this quantity is identical to $\mathsf{P}(W_C)$. Similar reasoning shows that $\operatorname{Tr}\left(\Pi\hat{\Lambda}^i\right) = \mathsf{P}(W_C)$.

Let $\Lambda^i_{\Omega X_i E_A E_B A_C B_C|W_C} = (\Pi\Lambda^i\Pi)/\mathsf{P}(W_C)$ and $\hat{\Lambda}^i_{\Omega X_i E_A E_B A_C B_C|W_C} = (\Pi\hat{\Lambda}^i\Pi)/\mathsf{P}(W_C)$ denote Λ^i and $\hat{\Lambda}^i$ *conditioned* on the event W_C. So we have

$$\mathop{\mathbb{E}}_i \left\| \Lambda^i_{\Omega X_i E_A E_B A_C B_C|W_C} - \hat{\Lambda}^i_{\Omega X_i E_A E_B A_C B_C|W_C} \right\|_1 \leq \frac{\delta^{1/4}}{\mathsf{P}(W_C)}. \tag{7.11}$$

Let us bundle together the Ω and $A_C B_C$ registers into R. For all $r = (\omega, a_C, b_C)$ and x_i, define

$$|\Upsilon_{r,x_i}\rangle = \frac{S_{\omega_{-i},x_i,a_C} \otimes T_{\omega,b_C}|\psi\rangle}{\left\|S_{\omega_{-i},x_i,a_C} \otimes T_{\omega,b_C}|\psi\rangle\right\|} \qquad |\Upsilon_r\rangle = \frac{S_{\omega,a_C} \otimes T_{\omega,b_C}|\psi\rangle}{\left\|S_{\omega,a_C} \otimes T_{\omega,b_C}|\psi\rangle\right\|}$$

Then we see that

$$\Lambda^i_{RX_iE_AE_B|W_C} = \mathop{\mathbb{E}}_{RX_i|W_C} |rx_i\rangle\langle rx_i| \otimes |\Upsilon_{r,x_i}\rangle\langle\Upsilon_{r,x_i}|$$

and

$$\hat{\Lambda}^i_{RX_iE_AE_B|W_C} = \mathop{\mathbb{E}}_{R|W_C} |r\rangle\langle r| \otimes \mathop{\mathbb{E}}_{X_i|\omega} |x_i\rangle\langle x_i| \otimes |\Upsilon_r\rangle\langle\Upsilon_r|.$$

We see that $\Lambda^i_{RX_iE_AE_B|W_C}$ and $\hat{\Lambda}^i_{RX_iE_AE_B|W_C}$ are both cq-states that are classical on RX_i and quantum on E_AE_B. The inequality in (7.11) implies that the trace distance between the classical parts of $\Lambda^i_{W_C}$ and $\hat{\Lambda}^i_{W_C}$ is at most $\delta^{1/4}/\mathsf{P}(W_C)$. Thus we can change the classical part of $\hat{\Lambda}^i_{W_C}$ to match the classical part of $\Lambda^i_{W_C}$ by at most doubling the error:

$$\mathop{\mathbb{E}}_i \left\| \mathop{\mathbb{E}}_{RX_i|W_C} |rx_i\rangle\langle rx_i| \otimes \left(|\Upsilon_{r,x_i}\rangle\langle\Upsilon_{r,x_i}| - |\Upsilon_r\rangle\langle\Upsilon_r|\right) \right\|_1 \leq 2\frac{\delta^{1/4}}{\mathsf{P}(W_C)}.$$

which implies that

$$\mathop{\mathbb{E}}_{i}\mathop{\mathbb{E}}_{RX_i|W_C} \| |\Psi_{r,x_i}\rangle\langle\Psi_{r,x_i}| - |\Psi_r\rangle\langle\Psi_r| \|_1 \leq \frac{2\delta^{1/4}}{\mathsf{P}(W_C)}.$$

By Lemma 89, $\mathbb{E}_i \|\mathsf{P}_{\Omega_i X_i|W_C} - \mathsf{P}_{\Omega_i X_i}\|_1 \leq \sqrt{\delta}$. Applying that to the above, we get

$$\mathop{\mathbb{E}}_{i}\mathop{\mathbb{E}}_{\Omega_i X_i}\left[\mathop{\mathbb{E}}_{R_{-i}|\omega_i,x_i,W_C} \| |\Psi_{r,x_i}\rangle\langle\Psi_{r,x_i}| - |\Psi_r\rangle\langle\Psi_r| \|_1\right] \leq \frac{2\delta^{1/4}}{\mathsf{P}(W_C)} + \sqrt{\delta}$$

where the middle expectation over $\Omega_i X_i$ is over the *prior* distribution (i.e. before conditioning on the event W_C). Now observe that in this prior distribution, Ω_i fixes Y_i with probability $1/2$, so we in fact get

$$\mathop{\mathbb{E}}_{i}\mathop{\mathbb{E}}_{X_i Y_i}\left[\mathop{\mathbb{E}}_{R_{-i}|x_i,y_i,W_C} \| |\Psi_{r_{-i},x_i,y_i}\rangle\langle\Psi_{r_{-i},x_i,y_i}| - |\Psi_{r_{-i},y_i}\rangle\langle\Psi_{r_{-i},y_i}| \|_1\right] \leq \frac{4\delta^{1/4}}{\mathsf{P}(W_C)} + 2\sqrt{\delta}$$

where the states $|\Psi_{r_{-i},x_i,y_i}\rangle$ were defined in Section 7.3.1, and $|\Psi_{r_{-i},y_i}\rangle$ is $|\Psi_r\rangle$ where $r = (r_{-i}, \omega_i)$ and ω_i fixes $Y_i = y_i$. Applying the Fuchs-van der Graaf inequality, we obtain a bound in terms of Euclidean distance:

$$\mathop{\mathbb{E}}_{i}\mathop{\mathbb{E}}_{X_i Y_i}\left[\mathop{\mathbb{E}}_{R_{-i}|x_i,y_i,W_C} \| |\Psi_{r_{-i},x_i,y_i}\rangle - |\Psi_{r_{-i},y_i}\rangle \|\right] \leq O\left((\delta^{1/4}/\mathsf{P}(W_C))^{1/2}\right) \tag{7.12}$$

Similar reasoning implies that

$$\mathop{\mathbb{E}}_{i}\mathop{\mathbb{E}}_{X_i Y_i}\left[\mathop{\mathbb{E}}_{R_{-i}|x_i,y_i,W_C} \| |\Psi_{r_{-i},x_i,y_i}\rangle - |\Psi_{r_{-i},x_i}\rangle \|\right] \leq O\left((\delta^{1/4}/\mathsf{P}(W_C))^{1/2}\right) \tag{7.13}$$

where $|\Psi_{r_{-i},x_i}\rangle$ is $|\Psi_r\rangle$ where $r = (r_{-i}, \omega_i)$ and ω_i fixes $X_i = x_i$. By triangle inequality, we have

$$\mathop{\mathbb{E}}_{i}\mathop{\mathbb{E}}_{X_i Y_i}\left[\mathop{\mathbb{E}}_{R_{-i}|x_i,y_i,W_C} \| |\Psi_{r_{-i},y_i}\rangle - |\Psi_{r_{-i},x_i}\rangle \|\right] \leq O\left((\delta^{1/4}/\mathsf{P}(W_C))^{1/2}\right). \tag{7.14}$$

Let $\eta := O\left((\delta^{1/4}/\mathsf{P}(W_C))^{1/2}\right)$. Fix r_{-i}, x_i, y_i. Since r_{-i} is public, Alice knows r_{-i}, x_i, and thus knows a classical description of the state $|\Phi_{r_{-i},x_i}\rangle$. Similarly, Bob knows a classical description of the state $|\Phi_{r_{-i},y_i}\rangle$. By the Quantum Correlated Sampling Lemma of [39] with parameter $\alpha = \eta$, there exists a dimension d' that depends only on d and α, and unitaries U_{r_{-i},x_i} and V_{r_{-i},y_i} such that

$$\|U_{r_{-i},x_i} \otimes V_{r_{-i},y_i} |E_{dd'}\rangle - |\Psi_{r_{-i},x_i}\rangle |E_{d'}\rangle\| \leq O(\max\{\alpha^{1/12}, \| \, |\Psi_{r_{-i},x_i}\rangle - |\Psi_{r_{-i},y_i}\rangle \, \|^{1/6}\}).$$

We can average this over i, x_i, y_i, and r_{-i} to get that

$$\begin{aligned}&\mathop{\mathbb{E}}_{i}\mathop{\mathbb{E}}_{X_i Y_i}\left[\mathop{\mathbb{E}}_{R_{-i}|x_i,y_i,W_C} \|U_{r_{-i},x_i} \otimes V_{r_{-i},y_i} |E_{dd'}\rangle - |\Psi_{r_{-i},x_i}\rangle |E_{d'}\rangle\|\right] \\ &\leq \mathop{\mathbb{E}}_{i}\mathop{\mathbb{E}}_{X_i Y_i}\left[\mathop{\mathbb{E}}_{R_{-i}|x_i,y_i,W_C} O(\max\{\alpha^{1/12}, \| \, |\Psi_{r_{-i},x_i}\rangle - |\Psi_{r_{-i},y_i}\rangle \, \|^{1/6}\})\right]\end{aligned}$$

$$\begin{aligned} &\leq O(\alpha^{1/12}) \\ &= O(\eta^{1/12}) \end{aligned}$$

where in the second inequality we used the following fact: for a random variable X taking values in $[0,1]$ with mean $\mu = \mathbb{E}\, X$, we can bound the expectation $\mathbb{E} \max\{\sqrt{\mu}, X\} \leq 2\sqrt{\mu}$. Using the bound (7.13), we get

$$\mathop{\mathbb{E}}_{i} \mathop{\mathbb{E}}_{X_i Y_i} \left[\mathop{\mathbb{E}}_{R_{-i}|x_i,y_i,W_C} \| U_{r_{-i},x_i} \otimes V_{r_{-i},y_i} |E_{dd'}\rangle - |\Psi_{r_{-i},x_i,y_i}\rangle |E_{d'}\rangle \| \right] \leq O(\eta^{1/12})$$

as desired.

Chapter 8

Classical and quantum message authentication in the presence of entangled adversaries

The work presented in this chapter was jointly conducted with Sumegha Garg and Mark Zhandry.

8.1 Introduction

Authenticating messages is one of the fundamental operations in classical cryptography. A sender Alice and receiver Bob share a secret key k, and Alice wishes to send a message m over an insecure channel to Bob, ensuring that the message was not tampered with in transit. Alice will affix a "signature" σ to m using the key k and send the message/signature pair (m, σ) to Bob. Bob receives some potentially altered pair (m', σ'), and will then verify that σ' is a valid signature on m'. If verification passes, Bob accepts m', and if verification fails, Bob ignores the message and discards it. The guarantee is that, even if the adversary has arbitrarily tamper with the communication channel, as long as the adversary does not know the secret key k, either Bob rejects, or the message he receives is m. Intuitively, this means the adversary cannot do anything but forward the message as is or send a junk message that is always rejected. We generally require that security holds for *any* m, reflecting the possibility that the adversary may be able to affect the message being sent. Such a (symmetric key) authentication protocol is usually referred to as a Message Authentication Code (MAC). As long as k is only used to authenticate a single message, information-theoretic security can be achieved: no computationally unbounded adversary can modify the message. Put another way, information-theoretic classical one-time MACs exist [101].

Just as authentication is fundamental to classical cryptography, it will continue to be an important tool in the coming age of quantum computers. In this work, we investigate authentication in the quantum setting. Namely, we explore both quantum attacks on *classical* protocols, as well as full-fledged quantum protocols for authenticating quantum data.

Quantum Attacks on Classical Protocols. A recent series of works [17, 34, 18, 19, 106, 63] have studied quantum superposition attacks on classical cryptosystems. In the case of message authentication codes, an adversary in such an attack is able to trick the sender into signing a superposition of messages. That is, the sender computes the map $|m\rangle \mapsto |m, \sigma_m\rangle$ in superposition, where σ_m is the signature on m. The adversary chooses some message superposition $\sum_m \alpha_m |m\rangle$, and the sender then applies the map, giving the adversary $\sum_m \alpha_m |m, \sigma_m\rangle$.

At this point, it is unclear what the security definition should actually be. Clearly, the adversary can tamper with the signed state: he can, for example, measure the entire state in the standard basis, obtaining the pair (m, σ_m) with probability $|\alpha_m|^2$. Then m, σ_m will pass verification, but will be different from the signed state the adversary received. If the adversary can change the message state, what sort of guarantees can we hope for?

Boneh and Zhandry [18] give the first definition of security for classical authentication against superposition attacks. They argue that, at a minimum, the adversary given a single signed superposition should only be able to produce a single signed message; he should not be able to produce both valid signed messages m, σ_m and $m', \sigma_{m'}$ for $m \neq m'$. In the classical setting, this requirement is equivalent to the traditional MAC security definition: an adversary who intercepts the signed message (m, σ), and is able to maul the message into (m', σ'), can also produce two signed messages: namely the original senders message (m, σ) and the mauled message (m', σ').

However, the Boneh-Zhandry definition has some unsatisfying properties. For example, consider the case where the sender only signs messages that start with the email address of some intended recipient, say, `bob@gmail.com`. Suppose the adversary tricks the sender into a signing a superposition of messages that all begin with `bob@gmail.com`, but then manipulates the signed superposition into a different superposition that includes valid signed messages that *do not* start with `bob@gmail.com`. Clearly, this is an undesirable outcome. Unfortunately, the Boneh-Zhandry definition does not rule out such attacks — it only rules out the possibility of an adversary producing $q + 1$ valid signed messages when given q signed superpositions. The situation illustrated here, however, is that the adversary is given *one* signed superposition, and now wants to produce *one* valid signed message that was not part of the original superposition.

Along similar lines, suppose an adversary tricks the sender into signing a uniform superposition on messages, and then produces a classical signed message (m, σ). From the sender's perspective, each message has weight $\frac{1}{|\mathcal{M}|}$, where $\mathcal{M}$ is the message space. The sender cannot prevent the adversary from measuring the message state to produce (m, σ) for a random m. However, it would be reasonable to expect that the adversary cannot bias the output of this measurement to obtain, say, (m^*, σ_{m^*}) with probability much higher than $\frac{1}{|\mathcal{M}|}$. Again, Boneh and Zhandry's definition does not preclude such a biasing, since the adversary only ever obtains a single signed message. Thus, the Boneh-Zhandry definition does not capture natural non-malleability properties one would hope for from an authentication scheme.

Boneh and Zhandry's definitions suffers from these weaknesses because it only considers what types of outputs the adversary can produce, ignoring the relationships between the output and the original signed state. In the classical setting, the two approaches are actually equivalent, but in the quantum setting this is not the case.

Quantum Authentication of Quantum Data. Barnum et al. [9] investigate the possibility of authenticating quantum data using a quantum protocol. They present a definition of non-interacting quantum authentication where, conditioned on the protocol succeeding, the sender has effectively teleported a quantum state to the receiver (provided that the probability of success is not too small). They then give a scheme which attains this definition. Interestingly, they show that quantum state authentication also implies quantum state *encryption*. Roughly, they argue that authentication in one basis (say, the computational or Fourier basis) implies encryption in the complementary basis. Their definition corresponds to authentication in all bases, which gives encryption in all bases.

However, their general definition of quantum authentication has some shortcomings: first, it does not explicitly handle the case of when the adversary has some quantum side information about the message. Second, the security definition averages over the secret key shared between the sender and receiver. Suppose Alice sends Bob the authenticated state $\mathsf{Auth}_k(\rho)$ using key k. Bob receives a (possibly tampered) state σ_k, and proceeds to verify the authentication. Let τ_k denote the Bob's state *conditioned* on successful verification. Roughly speaking, the definition given by Barnum, et al. state that the *average* state $\mathbb{E}_k\, \tau_k$ is close to the original state ρ. However, this does not immediately imply that τ_k is close to the original state ρ *with high probability*, which is a much more useful condition. When there is no quantum side information, their definition does in fact imply a "with high probability" statement, but this implication no longer seems to hold when the adversary can manipulate the side information.

The work of Hayden, Leung, and Mayers [53] later showed that the protocol given by [9] actually has *universal composable security*, which implies that it remains secure in the presence of side information. However, no general definition for authentication with quantum side information was given.

Furthermore, [53] show that the secret key used in the Barnum, et al. protocol can be partially *re-used* in further applications without compromising their security. When authenticating classical information, the key can even be re-used in its entirety [35]; as long as verification never fails, an unbounded number of messages can be authenticated. This is quite surprising, since in the classical setting such re-usability cannot be obtained without computational assumptions.

Again, unfortunately, the key re-usability property does not follow from the general security definition alone, but follows from an analysis of the particular [9] protocol. Moreover, it has been an open question of whether there is a quantum authentication scheme to allow for full re-usability of the key upon successful verification.

8.1.1 This Work

In this work, we address the above limitations by giving new security notions for authentication in the quantum setting. More generally, we present an abstract framework of security for both classical and quantum authentication schemes that not only captures existing security definitions (such as the Boneh-Zhandry definition for classical protocols or the Barnum, et al. definition of quantum state authentication), but also is more powerful in that it strongly *characterizes* the (effective) behavior of an adversary. In particular, the adversary may have access to quantum side information with the message state that is being authenticated. The characterization of the adversary's admissable actions is what allows us to easily deduce many desirable security properties (such as unforgeability, key reuse, and more). Furthermore, we will show that various natural authentication protocols satisfy our security definitions.

Our abstract security framework is inspired by the simulation paradigm in classical cryptography. In our framework, one first defines a class $\mathscr{A}$ of *ideal adversaries*. Intuitively, ideal adversaries are those that cannot be avoided in a real execution of an authentication protocol, such as those that discard messages, or ones that carry out actions explicitly allowed by the protocol. For example, in the case of classical protocols, one can define the class of ideal adversaries to be ones that "behave classically" on the message state – that is, they're restricted to measurements in the computational basis. In the case of quantum authentication, an ideal adversary can *only* act on the side information, but otherwise acts as the identity on the authenticated message.

An authentication protocol P satisfies our security definition with respect to the class $\mathscr{A}$ if for any adversary (not necessarily ideal), its behavior in the protocol P can be approximately simulated by an ideal adversary in $\mathscr{A}$. We take the most general notion of simulation possible: the joint state of the secret key, the message state after the receiver's verification procedure (after an arbitrary adversary's action), and the quantum side information held by the adversary must be (up to some error) indistinguishable from the joint state arising from the actions of *some* ideal adversary from the class $\mathscr{A}$.

We now discuss how security for both classical authentication schemes and fully quantum authentication protocols can be defined in this framework.

A new security definition for classical authentication. The Boneh-Zhandry definition focuses on what classical signed messages an adversary can produce, treating the superposition access to the sender as a tool to mount stronger attacks. Here, we instead think of a classical protocol giving rise to a weak form of authentication of quantum messages, where a superposition is authenticated by classically signing each message in the superposition. That is, a state $\sum_m \alpha_m |m\rangle$ is authenticated as the state $\sum_m \alpha_m |m, \sigma_m\rangle$. The state is similarly verified in superposition by running the classical verification algorithm in superposition, and measuring the result of the computation.

More generally, we think of the protocol acting on messages states that may be entangled with an adversary. For example, the sender could sign the $\mathcal{M}$ part of the state $\sum_m \alpha_m |m\rangle^{\mathcal{M}} \otimes |\varphi_m\rangle^{\mathcal{Z}}$, where the adversary has control of the quantum side information $|\varphi_m\rangle^{\mathcal{Z}}$ states. The signed state then would become $\sum_m \alpha_m |m, \sigma_m\rangle^{\mathcal{MT}} \otimes |\varphi_m\rangle^{\mathcal{Z}}$. Signing mixed states can also be expressed in this way, simply by purifying the mixture. By thinking of the protocol in this way, we are able to give security definitions that actually consider the relationship between the sender's signed state and the final state the adversary produces.

Clearly, such a classical scheme cannot fully protect the quantum state. An adversary could, for example measure m, σ_m, or any subset of bits of the state, and keep the result of such a measurement in his own private space. Also, the adversary can choose to replace the signed state with junk if the outcome of some measurement is 1, and forward the signed state if the outcome of a measurement is 0. None of these actions would be detected by the classical verification procedure.

Our security definition for classical protocols says that, roughly, an arbitrary adversary can be simulated by an ideal adversary that can only do the following: perform some measurement in the computational basis (perhaps perturbing his own private qubits based on the result of the measurement), and then perhaps conditionally replacing the state with junk. We also extend the definition to handle side information the adversary may have about the message state; for example, the adversary may possess the purification of the message state. Thus, our definition is essentially the best one could hope for, since is disallows the adversary from doing anything other than operations that are trivially possible on *any* classical protocol.

Our definition readily implies the Boneh-Zhandry security definition for one-time MACs, and does not suffer from the weakness of their definition[1]. Finally, we show that the classical Carter-Wegman MAC that uses three-universal hashing is sufficient for achieving this strong security definition.

Definitions for Quantum Authentication. We next turn to quantum protocols for authenticating quantum messages. For general quantum protocols, the adversary can always do the following. He can always act non-trivially on his own private workspace – the verification procedure can never detect this. Otherwise, he can forward the authenticated state as is, without recording any information about the state, or he can send junk to the receiver. Our strongest definition of security – which we call *total authentication* – says that this is essentially all an adversary can do in a secure quantum authentication protocol. In other words, a real adversary in a total authentication protocol can be approximated by an ideal adversary that behaves trivially on the authenticated state.

Our definition strengthens Barnum et al.'s definition, and due to the fact that we consider side information about the plaintext state, we obtain security guarantees that are similar to the universally composable variant of their definition [53]. However, our definition is actually strictly stronger, due to the fact that we consider the receiver's view to include the authentication key as well as whatever information the adversary may learn about the key. The ideal adversary must approximate the real adversary, even considering the entire key. In contrast, existing definitions trace out the key — either partially or entirely — and therefore do not directly consider *arbitrary* information the adversary may learn about the key. Our security definition of total authentication thus rules out the possibility of the adversary learning anything about the key (because the ideal adversary does not interact with the authenticated state at all).

This fact has interesting consequences. For example, our definition immediately implies that, upon successful verification by the receiver, the key can actually be completely recycled to authenticate a new message. This is because, upon successful verification, the key is completely hidden from the adversary and can therefore be used again in the same protocol. We note that key recycling from quantum authentication was studied before by [53], but they were only able to demonstrate that *part* of the key in the Barnum, et al. protocol is reusable. Furthermore, no prior definition for authentication of quantum data directly implies key re-usability, and no prior protocol for quantum messages gets full key re-usability upon successful verification.

Our definition also gives a conceptually simple QKD protocol. Alice prepares a maximally entangled state, chooses a random key k, and authenticates half the state with the key. She then sends the authenticated half to Bob, keeping the unauthenticated half to herself. When Bob receives the state, he sends a "received" message back to Alice, who then sends the key k to Bob. Bob verifies the state using the key. Even though the adversary eventually sees the authentication key k, he does not know the key when he intercepts the quantum state, and must therefore interact with the state without the key. If Bob's verification passes, it implies, roughly, that the adversary could not have tampered with the state (by the security of total authentication); in particular, the adversary could not have learned

[1] One limitation of our definition is that we consider the signature registers as being initialized by the signer. Boneh and Zhandry, in contrast, allow the registers to be initialized by the adversary, with the signature being XORed into the registers

any information about the maximally entangled state. Therefore, Alice and Bob measure their halves of the maximally entangled state and obtain a shared key that is unknown to the eavesdropper. If Bob's verification rejects, the two try again. Though this is not a practical QKD scheme (because any tampering by the adversary would cause Alice and Bob to abort), it is conceptually very simple and illustrates the power of our definitions.

Next, we exhibit a protocol meeting our strong security notion. We present an authentication scheme based on *unitary designs*, which are efficiently sampleable distributions over unitary matrices that behave much like the uniform distribution over unitaries when only considering low degree moments. The protocol is simple: to authenticate a quantum state ρ, first the state ρ is padded with some number zero qubits, so that the state looks like $\rho \otimes |0\rangle\langle 0|^{\otimes s}$. Then, using the secret key k the sender selects a random unitary U_k from an appropriate unitary design. The state $U_k \rho \otimes |0\rangle\langle 0|^{\otimes s} U_k^\dagger$ is then sent across the quantum channel. To verify, the receiver applies the inverse unitary $U_k^\dagger$ and checks that the last s qubits are all 0. Recall that in the classical setting, padding a message before applying a non-malleable encryption gives authenticated encryption. Thus, our construction of authentication from unitary designs generalizes this idea to the quantum setting.

This scheme is very similar to the *non-malleable quantum encryption* scheme based on unitary 2-designs that was proposed by Ambainis, Bouda, and Winter [5]. However, their scheme does not provide any authentication, and does not consider quantum side information.

