THE UNIVERSITY *of* EDINBURGH

Nonlocal Games and Their Device-Independent Quantum Applications

Sean A. Adamson

Doctor of Philosophy

Laboratory for Foundations of Computer Science

School of Informatics

The University of Edinburgh

2023

Abstract

Device-independence is a property of certain protocols that allows one to ensure their proper execution given only classical interaction with devices and assuming the correctness of the laws of physics. This scenario describes the most general form of cryptographic security, in which no trust is placed in the hardware involved; indeed, one may even take it to have been prepared by an adversary. Many quantum tasks have been shown to admit device-independent protocols by augmentation with "nonlocal games". These are games in which noncommunicating parties jointly attempt to fulfil some conditions imposed by a referee. We introduce examples of such games and examine the optimal strategies of players who are allowed access to different possible shared resources, such as entangled quantum states. We then study their role in self-testing, private random number generation, and secure delegated quantum computation. Hardware imperfections are naturally incorporated in the device-independent scenario as adversarial, and we thus also perform noise robustness analysis where feasible.

We first study a generalization of the Mermin–Peres magic square game to arbitrary rectangular dimensions. After exhibiting some general properties, these "magic rectangle" games are fully characterized in terms of their optimal win probabilities for quantum strategies. We find that for $m \times n$ magic rectangle games with dimensions $m, n \geq 3$, there are quantum strategies that win with certainty, while for dimensions $1 \times n$ quantum strategies do not outperform classical strategies. The final case of dimensions $2 \times n$ is richer, and we give upper and lower bounds that both outperform the classical strategies. As an initial usage scenario, we apply our findings to quantum certified randomness expansion to find noise tolerances and rates for all magic rectangle games. To do this, we use our previous results to obtain the winning probabilities of games with a distinguished input for which the devices give a deterministic outcome and follow the analysis of C. A. Miller and Y. Shi [SIAM J. Comput. **46**, 1304 (2017)].

Self-testing is a method to verify that one has a particular quantum state from purely classical statistics. For practical applications, such as device-independent delegated verifiable quantum computation, it is crucial that one self-tests multiple Bell states in parallel while keeping the quantum capabilities required of one side to a minimum. We use our $3 \times n$ magic rectangle games to obtain a self-test for n Bell states where one side needs only to measure single-qubit Pauli observables. The protocol

requires small input sizes [constant for Alice and $O(\log n)$ bits for Bob] and is robust with robustness $O\left(n^{5/2}\sqrt{\varepsilon}\right)$, where ε is the closeness of the ideal (perfect) correlations to those observed. To achieve the desired self-test, we introduce a one-side-local quantum strategy for the magic square game that wins with certainty, we generalize this strategy to the family of $3 \times n$ magic rectangle games, and we supplement these nonlocal games with extra check rounds (of single and pairs of observables).

Finally, we introduce a device-independent two-prover scheme in which a classical verifier can use a simple untrusted quantum measurement device (the client device) to securely delegate a quantum computation to an untrusted quantum server. To do this, we construct a parallel self-testing protocol to perform device-independent remote state preparation of n qubits and compose this with the unconditionally secure universal verifiable blind quantum computation (VBQC) scheme of J. F. Fitzsimons and E. Kashefi [Phys. Rev. A **96**, 012303 (2017)]. Our self-test achieves a multitude of desirable properties for the application we consider, giving rise to practical and fully device-independent VBQC. It certifies parallel measurements of all cardinal and intercardinal directions in the XY-plane as well as the computational basis, uses few input questions (of size logarithmic in n for the client and a constant number communicated to the server), and requires only single-qubit measurements to be performed by the client device.

Lay summary

Quantum mechanics is a theory in physics dealing with the behavior of our universe at scales far smaller than can be seen with the naked eye. While it is true that the interactions with matter we observe in everyday life can be thought of as macroscopic manifestations of these quantum laws, certain properties of this matter predicted by quantum mechanics contradict our basic human intuition. Telltale signs of a quantum universe require such precisely controlled conditions to be picked out from the rest of the noisy world that, quite simply, they seldom appear to us. With the significant advancements in technology that have taken place over the last few decades, experimenters can now routinely isolate these quantum effects in the lab, while further progress may even allow exploiting them in so-called "quantum technologies". Quantum computers are an example that promises to perform certain computations faster than any traditional computer ever will. Given that the first quantum computers are likely to be held by large corporations and governments that fund their development, any clients wishing to perform their private computations using these cutting-edge machines will have to delegate to them. It is, therefore, a priority that we find a way to ensure to clients that both the data they send is protected and that the computation they request is performed correctly by the quantum server computer.

We show that it is possible to make such security assurances, not only in the case of a potentially malicious remote quantum computer but even when the client does not trust the internal workings of their own device used to delegate computations. Moreover, while the quantum computer is assumed to be large and powerful, client-side devices can be relatively simple (with technology that might fit inside a future mobile phone). To explore this possibility, we ask for the reverse of an earlier statement: what simple observations would convince us that quantum phenomena occurred? We achieve this in the form of new kinds of guessing games played between two players; if the players jointly succeed often enough in these games, then it means they are necessarily exploiting the sort of quantum phenomena needed for our security applications. Just this information is enough, for example, to generate truly random numbers that are unknowable to any outside party. However, suppose the players win the maximum possible fraction of the time. In that case, it is possible to characterize the existence and exact nature of the quantum phenomena they must have utilized. Such a strong characterization also opens the door to enhancing security in many other tasks manipulating quantum data.

Acknowledgements

I owe colossal gratitude to everyone who has helped me throughout the last few incredible years, and I would like to thank them here.

First and foremost, I would like to extend enormous thanks to my supervisor, Petros Wallden, for his unfaltering support and advice over the years. His passion and humor are in seemingly unending supply, and I have found our many lengthy discussions to be invaluable. He undoubtedly (and, for some of our time together, *nonlocally*) influenced the person I have become today.

I am grateful to my cosupervisor Chris Heunen for always being a friendly and stable source of help and suggestions and a fantastic mentor. I also thank Markulf Kohlweiss, tasked every year with attending my annual review meetings, for offering his sustained guidance and organizing the five a month PhD lightning talk series: a much-needed social experience during the pandemic.

I am indebted to my examiners Raúl García-Patrón Sánchez and Roger Colbeck for their time and effort in reviewing my thesis and for their feedback. Additionally, Raúl has been at the center of fun discussions, including his energetic and enlightening overview of quantum communications over a meal after a long day of talks.

I am also grateful to Matty J. Hoban and Alexandru Gheorghiu, who have provided indispensable feedback and comments on my work. Although mostly virtual, conversations with Andru have always been pleasant and incredibly insightful … never before have I seen someone pack so many books into a single suitcase!

I would like to thank Elham Kashefi, whom, although I did not have the pleasure of meeting until near the end of my PhD, cemented herself as one of the most enthusiastic and talented people I know during a visit from Sorbonne Université in Paris. All of the other members of the quantum team in Paris who visited also have my thanks for their many fruitful talks and exchanges. Conversations with other members of the quantum informatics group at Edinburgh, including Brian Coyle, Ioannis Kolotouros, and Miloš Prokop, were also of great help to me.

Outside of the academic world, several friends have been irreplaceable in the support they have offered me: Dylan Kennett and Ma Siyuan, to name just a couple. Finally, I would like to give special thanks to my parents and my one and only Chuqiao for all the emotional support, encouragement, and patience they have gifted me. It is with their help at all twists and turns that I have been able to see this thesis—or rather, this whole journey—to completion.

Declaration

I declare that this thesis was composed by myself, that the work contained herein is my own except where explicitly stated otherwise in the text, and that this work has not been submitted for any other degree or professional qualification except as specified.

(*Sean A. Adamson)*

Publications and manuscripts

Parts of this thesis have been published or made available as preprint manuscripts, as specified by the following references.

[1] **S. A. Adamson** and P. Wallden, "Quantum magic rectangles: characterization and application to certified randomness expansion", Phys. Rev. Research **2**, 043317 (2020).

[2] **S. A. Adamson** and P. Wallden, "Practical parallel self-testing of Bell states via magic rectangles", Phys. Rev. A **105**, 032456 (2022).

[3] **S. A. Adamson**, *Parallel remote state preparation for fully device-independent verifiable blind quantum computation*, Dec. 2022, arXiv:2212.05442 [quant-ph].

Contents

List of figures

List of tables

Chapter 1

Introduction

Quantum theory has been arguably one of the most successful scientific theories, especially in terms of accuracy of predictions and applications. We are currently in the midst of the second "quantum revolution", where the ability to control quantum systems with great precision has resulted in a new wave of technological applications. What makes quantum theory unique is the fact that our classical intuition frequently fails, and it has been proven that understanding the foundations of this theory is crucial to fully realize the possibilities it offers. Quantum nonlocality (and, more generally, contextuality) is an example of such a concept that defies our classical intuition. At the same time, this property enables one of the most interesting classes of applications of quantum theory: that of device-independent cryptographic protocols. Device-independence, first introduced by Mayers and Yao [4], is a property that allows parties to achieve cryptographic tasks without trusting the inner workings of their own devices. Examples of these tasks range from certified randomness expansion [5] to key distribution [6], secure quantum computation [7], and variants of oblivious transfer [8], among many others.

Nonlocality is frequently expressed in terms of "guessing" games, in which remote parties that share entanglement try to fulfill certain winning conditions (also called *predicates*) for the games. Finding the optimal winning strategies for quantum and classical observers in these games is key to using nonlocality for applications in device-independent cryptography, as well as being of foundational interest within quantum theory. For example, the most celebrated display of quantum nonlocality is possibly that expressed by physical violations of the CHSH inequality, a Bell inequality named after Clauser, Horne, Shimony, and Holt, who described it first [9]. Violation of this inequality was experimentally demonstrated by Freedman and

Clauser [10], while various experimental loopholes have subsequently been closed. The locality loophole was closed in 1982 by Aspect et al. [11] and, recently, the first experimental demonstrations of CHSH violations free from both the detection and locality loopholes have been reported [12–14]. Alain Aspect, John F. Clauser, and Anton Zeilinger, were awarded the Nobel Prize in Physics 2022 "for experiments with entangled photons, establishing the violation of Bell inequalities and pioneering quantum information science" [15]. Values observed as pertaining to the CHSH inequality can equivalently be rephrased as resulting from a nonlocal game (the *CHSH game*) in which the winning condition is as follows: the binary outputs of the two players must be equal unless their binary inputs are equal, in which case their outputs must be unequal [16]. In the CHSH game, classical players may only win at most 75% of the time, while players who are allowed to share entanglement can attain an approximately 85% probability of winning [17]. Another notable nonlocal game is based on the work of Mermin [18] and Peres [19], and is called the *magic square game* (we will introduce this game in further detail in Section 2.2). The magic square game has a special place in the foundations of quantum theory due to two notable properties. Firstly, it is one of the simplest examples in which quantum strategies can win with certainty (probability one) while classical strategies cannot. This property is also referred to as *quantum pseudotelepathy* [20] and can be used to illustrate (strong) contextuality in the spirit of the Kochen–Specker theorem [21]. Secondly, it is the simplest two-player game where the maximal nonlocality can be demonstrated using only Clifford computations [22] (as it requires only the preparation of Bell states and Pauli measurements). In comparison, the CHSH game requires one player to measure in a non-Pauli basis. The magic square game can, in principle, be used for any of the device-independent cryptographic tasks, and its performance in comparison to other games evaluated case-by-case.