Finally, we also give a definition of *total authentication with key leakage*. This is a notion of security where the real adversary can be simulated by an ideal trivial adversary that only acts on its own private workspace, *but in a manner that may depend on the key*. This is slightly weaker notion of security than total authentication, but it still implies simple QKD and some amount of key reuse. We note that the work of [53] essentially show that the Barnum et al. protocol satisfies total authentication with (minor) key leakage.

We give a simple authentication scheme that achieves this: first, one classically authenticates, performs the quantum Fourier transform, and classically authenticates again using a fresh key. We call this the "Auth-QFT-Auth" protocol, and show that it achieves total authentication where the key used in the second authentication may leak. In exchange we obtain secrecy for the quantum message as well as the key from the first authentication. This illustrates the surprising versatility of classical authentication schemes: combined with one quantum step (the Fourier transform), it can give full quantum authentication. This also gives a conceptually simple alternative to the protocol of [9].

8.2 Preliminaries

We will use caligraphic letters to denote Hilbert spaces, such as $\mathcal{H}$, $\mathcal{M}$, $\mathcal{T}$, $\mathcal{K}$, and so on. We write $\mathrm{S}(\mathcal{H})$ to denote the set of unit vectors in $\mathcal{H}$. For two Hilbert spaces $\mathcal{H}$ and $\mathcal{M}$, we write $\mathrm{L}(\mathcal{H}, \mathcal{M})$ to denote the set of matrices that map $\mathcal{H}$ to $\mathcal{M}$. We abbreviate $\mathrm{L}(\mathcal{H}, \mathcal{H})$ as simply $\mathrm{L}(\mathcal{H})$. The following are important subsets of $L(\mathcal{H})$ that we'll use throughout this chapter.

- $\mathrm{D}(\mathcal{H})$ denotes the set of *density matrices* on $\mathcal{H}$; that is, positive semidefinite operators on $\mathcal{H}$ with unit trace.

- $\mathrm{D}_{\leq}(\mathcal{H})$ denotes the set of *subnormalized* density matrices on $\mathcal{H}$; that is, positive semidefinite operators on $\mathcal{H}$ with trace at most one.

- $\mathrm{U}(\mathcal{H})$ denotes the set of unitary matrices acting on $\mathcal{H}$. For an integer N, we will also write $\mathrm{U}(N)$ to denote the set of all $N \times N$ complex unitary matrices.

Another important class of operators are *isometries*: these are like unitaries, except that can append ancilla qubits. We say that a map $V \in \mathrm{L}(\mathcal{H}, \mathcal{M})$ is an isometry if for all vectors $|\psi\rangle \in \mathcal{H}$, $\|V|\psi\rangle\| = \||\psi\rangle\|$. Note that this requires $\dim(\mathcal{M}) \geq \dim(\mathcal{H})$. We will let $\mathrm{J}(\mathcal{H}, \mathcal{M})$ denote the set of isometries in $\mathrm{L}(\mathcal{H}, \mathcal{M})$.

For a Hilbert space $\mathcal{H}$, we let $|\mathcal{H}|$ denote the dimension of $\mathcal{H}$.

We will typically decorate states and unitaries with subscripts to denote which spaces they act on. For example, let $\mathcal{Y}$ and $\mathcal{Z}$ be two Hilbert spaces. Let $U \in \mathrm{U}(\mathcal{Y})$ and let $V \in \mathrm{U}(\mathcal{Y} \otimes \mathcal{Z})$. Then when we write the product $U^{\mathcal{Y}} V^{\mathcal{Y}\mathcal{Z}}$ we mean the $(U^{\mathcal{Y}} \otimes \mathbb{I}^{\mathcal{Z}}) V^{\mathcal{Y}\mathcal{Z}}$; we will often omit mention of the identity unitary when it is clear from context.

Superoperators. In this paper we will consider *superoperators*, which are linear maps that act on a vector space of linear maps. For Hilbert spaces $\mathcal{H}$ and $\mathcal{M}$, let $\mathrm{T}(\mathcal{H}, \mathcal{M})$ denote the set of all linear maps that take elements of $\mathrm{L}(\mathcal{H})$ to $\mathrm{L}(\mathcal{M})$. While superoperators can be very general, we will focus on superoperators $\mathcal{O} \in \mathrm{T}(\mathcal{H}, \mathcal{M})$ that are *completely positive* and *trace non-increasing*, which have the following characterization: there exists an alphabet Σ and set of matrices (not necessarily Hermitian) $\{A_a\}_{a \in \Sigma} \subset \mathrm{L}(\mathcal{H}, \mathcal{M})$ such that

1. $\mathcal{O}(X) = \sum_{a \in \Sigma} A_a X A_a^\dagger$ for all $X \in \mathrm{L}(\mathcal{H})$, and
2. $\sum_{a \in \Sigma} A_a^\dagger A_a \preceq \mathbb{I}^{\mathcal{H}}$.

For the rest of this paper, when we speak of superoperators, we will always mean completely positive, trace non-increasing superoperators. Although the definition of superoperators is rather abstract, they capture general quantum operations on arbitrary quantum states, including post-selection, as demonstrated by Stinespring's dilation theorem:

Theorem 92 (Stinespring's dilation theorem). *A map $\mathcal{O} \in \mathrm{T}(\mathcal{H}, \mathcal{M})$ is a completely positive, trace non-increasing superoperator if and only if there exists auxiliary Hilbert spaces $\mathcal{Z}, \mathcal{Z}'$, an isometry $V \in \mathrm{J}(\mathcal{H} \otimes \mathcal{Z}, \mathcal{M} \otimes \mathcal{Z}')$, and a projector Π acting on $\mathcal{M} \otimes \mathcal{Z}'$ such that for all density matrices $\rho \in \mathrm{D}(\mathcal{H})$, we have*

$$\mathcal{O}(\rho) = \mathrm{Tr}_{\mathcal{Z}'}(\Pi V \rho V^\dagger \Pi).$$

8.3 Definitions

Spaces. We let $\mathcal{K}$ denote the **key space**, $\mathcal{M}$ denote the **message space**, and $\mathcal{Y}$ denote the **authenticated space**.

Authentication scheme. An δ-authentication scheme is a pair of keyed superoperators Auth, Ver where

- Auth_k for $k \in \mathcal{K}$ is a superoperator mapping $\mathrm{D}(\mathcal{M})$ to $\mathrm{D}(\mathcal{Y})$.
- Ver_k for $k \in \mathcal{K}$ is a superoperator mapping $\mathrm{D}(\mathcal{Y})$ to $\mathrm{D}(\mathcal{M})$.

satisfying the (approximate) correctness requirements that for any (potentially mixed) quantum state $\rho \in \mathrm{D}(\mathcal{M})$,

$$\left\| \left(\mathop{\mathbb{E}}_{k} |k\rangle\langle k| \otimes \mathsf{Ver}_k(\mathsf{Auth}_k(\rho)) \right) - \mathop{\mathbb{E}}_{k} |k\rangle\langle k| \otimes \rho \right\|_1 < \delta \tag{8.1}$$

where $\| \cdot \|_1$ denotes the trace norm.

This definition of authentication scheme is more general than we need in this paper. Throughout this work, we shall exclusively work with exact authentication schemes; that is, authentication schemes where $\mathsf{Ver}_k(\mathsf{Auth}_k(\rho)) = \rho$ for all k. Furthermore, we will assume that Auth_k behaves as an isometry taking $\mathcal{M}$ to $\mathcal{Y}$ (i.e. it isn't probabilistic).

We will treat Ver_k as a filter that only accepts states that were properly authenticated. More formally, we view $\mathsf{Ver}_k(\tau)$ as first projecting the input state τ onto the subspace of $\mathcal{Y}$ that is the image of $\mathcal{M}$ under Auth_k. Then, it applies the inverse isometry Auth_k on this projection ("undoes the authentication"). Thus $\mathsf{Ver}_k(\cdot)$ is not a trace-preserving quantum operation.

Note that normally, the verification or decoding procedure of an authentication scheme (e.g., as defined in [9]) is a trace preserving operation that additionally generates an additional bit b indicating whether verification accepted or rejected. Then the correctness requirement above would additionally require that $b = 1$ with probability (negligibly close to) 1, for inputs obtained by running Auth_k on some state. However, we note that this is equivalent to the formulation above. Indeed, starting from a verification operator Ver'_k that additionally outputs b, we obtain an operator Ver_k that projects onto $b = 1$, and then discards b. If $b = 0$ with non-negligible probability, then the trace of the result would be smaller than that of ρ. Hence, the result could not be close in trace distance. Therefore, a small trace distance implies that $b = 1$ with overwhelming probability. This view of the verification procedure Ver_k as a filter will be more useful in our paper.

We will also use Auth and Ver to denote the operators

$$\mathsf{Auth}(\cdot) = \sum_k |k\rangle\langle k| \otimes \mathsf{Auth}_k(\cdot) \qquad \mathsf{Ver}(\cdot) = \sum_k |k\rangle\langle k| \otimes \mathsf{Ver}_k(\cdot).$$

Classical Authentication. In a classical authentication protocol, the authentication operator Auth_k is specified by a classical function $\mathsf{Auth}_k : \mathcal{M} \mapsto \mathcal{Y}$ acting on the computational basis, run in superposition on the input state. The verification operator behaves the same as described above: Ver_k projects onto the subspace of $\mathcal{Y}$ spanned by classical strings $\mathsf{Auth}_k(m)$ for all $m \in \mathcal{M}$, and then applies the inverse map Auth_k^{-1}.

Oftentimes we will want to project onto the space of valid authenticated messages, without undo-ing the authentication. We use the operator Check to denote this:

$$\mathsf{Check}_k = \sum_m |\mathsf{Auth}_k(m)\rangle\langle \mathsf{Auth}_k(m)|$$

We will also let $\mathsf{Check}(\cdot) = \sum_k |k\rangle\langle k| \otimes \mathsf{Check}_k(\cdot)$.

Message authentication codes. A message authentication code (or MAC) is special type of classical authentication scheme $(\mathsf{Auth}, \mathsf{Ver})$ where for a message m, $\mathsf{Auth}_k(m) = (m, \sigma(k, m))$, where we call $\sigma(k, m)$ the *message tag*. We treat Ver_k as an operator that projects out messages that do not have valid tags, and for messages with valid tags, Ver_k will strip the tags away:

$$\mathsf{Ver}_k = \sum_m |m\rangle\langle m, \sigma(k,m)|.$$

In the case of a MAC, the check operator looks like:

$$\mathsf{Check}_k = \sum_m |m, \sigma(k,m)\rangle\langle m, \sigma(k,m)|.$$

Adversaries. The way we model adversaries is the most general – and the most conservative – way possible: the adversary prepares the initial message state $|\rho\rangle^{\mathcal{MZ}}$, where we can assume that the adversary possesses the purification of $\rho^{\mathcal{M}}$. After the state is authenticated with a secret key k, the adversary gets to attack the $\mathcal{YZ}$ spaces with an arbitrary completely positive trace non-increasing superoperator $\mathcal{O}$. After this attack, the state is un-authenticated with the same key k.

We don't require the superoperator $\mathcal{O}$ to be trace preserving; this is to allow adversaries to *discard* certain measurement outcomes (or, alternatively, *post-select* on measurement outcomes, without renormalizing). While this may seem to give the adversary far too much power, in our security definitions we take into account the probability of the event that the adversary post-selects on. If this probability is too small, the security guarantees are meaningless, which is necessary. Allowing for superoperators to be trace non-preserving will help make our definitions clean to state.

8.4 Security Framework for Quantum Authentication

We now give a framework of security definition for authentication protocols in the quantum setting, involving adversaries that may possess side information that is entangled with the messages. Our security definitions generalizes some of the known classical and quantum authentication definitions.

We present our security definitions using the real/ideal paradigm. Let $(\mathsf{Auth}, \mathsf{Ver})$ be an authentication protocol, with key space $\mathcal{K}$, message space $\mathcal{M}$, and authenticated space $\mathcal{Y}$. Let $\mathcal{Z}$ denote the space of auxiliary side information.

Definition 93. *Let* $(\mathsf{Auth}, \mathsf{Ver})$ *be an authentication scheme. Let* $\mathscr{A} \subseteq \mathrm{T}(\mathcal{YZ}, \mathcal{YZ})$ *denote a set of ideal adversaries. The scheme* $(\mathsf{Auth}, \mathsf{Ver})$ *is* ε-reduces to $\mathscr{A}$-adversaries *iff the following holds: for all initial message states* $|\rho\rangle^{\mathcal{MZ}}$*, for all adversaries* $\mathcal{O} \in \mathrm{T}(\mathcal{YZ}, \mathcal{YZ})$*, there exists an ideal adversary* $\mathcal{I} \in \mathscr{A}$ *such that the following (not necessarily normalized) states are* ε*-close in trace distance:*

- *(Real experiment)* $\mathbb{E}_k\, |k\rangle\langle k| \otimes \left[(\mathsf{Ver}_k \otimes \mathbb{I}^{\mathcal{Z}}) \circ \mathcal{O} \circ (\mathsf{Auth}_k \otimes \mathbb{I}^{\mathcal{Z}})\right] (\rho^{\mathcal{MZ}})$
- *(Ideal experiment)* $\mathbb{E}_k\, |k\rangle\langle k| \otimes \left[(\mathsf{Ver}_k \otimes \mathbb{I}^{\mathcal{Z}}) \circ \mathcal{I} \circ (\mathsf{Auth}_k \otimes \mathbb{I}^{\mathcal{Z}})\right] (\rho^{\mathcal{MZ}})$

Intuitively, our security definition states that for an authentication scheme $(\mathsf{Auth}, \mathsf{Ver})$ that is $\mathscr{A}$-secure, for all initial message states $\rho^{\mathcal{MZ}}$, an *arbitrary* adversary that acts on an authenticated state $\mathsf{Auth}_k(\rho^{\mathcal{MZ}})$ is *reduced* to an "ideal adversary" in $\mathscr{A}$; behaving differently will cause the verification procedure to abort. In other words, "all the adversary can do" is behave like some adversary in the class $\mathscr{A}$.

A comment about normalization. It is important that the states of the real experiment and ideal experiment are not requiried to have unit trace. This is because their trace corresponds to the probability that the verification procedure accepts. If the probability of acceptance is smaller than ε, then the security guarantee is vacuous. Intuitively, this corresponds to situations such as the adversary successfully guessing the secret key k, so we cannot expect any security guarantee in that setting. However, if the probability of acceptance is significantly larger than ε, then we can condition on acceptance, and still obtain a meaningful security guarantee: the distance between the (renormalized) real experiment and ideal experiments is small.

We now specialize the above definition to some important classes of ideal adversaries that we will consider in this paper. Note that for two classes of ideal adversaries $\mathscr{A}$ and $\mathscr{A}'$, if $\mathscr{A} \subset \mathscr{A}'$, then an authentication scheme reducing to $\mathscr{A}$-adversaries implies reducing to $\mathscr{A}'$-adversaries. Hence reducing to $\mathscr{A}$-adversaries is a stronger security guarantee.

8.4.1 Basis-dependent authentication

We first define a notion of security of authentication schemes that reduce to a *basis-respecting* adversary.

Definition 94 (Basis-respecting adversaries). *Let $\mathcal{B} = \{|\psi\rangle\}$ denote an orthonormal basis for $\mathcal{Y}$. Then an adversary $\mathcal{I} \in \mathrm{T}(\mathcal{YZ}, \mathcal{YZ})$ is $\mathcal{B}$-*respecting *iff it can be written as*

$$\mathcal{I}(\sigma) = \mathrm{Tr}_{\mathcal{Z}'}(\Pi V \sigma V^{\dagger} \Pi)$$

for all $\sigma \in \mathrm{D}(\mathcal{YZ})$, where Π is a projector acting on $\mathcal{ZZ}'$, and $V \in \mathrm{J}(\mathcal{YZ}, \mathcal{YZZ}')$ is an isometry that can be written as

$$V = \sum_{\psi \in \mathcal{B}} |\psi\rangle\langle\psi|^{\mathcal{Y}} \otimes V_{\psi}$$

where for each ψ, $V_{\psi} \in \mathrm{J}(\mathcal{Z}, \mathcal{ZZ}')$ is some isometry.

Without the second condition on V, by Stinespring's Dilation Theorem every superoperator can be written as $\mathcal{I}(\sigma) = \mathrm{Tr}_{\mathcal{Z}'}(\Pi V \sigma V^{\dagger} \Pi)$ for some choice of isometry V and projector Π. However, the second condition forces V to respect the basis $\mathcal{B}$. Intuitively, a basis-respecting adversary first measures the $\mathcal{Y}$ register in the $\mathcal{B}$ basis, and based on the measurement outcome, performs some further isometry on the side information in $\mathcal{Z}$. When $\mathcal{B}$ is simply the computational basis, then the adversary treats the $\mathcal{Y}$ register as classical.

Definition 95 (Security relative to a basis). *Let $\mathcal{B}$ be a basis for $\mathcal{Y}$. An authentication scheme* (Auth, Ver) *ε-*authenticates relative to basis *$\mathcal{B}$ iff it it ε-reduces to the class of $\mathcal{B}$-respecting adversaries.*

Intuitively, our new definition captures the "best possible" security definition for *classical* authentication protocols. With a classical protocol, the adversary can perform arbitrary measurements on the authenticated space without detection by the verification algorithm. Because measurements are now undetectable, the adversary can also perform σ-dependent operations to the auxiliary registers, where σ is the classical authenticated message observed in the authenticated registers. For example, he can copy σ into the auxiliary space.

He can also now choose to abort or not depending on σ. However, he should not be able to turn σ into $\sigma' \neq \sigma$.

In Section 8.5, we establish two properties that follow from our basis-dependent security definition. First, we show that from the point of view of an adversary, the state which was authenticated in superposition is indistinguishable from having been measured in the basis $\mathcal{B}$. Showing this uses our definition crucially: we reduce all potential distinguishers into adversaries that must behave in a basis-respecting manner, but then such an adversary cannot tell whether the state was measured or not.

Next, we show that our definition implies unforgeability: the adversary cannot produce two valid signed messages with non-negligible probability, when given access to only one superposition. Thus, our definition subsumes the Boneh-Zhandry security definition for one-time MACs.

In Section 8.7 we show that the classical Carter-Wegman MAC where the message m is appended with $h(m)$, where $h(\cdot)$ is drawn from a three-wise independent hash family, is a scheme that authenticates relative to the computational basis.

Theorem 96. *The Carter-Wegman MAC with three-universal hashing is $O(\sqrt{|\mathcal{M}|/|\mathcal{T}|})$-authenticating relative to the computational basis, where $\mathcal{T}$ is the range of the hash family.*

8.4.2 Total authentication

Here, we will define the strongest possible notion of secure quantum authentication.

Definition 97 (Oblivious adversary). *An adversary $\mathcal{I} \in \mathrm{T}(\mathcal{YZ}, \mathcal{YZ})$ is* oblivious *iff there exists a superoperator $\mathcal{O} \in \mathrm{T}(\mathcal{Z}, \mathcal{Z})$ such that*

$$\mathcal{I}(\sigma) = (\mathbb{I}^{\mathcal{Y}} \otimes \mathcal{O})(\sigma)$$

for all $\sigma \in \mathrm{D}(\mathcal{YZ})$.

In other words, an oblivious adversary does not act at all on the authenticated message, and only acts on the auxiliary side information that it possesses about the state.

Definition 98 (Total authentication). *An authentication scheme* (Auth, Ver) ε-totally authenticates *iff it ε-reduces to the class of oblivious adversaries.*

This is a generalization of the Barnum et al. definition to handle arbitrary auxiliary information about the input state. This is the strongest possible notion of security: for any authentication scheme, an adversary can always mount the following trivial attacks. First, he can arbitrarily modify the unauthenticated auxiliary state. Note that he cannot necessarily modify the contents of the auxiliary state based on the authenticated state, since this amounts to some measurement on the authenticated state, which verification may detect. Second, he can choose to either forward the authenticated state as is, or abort and forward nothing (equivalently, forward a junk state that is guaranteed to reject upon verification). Moreover, he can choose whether to abort or forward based on the contents of the auxiliary registers, and can even abort/forward in superposition. However, in an authentication scheme that totally authenticates the adversary can *only* behave in such trivial ways.

In Section 8.6 we establish a few properties of this definition. The first is that a totally authenticating scheme yields encryption of the quantum state. Barnum, et al. showed that quantum state authentication implies quantum state encryption [9]. However, they did not take into account quantum side information. We show that our definition very easily implies encryption even when the adversary may be entangled with the message state.

Then, we show how our notion of total authentication gives rise to a conceptually simple version of quantum key distribution (QKD). [53] have already observed that the universal composability of the Barnum et al. protocol implies that it can be used to perform QKD as well. Thus while our application of quantum authentication to QKD is not novel, we use this as another opportunity to showcase the strength of our definition. We also show how our definition easily implies full key reuse.

In Section 8.9 we present a scheme achieves total authentication, and hence is the strongest possible authentication scheme in the quantum setting. To our knowledge, this is the first authentication scheme that achieves this level of security. As described in the introduction, this is based on applying an (approximate) unitary design on the input state padded with some number s of $|0\rangle$ qubits.

Theorem 99. *The unitary design scheme is $2^{-s/2}$-totally authenticating, where s is the number of extra $|0\rangle$ qubits.*

As a consequence, this yields an authentication scheme where the key can be recycled fully, conditioned on successful verification by the receiver. In contrast, the protocol of Barnum et al. is not known to possess this property; [53] showed that most of the key can be securely recycled.

8.4.3 Total authentication with key leakage

Finally, we introduce a slight weakening of the definition of total authentication above: we consider schemes that achieve total authentication of quantum data, but incur some *key leakage*. We model this in the following way: let $K = |\mathcal{K}|$ (the size of the keyspace), and let $K' \leq K$. Define a *key leakage function* $\ell : \mathcal{K} \mapsto \{0,1\}^{\log K'}$. If K' is strictly less than K, then $\ell(k)$ must necessarily lose information about the key $k \in \mathcal{K}$, but it will leak some information about it.

In a total authentication scheme with key leakage, an arbitrary adversary is reduced to an oblivious adversary (i.e., is forced to only act on the side information), but the manner in which it acts on the side information *may depend on* $\ell(k)$.

Definition 100 (Authentication with key leakage). *Let* $(\mathsf{Auth}, \mathsf{Ver})$ *be an authentication scheme. Let $K' \leq |\mathcal{K}|$ and let $\ell : \mathcal{K} \to \{0,1\}^{\log K'}$ be a key leakage function. Let $\mathscr{A} \subseteq \mathrm{T}(\mathcal{YZ}, \mathcal{YZ})$ denote a set of ideal adversaries. The scheme* $(\mathsf{Auth}, \mathsf{Ver})$ ε-reduces to $\mathscr{A}$-adversaries with key leakage ℓ *iff the following holds: for all initial message states $|\rho\rangle^{\mathcal{MZ}}$, for all adversaries $\mathcal{O} \in \mathrm{T}(\mathcal{YZ}, \mathcal{YZ})$, there exists a collection of ideal adversaries $\{\mathcal{I}_h\} \subset \mathscr{A}$, indexed by $h \in \{0,1\}^{\log K'}$, such that the following (not necessarily normalized) states are ε-close in trace distance:*

- *(Real experiment)* $\mathbb{E}_k \, |k\rangle\langle k| \otimes \left[(\mathsf{Ver}_k \otimes \mathbb{I}^{\mathcal{Z}}) \circ \mathcal{O} \circ (\mathsf{Auth}_k \otimes \mathbb{I}^{\mathcal{Z}})\right] (\rho^{\mathcal{MZ}})$
- *(Ideal experiment)* $\mathbb{E}_k \, |k\rangle\langle k| \otimes \left[(\mathsf{Ver}_k \otimes \mathbb{I}^{\mathcal{Z}}) \circ \mathcal{I}_{\ell(k)} \circ (\mathsf{Auth}_k \otimes \mathbb{I}^{\mathcal{Z}})\right] (\rho^{\mathcal{MZ}})$.

Definition 101 (Total authentication with key leakage). *Let $K' \leq |\mathcal{K}|$ and let $\ell : \mathcal{K} \to \{0,1\}^{\log K'}$ be a key leakage function. An authentication scheme* $(\mathsf{Auth}, \mathsf{Ver})$ ε-totally authenticates with key leakeage ℓ *iff it ε-reduces to the class of oblivious adversaries with key leakeage ℓ.*

This definition may seem somewhat strange: how is an ideal adversary able to learn bits $\ell(k)$ of the key k, if it doesn't act on the authenticated part of the state at all? Of course, any adversary that learns something about the key must have acted on the authenticated state, but the point is that, conditioned on successful verification, the adversary "effectively" behaved like an oblivious adversary that had access to $\ell(k)$.