As already mentioned, one of the first quantum device-independent cryptographic protocols proposed was that of certified private randomness expansion. The idea of using Bell tests, that exploit the quantum-mechanical property of nonlocality, to certify the presence of private randomness was first introduced by Colbeck and Kent [5]. Clearly, some randomness must be consumed in order to perform the required Bell tests. Conversely, any protocol that does not begin with some initial private randomness held by its user cannot generate any private randomness, since an adversary could simply presupply the untrusted devices with output data such that all tests (which are, in this case, known ahead of time) are passed. Thus, the goal of

randomness expansion is to take a private, uniformly random string and produce a strictly longer (ideally arbitrary in size) random string, which cannot be predicted by any outside party.

Interestingly, beyond being able to certify that there is necessarily some underlying quantumness at work, nonlocality also makes it possible to deduce (up to some local isometry) the exact quantum state of a physical experimental system based on purely classical statistics [4]. This property is known as "self-testing" [23], and is another exciting device-independent concept (see, for example, [24]). The magic square game also finds a use in efficient self-testing [25–28]. Beyond the foundational importance of being able to verify the quantum state of a totally untrusted black-box experimental setup, self-testing has many practical uses due to the high levels of security it is able to offer. While the standard notions of nonlocality lead to device-independent cryptography (for example, [5, 6]), self-testing enables applications such as device-independent secure delegated (verifiable) quantum computation [7, 29–31] among other device-independent protocols that involve quantum *computation*. The crucial point is that to enable device-independent quantum computation one needs to test the quantum state itself (that is, one must perform self-testing); observation of the presence of nonlocal correlations alone does not suffice. In addition to tasks of delegation, one might also envisage other kinds of applications that fit within the client–server scenario (for example, key distribution performed between parties holding asymmetric levels of hardware capabilities). Ideally, in all such cases, the client party would only require strictly classical capabilities. However, as we will see, this may come with significant drawbacks. Instead, one may allow the client party to have some minimal quantum technological capabilities (such as the ability to perform single-qubit measurements) that are foreseeable of possible future personal quantum devices (e.g. those that might fit inside a mobile phone).

With the advent of cloud-based quantum computing services (such as those now offered by IBM, Amazon, and Microsoft among others [32–37]), it is becoming increasingly important to allow the secure delegation of quantum computations to powerful remote quantum servers. In such a scenario, a client wishes to securely delegate some computation to one of these remote servers. Such a client desires that the remote server cannot learn about the computation (a property called "blindness") and that they can be sure that the computation was performed correctly by the server (called "verifiability"). This is known succinctly as verifiable blind delegated quantum computation (VBQC). Delegated quantum computation protocols have been created in

which the delegating party only requires strictly classical capabilities [28, 38, 39], but such protocols come with major disadvantages such as not exhibiting blindness, requiring many provers, or assuming a tensor product structure of the provers' systems. Unconditionally secure protocols for VBQC already exist provided instead that the client can initially ensure the preparation of a product of single-qubit states on the server side. One of the most prevalent of these is the seminal protocol of Fitzsimons and Kashefi [40], which we will henceforth refer to as the *FK protocol*. It requires input states to be prepared in any of the eight cardinal and intercardinal directions of the XY-plane or the computational basis, and is based on the measurement-based quantum computing (MBQC) model [41–43]. Further improvements have since been made to the protocol such as reducing the overhead of qubits involved in verification [44, 45]. While possible deviations by the server are taken into account in such protocols, the level of trust given to client side devices must also be taken into consideration. This is important since the devices held by a client are likely to be error-prone and to have been prepared by external parties. As we have already discussed, the most general form of security for protocols in this context is known as "device-independence" [4, 5], in which no assumptions are made about the honesty of the devices (they may even be adversarially prepared). In contrast, blind verifiable delegation protocols such as [38, 40, 46–51] are not inherently device-independent [52]. One promising approach to the desired device-independent remote state preparation is that of self-testing. The idea is for a classical verifier (in this case the client) to certify the existence of maximally-entangled states shared between two provers (in this case one being the quantum device of the client and the other being the server) from measurement statistics alone. The client side prover then performs particular measurements on the entangled states which, depending on their outcomes, teleports particular states to the server side. Most self-testing protocols, however, do not exhibit the qualities required for practical composability with FK-type VBQC protocols [7]. Typical approaches have thus far either prepared states sequentially [30] or have appealed to other verifiable protocols such as [49] and proven their blindness property separately as inherited from the use of self-testing itself [53].

1.1 Thesis overview

The thesis is organized into chapters as follows.

Chapter 2 This chapter is dedicated to the preliminary and background information

required by the rest of the thesis. We introduce the notation used throughout the thesis (some slightly unconventional), as well as a number of useful elementary results. The chapter also includes information on the Mermin–Peres magic square game, the NPA hierarchy for characterizing experimental behaviors, some established results in randomness expansion, an introduction to self-testing, consequences of the sum-of-squares decomposition for Bell operators, and an explanation of the unitary regularization of Hermitian operators.

Chapter 3 We define magic rectangle games: a set of nonlocal games that are generalizations to the magic square game of arbitrary sizes. These games also have the CHSH game as a special case (the 2×2 rectangle games). We first show that many of the games are equivalent under natural transformations with respect to their maximum attainable winning probabilities at different levels of the NPA hierarchy. Specifically, the games may be transposed and constraints on their rows and columns modified without affecting winning probabilities. We show that $1\times n$ games exhibit entirely classical behavior, while games larger than 3×3 in size behave similarly to the standard magic square game. The remaining $2\times n$ games cannot be won with certainty using behaviors in the quantum set, but there exist quantum strategies that win more often than is classically possible. Numerical values for optimal winning probabilities at low enough levels of the NPA hierarchy and for small enough $2\times n$ games are shown (Table 3.2), and we conjecture a closed-form expression for the *almost* quantum level $1 + AB$ set. Interestingly, the 2×3 game appears to be the first known nonlocal game that can be won with certainty using NPA level 1 correlations, but not with level $1 + AB$ correlations. We give an explicit NPA level 1 strategy for this game. These results allow us to state bounds on the win probabilities attainable with truly quantum strategies.

This chapter is based on work published in [1].

Chapter 4 In this chapter, we take the magic rectangle games defined in Chapter 3 and apply them in the context of certified private randomness. We show which of our games can be used to generate private randomness and find bounds on the noise tolerances and rates of randomness expansion for each of the games. In order to give a general analysis of the rates, we use results on the well-known spot-checking protocol of Miller and Shi [54]. However, we note that there now exist techniques based on entropy accumulation that could be used to achieve

much better rates for magic rectangle games of interest. Such techniques would require a case-by-case analysis of (an unlimited number of) different games and, at the time the presented research was performed, were very new.

This chapter is also based on work published in [1].

Chapter 5 Again making use of our magic rectangle games, we turn our attention to the very general application of nonlocality that is the self-testing of quantum systems. First, we introduce a perfect winning quantum strategy for the Mermin–Peres magic square game that, unlike the standard strategy, allows for one of the two players to make only simple single-qubit Pauli measurements (locally to individual qubit registers of their system). This comes at the cost of three entangled EPR pairs having to be shared between the parties, rather than the usual two. Our magic square strategy is motivated by applications in the client–server scenario, where it is important that the client party (likely being technologically limited to a simple quantum device) need only perform simple quantum operations.

While our "one-side-local" magic square strategy is useful in any application as a drop-in replacement for the usual magic square strategy where measurement simplicity is more important than the extra entanglement required, we use it in this chapter as the basis for self-testing with a simple client device. We generalize our one-side-local 3×3 strategy to a deliberately unwieldy strategy for all $3 \times n$ magic rectangle games. Since observing a behavior consistent with any optimal strategy for the magic square game is only sufficient to certify the presence of two EPR pairs of entanglement, we supplement our requested observations with simple additional correlations to obtain a self-test of n Bell states.

This chapter is based on work published in [2].

Chapter 6 We focus specifically on the task of delegated universal quantum computation. Such delegation protocols that satisfy the properties of both blindness and verifiability require very specific preparations of qubits sent by the client to the server. In this chapter, we construct an efficient parallel self-testing protocol that allows the unconditionally secure Fitzsimons–Kashefi (FK) approach to universal verifiable blind quantum computation (VBQC) to be lifted into the fully device-independent security regime. Although the self-test given in Chap-

ter 5 is geared generally towards the device-independent client–server scenario and, moreover, could be used to teleport states to the server via client-side measurements of the certified Bell states, it is not immediately composable with the FK protocol due to a few missing properties (including the variety of qubits that can be prepared).

We begin the chapter by detailing each of eight properties required of self-testing protocols for them to be used for teleportation-based parallel remote state preparation in FK-type VBQC protocols. Rather than adapt the self-test introduced in Chapter 5, we choose to construct an entirely new protocol based on the careful observation of (triple) CHSH statistics in parallel. In the case of nonideal statistics, since self-testing protocols typically only certify *subnormalized* states resulting before measurements are conditioned on observed outcomes, and the appropriate parallel preparation of qubits for FK-type VBQC necessarily requires measurements with exponentially many outcomes in the number of qubits, we must be careful to ensure that the distance of *normalized* post-measurement states from the ideal does not also scale exponentially. We take care to show how this issue can be overcome in Theorem 6.4. We exhibit a result (Theorem 6.9) that allows certain relations between unknown physical observables measured in the protocol to be turned into appropriate self-testing isometries, with some of the additional properties required for FK-composability also covered. We then show that the observables used for our protocol satisfy these relations, and also that the remaining required properties are satisfied simultaneously. Importantly, each of eight qubits—evenly spaced in the XY-plane—and the two computational basis states can be prepared in parallel. Furthermore, any undetectable flipping of qubits due to quantum correlations being unaffected by complex conjugation of measurements only occurs globally across all qubits prepared in the computational basis. This ensures that trap patterns (qubit vertices in the measurement-based model surrounded by "dummy" computational basis states) used in FK protocols are still effective in verifying that computations are performed correctly.

This chapter is based on work that is also presented in [3].

Chapter 7 We conclude with a summary of our main findings and a discussion of the implications of our work, as well as problems that remain open for future attention.

Chapter 2

Preliminaries

We begin by introducing in Section 2.1 the notation that will be used throughout the thesis and some useful elementary results thereof. In Section 2.2, we give some background on the magic square game. In Section 2.3, a hierarchy of correlations by which given experimental behaviors can be classified (and certified by means of semidefinite programs) are introduced. We then introduce the idea of self-testing in Section 2.5, with definitions and some related results given. In Section 2.6 we discuss sum-of-squares decomposition for Bell operators. Finally, in Section 2.7, we detail the unitary regularization technique for operators and exhibit a convenient result on the anticommutativity of such operators.

2.1 Notation and elementary results

In this section, we introduce notation that will be used throughout the rest of thesis. We also state some useful properties of the mathematical objects presented.

2.1.1 Pauli observables and important states

The Pauli observables σ_{x}, σ_{y}, and σ_{z} will be denoted interchangeably by σ_1, σ_2, and σ_3, respectively. In the computational basis

$$\sigma_{\mathrm{x}} = \sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_{\mathrm{y}} = \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_{\mathrm{z}} = \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{2.1}$$

In some parts (particularly Chapter 5) it will also be convenient to denote the Pauli observables by $\hat{X}$, $\hat{Y}$, and $\hat{Z}$, respectively (this is not to be confused with the regularization of operators introduced in Section 2.7). We will define the $|\pm_\theta\rangle$ qubit states

for $\theta \in \mathbb{R}$ as

$$|\pm_\theta\rangle = \frac{|0\rangle \pm e^{i\theta}|1\rangle}{\sqrt{2}}. \tag{2.2}$$

We define operators $\sigma_{\mathrm{x+y}}$ and $\sigma_{\mathrm{x-y}}$ (denoted interchangeable by σ_4 and σ_5) as

$$\sigma_{\mathrm{x+y}} = \sigma_4 = \frac{\sigma_{\mathrm{x}} + \sigma_{\mathrm{y}}}{\sqrt{2}}, \quad \sigma_{\mathrm{x-y}} = \sigma_5 = \frac{\sigma_{\mathrm{x}} - \sigma_{\mathrm{y}}}{\sqrt{2}}. \tag{2.3}$$

The $|\pm_0\rangle = |\pm\rangle$ states are eigenvectors of σ_{x}, and the $|\pm_{2\pi/4}\rangle = |\pm i\rangle$ states are eigenvectors of σ_{y}. Meanwhile, the $|\pm_{\pi/4}\rangle$ states are eigenvectors of $\sigma_{\mathrm{x+y}}$, and the $|\pm_{3\pi/4}\rangle$ states are eigenvectors of $\sigma_{\mathrm{x-y}}$. We will denote by $|\Phi^+\rangle$ the maximally entangled Bell state

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}. \tag{2.4}$$

2.1.2 Complex conjugation and composition

For a vector $|v\rangle$ or linear map M, we will denote using a star symbol as $|v\rangle^*$ or M^* the complex conjugation of their matrix entries with respect to a fixed basis. To denote the composition of many linear maps, we will adopt product notation, with the convention for the order in which they are applied given by

$$\prod_{j=1}^{n} M_j = M_1 \dots M_n. \tag{2.5}$$

Given also some $s \in \{0,1\}^n$, we define the related notation denoted by an operator "raised to the power" of this string by

$$M^s = \prod_{j=1}^{n} M_j^{s_j}. \tag{2.6}$$

This is an abuse of notation in which M has not been defined on its own, but is nonetheless used in the notation on the left-hand side due to the same letter being used for all the given M_j on the right-hand side. It will always be clear in context to which set of operators $\{M_j \mid 1 \leq j \leq n\}$ the notation M^s is associated with due to the choice of capital letter being used.

2.1.3 Hilbert space notation

Hilbert spaces will be denoted using calligraphic symbols, for example $\mathcal{H}$. The set of linear operators on $\mathcal{H}$ will be denoted $\mathcal{L}(\mathcal{H})$. In the context of delegated computation,

Alice will refer to the client party, while Bob will refer to the server party. Hilbert spaces corresponding to the parties Alice and Bob will be denoted by variations of the symbols $\mathcal{A}$ and $\mathcal{B}$, respectively. In certain situations, it will be useful to explicitly write to which space a state belongs. To this end, we will sometimes write the Hilbert space as a subscript $|\psi\rangle_{\mathcal{H}} \in \mathcal{H}$. Similarly, for a linear map $M_{\mathcal{H}}$, a subscript or superscript calligraphic symbol denotes its domain. In the case of a joint space $\mathcal{A} \otimes \mathcal{B}$, we may omit the tensor product symbol in this notation, so that $|\psi\rangle_{\mathcal{AB}} \in \mathcal{A} \otimes \mathcal{B}$. Given a state $|\psi\rangle$ in a joint space $\mathcal{A} \otimes \mathcal{B}$ and a linear map M defined on $\mathcal{A}$, we will often also denote by M its extension to $\mathcal{A} \otimes \mathcal{B}$ which acts trivially on $\mathcal{B}$. That is, we adopt the notation

$$M|\psi\rangle = (M \otimes I_{\mathcal{B}})|\psi\rangle, \tag{2.7}$$

where $I_{\mathcal{B}}$ is the identity operator on $\mathcal{B}$.

2.1.4 Reflection operators

Frequently, we will deal with $\pm$-outcome projective measurements whose observables M have spectral decomposition $M = M_+ - M_-$ for some orthogonal projections M_+ and M_- satisfying $M_+ + M_- = I$ and $M_+M_- = M_-M_+ = 0$. Observables of this type are unitary and satisfy the involutory property $M^2 = I$. Such operators that are both Hermitian and unitary are also referred to as *reflection* operators.

2.1.5 Properties of norms

The norm $\|\cdot\|$ will refer throughout to that induced by the inner product of the Hilbert space being considered as $\||v\rangle\| = \sqrt{\langle v|v\rangle}$. In the case of a linear operator O defined on this Hilbert space, $\|O\|_p$ will refer to its Schatten p-norm.

Definition 2.1 (Schatten p-norm)**.** Let $\mathcal{H}_1$ and $\mathcal{H}_2$ be Hilbert spaces. For $1 \leq p < \infty$, the *Schatten p-norm* of a bounded linear operator $O : \mathcal{H}_1 \to \mathcal{H}_2$ is given by

$$\|O\|_p = \mathrm{tr}(|O|^p)^{\frac{1}{p}}, \tag{2.8}$$

where $|O| = (O^\dagger O)^{1/2}$. If, moreover, O is compact and both $\mathcal{H}_1$ and $\mathcal{H}_2$ are separable then, equivalently,

$$\|O\|_p = \left(\sum_j s_j^p\right)^{\frac{1}{p}}, \tag{2.9}$$

where the $s_j \geq 0$ are the singular values of O (i.e. the eigenvalues of $|O|$) given in descending order.

Of particular importance are the trace class norm (the case where $p = 1$) and the operator norm (conventionally denoted with $p = \infty$). We will also denote the operator norm without any subscript. The operator norm has the important properties that $\|O|v\rangle\| \leq \|O\| \cdot \||v\rangle\|$ for all vectors $|v\rangle$, and that $\|U\| = 1$ if U is unitary. The trace class norm satisfies

$$\|\mathrm{tr}_{\mathcal{B}}(O)\|_1 \leq \|O\|_1 \tag{2.10}$$

if O is defined on a joint Hilbert space $\mathcal{A} \otimes \mathcal{B}$ [55].

2.1.6 Tolerance relations

We define a tolerance relation $\overset{\varepsilon}{\approx}$ to denote when two vectors are ε-close in the vector norm distance. Given vectors $|u\rangle$ and $|v\rangle$ in the same Hilbert space, this relation is defined by

$$|u\rangle \overset{\varepsilon}{\approx} |v\rangle \iff \||u\rangle - |v\rangle\| \leq \varepsilon. \tag{2.11}$$

By the triangle inequality, we can then succinctly state the property that

$$|u\rangle \overset{\varepsilon}{\approx} |v\rangle \text{ and } |v\rangle \overset{\delta}{\approx} |w\rangle \implies |u\rangle \overset{\varepsilon+\delta}{\approx} |w\rangle. \tag{2.12}$$

The following lemma will prove useful to estimate the action of unitary operators on some state.

Lemma 2.2. *Let $|\varphi\rangle$ and $|\chi\rangle$ be normalized states belonging to the same Hilbert space and let $\varepsilon \geq 0$. The real part $\mathfrak{Re}\,\langle\varphi|\chi\rangle \geq 1 - \varepsilon$ if and only if*

$$|\varphi\rangle \overset{\sqrt{2\varepsilon}}{\approx} |\chi\rangle. \tag{2.13}$$

Proof. Using the property $\||v\rangle\| = \sqrt{\langle v|v\rangle}$, we can expand

$$\begin{aligned} \||\varphi\rangle - |\chi\rangle\|^2 &= \langle\varphi|\varphi\rangle + \langle\chi|\chi\rangle - \langle\varphi|\chi\rangle - \langle\chi|\varphi\rangle \\ &= 2 - \langle\varphi|\chi\rangle - \langle\varphi|\chi\rangle^* \\ &= 2(1 - \mathfrak{Re}\,\langle\varphi|\chi\rangle). \end{aligned} \tag{2.14}$$

Therefore, $\||\varphi\rangle - |\chi\rangle\|^2 \leq 2\varepsilon$ if and only if $1 - \mathfrak{Re}\,\langle\varphi|\chi\rangle \leq \varepsilon$. □

2.1.7 Number strings

Given any string of length n, which we will denote in bold by $\boldsymbol{x} = (x_1, \ldots, x_n)$, we will sometimes find it convenient to consider the same string but of length $n - 1$ and

with its ith element removed. We will write this as the original symbol (in bold) for the string with a subscript as

$$\boldsymbol{x}_i = (x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n). \tag{2.15}$$

To reiterate: x_i is the ith element of $\boldsymbol{x}$, while $\boldsymbol{x}_i$ is $\boldsymbol{x}$ with its ith element removed. An exception to this is given to the ith standard basis vector of length n, which we will always denote unambiguously by

$$\boldsymbol{e}_i^n = (\delta_{ij})_{j=1}^n. \tag{2.16}$$

Let $[P]$ denote the Iverson bracket of a statement P. We will sometimes use this notation as an alternative way to express the Kronecker delta function. That is, we will take

$$\delta_{jk} = [j = k]. \tag{2.17}$$

2.1.8 Complexity

We will interchangeably express the functions with argument n that are $2^{O(\log n)}$ by writing that they are poly(n).

2.1.9 Bell expressions

A (linear) Bell expression $\mathcal{I}$ is defined as a real-valued function taking experimental probabilities $\boldsymbol{p} = (p(a, b \mid x, y))_{a,b,x,y}$ to a linear combination

$$\mathcal{I}[\boldsymbol{p}] = \sum_{a,b,x,y} \beta_{x,y}^{a,b} p(a, b \mid x, y), \tag{2.18}$$

where $\beta_{x,y}^{a,b} \in \mathbb{R}$. For notational convenience, we will also write values of a Bell expression as $\mathcal{I}[p(a, b \mid x, y)]$, where it is understood that all probabilities (varying over a, b, x, and y) are arguments to $\mathcal{I}$.

2.1.10 Overloading of notation

Certain symbols will be refitted with different elementary purposes as is most convenient for the context of each surrounding chapter. We summarize the main differences here, and will recount that this is the case at the beginning of each relevant chapter.

In Chapters 3 and 4 we use the calligraphic letters $\mathcal{A}$ and $\mathcal{B}$ as outcome alphabets of random variables for the answers of observers Alice and Bob in a Bell scenario.

Hilbert spaces are denoted in Chapter 5 alongside results from Chapter 3, and thus to avoid any confusion we use notation such as $\mathcal{H}_A$, $\mathcal{H}'_A$, and $\tilde{\mathcal{H}}_A$ there to denote different Hilbert spaces on the side of Alice, and similarly with different subscript letters identifying other named observers. For this reason, rather than adopting our usual convention for linear maps by including their domain, for example $X_{\mathcal{H}'_A}$ (which is rather cumbersome), we instead opt in Chapter 5 to denote only to which observer the operator corresponds. That is, we would write X_A and leave the exact Hilbert space of Alice on which the operator acts (primed in this example) to be clear from the definition of the operator itself. In Chapter 6, we return to our usual notation with different Hilbert spaces of Alice denoted by variants of calligraphic letters such as $\mathcal{A}$, $\mathcal{A}'$, and $\tilde{\mathcal{A}}$.

There is also a double usage of the hat symbol placed above operators. Usually, the operator $\hat{X}$ is taken to mean the Pauli observable that is also denoted by σ_{x}. However, in Chapter 6, the operator $\hat{X}$ refers to the *regularized* version of some unknown operator X (the process of regularization will be introduced in Section 2.7), while the Pauli observable is consistently denoted by σ_{x} or σ_1. The same is true of the notation for the other Pauli observables.