In Section 8.8 we present a very simple scheme that achieves total authentication with some key leakage: to authenticate an arbitrary quantum state ρ, first apply the classical Carter-Wegman authentication scheme on it using key k. Then, apply $H^{\otimes n}$ to all the qubits in the authenticated state (i.e. apply the quantum Fourier transform over $\mathbb{Z}_2$). Finally, apply the classical Carter-Wegman scheme again using a fresh key h. Thus, we are authenticating the state ρ in complementary bases. We call this the "Auth-QFT-Auth" scheme.

We will show that this in fact achieves total authentication (and hence encryption of the state), but at the cost of leaking the "outer key" h:

Theorem 102 (Security of the Auth-QFT-Auth scheme). *The Auth-QFT-Auth scheme is δ-totally authenticating with outer key leakage, where $\delta = O(\sqrt{|\mathcal{M}|^{5/2}/|\mathcal{Y}|})$.*

While this scheme leaks some bits of the outer key, it preserves the secrecy of the state ρ and the "inner key" k. Furthermore, it is much more "lightweight" than the full unitary design scheme that achieves total authentication without key leakage. It also illustrates that applying a simple classical authentication scheme in complementary bases is already enough to reduce a full quantum adversary to performing only trivial attacks. Finally, the analysis of this scheme crucially relies on the basis dependent security definition above.

We note that Hayden, Leung, and Mayers show that the authentication scheme of [9] satisfies total authentication with key leakage [53], but it is unclear whether it satisfies the strongest definition of total authentication without key leakage.

8.5 Properties of basis-dependent authentication

8.5.1 Indistinguishability from measured

Here, we show that any classical scheme that authenticates relative to the computational basis implies that the authenticated state is indistinguishable from being measured in the computational basis. For concreteness we will work with the computational basis; this is without loss of generality.

Definition 103. *If* Auth *is a classical scheme that is ε-*indistinguishable from measured *in the computational basis, then for any state $\rho^{\mathcal{M}\mathcal{Z}}$, the following two states are ε close:*

- $\mathbb{E}_k\left[\mathsf{Auth}_k \otimes \mathbb{I}^{\mathcal{Z}}\right](\rho^{\mathcal{M}\mathcal{Z}})$ *(the unmeasured authenticated state), and*
- $\mathbb{E}_k\left[(\mathsf{Meas} \otimes \mathbb{I}^{\mathcal{Z}}) \circ (\mathsf{Auth}_k \otimes \mathbb{I}^{\mathcal{Z}})\right]()\rho^{\mathcal{M}\mathcal{Z}})$ *(the measured authenticated state), where* Meas *denotes measuring in the computational basis.*

Theorem 104. *If* (Auth, Ver) *ε-authenticates relative to the computational basis, then* Auth *is $7\sqrt{\varepsilon}$-indistinguishable from measured.*

Proof. We prove this theorem by contradiction: assuming an adversary can distinguish from measured, we will obtain a violation of the security of authentication. Analogous to the proof that authentication implies encryption of Barnum et al. [9], our proof will proceed in two parts. First, we will reduce to the case where we assume the distinguishing adversary has very high success probability. Second, we will show that by iterating the scheme, we boost a low success probability adversary into a high success probability adversary. For this proof, we will not need the full security where the key k is considered — instead, we will invoke the authentication security by tracing out and averaging over the key as in prior works.

Let $\rho^{\mathcal{M},\mathcal{Z}}$ be a quantum state. Let D be a distinguisher violating the indistinguishability from measured property. Suppose D has very large distinguishing advantage $1-\gamma$. This means that

- $D(\mathbb{E}_k\left[\mathsf{Auth}_k \otimes \mathbb{I}^{\mathcal{Z}}\right](\rho^{\mathcal{M}\mathcal{Z}}))$ outputs 1 with probability at least $1-\gamma$, and
- $D(\mathbb{E}_k\left[(\mathsf{Meas} \otimes \mathbb{I}^{\mathcal{Z}}) \circ (\mathsf{Auth}_k \otimes \mathbb{I}^{\mathcal{Z}})\right]()\rho^{\mathcal{M}\mathcal{Z}}))$ outputs 1 with probability at most γ

Now, we set up the state $(\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|) \otimes \rho^{\mathcal{M}\mathcal{Z}}$. We conditionally measure $\rho^{\mathcal{M}}$ in the computational basis based on the first bit: if 0, we measure, if 1 we leave intact. Next, we discard the first bit by tracing it out. The resulting state is $\left[\frac{1}{2}(\mathsf{Meas} + \mathbb{I}^{\mathcal{M}}) \otimes \mathbb{I}^{\mathcal{Z}}\right](\rho^{\mathcal{M}\mathcal{Z}})$.

Now we authenticate. Since the scheme is classical, authentication commutes with measurement in the computational basis. Therefore, the authenticated state is

$$\left[\frac{1}{2}((\mathsf{Meas} + \mathbb{I}^{\mathcal{Y}}) \circ \mathsf{Auth}_k) \otimes \mathbb{I}^{\mathcal{Z}}\right](\rho^{\mathcal{M}\mathcal{Z}})$$

The adversary now applies D, copying the result into its auxiliary state. Because D has high distinguishing advantage, applying D and conditioning on D giving the right answer only negligibly affects the state. Therefore, it is straightforward to show the resulting state is $4\sqrt{2\gamma}$-close to:

$$\frac{1}{2}\mathop{\mathbb{E}}_{k}\left[\mathbb{I}^{\mathcal{Y}\mathcal{Z}} \circ (\mathsf{Auth}_k \otimes \mathbb{I}^{\mathcal{Z}})\right](\rho^{\mathcal{M}\mathcal{Z}}) \otimes |1\rangle\langle 1| + \frac{1}{2}\mathop{\mathbb{E}}_{k}\left[(\mathsf{Meas} \otimes \mathbb{I}^{\mathcal{Z}}) \circ (\mathsf{Auth}_k \otimes \mathbb{I}^{\mathcal{Z}})\right](\rho^{\mathcal{M}\mathcal{Z}}) \otimes |0\rangle\langle 0|$$

Now, this state will pass verification with probability 1, since the authentication scheme is classical. Therefore, this state is approximated by an ideal adversary that is computational basis respecting. Note that such adversaries commute with the measurement in the computational basis. Therefore, the final bit in the approximated superposition is either 0 or 1 or some mixture of the two, but the mixture is independent of whether the authenticated space is measured or not.

Therefore, the state above has a distance of $\frac{1}{2}$ from any ideal adversary, a contradiction.

Thus, we have that if the scheme $\frac{1}{2} - 4\sqrt{2\gamma}$-authenticates in the computational basis, there is no distinguisher with advantage $1-\gamma$.

Next, we show how to boost a low-advantage distinguisher for a scheme $(\mathsf{Auth}, \mathsf{Ver})$ into a high-advantage distinguisher for the product scheme $(\mathsf{Auth}^t, \mathsf{Ver}^t)$ which acts on message space $\mathcal{M}^t$ by applying Auth to each message component with an independent key.

A simple hybrid argument shows that, if $(\mathsf{Auth}, \mathsf{Ver})$ ε-authenticates in the computational basis, then $(\mathsf{Auth}^t, \mathsf{Ver}^t)$ $t\varepsilon$-authenticates in the computational basis. Note that Barnum et al.'s proof of this required somewhat more effort; however, for us, due tot he fact that we consider side information in our definition, in our case the security of the product scheme comes essentially for free.

Next, assume D distinguishes from measured for the state $\rho^{\mathcal{M}\mathcal{Z}}$ in the scheme $(\mathsf{Auth}, \mathsf{Ver})$ with advantage δ. Then we can boost the success probability to a distinguisher D^t for the state $(\rho^{\mathcal{M}\mathcal{Z}})^{\otimes t}$ in scheme $(\mathsf{Auth}^t, \mathsf{Ver}^t)$ with advantage $1 - 2e^{-t\delta^2/2}$. But from the above, this means that the scheme $(\mathsf{Auth}^t, \mathsf{Ver}^t)$ cannot $\frac{1}{2} - 8e^{-t\delta^2/4}$-authenticate. Thus,

$$t\varepsilon > \frac{1}{2} - 8e^{-t\delta^2/4}$$

Choosing $t = 1/3/\varepsilon$ gives $\delta < 7\sqrt{\varepsilon}$.

□

8.5.2 Unforgeability

In this section we show that our security definition of authentication schemes relative to a basis implies the classical security definition of authentication schemes – namely, that the adversary, after having received the authenticated message state, cannot produce two distinct authenticated message-tag pairs with non-negligible probability. This property is called **unforgeability**. Thus this shows that our security definition recovers the Boneh-Zhandry security definition for one-time MACs.

Our model for signature forgery is the following. Let $(\mathsf{Auth}, \mathsf{Ver})$ be a classical authentication scheme that is $\mathcal{B}$-respecting for some basis. We will let $\mathcal{B}$ be the computational basis without loss of generality. Furthermore, we will restrict our attention to MACs where for a classical message $m \in \mathcal{M}$, $\mathsf{Auth}_k(m) = (m, \sigma(k, m))$, although our arguments extend to general classical authentication schemes.

Without loss of generality we can assume that the initial message state is a pure state $|\rho\rangle^{\mathcal{M}\mathcal{Z}} = \sum_m \alpha_m |m\rangle^{\mathcal{M}} \otimes |\varphi_m\rangle^{\mathcal{Z}}$ where the $|\varphi_m\rangle$ are arbitary pure states held by the adversary. After signing, we have

$$\tau^{\mathcal{K}\mathcal{Y}\mathcal{Z}} = \mathop{\mathbb{E}}_{k} |k\rangle\langle k| \otimes \mathsf{Auth}_k(\rho^{\mathcal{M}\mathcal{Z}}).$$

The adversary applies some superoperator $\mathcal{E}$ on $\mathcal{Y}\mathcal{Z}$ and outputs a system on $\mathcal{Y}_1\mathcal{Y}_2\mathcal{Z}$. The spaces $\mathcal{Y}_1$ and $\mathcal{Y}_2$ are both isomorphic to $\mathcal{Y}$. Let the tampered state be denoted as

$$\tilde{\tau}^{\mathcal{K}\mathcal{Y}_1\mathcal{Y}_2\mathcal{Z}} = \mathop{\mathbb{E}}_{k} |k\rangle\langle k| \otimes \mathcal{E}(\mathsf{Auth}_k(\rho^{\mathcal{M}\mathcal{Z}})).$$

We define the **probability of forgery by $\mathcal{E}$ on input** ρ to be the probability that, upon measuring $\mathcal{K}$, $\mathcal{Y}_1$, and $\mathcal{Y}_2$ in the computational basis, we obtain a key k and two valid signed messages $(m, \sigma(k, m))$ and $(m', \sigma(k, m'))$ with $m \neq m'$.

The next theorem shows that quantum-secure authentication schemes possess the unforgeability property. The idea of the proof is as follows: suppose that there was an authentication scheme $(\mathsf{Auth}, \mathsf{Ver})$, an adversary $\mathcal{E}$ and an initial message state $\rho^{\mathcal{M}}$ such that $\mathcal{E}$ on input ρ could forge an authenticated message with non-negligible probability. Using the fact that the authentication scheme is secure, we can in fact find a *fixed* message $m \in \mathcal{M}$ and another adversary $\hat{\mathcal{E}}$ that, when given an authentication of message m, forges a valid signed message $(m', \sigma(k, m'))$ where $m' \neq m$ with non-negligible probability. The definition of secure authentication scheme easily implies this is impossible.

Theorem 105. *Let* $(\mathsf{Auth}, \mathsf{Ver})$ *be an authentication scheme that is ε-authenticating relative to the computational basis. Let $\mathcal{E}$ be a forger. Then for all initial message states $\rho^{\mathcal{M}\mathcal{Z}}$, the probability of* *forgery by $\mathcal{E}$ on input ρ is at most 3ε.*

Proof. Suppose for contradiction that the probability of forgery is at least $\delta = 3\varepsilon$. Since the scheme is ε-authenticating relative to the computational basis, we can simulate the forger by an ideal adversary $\mathcal{I}$ that respects the computational basis: on input $\tau^{\mathcal{KYZ}}$ (the authentication of ρ), it first measures the $\mathcal{Y}$ register to yield a valid signed message $(m, \sigma(k,m))$. Then, conditioned on this result, it applies an arbitrary quantum operation on the $\mathcal{Z}$ register. Since $\mathcal{E}$ is a forger, the ideal adversary $\mathcal{I}$ is also a forger: measuring $\mathcal{KYZ}$ in the computational basis will yield k, $(m, \sigma(k,m))$ and $(m', \sigma(k,m'))$ where $m \neq m'$ with probability at least $\delta - \varepsilon = 2\varepsilon$. Let E_m denote the event that measuring $\mathcal{Y}$ yields a valid signature of the message m. Let F_m denote the event that measuring $\mathcal{Z}$ yields a valid signature of a message that's distinct from m.

Thus

$$\sum_m \Pr[E_m] \cdot \Pr[F_m | E_m] \geq 2\varepsilon$$

where the probabilities are with respect to the ideal adversary $\mathcal{I}$. Thus by averaging there exists an m where $\Pr[F_m | E_m] \geq 2\varepsilon$. But notice that $\Pr[E_m]$ is independent of the key, and simply $|\alpha_m|^2$, because the ideal adversary only measures the $\mathcal{Y}$ register of τ in the computational basis. Thus, if we condition the state $\mathcal{I}(\tau)$ on the event E_m, we have the following state:

$$\mathcal{I}(\tau^{\mathcal{KYZ}})\big|_{E_m} = \mathop{\mathbb{E}}_{k} |k\rangle\langle k|^{\mathcal{K}} \otimes |m, \sigma(k,m)\rangle\langle m, \sigma(k,m)|^{\mathcal{Y}} \otimes \mathcal{I}_{m,\sigma(k,m)} \left(|\varphi_m\rangle\langle\varphi_m|^{\mathcal{Z}} \right)$$

where $\mathcal{I}_{m,\sigma(k,m)}$ denotes the attack that the ideal adversary performs on the side information, conditioned on reading $(m, \sigma(k,m))$ in $\mathcal{Y}$. However, $\Pr[F_m | E_m] \geq 2\varepsilon$ implies that measuring $\mathbb{E}_k |k\rangle\langle k| \otimes \mathcal{I}_{m,\sigma(k,m)} \left(|\varphi_m\rangle\langle\varphi_m|^{\mathcal{Z}} \right)$ in the computational basis yields k and a forgery $(m', \sigma(k,m'))$ where $m' \neq m$ with probability at least 2ε. However this is impossible, as a real adversary could, given the authenticated message/tag pair $(m, \sigma(k,m))$, perform $\mathcal{I}_{m,\sigma(k,m)}$ on the side information $|\varphi_m\rangle^{\mathcal{Z}}$, and then swap the $\mathcal{Y}$ registers with some registers in $\mathcal{Z}$. Upon verification, measuring the $\mathcal{Y}$ registers of this tampered state has probability of at least 2ε of obtaining a valid $(m', \sigma(k,m'))$, which contradicts the property that $(\mathsf{Auth}, \mathsf{Ver})$ is ε-authenticating relative to the computational basis.

□

8.6 Properties of total authentication

8.6.1 Encryption

Analogous to the Barnum et al.'s [9] result that authentication implies encryption, we show that authentication when considering side information must encrypt the state, even to an adversary that may be entangled with the state. This result is incompatible with Barnum et al.'s: we start from a stronger property that considers side information, and end with a stronger form of authentication that also considers side information.

Definition 106. *If* Auth *is an ε-secure encryption scheme with side information, then for any two states $\rho_0^{\mathcal{MZ}}, \rho_1^{\mathcal{MZ}}$ such that $\rho_0^{\mathcal{Z}}$ and $\rho_1^{\mathcal{Z}}$ are δ-close, the following two distributions are $\delta + \varepsilon$ close:*

- $\mathbb{E}_k \left[\mathsf{Auth}_k \otimes \mathbb{I}^{\mathcal{Z}} \right] (\rho_0^{\mathcal{MZ}})$ *and*

- $\mathbb{E}_k \left[\mathsf{Auth}_k \otimes \mathbb{I}^{\mathcal{Z}}\right] (\rho_1^{\mathcal{M}\mathcal{Z}})$

Theorem 107. *If* $(\mathsf{Auth}, \mathsf{Ver})$ *ε-authenticates, then* Auth *is an $14\sqrt{\varepsilon}$-secure encryption scheme.*

Proof. First, we observe that any scheme that gives ε secure encryption in the case $\delta = 0$ gives 2ε secure encryption in the general case. Indeed, by assumption, $\mathbb{E}_k \left[\mathsf{Auth}_k \otimes \mathbb{I}^{\mathcal{Z}}\right] (\rho_0^{\mathcal{M}\mathcal{Z}})$ is ε-close to $\mathbb{E}_k \mathsf{Auth}_k(|0\rangle\langle 0|) \otimes \rho_0^{\mathcal{Z}}$, which is δ close to $\mathbb{E}_k \mathsf{Auth}_k(|0\rangle\langle 0|) \otimes \rho_1^{\mathcal{Z}}$, which is ε close to $\mathbb{E}_k \left[\mathsf{Auth}_k \otimes \mathbb{I}^{\mathcal{Z}}\right] (\rho_1^{\mathcal{M}\mathcal{Z}})$.

Therefore, it suffices to prove that Auth is $7\sqrt{\varepsilon}$ secure for states with $\delta = 0$.

We prove this theorem by contradiction: assuming an adversary can distinguish from measured, we will obtain a violation of the security of authentication. Our proof will very similar to the proof of Theorem 104. First, we will reduce to the case where we assume the distinguishing adversary has very high success probability. Second, we will show that by iterating the scheme, we boost a low success probability adversary into a high success probability adversary. For this proof, we will not need the full security where the key k is considered — instead, we will invoke the authentication security by tracing out and averaging over the key as in prior works.

Let $\rho_0^{\mathcal{M},\mathcal{Z}}, \rho_1^{\mathcal{M},\mathcal{Z}}$ be quantum states. Let D be a distinguisher that distinguishes between the two with probability τ. Suppose D has very large distinguishing advantage $1 - \gamma$. This means that

- $D(\mathbb{E}_k \left[\mathsf{Auth}_k \otimes \mathbb{I}^{\mathcal{Z}}\right] (\rho_1^{\mathcal{M}\mathcal{Z}}))$ outputs 1 with probability at least $1 - \gamma$, and
- $D(\mathbb{E}_k \left[\mathsf{Auth}_k \otimes \mathbb{I}^{\mathcal{Z}}\right] (\rho_0^{\mathcal{M}\mathcal{Z}})$ outputs 1 with probability at most γ

Now, we set up the state $\frac{1}{2}|0\rangle\langle 0| \otimes \rho_0^{\mathcal{M}\mathcal{Z}} + \frac{1}{2}|1\rangle\langle 1| \otimes \rho_1^{\mathcal{M}\mathcal{Z}}$. Next, we discard the first bit by tracing it out. The resulting state is $\frac{1}{2}(\rho_0^{\mathcal{M}\mathcal{Z}} + \rho_1^{\mathcal{M}\mathcal{Z}})$. Then we authenticate. By the linearity of quantum operations, we have that the state is

$$\frac{1}{2}(\left[\mathsf{Auth}_k \otimes \mathbb{I}^{\mathcal{Z}}\right] (\rho_0^{\mathcal{M}\mathcal{Z}}) + \left[\mathsf{Auth}_k \otimes \mathbb{I}^{\mathcal{Z}}\right] (\rho_1^{\mathcal{M}\mathcal{Z}}))$$

The adversary now applies D, copying the result into its auxiliary state. Because D has high distinguishing advantage, applying D and conditioning on D giving the right answer only negligibly affects the state. Therefore, it is straightforward to show the resulting state is $4\sqrt{2\gamma}$-close to:

$$\frac{1}{2}\mathop{\mathbb{E}}_{k}\left[\mathsf{Auth}_k \otimes \mathbb{I}^{\mathcal{Z}}\right] (\rho_0^{\mathcal{M}\mathcal{Z}}) \otimes |0\rangle\langle 0| + \frac{1}{2}\mathop{\mathbb{E}}_{k}\left[\mathsf{Auth}_k \otimes \mathbb{I}^{\mathcal{Z}}\right] (\rho_1^{\mathcal{M}\mathcal{Z}}) \otimes |1\rangle\langle 1|$$

Now, this state will pass verification with probability 1, since each component is a valid authenticated state and authentication is linear. Therefore, this state is approximated by an ideal adversary that does nothing except forward the state as is or reject the state, and modify its auxiliary registers independently of the authenticated state. Therefore, the final bit in the approximated superposition is either 0 or 1 or some mixture of the two, and the mixture may depend on $\rho^{\mathcal{Z}}$, but not $\rho^{\mathcal{M}}$. But recall that by assumption $\rho_0^{\mathcal{Z}} = \rho_1^{\mathcal{Z}}$, and so an ideal adversary cannot distinguish the two cases. Therefore, the state above has a distance of $\frac{1}{2}$ from any ideal adversary, a contradiction.

Thus, we have that if the scheme $\frac{1}{2} - 4\sqrt{2\gamma}$-authenticates in the computational basis, there is no distinguisher with advantage $1 - \gamma$.

Next, we show how to boost a low-advantage distinguisher for a scheme (Auth, Ver) into a high-advantage distinguisher for the product scheme $(\mathsf{Auth}^t, \mathsf{Ver}^t)$ which acts on message space $\mathcal{M}^t$ by applying Auth to each message component with an independent key.

A simple hybrid argument shows that, if (Auth, Ver) ε-authenticates, then $(\mathsf{Auth}^t, \mathsf{Ver}^t)$ $t\varepsilon$-authenticates in the computational basis.

Next, assume D distinguishes from measured for the state $\rho^{\mathcal{MZ}}$ in the scheme (Auth, Ver) with advantage δ. Then we can boost the success probability to a distinguisher D^t for the state $(\rho^{\mathcal{MZ}})^{\otimes t}$ in scheme $(\mathsf{Auth}^t, \mathsf{Ver}^t)$ with advantage $1 - 2e^{-t\delta^2/2}$. But from the above, this means that the scheme $(\mathsf{Auth}^t, \mathsf{Ver}^t)$ cannot $\frac{1}{2} - 8e^{-t\delta^2/4}$-authenticate. Thus,

$$t\varepsilon > \frac{1}{2} - 8e^{-t\delta^2/4}$$

Choosing $t = 1/3/\varepsilon$ gives $\delta < 7\sqrt{\varepsilon}$.

□

8.6.2 Quantum Key Distribution

Suppose we have a total authentication scheme. Then as argued in the Introduction, we immediately get a simple method to perform quantum key distribution. However, the QKD scheme sketched in the Introduction is rather fragile: any small amount of tampering by the adversary will cause Alice and Bob to abort. Here we sketch a slightly more robust way of carrying out QKD using a total authentication scheme.

Suppose Alice and Bob want to generate n bits of perfectly correlated key bits. We now describe a protocol that takes 2 rounds and $O(n \log n)$ bits of communication, and tolerates the adversary attacking at most $O(n/\log n)$ qubits of communication. If this is the case, then Alice and Bob can distill at least $\Omega(n)$ bits of shared key. Let (Auth, Ver) be a scheme that encodes single qubits as $O(\log n)$ qubits, and is ε-totally authenticating for $\varepsilon = n^{-\Omega(1)}$. The unitary design scheme is one such example.

The QKD protocol is as follows:

1. Alice prepares the maximally entangled state over $2n$ qubits i.e. $|\Phi\rangle^{\mathcal{AB}} = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |xx\rangle^{\mathcal{AB}}$.

2. Alice will generate independent keys $k_1, \ldots, k_n$ for n uses of the authentication scheme (Auth, Ver). She authenticates each of the n qubits on the $\mathcal{B}$-half of $|\Phi\rangle^{\mathcal{AB}}$ using an independent key. She sends $\mathcal{B}$ to Bob.

3. Bob sends a bit to Alice acknowledging that he received some state through the quantum channel (that may have been tampered by the adversary).

4. Alice sends the keys $k_1, \ldots, k_n$ over an authenticated, but non-private, classical channel.

5. On the quantum state he received, Bob performs the verification procedure $\mathsf{Ver}_{k_1} \otimes \cdots \mathsf{Ver}_{k_n}$ on n parts of $\log n$ qubits each. He relays to Alice which parts successfully passed verification. Let $S \subset [n]$ denote the successfully unauthenticated qubits.

6. Alice and Bob measure the part of their respective states corresponding to S in the computational basis, and use these bits as their shared key.

Since (Auth, Ver) is totally authenticating, after Bob successfully unauthenticates the qubits in S, the qubits shared between Alice and Bob in S will be $\approx \varepsilon n$-close to the maximally entangled state. Thus when they both measure, they will both share a keys (x, x') that are εn-close to uniform, perfectly correlated, and private from any other system (because the maximally entangled state is in tensor product with any other quantum system). If we assume that the probability that Bob successfully verifies is not too small, then this means that Alice and Bob have successfully performed quantum key distribution.