2.2 The magic square game

The Mermin–Peres magic square game [56] consists of two players, Alice and Bob, who are not allowed to communicate during each round of the game. This could be achieved, for example, by ensuring a spacelike separation between the two players. Each round consists of Alice and Bob, respectively, being assigned a row and column of an empty 3×3 table uniformly at random, which they must fill according to the following rules.

S1. Each filled cell must belong to the set $\{+1, -1\}$.

S2. Rows must contain an even number of negative entries (i.e., the product of Alice's entries to any assigned row must be $+1$).

S3. Columns must contain an odd number of negative entries (i.e., the product of Bob's entries to any assigned column must be -1).

Neither player has knowledge of which row or column the other has been assigned, nor does either player know what values the other has entered. The game is won if both players enter the same value into the cell shared by their row and column.

Concretely, interactions between a referee (who arbitrates the game) and the players (Alice and Bob) in a round of the magic square game proceed in the following way.

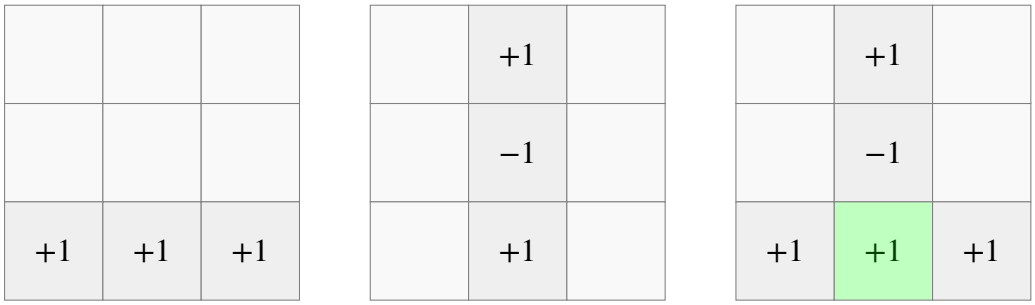
1. The referee chooses $x \in \{1, 2, 3\}$ and $y \in \{1, 2, 3\}$ both uniformly at random. These are the inputs (also called *questions*) to the players Alice and Bob.

2. The referee sends the value x to Alice and the value y to Bob. Importantly, Alice does not learn y and Bob does not learn x, as the players are unable to communicate with one another during a round.

3. Alice returns $\boldsymbol{a} \in \{+1, -1\}^3$ and Bob returns $\boldsymbol{b} \in \{+1, -1\}^3$ to the referee. These strings, each comprised of three bits, are the outputs (also called *answers*) from the players Alice and Bob. They are also required to satisfy $a_1 a_2 a_3 = +1$ and $b_1 b_2 b_3 = -1$, otherwise the round is considered invalid.

4. The referee arranges $\boldsymbol{a}$ as row x and $\boldsymbol{b}$ as column y of a 3×3 table and checks the cell where row x and column y coincide. If the elements of $\boldsymbol{a}$ and $\boldsymbol{b}$ placed in this cell are equal (that is, if $a_y = b_x$) then the round is recorded as a win. Otherwise, the round is recorded as a loss.

This procedure is also depicted graphically (with the 3×3 table displayed) in Fig. 2.1.



(a) Alice's output. **(b)** Bob's output. **(c)** Referee combined outputs.

Figure 2.1: An example round of the magic square game in which inputs $x = 3$ for Alice and $y = 2$ for Bob have been provided by the referee. The 3×3 table on which the game can be thought of as being played is displayed. **(a)** Alice's output depicted as a string of three ± 1 bits placed in row $x = 3$. **(b)** Bob's output depicted as a string of three ± 1 bits placed in column $y = 2$. **(c)** The outputs of both players combined together, as can only be seen by the referee. After examining the outputs of Alice and Bob placed in the shared cell of the table (shaded green), the referee records a win in this example round (both players entered $+1$ where the chosen row and column coincide).

The optimal classical strategy succeeds with probability 8/9 only, and may be achieved by both players agreeing to each follow a particular configuration for their

entire table before the game begins. This can be seen as follows. The success probability of general probabilistic classical strategy cannot exceed that of the best deterministic strategies (in which each player systematically outputs according to some function of their possible inputs), since these are just probability distributions over finite sets of deterministic strategies [20]. It is therefore sufficient to consider only deterministic strategies. Deterministic strategies for the magic square game correspond to fixed assignments of all cells in a 3×3 table for each player, which they decide upon beforehand and refer to during the game in order to produce their answers. In order to satisfy Rules S2 and S3, each row of Alice's assignment must have product $+1$, and each column of Bob's assignment must have product -1. In order to win upon all possible inputs (each corresponding to a different cell of the table in which the players must match their outputs), both players must refer to the same fixed assignment of table. However, it is impossible to produce such an assignment for all cells, since otherwise the product of all cells in the assignment would have to be $+1$ and -1 simultaneously (the product of all rows must be $+1$ while the product of all columns must be -1, a contradiction). Hence, since there are 9 possible questions and the game cannot be deterministically won upon all questions, the overall classical success probability is at most 8/9 where the different inputs are asked with uniform probability. Finally, there exist strategies that attain this 8/9 success probability (see Fig. 2.2), and so the optimal classical success probability is equal to 8/9.

Strikingly, if the players are allowed to share an entangled quantum state, it has been shown to be possible for them to win the magic square game with certainty [18, 19]. Such games are said to exhibit quantum *pseudotelepathy* [20], setting them apart from many other nonlocal games (including the CHSH game) for which optimal quantum strategies are not guaranteed to win.

A possible quantum winning strategy for the magic square allows the players to share the entangled state

$$|\Psi\rangle = |\Phi^+\rangle_{1,2} \otimes |\Phi^+\rangle_{3,4}, \tag{2.19}$$

which is the product of two maximally entangled two-qubit Bell states

$$|\Phi^+\rangle_{a,b} \equiv \frac{|0\rangle_a \otimes |0\rangle_b + |1\rangle_a \otimes |1\rangle_b}{\sqrt{2}}. \tag{2.20}$$

That is, Alice's quantum system is composed of qubits 1 and 3, and Bob's system of qubits 2 and 4. Depending on which row is asked of Alice and column is asked of Bob by the referee, the players make measurements on their respective quantum

+1	+1	+1
+1	−1	−1
−1	+1	−1

(a) Alice's deterministic strategy.

+1	+1	+1
+1	−1	−1
−1	+1	+1

(b) Bob's deterministic strategy.

Figure 2.2: Fixed arrangements of 3×3 tables for **(a)** Alice and **(b)** Bob forming a deterministic strategy for the magic square game that wins with probability 8/9. Upon being provided a question, players refer to their respective table (different rows for Alice and columns for Bob) in order to produce an answer. The entries in the two tables match in all but the bottom right cell (shaded in red). Therefore, the players will win the game upon all inputs other than $(x, y) = (3, 3)$; i.e. in only eight out of nine uniformly distributed cases.

systems by referring to the observables given in the corresponding cells of Fig. 2.3. The outcomes of these measurements determine the values that Alice and Bob enter into their respective row and column to win with certainty.

Let us explain the quantum strategy of Fig. 2.3 in more detail by way of an example. If Alice was provided the question $x = 1$ then according to the strategy of Fig. 2.3 she would produce an answer $\boldsymbol{a} = (a_1, a_2, a_3)$ by letting the measurement outcome of the binary observable $\hat{X} \otimes I$ give a_1, $\hat{X} \otimes \hat{X}$ give a_2, and $I \otimes \hat{X}$ give a_3. These three observables can be measured on her two-qubit system in any order since they are pairwise commutative. Moreover, the outcomes are guaranteed to satisfy Rule S2 that $a_1 a_2 a_3 = 1$ since

$$(\hat{X} \otimes I)(\hat{X} \otimes \hat{X})(I \otimes \hat{X}) = I. \tag{2.21}$$

At the same time, if Bob was provided the question $y = 2$ then he would produce an answer by measuring the observables in the second column—letting the measurement outcome of $\hat{X} \otimes \hat{X}$ give b_1, $\hat{Y} \otimes \hat{Y}$ give b_2, and $\hat{Z} \otimes \hat{Z}$ give b_3. These observables also pairwise commute, and result in outcomes that satisfy Rule S3 that $b_1 b_2 b_3 = -1$ since

$$(\hat{X} \otimes \hat{X})(\hat{Y} \otimes \hat{Y})(\hat{Z} \otimes \hat{Z}) = -I. \tag{2.22}$$

Now, for the inputs $(x, y) = (1, 2)$ given in this example, the referee will record the round as a win if and only if $a_2 = b_1$. The strategy of Fig. 2.3 is constructed such

$\hat{X} \otimes I$	$\hat{X} \otimes \hat{X}$	$I \otimes \hat{X}$
$-\hat{X} \otimes \hat{Z}$	$\hat{Y} \otimes \hat{Y}$	$-\hat{Z} \otimes \hat{X}$
$I \otimes \hat{Z}$	$\hat{Z} \otimes \hat{Z}$	$\hat{Z} \otimes I$

Figure 2.3: A quantum strategy for the magic square game, in which the players share the entangled state $|\Psi\rangle$ given in Eq. (2.19). Observables $\hat{X}$, $\hat{Y}$, and $\hat{Z}$ are the Pauli spin operators, and I is the identity operator. Answers of Alice correspond to measurement outcomes of rows, and answers of Bob to measurement outcomes of columns. Each row is formed of mutually commuting observables whose product is equal to I, and each column of mutually commuting observables whose product is $-I$. The eigenvalues of each observable are $+1$ and -1. These facts combined show Rules S1 to S3 are automatically satisfied. Moreover, if M_A is any of the given observables for Alice's system, and M_B is the corresponding observable for Bob's system, the fact that $\langle\Psi| M_A M_B |\Psi\rangle = 1$ guarantees the players always win. This strategy cannot be realized with either player performing only measurements localized to single-qubit registers.

that both a_2 and b_1 are precisely the measurement outcomes of the observable $\hat{X} \otimes \hat{X}$, measured once on Alice's subsystem and once on Bob's subsystem, respectively. Therefore, it must be the case that the round is won, since using the shared state of Eq. (2.19) these observables are perfectly correlated

$$\langle\Psi| \hat{X} \otimes \hat{X} \otimes \hat{X} \otimes \hat{X} |\Psi\rangle = 1, \tag{2.23}$$

where the first and third $\hat{X}$ act on Alice's side and the second and fourth act on Bob's side. The same argument can be performed for all possible inputs (x, y), and so this quantum strategy wins the magic square game with certainty. Figure 2.3 also shows that (unlike, say, the CHSH game) optimal quantum strategies can be implemented by performing measurements of the two-qubit Pauli group only.