8.6.3 Key Reuse

Alice reuses the key once she gets back an acknowledgement from Bob that he accepted the authenticated state. We have ε-secure Total Authentication implying

$$||\mathbb{E}_k|k\rangle\langle k| \otimes [(\mathrm{Ver}_k \otimes \mathbb{I}^{\mathcal{Z}}) \circ \mathcal{O}(\sigma^{\mathcal{YZ}})] - \mathbb{E}_k|k\rangle\langle k| \otimes [(\mathrm{Ver}_k \otimes \mathbb{I}^{\mathcal{Z}}) \circ (\mathbb{I}^{\mathcal{Y}} \otimes \mathcal{S})(\sigma^{\mathcal{YZ}})]||_1 \leq \varepsilon$$

where $\mathcal{I} = \mathbb{I}^{\mathcal{Y}} \otimes \mathcal{S}$ is the ideal adversary. As in the ideal case, adversary never touches k and the authenticated state, final state after verification is completely unentangled with the key k and distribution of k is uniform. Therefore, for a scheme satisfying total authentication, when Bob accepts, the final state (including adversary's register) is close in trace distance to an ideal state and we can reuse the key k again.

8.7 Quantum MACs from 3-universal hashing

In the classical setting, secure one-time MACs can be constructed via universal hashing. Let $\{h_k\}_k$ be a strongly (2-)universal hash family. Then it is well known that the classical authenticiation protocol $\mathsf{Auth}_k(m) = (m, h_k(m))$ is secure against classical adversaries [101]. Here, we show that the *same* authentication protocol is also quantum-secure, provided that the hash family $\{h_k\}_k$ satisfies the following: for all distinct m_1, m_2, m_3, the distribution of $(h_k(m_1), h_k(m_2), h_k(m_3))$ for a randomly chosen $k \in \mathcal{K}$ is uniform in $\mathcal{T}^3$. Such a family is called a *3-universal hash family*. We will overload notation and use $k(\cdot)$ to denote the function $h_k(\cdot)$.

We note that Boneh and Zhandry showed that, when authenticating classical messages in the one-time setting, pairwise independence is sufficient to ensure that a quantum adversary cannot forge a new signed message, as long as the length of the tag is longer than the message! When the tag is shorter than the message, they showed that pairwise independence is insecure, and 3-wise independence is necessary.

Our analysis of the 3-wise independent Carter-Wegman MAC requires that, in order to obtain security against quantum side information, the message tag needs to be longer than the message. Thus it is conceivable that pairwise independence is sufficient for the same guarantee; we leave this as an open question.

Theorem 108. *Let $\mathcal{K} = \{k\}$ be a 3-universal hash family. Let $\mathsf{Auth}_k(m) = (m, k(m))$ and Ver_k be the corresponding verification function. Then the authentication scheme* (Auth, Ver) *is $O(\sqrt{|\mathcal{M}|/|\mathcal{T}|})$-authenticating relative to the computational basis.*

Before beginning the proof we first state what the implications for key length are. Suppose we wish to guarantee that the Carter-Wegman MAC is ε-authenticating relative to the computational basis, then $|\mathcal{M}|/|\mathcal{T}| \leq O(\varepsilon^2)$, which implies that $\log|\mathcal{T}| \geq$

$\log|\mathcal{M}| + 2\log\frac{1}{\varepsilon} + O(1)$. To ensure three-wise independence, it is sufficient for the key to have length $3\log|\mathcal{M}| + 6\log\frac{1}{\varepsilon} + O(1)$.

Proof. To prove this, we need to show that for all message states $\rho^{\mathcal{M}\mathcal{Z}}$ and all adversaries $\mathcal{E} \in \mathrm{T}(\mathcal{Y}\mathcal{Z}, \mathcal{Y}\mathcal{Z})$, the result of the QMAC is to reduce the action of the adversary on the authenticated message to an ideal, computational basis-respecting adversary.

We will concentrate on the case of signing pure state messages – this is because we can always purify the initial message state, and give the purification to the adversary. In other words, we will show that Carter-Wegman MAC is a quantum secure MAC when the initial message state is a state $|\rho\rangle^{\mathcal{M}\mathcal{Z}} = \sum_m \alpha_m |m\rangle^{\mathcal{M}} \otimes |\varphi_m\rangle^{\mathcal{Z}}$. The register $\mathcal{M}$ corresponds to the message, and the register $\mathcal{Z}$ is held by the adversary.

It will actually be more useful to work with the Schmidt decomposition of $|\rho\rangle$, which we write as

$$|\rho\rangle^{\mathcal{M}\mathcal{Z}} = \sum_z \sqrt{\lambda_z}\left(\sum_m \alpha_{zm}|m\rangle^{\mathcal{M}}\right) \otimes |\varphi_z\rangle^{\mathcal{Z}}$$

where for $z \neq z'$, we have $\langle\varphi_z|\varphi_{z'}\rangle = 0$, and the λ_z's are nonnegative numbers summing to 1. Furthermore, the dimension of the span of $\{|\varphi_z\rangle\}_z$ is at most $|\mathcal{M}|$.

After signing, the state becomes

$$\sigma^{\mathcal{K}\mathcal{Y}\mathcal{Z}} = \mathop{\mathbb{E}}_k |k\rangle\langle k| \otimes \mathsf{Auth}_k(\rho)$$

where $\mathcal{Y} = \mathcal{M}\mathcal{T}$. Now consider an attack $\mathcal{E}$ of the adversary. By Stinespring's Dilation Theorem, the superoperator $\mathcal{E}$ can be implemented by applying a unitary V on registers $\mathcal{Y}\mathcal{Z}$, as well as some auxiliary register $\mathcal{Z}'$ held by the adversary, followed by a projective measurement P on $\mathcal{Z}\mathcal{Z}'$, followed by tracing out $\mathcal{Z}'$.

First, we will assume that the auxiliary space $\mathcal{Z}'$ is part of the purification in $|\rho\rangle^{\mathcal{M}\mathcal{Z}}$. Secondly, we will ignore the projector P for now, and handle it later.

We specify the action of V on $\mathcal{Y}\mathcal{Z}$ as

$$V : |m,t\rangle^{\mathcal{M}\mathcal{T}} \otimes |\varphi_z\rangle^{\mathcal{Z}} \mapsto |\psi_{mtz}\rangle^{\mathcal{M}\mathcal{T}\mathcal{Z}}$$

where $\{|\psi_{mtz}\rangle\}$ are a collection of states in $\mathcal{M}\mathcal{T}\mathcal{Z}$ such that for all $(m,t,z) \neq (m',t',z')$, $\langle\psi_{mtz}|\psi_{m't'z'}\rangle = 0$. Furthermore, write the states as follows:

$$|\psi_{mtz}\rangle = \sum_{a,b} \beta^{mtz}_{ab}|a,b\rangle \otimes |\phi^{mtz}_{ab}\rangle$$

where the $\{|\phi^{mtz}_{a,}\rangle\}$ are an arbitrary collection of unit vectors residing in the space $\mathcal{Z}$, and $|a,b\rangle$ are vectors in $\mathcal{Y} = \mathcal{M}\mathcal{T}$. Therefore after the attack we have

$$\widetilde{\sigma}^{\mathcal{K}\mathcal{Y}\mathcal{Z}} = \mathop{\mathbb{E}}_k |k\rangle\langle k| \otimes V\,\mathsf{Auth}_k(\rho)\,V^{\dagger}.$$

Now we apply the verification procedure to this state to obtain τ, where we've conditioned on the procedure accepting:

$$\tau^{\mathcal{K}\mathcal{Y}\mathcal{Z}} = \mathsf{Ver}(\widetilde{\sigma}^{\mathcal{K}\mathcal{Y}\mathcal{Z}}) = \mathop{\mathbb{E}}_k |k\rangle\langle k| \otimes \mathsf{Ver}_k\left(V\,\mathsf{Auth}_k(\rho)\,V^{\dagger}\right)$$

Note that τ does not have unit trace in general (because the verification procedure Ver_k

may not pass with probability 1). For a fixed key k, we can write

$$|\tau_k\rangle = \mathsf{Ver}_k \, V \, \mathsf{Auth}_k|\rho\rangle = \sum_{z,m,a} \sqrt{\lambda_z}\alpha_{zm}\beta_{ak_a}^{mk_m z} \; |a\rangle^{\mathcal{M}} \otimes |\phi_{ak_a}^{mk_m z}\rangle^{\mathcal{T}}$$

where we abbreviate $k(m)$ and $k(a)$ by k_m and k_a respectively. We can decompose the vector $|\tau_k\rangle = |\tau_{k,ideal}\rangle + |\tau_{k,err}\rangle$ where

$$|\tau_{k,ideal}\rangle^{\mathcal{M}\mathcal{T}\mathcal{Z}} = \sum_{z,m} \sqrt{\lambda_z}\alpha_{zm}\beta_{mk_m}^{mk_m z} \; |m\rangle^{\mathcal{M}} \otimes |\phi_{mk_m}^{mk_m z}\rangle^{\mathcal{Z}} \tag{8.2}$$

$$|\tau_{k,err}\rangle^{\mathcal{M}\mathcal{T}\mathcal{Z}} = \sum_{z,m,a:a\neq m} \sqrt{\lambda_z}\alpha_{zm}\beta_{ak_a}^{mk_m z} \; |a\rangle^{\mathcal{M}} \otimes |\phi_{ak_a}^{mk_m z}\rangle^{\mathcal{Z}} \tag{8.3}$$

Thus $\tau^{\mathcal{K}\mathcal{Y}\mathcal{Z}} = \tau_{ideal} + \tau_{err}$ where

$$\tau_{ideal} = \mathop{\mathbb{E}}_{k} |k\rangle\langle k| \otimes |\tau_{k,ideal}\rangle\langle\tau_{k,ideal}|,$$

and let

$$\tau_{err} = \mathop{\mathbb{E}}_{k} |k\rangle\langle k| \otimes \left(|\tau_{k,ideal}\rangle\langle\tau_{k,err}| + |\tau_{k,err}\rangle\langle\tau_{k,ideal}| + |\tau_{k,err}\rangle\langle\tau_{k,err}|\right).$$

The τ_{ideal} represents the part of τ that looks like it underwent an *ideal* attack, while the term τ_{ideal} represents the rest of τ. We will bound this error term and show that its size is small within τ, and thus this will show that τ is close to the result of an ideal attack.

To bound the size of τ_{err}, we note that

$$\begin{aligned}
\|\tau_{err}\|_1 &\leq \mathop{\mathbb{E}}_{k} [2\| \; |\tau_{k,ideal}\rangle\langle\tau_{k,err}| \; \|_1 + \| \; |\tau_{k,err}\rangle\langle\tau_{k,err}| \; \|_1] \\
&= \mathop{\mathbb{E}}_{k} \left[2\sqrt{\langle\tau_{k,err}|\tau_{k,err}\rangle \cdot \langle\tau_{k,ideal}|\tau_{k,ideal}\rangle} + \langle\tau_{k,err}|\tau_{k,err}\rangle\right] \\
&\leq 3 \mathop{\mathbb{E}}_{k} \sqrt{\langle\tau_{k,err}|\tau_{k,err}\rangle} \\
&\leq 3\sqrt{\mathop{\mathbb{E}}_{k}\langle\tau_{k,err}|\tau_{k,err}\rangle}
\end{aligned}$$

where in the equality we used that for two pure states $|\varphi\rangle$ and $|\psi\rangle$, $\| \; |\varphi\rangle\langle\psi| \; \|_1 = \sqrt{\langle\varphi|\varphi\rangle \cdot \langle\psi|\psi\rangle}$. In the second-to-last inequality we used that $\langle\tau_{k,ideal}|\tau_{k,ideal}\rangle \leq 1$, and in the last inequality we used the concavity of the square-root function. Now,

$$\mathop{\mathbb{E}}_{k}\langle\tau_{k,err}|\tau_{k,err}\rangle = \mathop{\mathbb{E}}_{k} \sum_{\substack{z,z' \\ a,m,m':a\notin\{m,m'\}}} \sqrt{\lambda_z\lambda_{z'}} \cdot \alpha_{zm}\overline{\alpha}_{z'm'} \cdot \beta_{ak_a}^{mk_m z}\overline{\beta}_{ak_a}^{m'k_{m'}z'} \cdot \langle\phi_{ak_a}^{m'k_{m'}z'}|\phi_{ak_a}^{mk_m z}\rangle \tag{8.4}$$

$$= \sum_{\substack{z,z' \\ a,m,m':a\notin\{m,m'\}}} \sqrt{\lambda_z\lambda_{z'}} \cdot \alpha_{zm}\overline{\alpha}_{z'm'} \cdot \left(\mathop{\mathbb{E}}_{k} \beta_{ak_a}^{mk_m z}\overline{\beta}_{ak_a}^{m'k_{m'}z'} \cdot \langle\phi_{ak_a}^{m'k_{m'}z'}|\phi_{ak_a}^{mk_m z}\rangle\right) \tag{8.5}$$

Observe that, for every a, m, m' such that $a \notin \{m, m'\}$, k_a is independent of k_m and $k_{m'}$ (this is where we use 3-wise independence of k). Therefore, we can write

$$\mathop{\mathbb{E}}_{k} \beta_{ak_a}^{mk_m z}\overline{\beta}_{ak_a}^{m'k_{m'}z'} \cdot \langle\phi_{ak_a}^{m'k_{m'}z'}|\phi_{ak_a}^{mk_m z}\rangle = \mathop{\mathbb{E}}_{k,h} \beta_{ah_a}^{mk_m z}\overline{\beta}_{ah_a}^{m'k_{m'}z'} \cdot \langle\phi_{ah_a}^{m'k_{m'}z'}|\phi_{ah_a}^{mk_m z}\rangle$$

where the expectation on the right hand side is over two independent hash families k and h. We have equality because $(k_m, k_{m'}, k_a)$ and $(k_m, k_{m'}, h_a)$ are identically distributed.

This motivates us to define

$$\zeta_1 = \mathop{\mathbb{E}}_{k,h} \sum_{z,z',m,m'} \sqrt{\lambda_z \lambda_{z'}} \cdot \alpha_{zm} \overline{\alpha}_{z'm'} \cdot \beta_{mh_m}^{mk_m z} \overline{\beta}_{mh_m}^{m'k_{m'}z'} \cdot \langle \phi_{mh_m}^{m'k_{m'}z'} | \phi_{mh_m}^{mk_m z} \rangle$$

$$\zeta_2 = \mathop{\mathbb{E}}_{k,h} \sum_{z,z',m} \sqrt{\lambda_z \lambda_{z'}} \cdot \alpha_{zm} \overline{\alpha}_{z'm} \cdot \beta_{mh_m}^{mk_m z} \overline{\beta}_{mh_m}^{mk_m z'} \cdot \langle \phi_{mh_m}^{mk_m z'} | \phi_{mh_m}^{mk_m z} \rangle.$$

We will momentarily show that ζ_1 and ζ_2 are small in magnitude. Assuming this, we add ζ_1 and ζ_2 to (8.5) to get a nicer-looking sum:

$$\begin{aligned}
(8.5) + \zeta_1 + \overline{\zeta}_1 - \zeta_2 &= \sum_{\substack{z,z' \\ a,m,m'}} \sqrt{\lambda_z \lambda_{z'}} \cdot \alpha_{zm} \overline{\alpha}_{z'm'} \cdot \left(\mathop{\mathbb{E}}_{k,h} \beta_{ah_a}^{mk_m z} \overline{\beta}_{ah_a}^{m'k_{m'}z'} \cdot \langle \phi_{ah_a}^{m'k_{m'}z'} | \phi_{ah_a}^{mk_m z} \rangle \right) && (8.6) \\
&= \frac{1}{|\mathcal{T}|} \sum_{z,z',m,m'} \sqrt{\lambda_z \lambda_{z'}} \cdot \alpha_{zm} \overline{\alpha}_{z'm'} \cdot \mathop{\mathbb{E}}_{k} \sum_{a,b} \beta_{ab}^{mk_m z} \overline{\beta}_{ab}^{m'k_{m'}z'} \cdot \langle \phi_{ab}^{m'k_{m'}z'} | \phi_{ab}^{mk_m z} \rangle && (8.7) \\
&= \frac{1}{|\mathcal{T}|} \sum_{z,m} \lambda_z \cdot |\alpha_{zm}|^2 \mathop{\mathbb{E}}_{k} \sum_{a,b} |\beta_{ab}^{mk_m z}|^2 && (8.8) \\
&= \frac{1}{|\mathcal{T}|}. && (8.9)
\end{aligned}$$

To go from the second line to the third line we used the orthogonality conditions

$$\langle \psi_{m't'z'} | \psi_{mtz} \rangle = \sum_{a,b} \beta_{ab}^{mtz} \overline{\beta}_{ab}^{m't'z'} \langle \phi_{ab}^{m't'z'} | \phi_{ab}^{mtz} \rangle = 0$$

whenever $(m,t,z) \neq (m',t',z')$.

Now we bound the magnitudes of ζ_1 and ζ_2. We use Cauchy-Schwarz repeatedly to bound $|\zeta_1|$:

$$\begin{aligned}
|\zeta_1| &= \frac{1}{|\mathcal{T}|} \left| \mathop{\mathbb{E}}_{k} \sum_{z,z',m,m'} \sqrt{\lambda_z \lambda_{z'}} \cdot \alpha_{zm} \overline{\alpha}_{z'm'} \cdot \sum_{b} \beta_{mb}^{mk_m z} \overline{\beta}_{mb}^{m'k_{m'}z'} \cdot \langle \phi_{mb}^{m'k_{m'}z'} | \phi_{mb}^{mk_m z} \rangle \right| && (8.10) \\
&\leq \frac{1}{|\mathcal{T}|} \mathop{\mathbb{E}}_{k} \sqrt{ \sum_{z,z',m,m'} |\alpha_{zm}|^2 |\alpha_{z'm'}|^2 \cdot \left| \sum_{b} \beta_{mb}^{mk_m z} \overline{\beta}_{mb}^{m'k_{m'}z'} \cdot \langle \phi_{mb}^{m'k_{m'}z'} | \phi_{mb}^{mk_m z} \rangle \right|^2 } && (8.11) \\
&\leq \frac{1}{|\mathcal{T}|} \mathop{\mathbb{E}}_{k} \sqrt{ \sum_{z,z',m,m'} |\alpha_{zm}|^2 |\alpha_{z'm'}|^2 \cdot \left(\sum_{b} |\beta_{mb}^{mk_m z}|^2 \cdot \| |\phi_{mb}^{mk_m z} \rangle \|^2 \right) \left(\sum_{b} |\beta_{mb}^{m'k_{m'}z'}|^2 \cdot \| |\phi_{mb}^{m'k_{m'}z'} \rangle \|^2 \right) } && (8.12) \\
&\leq \frac{1}{|\mathcal{T}|} \mathop{\mathbb{E}}_{k} \sqrt{ \sum_{z,z',m,m'} |\alpha_{zm}|^2 |\alpha_{z'm'}|^2 \cdot \left(\sum_{a,b} |\beta_{ab}^{mk_m z}|^2 \cdot \| |\phi_{ab}^{mk_m z} \rangle \|^2 \right) \left(\sum_{a,b} |\beta_{ab}^{m'k_{m'}z'}|^2 \cdot \| |\phi_{ab}^{m'k_{m'}z'} \rangle \|^2 \right) } && (8.13)
\end{aligned}$$

$$\leq \frac{1}{|\mathcal{T}|} \mathop{\mathbb{E}}_{k} \sqrt{\sum_{z,z',m,m'} |\alpha_{zm}|^2 |\alpha_{z'm'}|^2 \cdot 2} \tag{8.14}$$

$$\leq \sqrt{2}\frac{|\mathcal{M}|}{|\mathcal{T}|}. \tag{8.15}$$

In the last line, we used the fact that the dimension of the span of the $|\varphi_z\rangle$'s is at most $|\mathcal{M}|$. A similar calculation will show that $|\xi_2| \leq \sqrt{2}|\mathcal{M}|/|\mathcal{T}|$ as well. Putting everything together, we get that

$$\left| \mathop{\mathbb{E}}_{k} \langle \tau_{k,err} | \tau_{k,err} \rangle \right| \leq (1 + 3\sqrt{2})|\mathcal{M}|/|\mathcal{T}|.$$

This implies that

$$\|\tau - \tau_{ideal}\|_1 \leq 3\sqrt{6/|\mathcal{T}|}.$$

Recall that we have ignored the final projector P that the real adversary $\mathcal{E}$ may have applied after applying the unitary V. Since P acts on $\mathcal{Z}$ only, it commutes with the verification operation, and thus we have that

$$\|P\tau P^\dagger - P\tau_{ideal}P^\dagger\|_1 \leq 3\sqrt{6/|\mathcal{T}|}.$$

where $P\tau P^\dagger = \mathbb{E}_k\, |k\rangle\langle k| \otimes \mathsf{Ver}_k \circ \mathcal{E} \circ \mathsf{Auth}_k(\rho^{\mathcal{MZ}})$, the true final state of the protocol.

Finally, we have to argue that $P\tau_{ideal}P^\dagger$ is actually equal to $\mathbb{E}_k\, |k\rangle\langle k| \otimes \mathsf{Ver}_k \circ \mathcal{I} \circ \mathsf{Auth}_k(\rho^{\mathcal{MZ}})$ for some computational basis-respecting adversary $\mathcal{I}$. The ideal adversary behaves as follows when given the $\mathcal{YZ}$ registers of $\sigma^{\mathcal{KYZ}}$:

1. The adversary prepares auxiliary registers $\mathcal{M}'\mathcal{T}'\mathcal{Z}_2$ in the $|0\cdots 0\rangle$ state. The $\mathcal{Y}' = \mathcal{M}'\mathcal{T}'$ registers are isomorphic to $\mathcal{MT}$, and $\mathcal{Z}_2$ is a qubit register.

2. First the ideal adversary makes a copy of the $\mathcal{MT}$ registers in the computational basis and coherently stores the copy in auxiliary registers $\mathcal{M}'\mathcal{T}'$.

3. The ideal adversary then applies the original adversary unitary V to registers $\mathcal{M}'\mathcal{T}'\mathcal{Z}$.

4. The adversary checks whether the values of the $\mathcal{MT}$ and $\mathcal{M}'\mathcal{T}'$ registers are the same in the computational basis; if so, the $\mathcal{Z}_2$ qubit is set to $|0\rangle$, and the $\mathcal{M}'\mathcal{T}'$ registers are set to $|0\cdots 0\rangle$. Otherwise, it is kept at $|1\rangle$. In other words, the basis vector $|m,t,m',t',0\rangle^{\mathcal{MTM}'\mathcal{T}'\mathcal{Z}_2}$ is mapped to $|m,t,0\cdots 0\rangle^{\mathcal{MTM}'\mathcal{T}'\mathcal{Z}_2}$ iff $m = m'$ and $t = t'$.

5. The adversary measures the $\mathcal{Z}_2$ qubit register, and the $\mathcal{Z}$ register using the POVM element $\{P, \mathbb{I} - P\}$, and accepts only on outcome $|0\rangle$ for $\mathcal{Z}_2$ and P for $\mathcal{Z}$.

Observe that this ideal attack $\mathcal{I}$ can be implemented as

$$\mathcal{I} : \sigma^{\mathcal{YZ}} \mapsto \mathrm{Tr}_{\mathcal{Y}'\mathcal{Z}_2}\left((P \otimes |0\rangle\langle 0|^{\mathcal{Z}_2}) V_{ideal} \sigma^{\mathcal{YZ}} V_{ideal}^\dagger (P \otimes |0\rangle\langle 0|^{\mathcal{Z}_2}) \right)$$

where V_{ideal} is an isometry mapping the space $\mathcal{YZ}$ to the space $\mathcal{YY}'\mathcal{ZZ}_2$, $P \otimes |0\rangle\langle 0|^{\mathcal{Z}_2}$ is a projector acting on $\mathcal{ZZ}_2$, and $\mathrm{Tr}_{\mathcal{Y}'\mathcal{Z}_2}(\cdot)$ is the partial trace over system $\mathcal{Y}'\mathcal{Z}_2$. Furthermore, V_{ideal} is an isometry that leaves the $\mathcal{MT}$ registers unchanged, and hence is a computational basis-respecting adversary. Since $P\tau_{ideal}^{\mathcal{KYZ}}P^\dagger = \mathsf{Ver}\left(\mathcal{I}(\sigma^{\mathcal{KYZ}})\right)$, and this holds for every adversary and every input state, this implies that (Auth, Ver) is $O(\sqrt{M/T})$-authenticating relative to the computational basis.

□

Finally, we note that [53] claim that the Carter-Wegman MAC is quantum universally composable. However, it appears to be lacking some formal details, and it isn't clear that it correctly handles the case when the messages are authenticated in superposition, or when the adversary has quantum side information.