In the context of practical quantum strategies, we refer to measurements as *local* in the sense that they are performed on only a single-qubit register. It will be important for our purposes to understand that the strategy depicted here **cannot** be implemented, for either player, entirely with local measurements. To see this for

Bob, consider the three binary observables contained in the second column of Fig. 2.3. Upon being given the input $y = 2$, Bob is required to answer with three bits, produced as outcomes to measurements of all three observables performed on his same two-qubit subsystem. The three observables to be measured $\hat{X} \otimes \hat{X}$, $\hat{Y} \otimes \hat{Y}$, and $\hat{Z} \otimes \hat{Z}$ are compatible when considered over Bob's entire subsystem, since they are pairwise commutative. Now suppose that Bob is limited to making only local measurements. In this case, he would still be able to implement the measurement of the two-qubit observable $\hat{X} \otimes \hat{X}$ by instead measuring both the compatible observables $\hat{X} \otimes I$ and $I \otimes \hat{X}$ and multiplying the outcomes obtained. Similar statements can also be made about the other two required observables $\hat{Y} \otimes \hat{Y}$ and $\hat{Z} \otimes \hat{Z}$ individually. However, while this can be said for each of the three two-qubit observables separately, Bob cannot implement measurements of all three simultaneously in a local manner. This is because the set of all six single-qubit observables required for this

$$\hat{X} \otimes I, \quad I \otimes \hat{X}, \quad \hat{Y} \otimes I, \quad I \otimes \hat{Y}, \quad \hat{Z} \otimes I, \quad I \otimes \hat{Z} \tag{2.24}$$

do not all commute with one another when considered together as a single set. For instance, the commutator $[\hat{Z} \otimes I, \hat{X} \otimes I] = 2i\hat{Y} \neq 0$. Similarly, consideration of the second row of Fig. 2.3 shows that the strategy for Alice cannot be implemented by performing only local measurements. We present in Section 5.4 a strategy for the magic square game that can be realized using only local measurements for one of the players, at the cost of requiring three shared Bell states.

2.3 Levels of correlations

We consider local measurements made on a system shared by two observers, Alice and Bob (multipartite generalizations exist, however, we will only focus on two parties, as it is the setting that we consider in Chapters 3 and 4). Alice chooses an input $x \in \mathcal{X}$ and observes a corresponding measurement output $a \in \mathcal{A}_x$. Similarly, Bob chooses an input $y \in \mathcal{Y}$ and observes a measurement output $b \in \mathcal{B}_y$. We may implicitly assume that inputs for Alice and Bob are distinguishable from one another, and further that each output is labeled by its corresponding input. Hence, we may write the sets of all possible outputs for Alice and Bob respectively as the *disjoint* unions $\mathcal{A} = \bigcup_{x \in \mathcal{X}} \mathcal{A}_x$ and $\mathcal{B} = \bigcup_{y \in \mathcal{Y}} \mathcal{B}_y$. We refer to a fixed configuration of all probabilities $P(a, b \mid x, y)$ as a *behavior*. These behaviors can also be thought of as vectors in $\mathbb{R}^{|\mathcal{A} \times \mathcal{B}|}$, a convention that is particularly useful for dealing with classes of behaviors that are

then mapped to sets of vectors.

Behaviors can be characterized according to properties they have, or according to what physical theories can give rise to such behaviors. The weakest condition (and thus the most general set of behaviors) one typically imposes is that "signaling" should be forbidden; behaviors should not allow for superluminal communication. A behavior is said to exhibit *nonsignaling* correlations [57] if it satisfies both

$$P(a \mid x) = P(a \mid x, y), \tag{2.25a}$$

$$P(b \mid y) = P(b \mid x, y), \tag{2.25b}$$

i.e., the input of one party does not influence the probability of outcomes for the other party. Similarly, a behavior exhibits *quantum* correlations if it is realizable under the laws of quantum mechanics, meaning that there exists a joint state $|\psi\rangle$ and "local" measurement operators satisfying $[E_x^a, E_y^b] = 0$ that reproduce the behavior, i.e., such that

$$P(a, b \mid x, y) = \langle\psi| E_x^a E_y^b |\psi\rangle. \tag{2.26}$$

A behavior exhibits *classical* correlations if there exists a unique joint probability distribution such that the behavior arises as marginals. By a theorem of Fine [58], such behaviors are equivalently local

$$P(a, b \mid x, y) = \int p_A(a \mid \lambda, x) p_B(b \mid \lambda, y) p(\lambda)\, d\lambda, \tag{2.27}$$

where the "hidden variable" value λ represents a classical description of a strategy that Alice and Bob may share beforehand with probability density $p(\lambda)$. We denote the sets of nonsignaling, quantum, and local behaviors by N, Q, and L, respectively.

Given a behavior, it is not easy to check whether there exists a corresponding quantum model (and thus whether the behavior belongs to Q). In order to characterize the set of quantum behaviors, Navascués et al. [59, 60], defined an infinite decreasing hierarchy of nonsignaling correlations (known as the NPA hierarchy). These levels of correlations are intermediate; they are stronger than nonsignaling correlations, but weaker than the quantum set. The different sets of behaviors in the NPA hierarchy are denoted by $Q_1 \supseteq Q_2 \supseteq \ldots$, and converge to the quantum set in the sense that $\bigcap_{i\geq 1} Q_i = Q$. Each set Q_i can be certified by a different semidefinite program. Note that we refer to a set of correlations S as *stronger* than another set W if the former is a subset of the latter $S \subset W$, since knowing that a behavior belongs to S also tells us that it is in W. We thus say that quantum correlations are stronger than

nonsignaling correlations but weaker than local correlations, for instance. Note that the reverse convention is not uncommon in the literature, and many authors would refer to N as stronger than Q since behaviors unique to $N \setminus Q$ typically correspond to more strongly correlated measurement outcomes than those found in Q.

A further important set of supra-quantum behaviors are the *almost quantum* correlations [61], which we denote $\tilde{Q} \supsetneq Q$. It has been argued that this set is special, as it is the smallest set that contains the quantum set and arises naturally from some information theoretic principle (e.g. local orthogonality [62], nontrivial communication complexity [63], etc.). These correlations arise naturally by weakening a single one of the principles defining quantum correlations. Namely, instead of requiring the local measurement operators to commute, one only requires that they commute when acting on the special state that gives the behavior, i.e. $[E_x^a, E_y^b]|\psi\rangle = 0$. It is shown in [61] that $\tilde{Q} = Q_{1+AB}$, where Q_{1+AB} is a set of correlations defined in [60] and satisfying $Q_1 \supsetneq Q_{1+AB} \supsetneq Q_2$ in the NPA hierarchy.

Overall, the above correlations satisfy the inclusions

$$N \supsetneq Q_1 \supsetneq Q_{1+AB} = \tilde{Q} \supsetneq Q_2 \supseteq \cdots \supseteq Q \supsetneq L. \tag{2.28}$$

Here, it is worth stressing that the win probabilities in any game can only increase when considering a larger set of behaviors. It follows that to (upper or lower) bound the win probabilities for players of a nonlocal game in one level, one can use other levels of correlations that are easier to deal with. In Chapters 3 and 4, we will mainly be concerned with the nonsignaling, almost quantum, quantum, and local levels of correlations N, $\tilde{Q}$, Q, and L respectively, where the almost quantum set is used to upper bound the win probabilities for quantum behaviors.

2.4 Randomness expansion

Given a nonlocal game, we will denote by ω its maximal win probability over all quantum devices (those devices whose behaviors can be described as belonging to the set of quantum correlations), and by $\bar{\omega}$ its maximal win probability over all quantum devices with a *distinguished input* (that is, quantum devices that are restricted to give deterministic outputs upon a single one of their possible inputs).

Definition 2.3 (Distinguished input)**.** That a device gives a deterministic output upon some input $\bar{\boldsymbol{x}} = (\bar{x}, \bar{y}) \in \mathcal{X} \times \mathcal{Y}$ means that there exists an output $\bar{\boldsymbol{a}} = (\bar{a}, \bar{b}) \in \mathcal{A} \times \mathcal{B}$

such that $\Pr(\bar{\boldsymbol{a}} \mid \bar{\boldsymbol{x}}) = 1$. That is, equivalently,

$$\Pr(\boldsymbol{A} = \bar{a} \cap \boldsymbol{B} = \bar{b} \mid X = \bar{x} \cap Y = \bar{y}) = 1. \tag{2.29}$$

A device for which this statement is satisfied for the input $\bar{\boldsymbol{x}}$ is said to have a *distinguished input* $\bar{\boldsymbol{x}}$.

Remark. The word "device" here in fact refers to two separate parts considered together, one held by Alice and the other by Bob. Since signaling between Alice and Bob is forbidden, it is implied by Eq. (2.29) that both

$$\Pr(\boldsymbol{A} = \bar{a} \mid X = \bar{x}) = 1, \tag{2.30a}$$

$$\Pr(\boldsymbol{B} = \bar{b} \mid Y = \bar{y}) = 1. \tag{2.30b}$$

That is, it can be said that the local outputs from the device parts held by Alice and Bob are deterministic upon inputs $\bar{x}$ and $\bar{y}$, respectively.

To illustrate the concept of devices with distinguished inputs consider the CHSH game, whose inputs and outputs belong to the alphabet $\{0,1\} \times \{0,1\}$ (with the inputs drawn uniformly from this set). The measurement statistics of general quantum devices may follow any behavior in the set of quantum correlations $\boldsymbol{Q}$ (resulting in a maximal win probability of $\omega \approx 85.4\%$). However, if we consider only those quantum devices that have a distinguished input $(0,0)$, then the measurement statistics must follow a behavior that is in the subset $\bar{\boldsymbol{Q}} \subset \boldsymbol{Q}$, where

$$\bar{\boldsymbol{Q}} = \left\{ \boldsymbol{P} = (P(a,b \mid x,y))_{a,b,x,y} \in \boldsymbol{Q} \;\middle|\; \exists(\bar{a},\bar{b}) \text{ s.t. } P(\bar{a},\bar{b} \mid 0,0) = 1 \right\}. \tag{2.31}$$

When only devices implementing this set are considered (devices with a choice $(0,0)$ of distinguished input), it can be shown that the maximal win probability is 75%—equal to that of classical devices in this case [54, Appendix D].

Protocol $\boldsymbol{R}_{gen}$ given by Miller and Shi [54, Figure 2] produces quantum-secure extractable bits over N rounds, provided its *score acceptance threshold* parameter χ satisfies $\chi > \bar{\omega}$. We reproduce $\boldsymbol{R}_{gen}$ in Protocol 2.1 for convenience.

In our notation, the main result of Miller and Shi [54] can be stated as in the following theorem.

Theorem 2.4 (Miller and Shi [54, Theorem 1.1])**.** *For any game, there are functions* $\pi : [0,\omega] \to \mathbb{R}_{\geq 0}$ *and* $\Delta : (0,1]^2 \to \mathbb{R}_{\geq 0}$ *such that the following hold:*

1. *For any* $b \in (0,1]$*, Protocol* $\boldsymbol{R}_{gen}$ *produces at least* $N[\pi(\chi) - \Delta(b,q)]$ *extractable bits with soundness error* $3 \cdot 2^{-bqN}$.

Protocol 2.1: The Protocol R_{gen} of Miller and Shi [54, Figure 2].

Let the following arguments of the protocol be given:

- A game G with a distinguished input $\bar{x}$.
- A quantum device D compatible with G.
- The *output length* $N \in \mathbb{N}^*$.
- The *test (game round) probability* $0 < q < 1$.
- The *score acceptance threshold* $0 < \chi < 1$.

Execute the following steps, resulting in the protocol either **aborting** or **succeeding**:

1. Let c denote a real variable which we initially set to 0.
2. Choose a bit $t \in \{0, 1\}$ according to the Bernoulli distribution taking value 1 with probability q. Depending on t, perform one of the following:
   (a) *Generation round* ($t = 0$): Given distinguished input $\bar{x}$ to D and record the output.
   (b) *Game round* ($t = 1$): Play the game G with D and record the output. Add the score achieved to the variable c.
3. Repeat Step 2 until it has been performed N times in total.
4. If $c < \chi q N$, then the protocol **aborts**. Otherwise, it **succeeds**.