8.8 Total authentication (with key leakage) from complementary classical authentication

In the previous section, we saw how the classical Carter-Wegman message authentication scheme is still secure even when used on a superposition of messages, and even if the adversary has access to quantum side information about the messages. Here, we will show that using the Carter-Wegman scheme as a primitive, we obtain *total quantum state authentication,* which implies encryption of the quantum state.

The quantum state authentication scheme is simple: the sender authenticates the message state using the Carter-Wegman MAC in the computational basis, and then authenticates again in the Fourier basis (using a new key). To verification procedure is the reverse of this: the receiver first checks the outer authentication, performs the inverse Fourier transform, and then checks the inner authentication. We call this the "Auth-QFT-Auth" scheme. This is pleasingly analogous to the quantum one-time pad (QOTP), which encrypts quantum data using the classical one-time pad in complementary bases. However, the QOTP does not have authentication properties.

There is one slight caveat: we show that Auth-QFT-Auth achieves total authentication *with key leakage*. That is, we argue that conditioned on the receiver verification succeeding, the effect of an arbitrary adversary is to have ignored the authenticated state, and only act on the adversary's side information, in a manner that may depend on the key used for the second authentication (what we call the "outer key"). In other words, we sacrifice the secrecy of the outer key, but in exchange we get complete quantum state encryption.

8.8.1 The Auth-QFT-Auth scheme

Let $|\rho\rangle^{\mathcal{MZ}} = \sum_m \alpha_m |m\rangle^{\mathcal{M}} \otimes |\varphi_m\rangle^{\mathcal{Z}}$ be the initial message state, where $\mathcal{Z}$ is held by the adversary. Again, it will be advantageous to rewrite this state in terms of the Schmidt decomposition:

$$|\rho\rangle^{\mathcal{MZ}} = \sum_z \sqrt{\lambda_z} \left(\sum_m \alpha_{zm} |m\rangle^{\mathcal{M}} \right) \otimes |\varphi_z\rangle^{\mathcal{Z}}$$

where for $z \neq z'$, we have $\langle \varphi_z | \varphi_{z'} \rangle = 0$, and the λ_z's are nonnegative numbers summing to 1. Furthermore, the dimension of the span of $\{ |\varphi_z\rangle \}_z$ is at most $|\mathcal{M}|$.

The authentication scheme is the composed operation $\mathsf{Auth}_2(H^{\otimes N}(\mathsf{Auth}_1(\rho)))$, where Auth_1 is the *inner* authentication scheme that uses key k, $H^{\otimes N}$ is the quantum Fourier transform over $\mathbb{Z}_2$, and Auth_2 is the *outer* authentication that uses key h. The keys k and h are independent.

The inner authentication scheme Auth_1 maps $\mathcal{M}$ to $\mathcal{Y}_1 = \mathcal{M}\mathcal{T}_1$. We define $N = |\mathcal{Y}_1|$. H is the single-qubit Hadamard unitary, and the Fourier transform $H^{\otimes N}$ acts on $\mathcal{Y}_1$. The outer authentication scheme Auth_2 maps $\mathcal{Y}_1$ to $\mathcal{Y}_2 = \mathcal{M}\mathcal{T}_1\mathcal{T}_2$. The keys k and h live in the registers $\mathcal{K}$ and $\mathcal{H}$, respectively. The evolution of the initial message state is as follows:

1. **Inner authentication**. When the inner authentication key (henceforth called the *inner key*) is k, the state becomes

$$\sum_z \sqrt{\lambda_z} \left(\sum_m \alpha_{zm} |m, k(m)\rangle^{\mathcal{Y}_1} \right) \otimes |\varphi_z\rangle^{\mathcal{Z}}$$

2. **Fourier transform over $\mathbb{Z}_2$**: Let $\{|x\rangle\}$ be a basis for $\mathcal{Y}_1$. Then:

$$\frac{1}{\sqrt{N}} \sum_z \sqrt{\lambda_z} \left(\sum_{m,x} \alpha_{zm} (-1)^{(m,k(m))\cdot x} |x\rangle^{\mathcal{Y}_1} \right) \otimes |\varphi_z\rangle^{\mathcal{Z}}.$$

3. **Outer authentication**. The outer key is denoted by h. The final authenticated state is then

$$|\sigma_{kh}\rangle^{\mathcal{Y}\mathcal{T}_2\mathcal{Z}} = \frac{1}{\sqrt{N}} \sum_z \sqrt{\lambda_z} \left(\sum_{m,x} \alpha_{zm} (-1)^{(m,k(m))\cdot x} |x, h(x)\rangle^{\mathcal{Y}_1\mathcal{T}_2} \right) \otimes |\varphi_z\rangle^{\mathcal{Z}}$$

   where $\mathcal{T}_2$ is the space of the tag $h(x)$.

Let

$$\sigma^{\mathcal{K}\mathcal{H}\mathcal{Y}_1\mathcal{T}_2\mathcal{Z}} = \mathop{\mathbb{E}}_{kh} |kh\rangle\langle kh|^{\mathcal{K}\mathcal{H}} \otimes |\sigma_{kh}\rangle\langle\sigma_{kh}|^{\mathcal{Y}_1\mathcal{T}_2\mathcal{Z}}.$$

The adversary is then given the $\mathcal{Y}_1\mathcal{T}_2$ registers of σ, and performs a general unitary attack V that acts on $\mathcal{Y}_1\mathcal{T}_2\mathcal{Z}$:

$$\tilde{\sigma}^{\mathcal{K}\mathcal{H}\mathcal{Y}_1\mathcal{T}_2\mathcal{Z}} = V\sigma V^{\dagger}.$$

Let $\tilde{\tau}^{\mathcal{K}\mathcal{H}\mathcal{M}\mathcal{Z}} = \mathsf{Auth}_1^{-1} \circ \mathsf{Ver}_1 \circ \mathrm{QFT}^{-1} \circ \mathsf{Auth}_2^{-1} \circ \mathsf{Ver}_2(\tilde{\sigma})$.

Let the inner authentication scheme be the 3-wise independent hashing QMAC with tag length $\log T$, and message length $\log M$. Let the outer authentication scheme be a QMAC that ε-authenticates with respect to the computational basis.

The Auth-QFT-Auth scheme can potentially leak some bits of the outer key h, but we will show that this is the *only* thing that is leaked; otherwise, it is performs total authentication (and hence encryption).

Theorem 109 (Security of the Auth-QFT-Auth scheme). *The Auth-QFT-Auth scheme is δ-totally authenticating with outer key leakage, where $\delta = \varepsilon + O(\sqrt{|\mathcal{M}|^{3/2}/|\mathcal{T}_1|})$.*

Again before starting the proof we consider the key requirements. The outer authentication scheme need not be a Carter-Wegman MAC, but let's assume that it is. In order to achieve δ-total authentication, the inner MAC must be such that $|\mathcal{M}|^{3/2}/|\mathcal{T}_1| \leq O(\delta^2)$, or in other words, $\log|\mathcal{T}_1| \geq \frac{3}{2}\log|\mathcal{M}| + 2\log\frac{1}{\delta} + O(1)$. The key needed for the inner MAC must be at least $\frac{9}{2}\log|\mathcal{M}| + 6\log\frac{1}{\delta} + O(1)$. The "message length" that is given to the outer MAC is $\log|\mathcal{M}| + \log|\mathcal{T}_1| \geq \frac{5}{2}\log|\mathcal{M}| + 2\log\frac{1}{\delta} + O(1)$, and thus $\log|\mathcal{T}_2| \geq \frac{5}{2}\log|\mathcal{M}| + 4\log\frac{1}{\delta} + O(1)$. The key length for the outer MAC needs to be at least $\frac{15}{2}\log|\mathcal{M}| + 12\log\frac{1}{\delta} + O(1)$, so the total key needed is $12\log|\mathcal{M}| + 18\log\frac{1}{\delta} + O(1)$.

While the inner key can be recycled (upon successful verification), the outer key unfortunately cannot be.

Proof. We will let $M = |\mathcal{M}|, T = |\mathcal{T}_1|$, and $N = MT = |\mathcal{Y}_1|$. We will assume that $M^{3/2} \leq T$; otherwise the theorem statement is vacuous.

Suppose the outer authentication scheme was ε-secure. By definition, there exists an ideal computational basis adversary $\mathcal{I}$ such that $\|\mathsf{Ver}_2(\widetilde{\sigma}) - \mathsf{Ver}_2(\mathcal{I}(\sigma))\|_1 \leq \varepsilon$, where Ver_2 denotes the verification procedure for the outer authentication scheme. There exists a computational basis-respecting linear map $\Lambda \in \mathrm{L}(\mathcal{Y}_2\mathcal{Z})$ such that

$$\mathcal{I} : \sigma \mapsto \Lambda\sigma\Lambda^\dagger.$$

Since Λ is computational basis-respecting, we have for all (x, s, z):

$$\Lambda|x,s\rangle^{\mathcal{Y}_1\mathcal{T}_2} \otimes |\varphi_z\rangle^{\mathcal{Z}} = |x,s\rangle^{\mathcal{Y}_1\mathcal{T}_2} \otimes |\phi_{xsz}\rangle^{\mathcal{Z}}.$$

for some collection of (not necessarily normalized) states $\{|\phi_{xsz}\rangle\}$.

Therefore the effect of the adversary on the authenticated state (after verification) is to be close to $\mathcal{I}(\sigma) = \mathbb{E}_{k,h}\, |kh\rangle\langle kh| \otimes |\tau_{kh}\rangle\langle\tau_{kh}|$ where for fixed inner/outer keys k, h

$$|\tau_{kh}\rangle = \frac{1}{N}\sum_z \sqrt{\lambda_z} \sum_{m,x} \alpha_{zm}(-1)^{(m,k(m))\cdot x}|x\rangle \otimes |\phi_{xh_xz}\rangle.$$

Thus, the final state that Bob has, after performing full (i.e. inner and outer) verification, is ε-close to

$$\mathop{\mathbb{E}}_{k,h} |kh\rangle\langle kh| \otimes |\mu_{kh}\rangle\langle\mu_{kh}|$$

where

$$|\mu_{kh}\rangle = \sum_z \sqrt{\lambda_z} \sum_m \left(\frac{1}{N} \sum_{x,m'} \alpha_{zm'}(-1)^{(m+m',k(m)+k(m'))\cdot x} \right) |m\rangle \otimes |\phi_{xh_xz}\rangle.$$

Then security of Auth-QFT-Auth is established if we show that for every h,

$$\mathop{\mathbb{E}}_{k} \| |\mu_{kh}\rangle - |\nu_h\rangle \|^2$$

is small, where

$$|\nu_h\rangle^{\mathcal{M}\mathcal{Z}} = \sum_z \sqrt{\lambda_z} \sum_m \alpha_{zm}|m\rangle^{\mathcal{M}} \otimes |\eta_{hz}\rangle^{\mathcal{Z}}$$

with $|\eta_{hz}\rangle^{\mathcal{Z}} = \frac{1}{N}\sum_x |\phi_{xh_xz}\rangle^{\mathcal{Z}}$. Assuming this, the next Lemma will show that there is an ideal oblivious, but outer key-dependent, adversary whose actions lead to the global state $\mathbb{E}_{kh}\, |kh\rangle\langle kh| \otimes |\nu_h\rangle\langle\nu_h|$.

Lemma 110 (Constructing the ideal oblivious adversary). *For all h there exists an ideal oblivious adversary $\mathcal{I}_h$ acting on $\mathcal{Z}$ only such that*

$$|\nu_h\rangle\langle\nu_h|^{\mathcal{M}\mathcal{Z}} = \mathcal{I}_h(|\rho\rangle\langle\rho|^{\mathcal{M}\mathcal{Z}}).$$

Proof. We now construct an ideal adversary $\mathcal{I}_h$, derived from the computational basis adversary $\mathcal{I}$. By definition of $\mathcal{I}$, there exists a computational basis-respecting isometry

$V \in \mathrm{J}(\mathcal{Y}_2\mathcal{Z}, \mathcal{Y}_2\mathcal{Z}\mathcal{Y}_2'\mathcal{Z}_2)$ where $\mathcal{Y}_2'$ is an auxiliary register isomorphic to $\mathcal{Y}_2$, and $\mathcal{Z}_2$ is an auxiliary qubit register, such that

$$\mathcal{I} : \sigma^{\mathcal{Y}\mathcal{Z}} \mapsto \mathrm{Tr}_{\mathcal{Y}'\mathcal{Z}_2}\left(\Pi V \sigma^{\mathcal{Y}\mathcal{Z}} V^{\dagger} \Pi\right).$$

Here $\Pi = P \otimes |0\rangle\langle 0|^{\mathcal{Z}_2}$ for some projector P acting on $\mathcal{Z}$. Furthermore, V is computational basis respecting:

$$\Pi V |x,s\rangle^{\mathcal{Y}_2} \otimes |\varphi_z\rangle^{\mathcal{Z}} = |x,s\rangle^{\mathcal{Y}_2} \otimes |\phi_{xsz}\rangle^{\mathcal{Z}} \otimes |0\cdots 0\rangle^{\mathcal{Y}_2'\mathcal{Z}_2}$$

where the $|\phi_{xsz}\rangle^{\mathcal{Z}}$ were defined above.

Now we construct the ideal general adversary $\mathcal{I}_h$ as follows:

1. First, the adversary creates the entangled state $|\Phi_h\rangle^{\mathcal{A}\mathcal{A}'} = \frac{1}{\sqrt{N}}\sum_x |x, h(x)\rangle^{\mathcal{A}} |x, h(x)\rangle^{\mathcal{A}'}$ in new registers $\mathcal{A} \otimes \mathcal{A}'$, which are isomorphic to $\mathcal{Y}_2 \otimes \mathcal{Y}_2$, and $\{|x\rangle\}$ is a basis for $\mathcal{Y}_1$.

2. It then applies the unitary V to half of $|\Phi_h\rangle^{\mathcal{A}\mathcal{A}'}$ that resides in $\mathcal{A}$, and the $\mathcal{Z}$ part of the input state $|\rho\rangle$.

3. The adversary measures $\mathcal{A}\mathcal{A}'\mathcal{Z}\mathcal{Z}_2$ using the projective measurement $\{Q, \mathbb{I} - Q\}$, where $Q = |\Phi_h\rangle\langle\Phi_h|^{\mathcal{A}\mathcal{A}'} \otimes \Pi$. The adversary discards the outcome corresponding to $\mathbb{I} - Q$, and leaves the state unnormalized:

$$\frac{1}{N}\sum_{z,x,m} \sqrt{\lambda_z}\alpha_{zm}|m\rangle^{\mathcal{M}} |\phi_{xsz}\rangle^{\mathcal{Z}} |\Phi\rangle^{\mathcal{A}\mathcal{A}'} |0\cdots 0\rangle^{\mathcal{Y}_2'\mathcal{Z}_2}$$

4. The adversary discards the $\mathcal{A}\mathcal{A}'\mathcal{Y}_2'\mathcal{Z}_2$ registers:

$$\frac{1}{N}\sum_{z,x,m} \sqrt{\lambda_z}\alpha_{zm}|m\rangle^{\mathcal{M}} \otimes |\phi_{xsz}\rangle^{\mathcal{Z}}$$

This is precisely the state $|\nu_h\rangle$, and the $\mathcal{I}_h$ only interacts with $\mathcal{Z}$ and auxiliary registers in the adversary's control, so it is an ideal general adversary. □

We now turn to bounding $\mathbb{E}_k \, \| |\mu_{kh}\rangle - |\nu_h\rangle \|^2$:

$$\begin{aligned}
&\mathop{\mathbb{E}}_{k} \| |\mu_{kh}\rangle - |\nu_h\rangle \|^2 \\
&= \frac{1}{N^2} \mathop{\mathbb{E}}_{k} \sum_{m,z,z'} \sqrt{\lambda_z \lambda_{z'}} \sum_{\substack{x',x'',m',m'' \\ m \notin \{m',m''\}}} \overline{\alpha}_{z'm'}\alpha_{zm''}(-1)^{(m+m',k(m)+k(m'))\cdot x'}(-1)^{(m+m'',k(m)+k(m''))\cdot x''}\langle\phi^h_{x'z'}|\phi^h_{x''z}\rangle \\
&= \frac{1}{N^2} \sum_{\substack{m,z,z' \\ x',x'',m',m'' \\ m \notin \{m',m''\}}} \sqrt{\lambda_z \lambda_{z'}}\overline{\alpha}_{z'm'}\alpha_{zm''}(-1)^{(m+m')\cdot x_1' + (m+m'')\cdot x_2''}\langle\phi^h_{x'z'}|\phi^h_{x''z}\rangle \mathop{\mathbb{E}}_{k}(-1)^{(k(m)+k(m'))\cdot x_2'}(-1)^{(k(m)+k(m''))\cdot x_2''}.
\end{aligned}$$

We use the abbreviation $|\phi^h_{xz}\rangle = |\phi_{xh_xz}\rangle$. In the second line, we divided x into two parts (x_1, x_2), where x_1 corresponds to $\mathcal{M}$, and x_2 corresponds to $\mathcal{T}_1$. We focus on the expectation $\chi_{m,m',m'',x_2',x_2''} = \mathbb{E}_k(-1)^{(k(m)+k(m'))\cdot x_2'}(-1)^{(k(m)+k(m''))\cdot x_2''}$. We consider two cases:

Case 1: $m' = m'', m' \neq m$. Then $\chi_{m,m',m'',x'_2,x''_2} = 0$ if $x'_2 \neq x''_2$, otherwise $\chi_{m,m',m'',x'_2,x''_2} = 1$.

$$
\begin{aligned}
&\frac{1}{N^2}\left| \sum_{\substack{z,z',x',x'' \\ m,m':m\neq m'}} \sqrt{\lambda_z\lambda_{z'}}\overline{\alpha}_{z'm'}\alpha_{zm'}(-1)^{(m+m')\cdot(x'_1+x''_1)}\langle\phi^h_{x'z'}|\phi^h_{x''z}\rangle\chi_{m,m',m',x',x''}\right| \\
&= \frac{1}{N^2}\left| \sum_{\substack{z,z',x',x''_1 \\ m,m':m\neq m'}} \sqrt{\lambda_z\lambda_{z'}}\overline{\alpha}_{z'm'}\alpha_{zm'}(-1)^{(m+m')\cdot(x'_1+x''_1)}\langle\phi^h_{x'z'}|\phi^h_{x''_1x'_2z}\rangle\right| \\
&\leq \frac{1}{N^2}\sum_{z,z'}\sqrt{\lambda_z\lambda_{z'}}\sqrt{\sum_{m\neq m'}\left|\sum_{x',x''_1}(-1)^{(m+m')\cdot(x'_1+x''_1)}\langle\phi^h_{x'z'}|\phi^h_{x''_1x'_2z}\rangle\right|^2} \qquad \text{(Cauchy-Schwarz)} \\
&\leq \frac{1}{N^2}\sum_{z,z'}\sqrt{\lambda_z\lambda_{z'}}\sqrt{\sum_{m,m'}\sum_{x',x''_1,\widetilde{x}',\widetilde{x}''_1}(-1)^{(m+m')\cdot(x'_1+x''_1+\widetilde{x}'_1+\widetilde{x}''_1)}\langle\phi^h_{\widetilde{x}''_1\widetilde{x}'_2z}|\phi^h_{\widetilde{x}'z'}\rangle\langle\phi^h_{x'z'}|\phi^h_{x''_1x'_2z}\rangle} \\
&= \frac{1}{N^2}\sum_{z,z'}\sqrt{\lambda_z\lambda_{z'}}\sqrt{M^2\sum_{\substack{x',x''_1,\widetilde{x}',\widetilde{x}''_1 \\ x'_1+x''_1+\widetilde{x}'_1+\widetilde{x}''_1=0}}\langle\phi^h_{\widetilde{x}''_1\widetilde{x}'_2z}|\phi^h_{\widetilde{x}'z'}\rangle\langle\phi^h_{x'z'}|\phi^h_{x''_1x'_2z}\rangle} \\
&\leq \frac{1}{N^2}\sum_{z,z'}\sqrt{\lambda_z\lambda_{z'}}\sqrt{M^3N^2} \\
&\leq \frac{M^{5/2}}{N} \qquad \text{(at most } M\ z\text{'s)} \\
&= \frac{M^{3/2}}{T}.
\end{aligned}
$$

Case 2: m, m', m'' **are all distinct.** Then $\chi_{m,m',m'',x'_2,x''_2} = 0$ unless $x'_2 = x''_2 = 0$, in which case $\chi_{m,m',m'',x'_2,x''_2} = 1$. This uses the three-independence of $k(\cdot)$.

$$
\begin{aligned}
&\frac{1}{N^2}\left| \sum_{\substack{z,z',x',x'' \\ m,m',m''\text{ distinct}}} \sqrt{\lambda_z\lambda_{z'}}\overline{\alpha}_{z'm'}\alpha_{zm'}(-1)^{(m+m')\cdot x'_1+(m+m'')\cdot x''_1}\langle\phi^h_{x'z'}|\phi^h_{x''z}\rangle\chi_{m,m',m'',x',x''}\right| \\
&= \frac{1}{N^2}\left| \sum_{\substack{z,z',x'_1,x''_1 \\ m,m',m''\text{ distinct}}} \sqrt{\lambda_z\lambda_{z'}}\overline{\alpha}_{z'm'}\alpha_{zm'}(-1)^{(m+m')\cdot x'_1+(m+m'')\cdot x''_1}\langle\phi^h_{x'_10z'}|\phi^h_{x''_10z}\rangle\right| \\
&\leq \frac{1}{N^2}\sum_{z,z'}\sqrt{\lambda_z\lambda_{z'}}\sqrt{\sum_{m,m',m''\text{ distinct}}\left|\sum_{x'_1,x''_1}(-1)^{(m+m')\cdot x'_1+(m+m'')\cdot x''_1}\langle\phi^h_{x'_10z'}|\phi^h_{x''_10z}\rangle\right|^2} \qquad \text{(Cauchy-Schwarz)} \\
&\leq \frac{M^{9/2}}{N^2} \\
&\leq \frac{M^{3/2}}{T}
\end{aligned}
$$

where we used the fact that $M^{3/2} \leq T$. Therefore, for every h we have

$$\mathop{\mathbb{E}}_{k} \| |\mu_{kh}\rangle - |\nu_h\rangle \|^2 = O(M^{3/2}/T)$$

as desired. Using Jensen's inequality, $\mathbb{E}_{kh} \| |\mu_{kh}\rangle\langle\mu_{kh}| - |\nu_h\rangle\langle\nu_h| \| \leq O(\sqrt{M^{3/2}/T})$.

Thus, the final state of Bob is $\varepsilon + O(\sqrt{M^{3/2}/T})$-close to

$$\mathop{\mathbb{E}}_{kh} |kh\rangle\langle kh| \otimes |\nu_h\rangle\langle\nu_h| = \mathop{\mathbb{E}}_{kh} |kh\rangle\langle kh| \otimes \mathcal{I}_h(|\rho\rangle\langle\rho|)$$

where $\mathcal{I}_h$ are the ideal adversaries given by Lemma 110.

□

8.9 Total authentication from approximate unitary designs

We now present a scheme that satisfies the strongest security definition, that of total authentication (without *any* key leakage). In particular, this implies complete reuse of the entire key. This property of complete reuse of the key was not known before; it is not known whether the entire key can be reused in the authentication scheme of Barnum, et al [9].

This scheme is based on *unitary designs*, which are in some sense the quantum analogue of t-wise independent hash functions: a t-unitary design (also simply called a *t-design*) is a distribution $\mathscr{D}$ over unitary matrices such that degree t polynomials cannot distinguish between a unitary drawn from $\mathscr{D}$ and a fully random unitary. Furthermore, there are constructions of efficient unitary designs [20].

8.9.1 The unitary design scheme

We call this scheme the *unitary design scheme*. Let s be a security parameter. The input state is $|\rho\rangle^{\mathcal{MZ}}$, where the $\mathcal{Z}$ register is held by the adversary.

1. The sender Alice first appends s $|0\rangle$ qubits in an auxiliary $\mathcal{T}$ register.
2. Using her secret key k, Alice samples a random unitary U_k drawn from an (approximate) unitary t-design that acts jointly on $\mathcal{M} \otimes \mathcal{T}$. We will set the parameter $t = 4$.
3. Alice applies U_k to the $\mathcal{M} \otimes \mathcal{T}$ register, and sends $\mathcal{M} \otimes \mathcal{T}$ across the quantum channel to Bob.
4. Bob receives some state, and applies the inverse unitary $U_k^\dagger$ to it. He measures the last s qubits and accepts if they all measure to be 0. Otherwise he rejects.

Theorem 111. *The unitary design scheme is efficiently computable, and is $2^{-s/2}$-totally authenticating.*

This is very similar to the *non-malleable quantum encryption scheme* proposed by Ambainis, Bouda, and Winter [5]. A quantum encryption scheme is non-malleable if, in addition to revealing no information about the state to an eavesdropper, the eavesdropper cannot effect any controlled modifications to the encrypted state. Ambainis, Bouda and Winter show that applying a random unitary drawn from a 2-design to a state will encrypt it, and reduces the adversary to one that either forwards the state, or replaces it with the maximally mixed state. Clearly, such a scheme does not provide any authentication, but our scheme, where one additionally appends some dummy zeroes before authenticating, provides *both* encryption and authentication. Furthermore, their analysis does not handle the case of quantum side information, and it only gives a security guarantee *on average* over the key. Here, we will show that we obtain authentication and encryption *with high probability* over the key.

The key requirements of this scheme are rather significant, as constructions of approximate unitary 4-designs acting on n qubits involve choosing a random quantum circuit of size $\Theta(n^2)$, and thus the randomness required is at least $\Omega(n^2)$ [20]. Furthermore, this scheme requires a full-fledged quantum computer running for at least $\Omega(n)$ sequential time steps. However we feel that this scheme is conceptually simple ("To encrypt and authenticate quantum data, apply a random quantum circuit for a while"), and it also confers the benefit that the *entire key* can be reused (upon successful verification), something that was not known before. We also believe that our analysis of this scheme may be of independent interest.

Notation and useful lemmas. We set up some notation. We let $\mathcal{M}$ denote the message space, $\mathcal{T}$ to denote the space of the dummy zero qubits. We let $\mathcal{Y} = \mathcal{M} \otimes \mathcal{T}$. We let $M = |\mathcal{M}|$, $|\mathcal{T}| = 2^s$, and $N = M2^s = |\mathcal{Y}|$.

Let $\mathcal{E}$ be an adversary acting on $\mathcal{Y} \otimes \mathcal{Z}$. By the Stinespring representation theorem, there exists a unitary V acting on a possibly larger space $\mathcal{Y} \otimes \mathcal{Z} \otimes \mathcal{Z}'$, followed by a projection P that acts on $\mathcal{Z}\mathcal{Z}'$, followed by a partial trace over $\mathcal{Z}'$. However without loss of generality we shall simply treat this additional space $\mathcal{Z}'$ as part of $\mathcal{Z}$, and ignore the partial trace operation. Thus, the adversary's action is to perform some unitary V on $\mathcal{Y} \otimes \mathcal{Z}$, followed by a projection on P on $\mathcal{Z}$.

To analyze the behavior of this scheme, we will first analyze the case when the randomizing unitary U is drawn from the Haar measure over the unitary group $U(\mathcal{Y})$, rather from a t-design. We will show that this scheme is totally authenticating. Then, we will show that actually using a $O(1)$-unitary design will suffice.

The crucial hammer we will need is a version of *Levy's Lemma*:

Definition 112. *A function $f : U(d) \to \mathbb{R}$ is η-Lipschitz if*

$$\sup_{U_1,U_2 \in U(d)} \frac{|f(U_1) - f(U_2)|}{\|U_1 - U_2\|_2} \leq \eta.$$

Lemma 113 (Levy's Lemma [77]). *Let $f : U(d) \to \mathbb{R}$ be an η-Lipschitz function on the unitary group of dimension d with mean $\mathbb{E} f$. Then*

$$\Pr\left(\left|f - \mathbb{E} f\right| \geq \delta\right) \leq 4 \exp\left(-\frac{Cd\delta^2}{\eta^2}\right)$$

where $C = 2/9\pi^3$ and the probability is over U drawn from the Haar measure on $U(d)$.

Another useful lemma we will need is the following, giving two formulas for averaging over the (Haar measure of the) unitary group. We use δ_{ij} to denote the Dirac delta function that is 1 if $i = j$ and 0 otherwise.

Lemma 114 (Appendix B.5 of [13]). *For a function $f : \mathrm{U}(d) \to \mathbb{R}$, we let $\langle f \rangle$ to denote $\int f(U)\, dU$, where $\int \cdot dU$ is integration over the Haar measure on $\mathrm{U}(d)$. Then*

$$\begin{aligned}\langle U_{ab}U_{ij}U^*_{a'b'}U^*_{i'j'}\rangle = {} & \frac{1}{d^2-1}(\delta_{aa'}\delta_{bb'}\delta_{ii'}\delta_{jj'} + \delta_{ai'}\delta_{bj'}\delta_{ia'}\delta_{jb'}) \\ & - \frac{1}{d(d^2-1)}(\delta_{aa'}\delta_{bj'}\delta_{ii'}\delta_{jb'} + \delta_{ai'}\delta_{bb'}\delta_{ia'}\delta_{jj'})\end{aligned}$$

8.9.2 Total authentication with Haar-random unitaries

We now prove that the unitary design scheme yields total authentication. Let $\Lambda_U = \langle 0|^{\otimes s} U^\dagger V U |0\rangle^{\otimes s}$ is be a map from $\mathcal{M} \otimes \mathcal{Z}$ to $\mathcal{M} \otimes \mathcal{Z}$.

Lemma 115. *Let $N = \dim(\mathcal{Y})$. For all $\delta > 0$, for all initial message states $|\rho\rangle^{\mathcal{M}\mathcal{Y}}$ have that*

$$\Pr_U \left(\|\Gamma_V|\rho\rangle - \Lambda_U|\rho\rangle\|_2^2 \geq 2^{-s} + \delta \right) \leq \exp(-C'N\delta^2)$$

where $\Gamma_V = \mathrm{Tr}_{\mathcal{Y}}(V)/\dim(\mathcal{Y})$, C' is a universal constant, and U is a Haar-random unitary.

Proof. First, we write $|\rho\rangle^{\mathcal{M}\mathcal{Y}} = \sum_x \rho_x |x\rangle^{\mathcal{M}} \otimes |\varphi_x\rangle^{\mathcal{Z}}$ where $\{|x\rangle\}$ is a basis for $\mathcal{M}$, and $\{|\varphi_x\rangle\}$ are arbitrary unit vectors in $\mathcal{Z}$.

Write U as the following:

$$U = \sum_{u,x} |\psi_{u,x}\rangle\langle u, x|$$

where $|u\rangle \in \mathcal{T}, |x\rangle \in \mathcal{M}$ are standard basis vectors, and $\{|\psi_{u,x}\rangle\} \subset \mathcal{T} \otimes \mathcal{M}$ is a set of orthonormal unit vectors. Then $U|0\rangle^{\otimes s}$ becomes a linear operator that accepts vectors in $\mathcal{M}$ and outputs vectors in $\mathcal{Y} = \mathcal{T} \otimes \mathcal{M}$:

$$U|0\rangle^{\otimes s} = \sum_x |\psi_{0^s,x}\rangle\langle x|$$

We will simply write $|\psi_x\rangle$ to denote $|\psi_{0^s,x}\rangle$. We can write Λ_U as

$$\Lambda_U = \sum_{x,x'} |x'\rangle\langle x|\ \langle \psi_{x'}|V|\psi_x\rangle.$$

Let's compute the average operator

$$\begin{aligned}\int \Lambda_U\, dU &= \sum_{x,x'} |x\rangle\langle x'| \int \langle \psi_x|V|\psi_{x'}\rangle\, dU && (8.16)\\ &= \sum_x |x\rangle\langle x| \int \langle \psi_x|V|\psi_x\rangle\, dU + \sum_{x \neq x'} |x\rangle\langle x'| \int \langle \psi_x|V|\psi_{x'}\rangle\, dU && (8.17)\\ &= \sum_x |x\rangle\langle x| \otimes \frac{1}{\dim(\mathcal{Y})}\mathrm{Tr}_{\mathcal{Y}}(V) && (8.18)\\ &= \mathbb{I}^{\mathcal{M}} \otimes \Gamma_V && (8.19)\end{aligned}$$

The second term in (8.17) (the sum over off-diagonal elements) averages to 0, because for $x \neq x'$, the vectors $|\psi_{x'}\rangle$ and $|\psi_x\rangle$ are random orthogonal unit vectors. Conditioned on a fixing of $|\psi_x\rangle$, for any vector $|\varphi\rangle$ that is orthogonal to $|\psi_x\rangle$, $|\psi_{x'}\rangle$ is equally likely to be $|\varphi\rangle$ or $-|\varphi\rangle$, so $\int \langle \psi_{x'}|V|\psi_x\rangle\, dU = 0$.

In the last step we used the fact that given an operator X mapping $\mathcal{Y} \otimes \mathcal{Z}$ to $\mathcal{Y} \otimes \mathcal{Z}$, if we average over the unit sphere, $\int (\langle \psi|^{\mathcal{Y}} \otimes \mathbb{I}^{\mathcal{Z}}) X (|\psi\rangle^{\mathcal{Y}} \otimes \mathbb{I}^{\mathcal{Z}})\ d\psi$ is equal to the partial trace $\mathrm{Tr}_{\mathcal{Y}}(X)/\dim(\mathcal{Y})$. We'll let N denote $\dim(\mathcal{Y})$.

Thus, this tells us that on average, this operator should act as the identity on $\mathcal{M}$ and some linear map (not necessarily unitary) Γ_V on $\mathcal{Z}$. We now prove that Λ_U behaves this way on $|\rho\rangle$ with high probability. Define

$$f(U) = \| \Gamma_V |\rho\rangle - \Lambda_U |\rho\rangle \|_2^2.$$

Bounding the average of f. Expanding f and averaging, we get

$$\int f(U)\ dU = \int \left((\langle \rho | \Gamma_V^\dagger - \langle \rho | \Lambda_U^\dagger)(\Gamma_V |\rho\rangle - \Lambda_U |\rho\rangle) \right) dU \tag{8.20}$$

$$= \int \langle \rho | \Gamma_V^\dagger \Gamma_V |\rho\rangle - \langle \rho | \Lambda_U^\dagger \Gamma_V |\rho\rangle - \langle \rho | \Gamma_V^\dagger \Lambda_U |\rho\rangle + \langle \rho | \Lambda_U^\dagger \Lambda_U |\rho\rangle\ dU \tag{8.21}$$

$$= -\langle \rho | \Gamma_V^\dagger \Gamma_V |\rho\rangle + \int \langle \rho | \Lambda_U^\dagger \Lambda_U |\rho\rangle\ dU \tag{8.22}$$

where in the last line we used our calculation of $\int \Lambda_U\ dU$ above. We bound this last term. We have that

$$\Lambda_U |\rho\rangle = \sum_{x,x'} \rho_{x'} |x\rangle\ \langle \psi_x | V(|\psi_{x'}\rangle \otimes |\varphi_{x'}\rangle)$$

Thus

$$\int \langle \rho | \Lambda_U^\dagger \Lambda_U |\rho\rangle\ dU = \int \sum_{x,x',x''} \rho_{x'} \rho_{x''}^* ((\langle \psi_{x''}| \otimes \langle \varphi_{x''}|) V^\dagger |\psi_x\rangle \langle \psi_x | V(|\psi_{x'}\rangle \otimes |\varphi_{x'}\rangle))\ dU \tag{8.23}$$

$$= \sum_{x'} |\rho_{x'}|^2 \sum_x \int ((\langle \psi_{x'}| \otimes \langle \varphi_{x'}|) V^\dagger |\psi_x\rangle \langle \psi_x | V(|\psi_{x'}\rangle \otimes |\varphi_{x'}\rangle))\ dU \tag{8.24}$$

$$= \sum_{x'} |\rho_{x'}|^2 \sum_x \int \| \langle \psi_x | V(|\psi_{x'}\rangle \otimes |\varphi_{x'}\rangle) \|_2^2\ dU \tag{8.25}$$

$$= \sum_{x'} |\rho_{x'}|^2 \sum_{x \neq x'} \int \| \langle \psi_x | V(|\psi_{x'}\rangle \otimes |\varphi_{x'}\rangle) \|_2^2\ dU + \tag{8.26}$$

$$\sum_x |\rho_x|^2 \int \| \langle \psi_x | V(|\psi_x\rangle \otimes |\varphi_x\rangle) \|_2^2\ dU. \tag{8.27}$$

Let $\{|z\rangle\}$ be a basis for $\mathcal{Z}$. Now notice that

$$\| \langle \psi_x | V(|\psi_{x'}\rangle \otimes |\varphi_{x'}\rangle) \|_2^2 = \| \sum_z |z\rangle\langle z|^{\mathcal{Z}}\ \langle \psi_x | V(|\psi_{x'}\rangle \otimes |\varphi_{x'}\rangle) \|_2^2 \tag{8.28}$$

$$= \sum_z |((\langle \psi_x | \otimes \langle z|) V(|\psi_{x'}\rangle \otimes |\varphi_{x'}\rangle))|^2. \tag{8.29}$$

Write $|\varphi_x'\rangle = \sum_z \beta_{x'z} |z\rangle$. Then we have

$$|((\langle \psi_x | \otimes \langle z|) V(|\psi_{x'}\rangle \otimes |\varphi_{x'}\rangle))|^2 = \left| \sum_{z'} \beta_{x'z'} ((\langle \psi_x | \otimes \langle z|) V(|\psi_{x'}\rangle \otimes |z'\rangle)) \right|^2 \tag{8.30}$$

$$= \left|\sum_{z'} \beta_{x'z'} \sum_{ij} V_{(i,z),(j,z')} U^*_{ix} U_{jx'}\right|^2 \tag{8.31}$$

$$= \sum_{z',z''} \beta_{x'z'} \beta^*_{x'z''} \sum_{iji'j'} V_{(i,z),(j,z')} V^*_{(i',z),(j',z'')} U_{i'x} U_{jx'} U^*_{ix} U^*_{j'x'} \tag{8.32}$$

where the rows and columns of V are indexed by (i,z) and (j,z'), respectively. Again, we identify $|\psi_x\rangle$ as the x'th column of U, and U_{ix} denotes the i'th entry of $|\psi_x\rangle$.

We now go back to bound the sum over $x \neq x'$ in (8.27). Fix x, x' such that $x \neq x'$. Substituting (8.32) in and using Lemma 114, we get:

$$\int \| \langle \psi_{x'} | V(|\psi_x\rangle \otimes |\varphi_{x'}\rangle) \|_2^2 \, dU \tag{8.33}$$

$$= \int \sum_{z,z',z''} \beta_{x'z'} \beta^*_{x'z''} \sum_{iji'j'} V_{(i,z),(j,z')} V^*_{(i',z),(j',z'')} U_{i'x} U_{jx'} U^*_{ix} U^*_{j'x'} \, dU \tag{8.34}$$

$$= \sum_{z',z''} \beta_{x'z'} \beta^*_{x'z''} \left[\frac{1}{N^2-1} \sum_{ijz} V_{(i,z),(j,z')} V^*_{(i,z),(j,z'')} - \frac{1}{N(N^2-1)} \sum_{ii'z} V_{(i,z),(i,z')} V^*_{(i',z),(i',z'')} \right] \tag{8.35}$$

$$= \frac{N}{N^2-1} - \frac{1}{N(N^2-1)} \sum_{z',z''} \beta_{x'z'} \beta^*_{x'z''} \sum_{ii'z} V_{(i,z),(i,z')} V^*_{(i',z),(i',z'')} \tag{8.36}$$

$$= \frac{N}{N^2-1} - \frac{1}{N(N^2-1)} \sum_z \left| \sum_{z',i} \beta_{x',z'} V_{(i,z),(i,z')} \right|^2 \tag{8.37}$$

$$\leq \frac{N}{N^2-1} \tag{8.38}$$

where we used the fact that V is unitary and that $\sum_{z'} |\beta_{x'z'}|^2 = 1$. Summing (8.38) over all $x \neq x'$, we get

$$\sum_{x'} |\rho_{x'}|^2 \sum_{x \neq x'} \int \| \langle \psi_x | V(|\psi_{x'}\rangle \otimes |\varphi_{x'}\rangle) \|_2^2 \, dU \leq \sum_{x'} |\rho_{x'}|^2 \sum_{x \neq x'} \frac{N}{N^2-1} = \frac{N(M-1)}{N^2-1}.$$

Now fix an x; we bound the second term of (8.27). Using Lemma 114 again, we have

$$\int \| \langle \psi_x | V(|\psi_x\rangle \otimes |\varphi_x\rangle) \|_2^2 \, dU \tag{8.39}$$

$$= \sum_{z,z',z''} \beta_{xz'} \beta^*_{xz''} \int \sum_{iji'j'} V_{(i,z),(j,z')} V^*_{(i',z),(j',z'')} U_{i'x} U_{jx'} U^*_{ix} U^*_{j'x'} \, dU \tag{8.40}$$

$$= \left[\frac{1}{N^2-1} - \frac{1}{N(N^2-1)} \right] \cdot \left[\sum_z \left| \sum_{z',i} \beta_{x',z'} V_{(i,z),(i,z')} \right|^2 + N \right] \tag{8.41}$$

$$= \frac{1}{N(N+1)} \cdot \left[\sum_z \left| \sum_{z',i} \beta_{x',z'} V_{(i,z),(i,z')} \right|^2 + N \right] \tag{8.42}$$

Putting everything together, we can bound (8.27) by

$$\int \langle\rho|\Lambda_U^\dagger\Lambda_U|\rho\rangle \; dU \leq \frac{N(M-1)}{N^2-1} + \frac{1}{N(N+1)} \cdot \left[\sum_z \left|\sum_{z',i} \beta_{x',z'} V_{(i,z),(i,z')}\right|^2 + N\right] \tag{8.43}$$

$$= \frac{NM-1}{N^2-1} + \frac{1}{N(N+1)} \sum_z \left|\sum_{z',i} \beta_{x',z'} V_{(i,z),(i,z')}\right|^2 . \tag{8.44}$$

We have to compare this to $\langle\rho|\Gamma_V^\dagger\Gamma_V|\rho\rangle = \||\Gamma_V|\rho\rangle\|_2^2$. We expand $\Gamma_V|\rho\rangle$:

$$\Gamma_V|\rho\rangle = \frac{1}{N}\mathrm{Tr}_{\mathcal{Y}}(V)|\rho\rangle \tag{8.45}$$

$$= \frac{1}{N}\sum_{i,z} |z\rangle^{\mathcal{Z}} \langle i,z|V|i\rangle \left(\sum_{x,z'} \rho_x\beta_{xz'}|x\rangle^{\mathcal{M}} \otimes |z'\rangle^{\mathcal{Z}}\right) \tag{8.46}$$

$$= \frac{1}{N}\sum_{x,z} \rho_x|x,z\rangle^{\mathcal{M}\mathcal{Z}} \left(\sum_{i,z'} \beta_{xz'}\langle i,z|V|i,z'\rangle\right) \tag{8.47}$$

$$= \frac{1}{N}\sum_{x,z} \rho_x|x,z\rangle^{\mathcal{M}\mathcal{Z}} \left(\sum_{i,z'} \beta_{xz'} V_{(i,z),(i,z')}\right) \tag{8.48}$$

So therefore

$$\langle\rho|\Gamma_V^\dagger\Gamma_V|\rho\rangle = \frac{1}{N^2}\sum_z \left|\sum_{z',i} \beta_{x',z'} V_{(i,z),(i,z')}\right|^2 .$$

This shows that our desired average of f is small:

$$\int f(U) \; dU \leq \frac{NM-1}{N^2-1}.$$

Bounding the Lipschitz constant of f. We compute the Lipschitz continuity of f in parts. Let $g(U) = \langle\rho|\Gamma_V^\dagger\Lambda_U|\rho\rangle$, where $|\rho\rangle = \sum_x \rho_x|x\rangle \otimes |\varphi_x\rangle$. Expanding, we get

$$g(U) = \langle\rho|(\mathbb{I}^{\mathcal{Y}} \otimes \Gamma_V^\dagger) \sum_{x,x'} |x\rangle\langle x'| \otimes \langle\psi_x|V|\psi_{x'}\rangle|\rho\rangle \tag{8.49}$$

$$= \sum_{x,x'} \rho_x^*\rho_{x'}(\langle\psi_x| \otimes \langle\varphi_x|)\Gamma_V^\dagger V(|\psi_{x'}\rangle \otimes |\varphi_{x'}\rangle) \tag{8.50}$$

$$= \left(\sum_x \rho_x^*\langle\psi_x| \otimes \langle\varphi_x|\right) \Gamma_V^\dagger V \left(\sum_x \rho_x|\psi_x\rangle \otimes |\varphi_x\rangle\right) \tag{8.51}$$

$$= \langle\theta|\Gamma_V^\dagger V|\theta\rangle \tag{8.52}$$

where we used that $\Gamma_V^\dagger$ is an operator that acts on $\mathcal{Z}$ only, and we define $|\theta\rangle = \sum_x \rho_x|\psi_x\rangle \otimes |\varphi_x\rangle$. Thus for two unitaries $U, \hat{U}$, we have

$$|g(U) - g(\hat{U})| = |\langle\theta|\Gamma_V^\dagger V|\theta\rangle - \langle\hat{\theta}|\Gamma_V^\dagger V|\hat{\theta}\rangle| \tag{8.53}$$

$$= \left|\mathrm{Tr}\left(\Gamma_V^\dagger V(|\theta\rangle\langle\theta| - |\hat{\theta}\rangle\langle\hat{\theta}|)\right)\right| \tag{8.54}$$

$$\leq \left\|\Gamma_V^\dagger V\right\|_\infty \cdot \|\,|\theta\rangle\langle\theta| - |\hat{\theta}\rangle\langle\hat{\theta}|\,\|_1 \tag{8.55}$$

where in the inequality we used Hölder's inequality for matrices: $\mathrm{Tr}(AB) \leq \|A\|_\infty \|B\|_1$. Now, the operator norm is submultiplicative, so $\|\Gamma_V^\dagger V\|_\infty \leq \|\Gamma_V^\dagger\|_\infty \cdot \|V\|_\infty \leq \|\Gamma_V^\dagger\|_\infty$, because V is a unitary and hence its operator norm is 1. But then $\|\Gamma_V^\dagger\|_\infty = \frac{1}{N}\|\sum_y \langle y|V|y\rangle\|_\infty \leq \frac{1}{N}\sum_y \|\langle y|V|y\rangle\|_\infty$, because the operator norm satisfies the triangle inequality. Here, $|y\rangle$ is a basis element of $\mathcal{Y}$, and $\langle y|V|y\rangle$ is an operator that maps $\mathcal{Z}$ to $\mathcal{Z}$. For each y, we can bound $\|\langle y|V|y\rangle\|_\infty \leq 1$. This implies that $|g(U) - g(\hat{U})| \leq \|\,|\theta\rangle\langle\theta| - |\hat{\theta}\rangle\langle\hat{\theta}|\,\|_1$.

Thus the Lipschitz constant of g can be bounded by

$$\eta_g \leq \sup_{U,\hat{U}} \frac{2\|\,|\theta\rangle - |\hat{\theta}\rangle\,\|_2}{\|U - \hat{U}\|_2}.$$

Since the columns of $U, \hat{U}$ are $|\psi_{u,x}\rangle$ and $|\hat{\psi}_{u,x}\rangle$, the denominator $\|U - \hat{U}\|_2$ can be written as $\sqrt{\sum_{u,x}\|\,|\psi_{u,x}\rangle - |\hat{\psi}_{u,x}\rangle\|_2^2}$. Notice that the numerator only depends on the column vectors $|\psi_{0^s,x}\rangle = |\psi_x\rangle$ and $|\hat{\psi}_{0^s,x}\rangle = |\hat{\psi}_x\rangle$, so the denominator can be minimized to to be $\sqrt{\sum_x \|\,|\psi_x\rangle - |\hat{\psi}_x\rangle\|_2^2}$ without affecting the numerator. The numerator can be bounded as

$$\|\sum_x \rho_x(|\psi_x\rangle \otimes |\varphi_x\rangle - |\hat{\psi}_x\rangle \otimes |\varphi_x\rangle)\|_2 \leq \sum_x |\rho_x| \cdot \|\,|\psi_x\rangle \otimes |\varphi_x\rangle - |\hat{\psi}_x\rangle \otimes |\varphi_x\rangle\|_2 \tag{8.56}$$

$$\leq \sqrt{\sum_x |\rho_x|^2 \sum_x \|\,|\psi_x\rangle - |\hat{\psi}_x\rangle\|_2^2} \tag{8.57}$$

$$= \sqrt{\sum_x \|\,|\psi_x\rangle - |\hat{\psi}_x\rangle\|_2^2} \tag{8.58}$$

where in the first line we used the triangle inequality, and in the second line we used Cauchy-Schwarz. Thus the Lipschitz constant of g is at most 2.