---

2. *The function π is nonzero on the interval $(\bar{\omega}, \omega]$.*

3. *The function Δ tends to 0 as $(b, q) \to (0, 0)$.*

In Theorem 2.4, the number of random bits extractable from the output is directly proportional to the output length N (which is also the number of rounds). Th proportionality constant (i.e. the number of bits per round obtained on average) is $\pi(\chi) - \Delta(b, q)$, where $\Delta(b, q)$ is a small error term. For this reason, the function π is called a "rate curve", as it indicates the rate of extractable randomness with respect to number of protocol rounds performed. The value of the rate curve depends on the score acceptance threshold χ, which is the minimum average score that must be observed in game rounds so that the protocol does not abort. This parameter offers a trade-off between the rate and noise tolerance of the protocol and must also satisfy $\chi > \bar{\omega}$ for any randomness to be produced. The error term $\Delta(b, q)$ vanishes when the test probability q and the soundness parameter b are sufficiently small. Here, $b \in (0, 1]$ can be chosen appropriately such that the balance between the soundness of the protocol and the rate decrease caused by $\Delta(b, q)$ is as desired.

Choosing the test probability parameter to be $q = (\log N)^2/N$, the protocol consumes poly$(\log N)$ bits of initial random seed to both approximate the input distribution for the protocol (which of the rounds are game rounds and the game inputs in these rounds) [64–66] and perform randomness extraction on the final output [67]. Since the number of extractable random bits contained in the final output is $\Theta(N)$, the protocol achieves exponential randomness expansion.

Modeling noise as a process in which an adversary is allowed to change the outputs of a device arbitrarily with some probability, the noise tolerance of the protocol is $\omega - \chi$ (the adversary is allowed to change the expected score at the game by at most this amount). The noise tolerance is then maximally $\omega - \bar{\omega}$. Intuitively, that $\omega > \bar{\omega}$ means that the score achieved in game rounds (which appear identical to randomness generation rounds from the perspective of the players) can be used to make sure that the players are employing a strategy wherein some randomness is present when they are provided the input used for generation rounds. The worst case is that they do not produce randomness, and are instead acting entirely deterministic upon being given the randomness generation input (whereupon they will achieve a score of $\bar{\omega}$ over game rounds). Thus, the size of the gap $\omega - \bar{\omega}$ corresponds to how convincingly the protocol can be made to show that they do indeed generate randomness when asked. Practically, we do not allow the protocol to succeed whenever $\omega > \bar{\omega}$ is

observed, but rather when $\omega \geq \chi$, where $\chi > \bar{\omega}$ is some choice of score acceptance threshold. Opting for a larger χ generally improves the randomness rate (since we can be more sure of the gap), but at the cost that the protocol will be more likely to abort in the presence of experimental noise.

An explicit lower bound on the rate curve function π was also proved by Miller and Shi [54], and can be stated as follows.

Theorem 2.5 (Miller and Shi [54, Theorem 5.8])**.** *Let G be a game with output alphabet size $r \geq 2$, and let $\bar{\omega}$ be the maximum win probability of this game over compatible devices with a distinguished input. Then, the following function is a rate curve:*

$$\pi(\chi) = \begin{cases} \frac{2(\log_2 e)(\chi-\bar{\omega})^2}{r-1} & \text{if } \chi > \bar{\omega}, \\ 0 & \text{otherwise.} \end{cases} \tag{2.32}$$

2.5 Self-testing (with complex measurements)

In a self-testing scenario, two observers Alice and Bob (who are unable to communicate) share an unknown physical quantum state ρ on $\mathcal{A} \otimes \mathcal{B}$. No other assumptions about the physical state spaces of Alice and Bob are made. In particular, their dimensions are not assumed. Given a probability distribution defining the behavior of untrusted measurement devices held by Alice and Bob, it is often possible to deduce (up to some local isometry) the quantum state they share. Moreover, one can also often deduce the local quantum measurements corresponding to different inputs and outputs for each device. For convenience, it is common to work with a purification $|\psi\rangle \in \mathcal{A} \otimes \mathcal{B} \otimes \mathcal{P}$ of the physical state for some purifying space $\mathcal{P}$ separate from the observers. Since all operations accessible to the observers act trivially on this purifying space, we will usually suppress it in our notation, and treat $|\psi\rangle \in \mathcal{A} \otimes \mathcal{B}$ as the physical state. One may also assume that the measurements are projective (see [24, Appendix B] for a detailed discussion of this topic). The Born rule states that the probability of outcomes a and b upon being provided with inputs x and y is given by

$$\begin{aligned} p(a, b \mid x, y) &= \operatorname{tr}(|\psi\rangle\langle\psi| M_{a|x} \otimes N_{b|y}) \\ &= \langle\psi| M_{a|x} \otimes N_{b|y} |\psi\rangle, \end{aligned} \tag{2.33}$$

where $\{M_{a|x}\}_a$ and $\{N_{b|y}\}_b$ are the physical, projective, local measurements of Alice and Bob for questions x and y, respectively. We now state a first definition of what it means to robustly self-test some reference state and measurements.

Definition 2.6 (Self-testing of states and real measurements)**.** The probabilities $p(a, b \mid x, y)$ are said to δ-approximately *self-test* the state $|\psi'\rangle \in \mathcal{A}' \otimes \mathcal{B}'$ and measurement operators $M'_{a|x} \in \mathcal{L}(\mathcal{A}')$ and $N'_{b|y} \in \mathcal{L}(\mathcal{B}')$ if, for any state $|\psi\rangle \in \mathcal{A} \otimes \mathcal{B}$ and measurement operators $M_{a|x} \in \mathcal{L}(\mathcal{A})$ and $N_{b|y} \in \mathcal{L}(\mathcal{B})$ from which these probabilities may arise, there exists a junk state $|\xi\rangle \in \tilde{\mathcal{A}} \otimes \tilde{\mathcal{B}}$ and isometries $V_{\mathcal{A}} : \mathcal{A} \to \mathcal{A}' \otimes \tilde{\mathcal{A}}$ and $V_{\mathcal{B}} : \mathcal{B} \to \mathcal{B}' \otimes \tilde{\mathcal{B}}$ defining the local isometry $V = V_{\mathcal{A}} \otimes V_{\mathcal{B}}$ such that for all a, b, x, and y

$$V|\psi\rangle \overset{\delta}{\approx} |\psi'\rangle \otimes |\xi\rangle, \tag{2.34a}$$

$$V(M_{a|x} \otimes N_{b|y})|\psi\rangle \overset{\delta}{\approx} (M'_{a|x} \otimes N'_{b|y})|\psi'\rangle \otimes |\xi\rangle. \tag{2.34b}$$

This definition is standard, and accounts for the unobservable possibilities of local unitary basis transformations applied to the state and measurements, as well as embedding of the state and measurement operators in a Hilbert space of larger dimension, or the existence of additional degrees of freedom (on which the measurement operators do not act). We may assume without loss of generality that the reference state $|\psi'\rangle$ is *real*, meaning that $|\psi'\rangle^* = |\psi'\rangle$, since the Schmidt decomposition guarantees the existence of local orthonormal bases in which all entries to its matrix are real. Unless it is also assumed that $(M'_{a|x})^* = M'_{a|x}$ and $(N'_{b|y})^* = N'_{b|y}$ (that the reference measurements are real in this basis), Definition 2.6 does not account for the unobservable possibility that Alice and Bob actually implement complex conjugated versions of the reference measurements in a correlated fashion [68, 69]. This is because probabilities are real numbers, and so

$$\begin{aligned} p(a, b \mid x, y) &= \operatorname{tr}(|\psi'\rangle\langle\psi'| M'_{a|x} \otimes N'_{b|y}) \\ &= \operatorname{tr}(|\psi'\rangle\langle\psi'| (M'_{a|x})^* \otimes (N'_{b|y})^*) \\ &= p(a, b \mid x, y)^*, \end{aligned} \tag{2.35}$$

but complex conjugation is not a unitary transformation.

It is sufficient for our purposes to consider complex conjugation performed in some convenient fixed local orthonormal bases for which $|\psi'\rangle$ is real. This is because complex conjugation of projectors performed in arbitrary local orthonormal bases is equivalent (up to some local unitary transformation) to conjugation performed in the original fixed bases (the complex conjugate of a unitary matrix is also unitary). In particular, we cannot use Definition 2.6 to self-test a reference state $|\Phi^+\rangle$ and (on one side) the observables σ_x, σ_y, and σ_z; there is no local orthonormal bases in which the state and corresponding projectors are all real. In cases with complex measurements,

the following definition allowing also for correlated complex conjugation can be used.

Definition 2.7 (Self-testing of states and complex measurements)**.** The probabilities $p(a, b \mid x, y)$ are said to δ-approximately *self-test* the state $|\psi'\rangle \in \mathcal{A}' \otimes \mathcal{B}'$ and measurement operators $M'_{a|x} \in \mathcal{L}(\mathcal{A}')$ and $N'_{b|y} \in \mathcal{L}(\mathcal{B}')$ if, for any state $|\psi\rangle \in \mathcal{A} \otimes \mathcal{B}$ and measurement operators $M_{a|x} \in \mathcal{L}(\mathcal{A})$ and $N_{b|y} \in \mathcal{L}(\mathcal{B})$ from which these probabilities may arise, there exists a junk state $|\xi\rangle \in \tilde{\mathcal{A}} \otimes \mathcal{A}'' \otimes \tilde{\mathcal{B}} \otimes \mathcal{B}''$ and isometries $V_{\mathcal{A}} : \mathcal{A} \to \mathcal{A}' \otimes \tilde{\mathcal{A}} \otimes \mathcal{A}''$ and $V_{\mathcal{B}} : \mathcal{B} \to \mathcal{B}' \otimes \tilde{\mathcal{B}} \otimes \mathcal{B}''$ defining the local isometry $V = V_{\mathcal{A}} \otimes V_{\mathcal{B}}$ such that for all a, b, x, and y

$$V|\psi\rangle \overset{\delta}{\approx} |\psi'\rangle \otimes |\xi\rangle, \tag{2.36a}$$

$$V(M_{a|x} \otimes N_{b|y})|\psi\rangle \overset{\delta}{\approx} (\bar{M}_{a|x} \otimes \bar{N}_{b|y})|\psi'\rangle \otimes |\xi\rangle, \tag{2.36b}$$

where

$$\bar{M}_{a|x} = M'_{a|x} \otimes |0\rangle\langle 0|_{\mathcal{A}''} + (M'_{a|x})^* \otimes |1\rangle\langle 1|_{\mathcal{A}''}, \tag{2.37a}$$

$$\bar{N}_{b|y} = N'_{b|y} \otimes |0\rangle\langle 0|_{\mathcal{B}''} + (N'_{b|y})^* \otimes |1\rangle\langle 1|_{\mathcal{B}''}, \tag{2.37b}$$

and the state $|\xi\rangle$ has the form

$$|\xi\rangle = |\xi_0\rangle \otimes |0\rangle_{\mathcal{A}''}|0\rangle_{\mathcal{B}''} + |\xi_1\rangle \otimes |1\rangle_{\mathcal{A}''}|1\rangle_{\mathcal{B}''} \tag{2.38}$$

for some subnormalized $|\xi_0\rangle$ and $|\xi_1\rangle$ in $\tilde{\mathcal{A}} \otimes \tilde{\mathcal{B}}$ satisfying $\langle\xi_0|\xi_0\rangle + \langle\xi_1|\xi_1\rangle = 1$.