Now we bound the Lipschitz continuity of $h(U) = \langle\rho|\Lambda_U^\dagger\Lambda_U|\rho\rangle$. We have that

$$h(U) = \sum_{x,x',x''} \rho_{x'}\rho_{x''}^*(\langle\psi_{x''}| \otimes \langle\varphi_{x''}|)V^\dagger|\psi_x\rangle\langle\psi_x|V(|\psi_{x'}\rangle \otimes |\varphi_{x'}\rangle) \tag{8.59}$$

$$= \sum_x \langle\theta|V^\dagger|\psi_x\rangle\langle\psi_x|V|\theta\rangle \tag{8.60}$$

$$= \mathrm{Tr}\left(\sum_x |\psi_x\rangle\langle\psi_x|V|\theta\rangle\langle\theta|V^\dagger\right) \tag{8.61}$$

where $|\theta\rangle$ is the same as above. Let $\Pi_U = \sum_x |\psi_x\rangle\langle\psi_x|$. Therefore

$$|h(U) - h(\hat{U})| = \left|\mathrm{Tr}\left(\Pi_U V|\theta\rangle\langle\theta|V^\dagger - \Pi_{\hat{U}} V|\hat{\theta}\rangle\langle\hat{\theta}|V^\dagger\right)\right| \tag{8.62}$$

$$= \left|\mathrm{Tr}\left(\Pi_U V\left(|\theta\rangle\langle\theta| - |\hat{\theta}\rangle\langle\hat{\theta}|\right)V^\dagger + (\Pi_U - \Pi_{\hat{U}})V|\hat{\theta}\rangle\langle\hat{\theta}|V^\dagger\right)\right| \tag{8.63}$$

$$\leq \left\|\,|\theta\rangle\langle\theta| - |\hat{\theta}\rangle\langle\hat{\theta}|\,\right\|_1 + \left|\langle\hat{\theta}|V^\dagger(\Pi_U - \Pi_{\hat{U}})V|\hat{\theta}\rangle\right| \tag{8.64}$$

$$\leq \left\|\,|\theta\rangle\langle\theta| - |\hat{\theta}\rangle\langle\hat{\theta}|\,\right\|_1 + \|\Pi_U - \Pi_{\hat{U}}\|_\infty \tag{8.65}$$

where in the first inequality we use that $\Pi_U = \Pi_U \cdot \Pi_U$ is a projector, and that $\mathrm{Tr}(\Pi X) \leq$

$\|X\|_1$ for all operators X and $-\mathbb{I} \le \Pi \le \mathbb{I}$. The second term can be bounded by

$$\|\Pi_U - \Pi_{\hat{U}}\|_\infty = \sup_{|v\rangle} \|(\Pi_U - \Pi_{\hat{U}})|v\rangle\|_2 \tag{8.66}$$

$$= \sup_{|v\rangle} \left\| \sum_x (|\psi_x\rangle - |\hat{\psi}_x\rangle)(\langle\psi_x|v\rangle - \langle\hat{\psi}_x|v\rangle) \right\|_2 \tag{8.67}$$

$$\le \sup_{|v\rangle} \sum_x \| |\psi_x\rangle - |\hat{\psi}_x\rangle \|_2 \cdot |\langle\psi_x|v\rangle - \langle\hat{\psi}_x|v\rangle)| \tag{8.68}$$

$$\le \sup_{|v\rangle} \sum_x (|\langle\psi_x|v\rangle| + |\langle\hat{\psi}_x|v\rangle|) \cdot \| |\psi_x\rangle - |\hat{\psi}_x\rangle \|_2 \tag{8.69}$$

$$\le \sup_{|v\rangle} \sqrt{\sum_x |\langle\psi_x|v\rangle|^2 \sum_x \| |\psi_x\rangle - |\hat{\psi}_x\rangle \|_2^2} + \sqrt{\sum_x |\langle\hat{\psi}_x|v\rangle|^2 \sum_x \| |\psi_x\rangle - |\hat{\psi}_x\rangle \|_2^2} \tag{8.70}$$

$$\le 2\sqrt{\sum_x \| |\psi_x\rangle - |\hat{\psi}_x\rangle \|_2^2}. \tag{8.71}$$

Therefore the Lipschitz constant η_h of h is at most 4, so the Lipschitz constant η of f is at most 8.

Now we invoke Levy's Lemma once more, and we obtain

$$\Pr\left(\|\Gamma_V|\rho\rangle - \Lambda_U|\rho\rangle\|_2^2 \ge \delta\right) \le 4\exp\left(-\frac{CN\delta^2}{\eta^2}\right) \tag{8.72}$$

$$\le 4\exp\left(-C'M^2/N\right) \tag{8.73}$$

where $\delta = 2M/N$ and C' is some universal constant.

□

8.9.3 Constructing the ideal oblivious adversary

Now we demonstrate that the map $|\rho\rangle^{\mathcal{MZ}} \mapsto \Gamma_V|\rho\rangle^{\mathcal{MZ}}$ can be implemented by an ideal oblivious adversary.

Consider the following ideal adversary, which given a state $|\sigma\rangle^{\mathcal{YZ}}$ performs the following:

1. First, the adversary creates a maximally entangled state $|\Phi\rangle^{\mathcal{Y}'\mathcal{Y}''} = \frac{1}{\sqrt{N}}\sum_y |yy\rangle^{\mathcal{Y}'\mathcal{Y}''}$ in new registers $\mathcal{Y}' \otimes \mathcal{Y}''$.

2. It then applies the unitary V to half of $|\Phi\rangle^{\mathcal{Y}'\mathcal{Y}''}$ that resides in $\mathcal{Y}'$, and the $\mathcal{Z}$ part of $|\sigma\rangle^{\mathcal{YZ}}$. The state currently looks like:

$$\frac{1}{\sqrt{N}}\sum_y (\mathbb{I}^{\mathcal{Y}} \otimes V^{\mathcal{Z}\mathcal{Y}'})|\sigma\rangle^{\mathcal{YZ}} \otimes |yy\rangle^{\mathcal{Y}'\mathcal{Y}''} \tag{8.74}$$

$$= \frac{1}{\sqrt{N}}\sum_y (\mathbb{I}^{\mathcal{Y}} \otimes \mathbb{I}^{\mathcal{Y}'\mathcal{Y}''} \otimes V^{\mathcal{Z}\mathcal{Y}'})|\sigma\rangle^{\mathcal{YZ}} \otimes |yy\rangle^{\mathcal{Y}'\mathcal{Y}''} \tag{8.75}$$

$$= \frac{1}{\sqrt{N}}\sum_{y,y'} (\mathbb{I}^{\mathcal{Y}} \otimes \langle y'|^{\mathcal{Y}'} V^{\mathcal{Z}\mathcal{Y}'} |y\rangle^{\mathcal{Y}'})|\sigma\rangle^{\mathcal{YZ}} \otimes |y'y\rangle^{\mathcal{Y}'\mathcal{Y}''} \tag{8.76}$$

3. The adversary projects $\mathcal{Y}'\mathcal{Y}''$ using the projector $|\Phi\rangle\langle\Phi|^{\mathcal{Y}'\mathcal{Y}''}$ (and leaves the state unnormalized):
$$\frac{1}{N}\sum_{y}(\mathbb{I}^{\mathcal{Y}} \otimes \langle y|^{\mathcal{Y}'} V^{\mathcal{Z}\mathcal{Y}'} |y\rangle^{\mathcal{Y}'})|\sigma\rangle^{\mathcal{Y}\mathcal{Z}} \otimes |\Phi\rangle^{\mathcal{Y}'\mathcal{Y}''}$$

4. The adversary discards the $\mathcal{Y}'\mathcal{Y}''$ register:
$$\frac{1}{N}\sum_{y}(\mathbb{I}^{\mathcal{Y}} \otimes \langle y|^{\mathcal{Y}'} V^{\mathcal{Z}\mathcal{Y}'} |y\rangle^{\mathcal{Y}'})|\sigma\rangle^{\mathcal{Y}\mathcal{Z}}$$

This is precisely the state $\Gamma_V|\sigma\rangle^{\mathcal{Y}\mathcal{Z}}$, and the adversary described above never touches the $\mathcal{Y}$ register, so it is ideal.

8.9.4 Derandomizing the analysis using approximate unitary designs

The analysis of this scheme is nearly complete; however, the main missing component is that the analysis above assumes that the authentication scheme uses a truly random unitary U to scramble the message state and the tag. Unfortunately, sampling a truly random unitary on n qubits and applying it is infeasible: only a vanishing fraction of unitaries are succinctly describable or are efficiently computable.

The authentication scheme instead samples a unitary from a *unitary design*, discussed earlier. These are efficiently sampleable, efficiently computable ensembles of unitaries that are *pseudorandom*: they fool polynomials of low degree.

It won't be necessary to present formal definitions of a unitary design; we will use them in a black box manner. We will appeal to a general derandomization result of Low who proved that, if one establishes a measure of concentration result for a low degree polynomial f that's evaluated on a Haar-random unitary, then it still satisfies (nearly) the same measure of concentration when f is evaluated on a unitary drawn from an approximate t-design. More formally:

Theorem 116 ([71]). *Let $f : U(N) \to \mathbb{R}$ be a polynomial of degree K. Let $f(U) = \sum_i \alpha_i M_i(U)$ where $M_i(U)$ are monomials and let $\alpha(f) = \sum_i |\alpha_i|$. Suppose that f has probability concentration*
$$\Pr_{U\sim\nu_{Haar}}(|f-\mu| \geq \delta) \leq C\exp(-a\delta^2)$$
and let μ be an ε-approximate unitary t-design. Then
$$\Pr_{U\sim\mu}(|f-\mu| \geq \delta) \leq \frac{1}{\delta^{2m}}\left(C\left(\frac{m}{a}\right)^m + \varepsilon(\alpha+|\mu|)^{2m}\right)$$
for integer m with $2mK \leq t$.

Furthermore, there exist efficient constructions of approximate t-unitary designs, for any t.

Theorem 117 ([20]). *For every ε, t, and n, there exists a finite set of unitaries $D_{\varepsilon,t,n} \subset U(N)$ for $N = 2^n$, and a probability distribution $\mu_{\varepsilon,t,n}$ over $D_{\varepsilon,t,n}$ such that*

1. *$\mu_{\varepsilon,t,n}$ is an ε-approximate t-unitary design.*

2. *$\mu_{\varepsilon,t,n}$ can be sampled from in* $\mathrm{poly}(n, t, \log 1/\varepsilon)$ *time*

3. *Each unitary $U \in D_{\varepsilon,t,n}$ can be implemented by a quantum circuit acting on n qubits of size at most $O(n\log(4t)^2t^9(2nt+\log(1/\varepsilon)))$.*

We combine these two theorems to prove our final result:

Theorem 118 (Restatement of Theorem 111). *The unitary design scheme is efficiently computable, and is $2^{-s/2}$-totally authenticating.*

Proof. Note that $f(U)$ is a polynomial of degree 4 in the entries of U. We compute $\alpha(f)$ by computing $\alpha(f_0)$, $\alpha(g)$, and $\alpha(h)$ where $f_0 = \langle\rho|\Gamma_V^\dagger\Gamma_V|\rho\rangle$ is a constant, $g(U) = \langle\rho|\Gamma_V^\dagger\Lambda_U|\rho\rangle$, and $h(U) = \langle\rho|\Lambda_U^\dagger\Lambda_U|\rho\rangle$. Clearly, $\alpha(f) \le \alpha(f_0) + 2\alpha(g) + \alpha(h)$.

Since f_0 is a constant function, $\alpha(f_0)$ is at most $|f_0| \le 1$. We turn to g. Let $\{|x\rangle\}$ be a basis for $\mathcal{M}$. Then for x, x', define the operator $T^{xx'} = \langle\varphi_x|\Gamma_V^\dagger V|\varphi_{x'}\rangle$ to be the linear operator that maps $\mathcal{Y}$ to $\mathcal{Y}$ (recall that $|\rho\rangle = \sum_x \rho_x|x\rangle \otimes |\varphi_x\rangle$). Then,

$$g(U) = \sum_{x,x'} \rho_x^*\rho_{x'}\langle\psi_x|T^{xx'}|\psi_{x'}\rangle \tag{8.77}$$

$$= \sum_{x,x',y,y'} \rho_x^*\rho_{x'}T_{yy'}^{xx'}U_{yx}^*U_{y'x'} \tag{8.78}$$

For every x, x', y, y', we have a distinct monomial $U_{yx}^*U_{y'x'}$, and the corresponding coefficient is $\rho_x^*\rho_{x'}T_{yy'}^{xx'}$, which has absolute value at most 1. Therefore $\alpha(g) \le M^2N^2$.

Now we turn to $h(U)$. Recall that

$$h(U) = \sum_{x',x''} \rho_{x'}^*\rho_{x''}\sum_x(\langle\psi_{x'}| \otimes \langle\varphi_{x'}|)V^\dagger|\psi_x\rangle\langle\psi_x|V(|\psi_{x''}\rangle \otimes |\varphi_{x''}\rangle) \tag{8.79}$$

$$= \sum_{i,j,x',x''} \rho_{x'}^*\rho_{x''}U_{ix'}^*U_{jx''}\sum_x(\langle i| \otimes \langle\varphi_{x'}|)V^\dagger|\psi_x\rangle\langle\psi_x|V(|j\rangle \otimes |\varphi_{x''}\rangle) \tag{8.80}$$

where $|\psi_x\rangle = \sum_i U_{ix}|i\rangle$, $|\psi_{x'}\rangle = \sum_i U_{ix'}|i\rangle$ and $|\psi_{x''}\rangle = \sum_j U_{jx''}|j\rangle$. Define $|\tau^{ix'}\rangle = V|i\rangle \otimes |\varphi_{x'}\rangle$ and $|\tau^{jx''}\rangle = V|j\rangle \otimes |\varphi_{x''}\rangle$. Then we have

$$h(U) = \sum_{i,j,i',j'}\sum_{x,x',x''} U_{ix'}^*U_{jx''}U_{i'x}U_{j'x}^*\rho_{x'}^*\rho_{x''}\langle\tau^{ix'}|i'\rangle\langle j'|\tau^{jx''}\rangle \tag{8.81}$$

$$= \sum_{i,j,i',j'}\sum_{x,x',x''} U_{ix'}^*U_{jx''}U_{i'x}U_{j'x}^*\rho_{x'}^*\rho_{x''}\sum_z(\tau_{i'z}^{ix'})^*\ \tau_{j'z}^{jx''} \tag{8.82}$$

where we alternatively write $|\tau^{ix'}\rangle = \sum_z \tau_{i'z}^{ix'}|i', z\rangle$ and $|\tau^{jx''}\rangle = \sum_z \tau_{j'z}^{jx''}|j', z\rangle$. For every choice of i, j, i', j', x, x', x'', we have a distinct monomial, and the associated coefficient has norm at most

$$|\rho_{x'}^*\rho_{x''}\sum_z(\tau_{i'z}^{ix'})^*\ \tau_{j'z}^{jx''}|^2 \le \left(\sum_z|\tau_{i'z}^{ix'}|^2\right)\cdot\left(\sum_z|\tau_{j'z}^{jx''}|^2\right) \le 1.$$

Thus $\alpha(h)$ is at most M^3N^4. This implies that $\alpha(f) \le O(N^7)$.

Now we are ready to leverage Theorems 116 and 117. in Lemma 115 we proved that function $f(U) = \|\Gamma_V|\rho\rangle - \Gamma_U|\rho\rangle\|_2^2$ has probability concentration

$$\Pr_{U\sim\nu_{Haar}}(|f-\mu| \ge \delta) \le 4\exp(-CN\delta^2)$$

where C is a universal constant. Thus our parameters are:

1. (Average of f) $\mu = M/N$
2. (Error in probability concentration) $\delta = \sqrt{M/N}$
3. (Degree of f) $K = 4$
4. (Probability concentration exponent) $a = CN$
5. (Norm of f) $\alpha(f) = O(N^7)$

We will set $m = 1$, $\varepsilon = N^{-17}$, and $t = 8$.

By Theorem 117, there exists a distribution $\mu_{\varepsilon,t,n}$ over unitaries acting on n qubits that forms an efficiently computable ε-approximate t-unitary design. Then, plugging everything into Theorem 116, we have that

$$\Pr_{U \sim \mu_{\varepsilon,t,n}} (f \geq M/N + \sqrt{M/N}) \leq O(1/M) \tag{8.83}$$

Note that $M/N = 2^{-s}$. □

Appendix A

Communication with non-local boxes, and a simple proof of the Nayak-Salzman Theorem

The work presented in this Appendix was conducted with Xiaodi Wu.

A.1 Introduction

The most fundamental question in information theory is: "*How much information can be conveyed from one party to another, given some finite communication resource?*". The central resource considered by classical information theory is the one-way communication channel, with which Alice can transmit (potentially noisy) bits to Bob. Quantum information theory addresses this fundamental question when Alice and Bob are allowed to use quantum resources to communicate, such as the ability to send qubits, or use shared quantum entanglement. At first, one might hope that quantum resources might confer significant savings in communication costs over classical resources. Indeed, in the interactive communication setting (where both Alice and Bob can speak), there are cases when quantum protocols can solve a communication task much more efficiently than any classical protocol.

However, when the communication task is simply for Alice to transmit a classical message (say a uniformly random n-bit string) to Bob, quantum resources do not help. Holevo's famous theorem [57] implies that, in the one-way communication scenario (without preshared entanglement), for Bob for correctly decode Alice's input string with probability greater than p, Alice must send at least $pn - h(p)$ qubits, where $h(\cdot)$ is the binary entropy function. Nayak and Salzman significantly strengthen this bound [81] and show that if Alice and Bob engage in a two-way communication protocol (possibly with preshared entanglement), Alice is required to send at least $\frac{1}{2}(n - \log 1/p)$ qubits for Bob to recover Alice's input string with probability p – the amount of communication from Bob to Alice is completely irrelevant! Their proof uses a characterization of two-way quantum communication protocols by Kremer and Yao [70, 103], and separately handles the case when there is preshared entanglement versus when there is none.

In this note, we give a simple proof of their bound by showing that it is a consequence of the fact the *Non-signaling Principle*, which states that non-local correlations between space-like separated parties cannot be used to transmit messages faster than the speed of light. Non-local correlations that arise from quantum theory are non-signaling, but the converse is not true: there are non-local correlations (such as those maximally violating the CHSH bound) that are not explainable via quantum theory [14]. Recently, physicists and computer scientists have been studying the consequences of the Non-signaling Principle without appealing to a specific physical theory such as quantum mechanics (see, e.g., [85, 94]). Although the Non-signaling Principle is a weaker assumption on Nature, it turns out that many non-trivial information processing tasks are still possible, such as certified randomness expansion and delegated computation.

Here, we further this agenda by defining a general model of communication between two parties who are allowed to take advantage of non-local resources (such as Popescu-Rohrlich boxes). As long as these non-local resources are governed by the Non-signaling Principle, we show that they cannot be used to reliably transmit an n-bit message with less than n bits of communication.

Other related work. The idea of using super-quantum non-local correlations in a communication protocol can be traced back to van Dam's result showing that Popescu-Rohrlich (PR) boxes make communication complexity trivial: armed with PR boxes, Alice and Bob can compute any boolean function $f(x,y)$ (where x and y are inputs to Alice and Bob, respectively) with only one bit of communication [94]! Brassard, et al. showed that with "noisy" PR boxes (i.e. boxes that can work with probability $\approx$ 90.8%), this result still holds [21]. Recently, Navascues, et al. studied a set of super-quantum multipartite correlations called $\tilde{Q}$, and showed that one-way communication complexity of the Inner Product function on n bits is $\Omega(n)$, even if Alice and Bob are allowed to take advantage of correlations from $\tilde{Q}$ [80]. To prove this, they reduce to such an Inner Product protocol to a one-way protocol using non-signaling correlations where Bob guesses Alice's input string $x \in \{0,1\}^n$, and show that since the latter requires n bits of communication, and the former also requires $\Omega(n)$ bits of communication. Their proof of the latter fact is essentially the same as our Theorem 120.

Independently, [51] proves a special case of the result of [81] when the Alice and Bob are restricted to using classical communication (but can use any amount of shared entanglement).

A.2 Preliminaries and Model

A.2.1 Communication with non-local boxes

We formally define our model of *communication with non-local boxes*. A *non-signaling device* $\mathcal{D} = (\mathcal{A}, \mathcal{B})$ is a bipartite device, where $\mathcal{A}$ takes input u and outputs a $\mathcal{B}$ takes input y and outputs b, and there is a non-signaling probability distribution $\mathsf{P}_{AB|UV}(a,b|u,v)$ that describes the input/output behavior of the devices[1].

In this model, Alice and Bob communicate in rounds. In each round $i \geq 1$, Alice and Bob use a non-signaling device $\mathcal{D}_i = (\mathcal{A}_i, \mathcal{B}_i)$, where Alice operates $\mathcal{A}_i$ and Bob operates

[1] A bipartite conditional probability distribution $\mathsf{P}_{AB|UV}(a,b|u,v)$ is non-signaling if and only if for all a, b in the support of u, v,

$$\mathsf{P}_{A|U,V}(a|u,v) = \mathsf{P}_{A|U}(a|u) \quad \text{and} \quad \mathsf{P}_{B|U,V}(b|u,v) = \mathsf{P}_{B|V}(b|v).$$

$\mathcal{B}_i$. $\mathcal{A}_i$ takes two inputs: a_i and m_i^B, and outputs a pair (a_{i+1}, m_{i+1}^A). Similarly, $\mathcal{B}_i$ takes two inputs: b_i and m_{i+1}^A, and outputs a pair (b_{i+1}, m_{i+1}^B). One should think of a_i and b_i as "states" of Alice and Bob, respectively, and m_i^A and m_i^B as messages from Alice and Bob, respectively. In round i, Alice will execute A_i on input (a_i, m_i^B), where a_i is output by A_{i-1}, and m_i^B is output by B_{i-1} (if $i = 1$, then a_i can be Alice's external input, and m_1^B can be empty). $\mathcal{A}_i$ outputs (a_{i+1}, m_{i+1}^A). Then Bob will execute $\mathcal{B}_i$ on input (b_i, m_{i+1}^A), and produces output (b_{i+1}, m_{i+1}^B). This concludes the ith round. If the communication protocol has r rounds, then we declare the pair (m_{r+1}^A, m_{r+1}^B) as the output of the protocol.

For brevity, we will sometimes call this model *non-local communication*. This next theorem shows that our model of non-local communication is general enough to simulate any two-way quantum communication protocol. We consider the most general model of (noiseless) two-way quantum communication: Alice and Bob are allowed to share an arbitrary entangled state at the beginning of the communication protocol, and during the protocol they exchange qubits over a (noiseless) quantum channel. At the end of the protocol, Alice and Bob make a local measurement on their quatum state (which includes their portion of the shared entanglement, as well as the qubits they received over the communication channel), and they output their measurement outcomes a and b, respectively. If Alice and Bob take external inputs x and y, respectively, then there is some conditional probability distribution $\mathsf{P}_{AB|XY}(a, b|x, y)$ – which we call the input/output distribution of the protocol – describing the behavior of the protocol.

We say a communication protocol P simulates another protocol Q (which may use a different model of communication than P's) if their input/output distributions are identical.

Theorem 119. *Two-way quantum communication protocols can be simulated by communication with non-local boxes, with a factor* 2 *increase in communication complexity.*

Proof. Let Q be a two-way quantum communication protocol with prior shared entanglement. We first convert this to a quantum protocol Q' where all the communication is classical. This can be done using quantum teleportation, which uses twice as many bits of communication as qubits transmitted in Q. We perform a round-by-round simulation of Q' with a non-local communication protocol P, where in round i Alice and Bob use a non-local device $\mathcal{D}_i = (\mathcal{A}_i, \mathcal{B}_i)$ with the following behavior: Alice's box $\mathcal{A}_i$ will take input (a_i, m_i^B), where m_i^B is Bob's message from the previous round (empty if $i = 1$), and a_i is the Alice's view of the communication transcript of Q' up to round i, as well as her external input. Bob's box $\mathcal{B}_i$ has the symmetric input format. Together, a_i and b_i uniquely determine the quantum state that is shared by both Alice and Bob (which includes their communication qubits, workspace qubits, as well as their prior shared entanglement). The messages (m_{i+1}^A, m_{i+1}^B) that are output by $\mathcal{A}_i$ and $\mathcal{B}_i$ respectively will be distributed according to Alice's and Bob's messages in round i in protocol Q', conditioned on the transcript being consistent with a_i and b_i. It is easy to see that $\mathcal{D}_i$ is a non-signaling device. Thus P is a communication protocol with non-local boxes, and the input/output distribution of P will be identical to that of Q', which is identical to that of Q. The communication complexity of P is equal to that of Q'. □

A.3 One way communication

Theorem 120. *Suppose that Alice receives a random n-bit string X, and engages in a one-way communication protocol using non-local boxes with Bob. Let n_A denote the number of bits sent from Alice to Bob. The maximum probability that Bob can guess X is at most $Q(2^{n_A}, X)$, where $Q(\ell, X)$ is the probability mass of the ℓ most likely strings of X.*

Proof. We can model the protocol as follows: Alice and Bob have non-signaling boxes $\mathcal{A}$ and $\mathcal{B}$, whose joint input/output behavior is described by a non-signaling distribution $AB|UV$ (i.e., A is the random variable denoting the output of $\mathcal{A}$ on input U, and B is the random variable denoting the output of $\mathcal{B}$ on input V). In the protocol, Alice gets input $X = x$, runs $\mathcal{A}(x)$, and obtains a sample a. Alice sends a to Bob, who then runs $\mathcal{B}(a)$, and obtains sample b, which we can assume without loss of generality is an n-bit string. In this protocol, the final distribution of x, a, and b is $\mathsf{P}_X(x)\mathsf{P}_{A|U}(a|x)\mathsf{P}_{B|U,V,A}(b|x,a,a)$.