It is often sufficient to deduce a self-testing statement such that, instead of a full set of probabilities $p(a, b \mid x, y)$, one need only observe certain combinations of them given by the maximal violation of some Bell inequality $\mathcal{I}[p(a, b \mid x, y)] = \beta$. One may replace the probabilities in Definitions 2.6 and 2.7 with such a maximal violation. One may also choose to self-test measurement operators on only Alice's subsystem by simply taking Bob's measurement operators in these definitions to be identity operators. Similarly, one need not choose to make a self-testing statement certifying reference operators used to produce all of the probabilities $p(a, b \mid x, y)$, provided that the result is shown to hold for all compatible sets of physical measurements.

Let $M = M_+ - M_-$ be a ± 1-outcome observable on Alice's subsystem with corresponding projectors $M_\pm$, and suppose we have statements of the form

$$V|\psi\rangle \overset{\delta}{\approx} |\psi'\rangle \otimes |\xi\rangle, \tag{2.39a}$$

$$VM|\psi\rangle \overset{\delta}{\approx} \bar{M}|\psi'\rangle \otimes |\xi\rangle, \tag{2.39b}$$

where $\bar{M} = M' \otimes |0\rangle\langle 0| + (M')^* \otimes |1\rangle\langle 1|$ is defined for the reference observable $M' = M'_+ - M'_-$. In this case, one automatically obtains statements in terms of the projectors of the form of Definition 2.7

$$V M_\pm |\psi\rangle \overset{\delta}{\approx} \bar{M}_\pm |\psi'\rangle \otimes |\xi\rangle, \tag{2.40}$$

where $\bar{M}_\pm = M'_\pm \otimes |0\rangle\langle 0| + (M'_\pm)^* \otimes |1\rangle\langle 1|$. This follows from the linearity of V, along with the facts

$$M_\pm = \frac{I \pm M}{2}, \quad M'_\pm = \frac{I \pm M'}{2}, \quad (M'_\pm)^* = \frac{I \pm (M')^*}{2}. \tag{2.41}$$

Returning to real measurements only, the following theorem of Coladangelo [27] (based closely on the work of Chao et al. [70]) allows us to deduce the existence of a local isometry required for the parallel self-testing of n Bell states and (real) single-qubit Pauli observables. Rather than using measurement statistics directly, the theorem states sufficient conditions in terms of appropriate correlation, anticommutation, and commutation relations of unknown observables available to Alice and Bob. Much of Chapter 5 will be dedicated to proving such relations from certain given correlations. We state the theorem here in notation consistent with that used in Chapter 5.

Theorem 2.8 (Coladangelo [27, Theorem 3.5])**.** *Let $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$, where $\mathcal{H}_A$ and $\mathcal{H}_B$ have even dimension. Suppose there exist balanced reflections $X^i_A, Z^i_A \in \mathcal{L}(\mathcal{H}_A)$ and $X^i_B, Z^i_B \in \mathcal{L}(\mathcal{H}_B)$ for $i \in \{1, \dots, n\}$ such that, for D either A or B and for all distinct i and j, they satisfy*

$$\left\| \left(M^i_A - M^i_B \right) |\psi\rangle \right\| \leq \delta, \tag{2.42a}$$

$$\left\| \left\{ X^i_D, Z^i_D \right\} |\psi\rangle \right\| \leq \delta, \tag{2.42b}$$

$$\left\| \left[M^i_D, N^j_D \right] |\psi\rangle \right\| \leq \delta, \tag{2.42c}$$

where M and N can be either of X and Z. Then, there exists a state $|\xi\rangle \in \tilde{\mathcal{H}}_A \otimes \tilde{\mathcal{H}}_B$ and a local isometry $V = V_A \otimes V_B$, where isometries $V_D : \mathcal{H}_D \to \left(\mathbb{C}^2\right)^{\otimes n} \otimes \tilde{\mathcal{H}}_D$, such that for all i

$$\left\| V |\psi\rangle - |\Phi^+\rangle^{\otimes n}_{AB} \otimes |\xi\rangle \right\| = O\left(n^{\frac{3}{2}} \delta\right), \tag{2.43a}$$

$$\left\| V M^i_D |\psi\rangle - \hat{M}^i_D |\Phi^+\rangle^{\otimes n}_{AB} \otimes |\xi\rangle \right\| = O\left(n^{\frac{3}{2}} \delta\right), \tag{2.43b}$$

where $\hat{X}^i_D$ and $\hat{Z}^i_D$ are Pauli observables acting on the ith qubit subsystem of side D.

The assumptions of Theorem 2.8 that the unknown state spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ have even dimension and that the unknown reflection operators acting on these spaces are balanced (that is, their $+1$ and -1 eigenspaces have equal dimension) are not an issue for self-testing. In the construction of the isometry, one can always extend the $\mathcal{H}_D$ by direct sum with Hilbert spaces of appropriate dimensions on which the extension of $|\psi\rangle$ is defined to have no mass, and correspondingly extend each reflection to have eigenspaces of equal dimensions. Thus we may freely assume these are automatically satisfied by any unknown reflections defined later as part of our self-testing proofs.

2.6 Sum-of-squares (SOS) decomposition

A useful tool for proving robust self-testing statements from Bell inequalities is the sum-of-squares (SOS) decomposition [71, 72]. Suppose that a state $|\psi\rangle$ achieves the maximal quantum value β of some Bell operator O to within an amount $\varepsilon \geq 0$. That is, $\langle\psi| O |\psi\rangle \geq \beta - \varepsilon$. Suppose also that we can write the shifted Bell operator $\beta - O$ in the form

$$\beta - O = \sum_j F_j^\dagger F_j \tag{2.44}$$

for some linear operators F_j. Then

$$\begin{aligned} \varepsilon &\geq \langle\psi| (\beta - O) |\psi\rangle \\ &= \langle\psi| \sum_j F_j^\dagger F_j |\psi\rangle \\ &= \sum_j \| F_j |\psi\rangle \|^2. \end{aligned} \tag{2.45}$$

Therefore, for all j,

$$\| F_j |\psi\rangle \| \leq \sqrt{\varepsilon}. \tag{2.46}$$

As we shall also see in Section 6.3, the F_j may be found to have a form such that Eq. (2.46) gives useful relations from which a self-testing statement may ultimately be deduced.

2.7 Regularization of operators

We may wish to evolve a state by an operation that acts in the same way as a unitary operator, but is not itself known to be unitary. Given $|\psi\rangle \in \mathcal{A} \otimes \mathcal{B}$ and a Hermitian linear operator T on $\mathcal{B}$ such that $T|\psi\rangle \overset{\varepsilon}{\approx} U|\psi\rangle$ for some unitary Hermitian operator

U on $\mathcal{A}$ and $\varepsilon \geq 0$, it is possible to define a new operator $\hat{T}$ on $\mathcal{B}$ that is unitary and acts on $|\psi\rangle$ almost identically to T and U [24, 71, 72].

This *regularization* of T is performed in two steps. One first removes all zero eigenvalues from T by defining a new operator $\tilde{T} = T + P$, where P is the orthogonal projection onto $\ker T$ (although we will sometimes explicitly write its adjoint $\tilde{T}^\dagger$, it should be noted that this operator is Hermitian and $\tilde{T}^\dagger = \tilde{T}$, since both T and P are Hermitian). All nonzero vectors mapped to $\mathbf{0}$ under T remain unchanged under $\tilde{T}$ and so have eigenvalue 1 instead. We then have that $\tilde{T}^\dagger\tilde{T}$ is positive definite: that is $\langle v|\,\tilde{T}^\dagger\tilde{T}\,|v\rangle = \|\tilde{T}|v\rangle\|^2 > 0$ for all nonzero vectors $|v\rangle$ since $\tilde{T}|v\rangle \neq \mathbf{0}$ by construction. Thus, its principal square root $|\tilde{T}| = (\tilde{T}^\dagger\tilde{T})^{1/2}$ is also positive definite. Since this $|\tilde{T}|$ is positive definite, it is therefore also invertible.

In the second step, and using that $|\tilde{T}|$ is invertible, one defines

$$\hat{T} = \tilde{T}|\tilde{T}|^{-1}. \tag{2.47}$$

The regularized operator $\hat{T}$ is unitary by construction. Furthermore, by considering an eigenbasis of T, we see that $\hat{T}T = |T|$. We also have that $|T| = |U^\dagger T|$ (since $U^\dagger$ is unitary), and the property that $|U^\dagger T| \geq U^\dagger T$. This operator inequality is valid since the operator $U^\dagger T$ is Hermitian (U commutes with T and both are Hermitian by assumption). Therefore,

$$\begin{aligned}
\|\hat{T}|\psi\rangle - T|\psi\rangle\| &= \||\psi\rangle - \hat{T}T|\psi\rangle\| \\
&= \||\psi\rangle - |T||\psi\rangle\| \\
&= \||\psi\rangle - |U^\dagger T||\psi\rangle\| \\
&\leq \||\psi\rangle - U^\dagger T|\psi\rangle\| \\
&= \|U|\psi\rangle - T|\psi\rangle\| \\
&\leq \varepsilon.
\end{aligned} \tag{2.48}$$

In other words, $\hat{T}|\psi\rangle \overset{\varepsilon}{\approx} T|\psi\rangle$ and $\hat{T}|\psi\rangle \overset{2\varepsilon}{\approx} U|\psi\rangle$.

Note that the hat notation for regularization performed on operators labeled by X, Y, or Z should not be confused with that of Pauli observables. Regularization is only performed in Chapter 6 and a distinct notation for Pauli observables is consistently used there.

Given a state-dependent anticommutation relation between two Hermitian operators, we may wish to make a similar statement about their regularized versions.

Lemma 2.9. *Let $|\psi\rangle \in \mathcal{A} \otimes \mathcal{B}$. Suppose that T_1 and T_2 are Hermitian operators on $\mathcal{B}$ such that $T_1|\psi\rangle \overset{\varepsilon}{\approx} U_1|\psi\rangle$ and $T_2|\psi\rangle \overset{\varepsilon}{\approx} U_2|\psi\rangle$ for some unitary Hermitian operators U_1 and U_2 on $\mathcal{A}$ and $\varepsilon \geq 0$. Then the regularized operators $\hat{T}_1$ and $\hat{T}_2$ satisfy*

$$\{\hat{T}_1, \hat{T}_2\}|\psi\rangle \overset{c}{\approx} \{T_1, T_2\}|\psi\rangle, \tag{2.49}$$

where $c = (6 + \|T_1\| + \|T_2\|)\varepsilon$.