Consider the following thought experiment: instead of Alice sending a to Bob, Bob generates a uniformly random input v, and runs $\mathcal{B}(v)$ instead. The joint distribution of x, a, v, b is $\mathsf{P}_X(x)\mathsf{P}_V(v)\mathsf{P}_{A,B|U,V}(a,b|x,v)$. In this thought experiment, the probability that Bob's output is equal to x is at most $Q(1, X)$ (i.e. the probability of the most likely string of X):

$$\begin{aligned}\mathsf{P}(B = X) &= \sum_x \mathsf{P}_X(x) \sum_v \mathsf{P}_V(v)\mathsf{P}_{B|U,V}(x|x,v)\\ &= \sum_x \mathsf{P}_X(x)\mathsf{P}_B(x)\\ &\leq Q(1, X).\end{aligned}$$

If we *post-select* on $v = a$, then the distribution of x, a, b will be exactly as in the original protocol. Then,

$$\begin{aligned}\mathsf{P}(B = X|V = A) &= \frac{1}{\mathsf{P}(V = A)} \sum_{x,a} \mathsf{P}_X(x)\mathsf{P}_{A|U}(a|x)\mathsf{P}_V(a)\mathsf{P}_{B|U,V,A}(x|x,a,a)\\ &= \frac{1}{\mathsf{P}(V = A)} \sum_x \mathsf{P}_X(x) \sum_a \mathsf{P}_V(a)\mathsf{P}_{A,B|U,V}(a,x|x,a)\end{aligned}$$

For every x,

$$\frac{1}{\mathsf{P}(V = A)} \sum_a \mathsf{P}_V(a)\mathsf{P}_{A,B|U,V}(a,x|x,a) \leq \frac{1}{\mathsf{P}(V = A)}.$$

Noting that $1/\mathsf{P}(V = A) = 2^{n_A}$, we have $\mathsf{P}(B = X|V = A) \leq Q(2^{n_A}, X)$. □

A.4 Two-way communication

We extend this post-selection technique to the two-way case.

Theorem 121. *Suppose that Alice receives a random n-bit string X, and engages in a two-way communication protocol P using non-local boxes with Bob. Let n_A denote the total number of bits sent from Alice to Bob, over all rounds of communication. The maximum probability that Bob can guess X is at most $Q(2^{n_A}, X)$, where $Q(\ell, X)$ is the probability mass of the ℓ most likely strings of X.*

Proof. Consider the following modification to the protocol: whenever Alice sends a message m_i^A to Bob in round i, Bob will instead ignore the message and instead replace it with a uniformly random string v_i of the same length. Thus, this becomes a one-sided communication protocol, where only Bob is sending messages to Alice. Call this modified protocol P'. Observe that the original protocol P is recovered when we post-select on Bob correctly guessing Alice's messages in every round. We now analyze the ability of Bob to guess Alice's input X at the end of the protocol, in protocol P'. We will reduce this analysis to the one-way case, by arguing via induction that, after round i, the output B_{i+1} of box $\mathcal{B}_i$ is independent of Alice's input X. The case of $i = 1$ (the first round) is handled by the one-way argument above. Assume as our inductive hypothesis that B_i is independent of X. Then, for any fixed x, b_{i+1},

$$\begin{aligned}\mathsf{P}_{B_{i+1}|X}(b_{i+1}|x) &= \sum_{b_i} \mathsf{P}_{B_i|X}(b_i|x) \sum_{v_i} \mathsf{P}_{V_i}(v_i)\mathsf{P}_{B_{i+1}|B_i,V_i,X}(b_{i+1}|b_i,v_i,x) \\ &= \sum_{b_i} \mathsf{P}_{B_i|X}(b_i|x) \sum_{a_i,v_i} \mathsf{P}_{V_i}(v_i)\mathsf{P}_{A_i|X,B_i}(a_i|x,b_i)\mathsf{P}_{B_{i+1}|A_i,B_i,V_i}(b_{i+1}|a_i,b_i,v_i)\end{aligned}$$

where A_i is the input to the box $\mathcal{A}_i$ (we're omitting M_i^B for notational brevity), and we used that B_{i+1}'s dependency on X goes through A_i. Continuing,

$$\begin{aligned}&= \sum_{b_i} \mathsf{P}_{B_i|X}(b_i|x) \sum_{v_i} \mathsf{P}_{V_i}(v_i)\mathsf{P}_{B_{i+1}|B_i,V_i}(b_{i+1}|b_i,v_i) \sum_{a_i} \mathsf{P}_{A_i|X,B_i}(a_i|x,b_i) \\ &= \sum_{b_i} \mathsf{P}_{B_i|X}(b_i|x) \sum_{v_i} \mathsf{P}_{V_i}(v_i)\mathsf{P}_{B_{i+1}|B_i,V_i}(b_{i+1}|b_i,v_i) \\ &= \sum_{b_i} \mathsf{P}_{B_i}(b_i)\mathsf{P}_{B_{i+1}|B_i}(b_{i+1}|b_i) \\ &= \mathsf{P}_{B_{i+1}}(b_{i+1})\end{aligned}$$

where we used our inductive hypothesis, and the fact that $(\mathcal{A}_i, \mathcal{B}_i)$ is a non-signaling device. This completes the induction.

Bob's output in protocol P' can be reduced to the following one-way communication setup: Alice has box $\mathcal{A}_r$ and Bob has box $\mathcal{B}_r$, where r is the number of rounds in P (and P'). Alice receives inputs $A_1, \ldots, A_r$, and $M_1^B, \ldots, M_r^B$; and Bob receives $B_1, \ldots, B_r$, and $V_1, \ldots, V_r$. Alice's and Bob's inputs are correlated random variables, but crucially Bob's input is independent of the random variable X (as we've argued).

Alice executes $\mathcal{A}_r(A_r, M_r^B)$, and Bob executes $\mathcal{B}_r(B_r, V_r)$ to produce protocol output B. Since B is independent of Alice's input, and Bob's input is independent of X, this implies that $\mathsf{P}(B = X) \leq Q(1, X)$, as in the one-way case. But then we can condition on $V_i = M_i^A$ for all $i = 1, \ldots, r$, and conditioned on this event, Bob's output B is distributed exactly in protocol P. Then, Bob's probability of guessing Alice's input X is at most $Q(2^{n_A}, X)$.

□

Bibliography

[1] Scott Aaronson and Andris Ambainis. Quantum search of spatial regions. In *Foundations of Computer Science, 2003. Proceedings. 44th Annual IEEE Symposium on*, pages 200–209. IEEE, 2003.

[2] Scott Aaronson, Russell Impagliazzo, and Dana Moshkovitz. Am with multiple merlins. In *Computational Complexity (CCC), 2014 IEEE 29th Conference on*, pages 44–55. IEEE, 2014.

[3] Dorit Aharonov, Itai Arad, and Thomas Vidick. Guest column: the quantum pcp conjecture. *Acm sigact news*, 44(2):47–79, 2013.

[4] Ahmed Almheiri, Donald Marolf, Joseph Polchinski, and James Sully. Black holes: complementarity or firewalls? *Journal of High Energy Physics*, 2013(2):1–20, 2013.

[5] Andris Ambainis, Jan Bouda, and Andreas Winter. Nonmalleable encryption of quantum information. *Journal of Mathematical Physics*, 50(4):042106, 2009.

[6] Sanjeev Arora, Carsten Lund, Rajeev Motwani, Madhu Sudan, and Mario Szegedy. Proof verification and the hardness of approximation problems. *Journal of the ACM (JACM)*, 45(3):501–555, 1998.

[7] Ziv Bar-Yossef, Thathachar S Jayram, Ravindra Kumar, and D Sivakumar. An information statistics approach to data stream and communication complexity. In *Proceedings of the Foundations of Computer Science*, pages 209–218. IEEE, 2002.

[8] Boaz Barak, Anup Rao, Ran Raz, Ricky Rosen, and Ronen Shaltiel. Strong parallel repetition theorem for free projection games. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques*, pages 352–365. Springer, 2009.

[9] Howard Barnum, Claude Crépeau, Daniel Gottesman, Adam Smith, and Alain Tapp. Authentication of quantum messages. In *The Proceedings of the 43rd Annual IEEE Foundations of Computer Science, 2002.*, pages 449–458. IEEE, 2002.

[10] Jonathan Barrett, Lucien Hardy, and Adrian Kent. No signaling and quantum key distribution. *Physical review letters*, 95(1):010503, 2005.

[11] Mohammad Bavarian, Thomas Vidick, and Henry Yuen. Anchoring games for parallel repetition. *arXiv preprint arXiv:1509.07466*, 2015.

[12] Mohammad Bavarian, Thomas Vidick, and Henry Yuen. Parallel repetition via fortification: analytic view and the quantum case. *arXiv preprint arXiv:1603.05349*, 2016.

[13] Carlo WJ Beenakker. Random-matrix theory of quantum transport. *Reviews of modern physics*, 69(3):731, 1997.

[14] John S Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1(3), 1964.

[15] Daniel J Bernstein, Johannes Buchmann, and Erik Dahmen. *Post-quantum cryptography*. Springer Science & Business Media, 2009.

[16] Amey Bhangale, Ramprasad Saptharishi, Girish Varma, and Rakesh Venkat. On fortification of projection games. In *RANDOM*. (arXiv:1504.05556), 2015.

[17] Dan Boneh, Özgür Dagdelen, Marc Fischlin, Anja Lehmann, Christian Schaffner, and Mark Zhandry. Random Oracles in a Quantum World. In *Proceedings of ASIACRYPT*, 2011.

[18] Dan Boneh and Mark Zhandry. Quantum-secure message authentication codes. In *Advances in Cryptology–EUROCRYPT 2013*, pages 592–608. Springer, 2013.

[19] Dan Boneh and Mark Zhandry. Secure signatures and chosen ciphertext security in a quantum computing world. In *Advances in Cryptology–CRYPTO 2013*, pages 361–379. Springer, 2013.

[20] Fernando GSL Brandao, Aram W Harrow, and Michal Horodecki. Local random quantum circuits are approximate polynomial-designs. *arXiv preprint arXiv:1208.0692*, 2012.

[21] Gilles Brassard, Harry Buhrman, Noah Linden, André Allan Méthot, Alain Tapp, and Falk Unger. Limit on nonlocality in any world in which communication complexity is not trivial. *Physical Review Letters*, 96(25):250401, 2006.

[22] Mark Braverman and Ankit Garg. Small value parallel repetition for general games. In *Proceedings of the Forty-Seventh Annual ACM on Symposium on Theory of Computing*, STOC, 2015.

[23] Mark Braverman, Anup Rao, Omri Weinstein, and Amir Yehudayoff. Direct products in communication complexity. In *Foundations of Computer Science (FOCS), 2013 IEEE 54th Annual Symposium on*, pages 746–755. IEEE, 2013.

[24] André Chailloux and Giannicola Scarpa. Parallel repetition of entangled games with exponential decay via the superposed information cost. In *41st International Colloquium on Automata, Languages, and Programming - (ICALP)*, pages 296–307, 2014.

[25] André Chailloux and Giannicola Scarpa. Parallel repetition of free entangled games: Simplification and improvements. *arXiv preprint arXiv:1410.4397*, 2014.

[26] Kai-Min Chung, Yaoyun Shi, and Xiaodi Wu. Physical randomness extractors. *arXiv preprint arXiv:1402.4797*, 2014.

[27] Kai-Min Chung, Xiaodi Wu, and Henry Yuen. Parallel repetition for entangled k-player games via fast quantum search. In *30th Conference on Computational Complexity*, page 512, 2015.

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

[29] Richard Cleve, Peter Høyer, Benjamin Toner, and John Watrous. Consequences and limits of nonlocal strategies. In *Computational Complexity, 2004. Proceedings. 19th IEEE Annual Conference on*, pages 236–249. IEEE, 2004.

[30] Richard Cleve, William Slofstra, Falk Unger, and Sarvagya Upadhyay. Perfect parallel repetition theorem for quantum xor proof systems. *Computational Complexity*, 17(2):282–299, 2008.

[31] Roger Colbeck. Quantum and relativistic protocols for secure multi-party computation. *arXiv preprint arXiv:0911.3814*, 2009.

[32] Matthew Coudron, Thomas Vidick, and Henry Yuen. Robust randomness amplifiers: Upper and lower bounds. In Prasad Raghavendra, Sofya Raskhodnikova, Klaus Jansen, and Jose D. P. Rolim, editors, *APPROX-RANDOM*, volume 8096 of *Lecture Notes in Computer Science*, pages 468–483. Springer, 2013.

[33] 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*, pages 427–436. ACM, 2014.

[34] Ivan Damgård, Jakob Funder, Jesper Buus Nielsen, and Louis Salvail. Superposition attacks on cryptographic protocols. In *Information Theoretic Security*, pages 142–161. Springer, 2013.

[35] Ivan Damgård, Thomas Brochmann Pedersen, and Louis Salvail. A quantum cipher with near optimal key-recycling. In *Proceedings of the 25th Annual International Conference on Advances in Cryptology*, CRYPTO'05, pages 494–510, Berlin, Heidelberg, 2005. Springer-Verlag.

[36] 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.

[37] Irit Dinur and Omer Reingold. Assignment testers: Towards a combinatorial proof of the pcp theorem. *SIAM Journal on Computing*, 36(4):975–1024, 2006.

[38] Irit Dinur and David Steurer. Analytical approach to parallel repetition. In *Proceedings of the 46th Annual ACM Symposium on Theory of Computing*, pages 624–633. ACM, 2014.

[39] Irit Dinur, David Steurer, and Thomas Vidick. A parallel repetition theorem for entangled projection games. In *the 29th Conference on Computational Complexity, CCC*, pages 197–208, 2014.

[40] Albert Einstein, Boris Podolsky, and Nathan Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical review*, 47(10):777, 1935.

[41] Artur Ekert, Renato Renner, et al. The ultimate physical limits of privacy. *Nature*, 507(7493):443–447, 2014.

[42] Serge Fehr, Ran Gelles, and Christian Schaffner. Security and composability of randomness expansion from bell inequalities. *Physical Review A*, 87(1):012335, 2013.

[43] Uriel Feige. Error reduction by parallel repetition: The state of the art. *Technical Report CS95-32 of the Weizmann Institute*, 1995.

[44] Uriel Feige and Joe Kilian. Two-prover protocols—low error at affordable rates. *SIAM Journal on Computing*, 30(1):324–346, 2000.

[45] Uriel Feige and Oleg Verbitsky. Error reduction by parallel repetition: a negative result. *Combinatorica*, 22(4):461–478, 2002.

[46] Joseph Fitzsimons and Thomas Vidick. A multiprover interactive proof system for the local hamiltonian problem. *arXiv preprint arXiv:1409.0260*, 2014.

[47] Joseph Fitzsimons and Thomas Vidick. A multiprover interactive proof system for the local hamiltonian problem. In *Proceedings of the Conference on Innovations in Theoretical Computer Science*, pages 103–112. ACM, 2015.

[48] Lance Fortnow. *Complexity-theoretic aspects of interactive proof systems*. PhD thesis, Massachusetts Institute of Technology, May 1989. Tech Report MIT/LCS/TR-447.

[49] Alex B Grilo, Iordanis Kerenidis, and Attila Pereszlényi. Pointer quantum pcps and multi-prover games. *arXiv preprint arXiv:1603.00903*, 2016.

[50] Renan Gross and Scott Aaronson. Bounding the seed length of miller and shi's unbounded randomness expansion protocol. *arXiv preprint arXiv:1410.8019*, 2014.

[51] Shima Bab Hadiashar, Matthias Christandl, Ashwin Nayak, and Renato Renner. Communication complexity of one-shot remote state preparation. *Manuscript*, 2015.

[52] Johan Håstad. Some optimal inapproximability results. *Journal of the ACM (JACM)*, 48(4):798–859, 2001.

[53] Patrick M. Hayden, Debbie W. Leung, and Dominic Mayers. The universal composable security of quantum message authentication with key recycling. *In preparation*, 2011.

[54] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson. Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres. *Nature*, 526(7575):682–686, October 2015.

[55] 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.

[56] Thomas Holenstein. Parallel repetition: Simplification and the no-signaling case. 5(1):141–172, 2009.

[57] Alexander Semenovich Holevo. Bounds for the quantity of information transmitted by a quantum communication channel. *Problemy Peredachi Informatsii*, 9(3):3–11, 1973.

[58] R Jain, J Radhakrishnan, and P Sen. A lower bound for the bounded round quantum communication complexity of set disjointness. In *Foundations of Computer Science, 2003. Proceedings. 44th Annual IEEE Symposium on*, pages 220–229. IEEE, 2003.

[59] Rahul Jain. New strong direct product results in communication complexity. In *Electronic Colloquium on Computational Complexity (ECCC)*, volume 18, page 2, 2011.

[60] Rahul Jain, Attila Pereszlényi, and Penghui Yao. A parallel repetition theorem for entangled two-player one-round games under product distributions. *arXiv preprint arXiv:1311.6309*, 2013.

[61] Rahul Jain, Attila Pereszlényi, and Penghui Yao. A parallel repetition theorem for entangled two-player one-round games under product distributions. In *Proceedings of Conference on Computational Complexity (CCC)n*, pages 209–216, 2014.

[62] Zhengfeng Ji. Classical verification of quantum proofs. *arXiv preprint arXiv:1505.07432*, 2015.

[63] Marc Kaplan, Gaëtan Leurent, Anthony Leverrier, and María Naya-Plasencia. Breaking symmetric cryptosystems using quantum period finding. *arXiv preprint arXiv:1602.05973*, 2016.

[64] Julia Kempe, Oded Regev, and Ben Toner. Unique games with entangled provers are easy. In *Proceedings of Foundations of Computer Science (FOCS)*, 2008.

[65] Julia Kempe and Thomas Vidick. Parallel repetition of entangled games. In *Proceedings of the forty-third annual ACM symposium on Theory of computing (STOC)*, pages 353–362, 2011.

[66] Subhash Khot. On the power of unique 2-prover 1-round games. In *Proceedings of the thiry-fourth annual ACM symposium on Theory of computing*, pages 767–775. ACM, 2002.

[67] Alexei Yu Kitaev, Alexander Shen, and Mikhail N Vyalyi. *Classical and quantum computation*, volume 47. American Mathematical Society Providence, 2002.

[68] R Konig, Renato Renner, and Christian Schaffner. The operational meaning of min- and max-entropy. *Information Theory, IEEE Transactions on*, 55(9):4337–4347, 2009.

[69] 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.

[70] Ilan Kremer. *Quantum communication*. PhD thesis, Citeseer, 1995.

[71] Richard A Low. Large deviation bounds for k-designs. In *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, volume 465, pages 3289–3308. The Royal Society, 2009.

[72] Laura Mančinska and Thomas Vidick. Unbounded entanglement can be needed to achieve the optimal success probability. In *Automata, Languages, and Programming*, pages 835–846. Springer, 2014.

[73] Dominic Mayers and Andrew Yao. Quantum cryptography with imperfect apparatus. In *Proceedings of the 39th Annual Symposium on Foundations of Computer Science*, pages 503–509. IEEE, 1998.

[74] Matthew McKague, Tzyh Haur Yang, and Valerio Scarani. Robust self-testing of the singlet. *Journal of Physics A: Mathematical and Theoretical*, 45(45):455304, 2012.

[75] Carl A Miller and Yaoyun Shi. Optimal robust self-testing by binary nonlocal xor games. In *8th Conference on the Theory of Quantum Computation, Communication and Cryptography*, page 254, 2013.

[76] Carl A Miller and Yaoyun Shi. Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices. In *Proceedings of the 46th Annual ACM Symposium on Theory of Computing*, pages 417–426. ACM, 2014.

[77] Vitali D Milman and Gideon Schechtman. *Asymptotic Theory of Finite Dimensional Normed Spaces: Isoperimetric Inequalities in Riemannian Manifolds*, volume 1200. Springer, 2009.

[78] Dana Moshkovitz. Parallel repetition from fortification. In *Foundations of Computer Science (FOCS), 2014 IEEE 55th Annual Symposium on*, pages 414–423. IEEE, 2014.

[79] Anand Natarajan and Thomas Vidick. Constant-soundness interactive proofs for local hamiltonians. *arXiv preprint arXiv:1512.02090*, 2015.

[80] Miguel Navascués, Yelena Guryanova, Matty J Hoban, and Antonio Acín. Almost quantum correlations. *arXiv preprint arXiv:1403.4621*, 2014.

[81] Ashwin Nayak and Julia Salzman. Limits on the ability of quantum states to convey classical messages. *Journal of the ACM (JACM)*, 53(1):184–206, 2006.

[82] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010.

[83] Itzhak Parnafes, Ran Raz, and Avi Wigderson. Direct product results and the gcd problem, in old and new communication models. In *Proceedings of the Twenty-ninth Annual ACM Symposium on Theory of Computing*, STOC '97, pages 363–372, New York, NY, USA, 1997. ACM.

[84] S Pironio, A Acín, and S Massar. Random numbers certified by Bell's theorem. *Nature*, pages 1–26, 2010.

[85] Sandu Popescu and Daniel Rohrlich. Quantum nonlocality as an axiom. *Foundations of Physics*, 24(3):379–385, 1994.

[86] Robert T Powers and Erling Størmer. Free states of the canonical anticommutation relations. *Communications in Mathematical Physics*, 16(1):1–33, 1970.

[87] Anup Rao. Parallel repetition in projection games and a concentration bound. *SIAM Journal on Computing*, 40(6):1871–1891, 2011.

[88] Ran Raz. A parallel repetition theorem. *SIAM Journal on Computing*, 27(3):763–803, 1998.

[89] Ran Raz. A counterexample to strong parallel repetition. *SIAM Journal on Computing*, 40(3):771–777, 2011.

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

[91] Renato Renner. Security of quantum key distribution. *International Journal of Quantum Information*, 6(01):1–127, 2008.

[92] Mohan Sarovar, Akihito Ishizaki, Graham R Fleming, and K Birgitta Whaley. Quantum entanglement in photosynthetic light-harvesting complexes. *Nature Physics*, 6(6):462–467, 2010.

[93] 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.

[94] Wim Van Dam. Implausible consequences of superstrong nonlocality. *arXiv preprint quant-ph/0501159*, 2005.

[95] Wim van Dam and Patrick Hayden. Universal entanglement transformations without communication. *Physical Review A*, 67(6):060302, 2003.

[96] Umesh Vazirani and Thomas Vidick. Certifiable quantum dice. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 370(1971):3432–3448, 2012.

[97] Umesh Vazirani and Thomas Vidick. Fully device-independent quantum key distribution. *Physical review letters*, 113(14):140501, 2014.

[98] Oleg Verbitsky. Towards the parallel repetition conjecture. *Theoretical Computer Science*, 157(2):277–282, 1996.

[99] Guifre Vidal, José Ignacio Latorre, Enrique Rico, and Alexei Kitaev. Entanglement in quantum critical phenomena. *Physical review letters*, 90(22):227902, 2003.

[100] Thomas Vidick. Three-player entangled xor games are np-hard to approximate. In *Proceedings of the 54th Annual Symposium on Foundations of Computer Science*, pages 766–775. IEEE, 2013.

[101] Mark N Wegman and J Lawrence Carter. New hash functions and their use in authentication and set equality. *Journal of computer and system sciences*, 22(3):265–279, 1981.

[102] Mark M Wilde. *Quantum information theory*. Cambridge University Press, 2013.

[103] Andrew Chi-Chih Yao. Quantum circuit complexity. In *Proceedings of the 34th Annual Foundations of Computer Science*, pages 352–361. IEEE, 1993.

[104] Henry Yuen. Quantum randomness expansion: Upper and lower bounds. Master's thesis, Massachusetts Institute of Technology, 2013.

[105] Henry Yuen. A parallel repetition theorem for all entangled games. In *Proceedings of the 43rd International Colloquium on Automata, Languages, and Programming*, 2016.

[106] Mark Zhandry. How to Construct Quantum Random Functions. In *Proceedings of the 53rd IEEE Symposium on Foundations of Computer Science (FOCS)*, 2012.