Proof. As discussed earlier, the regularized operators satisfy $\hat{T}_j|\psi\rangle \overset{2\varepsilon}{\approx} U_j|\psi\rangle$. Thus,

$$\begin{aligned} \{\hat{T}_1, \hat{T}_2\}|\psi\rangle &\overset{4\varepsilon}{\approx} (\hat{T}_1 U_2 + \hat{T}_2 U_1)|\psi\rangle \\ &\overset{2\varepsilon}{\approx} (T_1 U_2 + T_2 U_1)|\psi\rangle, \end{aligned} \tag{2.50}$$

where we have also used the unitarity of $\hat{T}_1$ and $\hat{T}_2$ for the first estimate, and the unitarity of U_1 and U_2 for the second estimate. We also have that

$$\begin{aligned} \|(T_1 U_2 + T_2 U_1)|\psi\rangle - \{T_1, T_2\}|\psi\rangle\| &\leq \|T_1(U_2 - T_2)|\psi\rangle\| + \|T_2(U_1 - T_1)|\psi\rangle\| \\ &\leq (\|T_1\| + \|T_2\|)\varepsilon, \end{aligned} \tag{2.51}$$

and so the result follows. □

Chapter 3

Magic rectangle games

In this chapter, we introduce a class of generalizations to the Mermin–Peres magic square nonlocal game (see Section 2.2) that we call *magic rectangle* games. We characterize the winning probabilities that can be achieved in these games and what qualitative properties are preserved in the generalization. In the next chapter (Chapter 4), we will also explore how our generalization can be used in applications. The specific application we will focus on there is that of certified randomness expansion, while analyses of other device-independent cryptographic primitives using our games are deferred to future works. It is important to distinguish our work from that with a different usage of the term "magic rectangle" that has been used instead in the past to refer to observables arranged into a rectangular array in order to prove the Kochen–Specker theorem in 16 dimensions [73, 74]. The contributions we make in this chapter can be summarized as follows.

- We define a generalization of the Mermin–Peres magic square game to general rectangular dimensions (Definition 3.1).

- We fully characterize the optimal winning probabilities for quantum behaviors of all these magic rectangle games (Theorem 3.13).

- In order to achieve this characterization, we first prove a number of general properties, showing that the optimal winning probabilities for any set of behaviors (local, quantum, almost quantum, or nonsignaling) are: (i) the same for all games of the same dimension, (ii) symmetric with respect to row/column exchange, and (iii) monotonically increasing with the dimension of the rectangle.

- Using the known fact that the regular magic square game (which is a special case of 3×3 magic rectangle games) can be won for quantum strategies with certainty, we reduce the full characterization of magic rectangles to that of $1 \times n$ and $2 \times n$ games (Theorem 3.2). We also show that the CHSH game, according to our definitions, is a 2×2 magic rectangle game (Theorem 3.15). We then obtain the optimal winning probabilities for the $1 \times n$ case, while we lower and upper bound the winning probabilities for $2 \times n$ games. To upper bound the probabilities, we conjecture the almost quantum winning probability based on numerical evidence. As a side result, we get that $2 \times n$ games with $n \geq 3$ can be won with certainty using behaviors at level 1 of the NPA hierarchy (and so exhibit a version of "pseudotelepathy"), while the quantum and almost quantum sets both give winning probabilities strictly smaller than unity (thus not exhibiting pseudotelepathy).

Related works The magic square game was introduced by Mermin [18] and Peres [19], while Cabello [75, 76] and subsequently Aravind [77] stated it as a two-player nonlocal game. Aravind [56] has also given a nontechnical demonstration of the magic square game. The term quantum *pseudotelepathy* was first introduced by Brassard et al. [78], and the magic square game, along with many others that share the property that there exist perfect quantum (but not classical) strategies, were reviewed in [20]. There are a number of generalizations of the magic square that have been considered in literature. Cleve and Mittal [79] analyze quantum strategies for "binary constraint" games—a general class of games that contains the magic rectangles we define—and give some (weaker than our analysis) upper bounds on winning probabilities from quantum strategies. Arkhipov [80] generalized the magic square and magic pentagram games to be played on hypergraphs called *arrangements*, and characterized which arrangements can exhibit quantum pseudotelepathy. Coladangelo and Stark [81] considered "linear constraint" games, focusing on the uniqueness of winning quantum strategies in order to use such games for self-testing.

To determine optimal quantum strategies, it is important to be able to check if a given experimental behavior admits a quantum model/realization. This question is directly linked with the question of the "degree of nonlocality" present in quantum theory. Navascués et al. [59, 60] addressed this by giving an infinite hierarchy of conditions that are satisfied by quantum behaviors, known as the NPA hierarchy. Navascués et al. [61] defined the *almost quantum* set of behaviors, which is the set

closest to the quantum set that arises in a "natural" way and is easy to check. Sets of behaviors that are easy to handle and include the quantum set, as is the case for the levels of the NPA hierarchy and the almost quantum set, have been used successfully to bound the winning probabilities of quantum parties in many cryptographic settings—something we also exploit in this chapter.

Chapter organization In Section 3.1, we define magic rectangle games, and in Section 3.2 give some general results for these games. In Section 3.3 we give a full characterization of the winning probabilities of magic rectangle games. We conclude in Section 3.4, where we discuss our results and give future directions.

Notation In this chapter (and until Chapter 5), we do not refer to any Hilbert spaces explicitly. This makes available the notation $\mathcal{A}$ and $\mathcal{B}$ to denote alphabets for the outcomes of random variables associated with Alice and Bob.

3.1 Magic rectangle games: Definition

More generally than the magic square game of Section 2.2, it is possible to construct similar games for arbitrary sizes of table; a magic square game with m possible questions for Alice and n for Bob corresponds to an $m \times n$ table. Indeed, this may be more appropriately named a magic *rectangle*. In order to avoid trivially winning classical strategies, we must also generalize the game rules.

Definition 3.1 (Magic rectangle games)**.** An $m \times n$ game is specified by fixing some $\alpha_1, \ldots, \alpha_m$ and $\beta_1, \ldots, \beta_n$ each belonging to $\{+1, -1\}$, such that their product satisfies

$$\alpha_1 \ldots \alpha_m \cdot \beta_1 \ldots \beta_n = -1. \tag{3.1}$$

The rules of the given game are then:

R1. Each filled cell must belong to the set $\{+1, -1\}$.

R2. Upon being assigned the ith row, the product of Alice's entries must be α_i.

R3. Upon being assigned the jth column, the product of Bob's entries must be β_j.

As before, the game is won if both players enter the same value into their shared cell.

Notice that the standard 3×3 magic square game described in Section 2.2 is simply the special case where $\alpha_1 = \alpha_2 = \alpha_3 = 1$ and $\beta_1 = \beta_2 = \beta_3 = -1$. In fact, there are 2^{m+n-1} different specifications of $m \times n$ games allowed by Eq. (3.1). Another example of a magic rectangle game configuration is shown in Fig. 3.1. We will often suppress the numerical values $+1$ and -1 to the symbols $+$ and $-$ for simplicity.

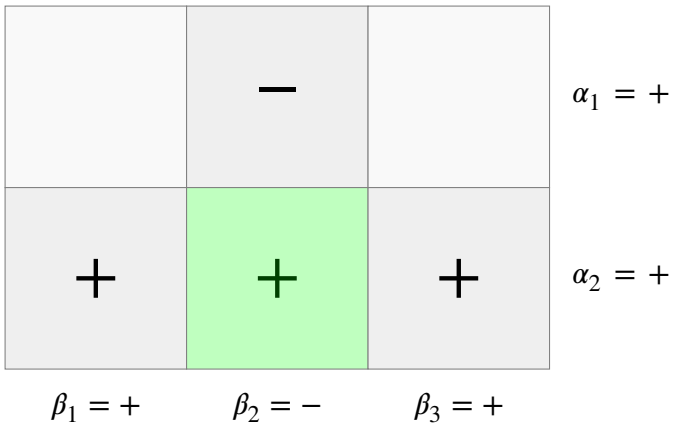


Figure 3.1: A 2×3 magic rectangle game with example answers (combined from example answers of Alice and Bob) entered into its table. This is a valid magic rectangle game since the requested row and column products satisfy $\alpha_1\alpha_2 \cdot \beta_1\beta_2\beta_3 = -1$, as required by Eq. (3.1) of Definition 3.1. Rules R1 to R3 are satisfied by the answers entered in this example. The game is won, with the shared cell containing $+1$ for both players (shaded green).

The requirement of Eq. (3.1) ensures that no deterministic classical strategy that wins with certainty can exist. In such a strategy, definite values would be assigned to each cell of the table which the players must both follow. The product of all cells would be $\alpha_1 \dots \alpha_m$ when calculated according to the rows, and $\beta_1 \dots \beta_n$ according to the columns, but Eq. (3.1) is exactly the statement that these products are not equal. Hence, the optimal classical success rate is at most $1 - (mn)^{-1}$. In fact, this success rate is attainable deterministically by Alice and Bob answering according to fixed (but different) tables satisfying Rules R1 to R3, since such tables can always be constructed which differ in only a single one of their cells (Alice's table need not consider Rule R3 and Bob's table need not consider Rule R2). We denote this optimal classical success rate for our $m \times n$ magic rectangle games by

$$\omega_L(m, n) = 1 - \frac{1}{mn}. \tag{3.2}$$

Let us introduce some further notation to describe our magic rectangle games. We will let X and Y be uniformly distributed random variables taking values in the alphabets $\mathcal{X} = \{1, \dots, m\}$ and $\mathcal{Y} = \{1, \dots, n\}$, respectively, labeling the possible input

rows and columns that may be assigned to Alice and Bob. We will denote the possible output rows of Alice and columns of Bob by the random vectors $\boldsymbol{A} = (A_1, \dots, A_n)$ and $\boldsymbol{B} = (B_1, \dots, B_m)^T$ with alphabets $\mathcal{A}$ and $\mathcal{B}$, respectively, where each A_j and B_i takes values in $\{+1, -1\}$. Referring to Rules R1 to R3, the event that the $m \times n$ magic rectangle game is won upon input $(X, Y) = (x, y)$ is given by

$$W_{x,y}^{m,n} \equiv (A_y = B_x) \cap \left(\prod_{j=1}^{n} A_j = \alpha_x \right) \cap \left(\prod_{i=1}^{m} B_i = \beta_y \right). \tag{3.3}$$

Perhaps more naturally for the games we consider, we can equivalently let $\mathscr{A}$ and $\mathscr{B}$ denote alphabets of the possible question/answer pairs for Alice and Bob allowed by the rules of Definition 3.1. To illustrate why this is the natural choice, we point out that Alice returning a string of ± 1's that is not compatible with Rule R2 is equally forbidden with her returning the value 5 for one cell, and thus it is the natural choice to exclude such outcomes from the alphabet altogether. This is mathematically expressed as

$$\mathscr{A} = \left\{ (x, \boldsymbol{a}) \in \mathcal{X} \times \mathcal{A} : \prod_j a_j = \alpha_x \right\}, \tag{3.4a}$$

$$\mathscr{B} = \left\{ (y, \boldsymbol{b}) \in \mathcal{Y} \times \mathcal{B} : \prod_i b_i = \alpha_y \right\}. \tag{3.4b}$$

Then, with $(X, \boldsymbol{A})$ and $(Y, \boldsymbol{B})$ instead taking values in alphabets $\mathscr{A}$ and $\mathscr{B}$, respectively, the winning event upon input $(X, Y) = (x, y)$ becomes simply

$$A_y = B_x. \tag{3.5}$$

We will refer to these $\mathscr{A}$ and $\mathscr{B}$ as the *natural* alphabets of a magic rectangle game.

In what follows, we characterize the different sizes of magic rectangle games in terms of their optimal win probabilities and strategies, under different levels of allowed nonsignaling correlations (notably quantum, almost quantum, and general nonsignaling correlations).

3.2 Properties of magic rectangle games

To begin our characterization of the magic rectangle games of Definition 3.1, we first show some general properties of these games, which allow us to narrow the considerations required for a full characterization.

Lemma 3.5 shows in what sense it is possible to identify games of the same dimension together. Corollary 3.6 then shows that for magic rectangle games of a given

dimension $m \times n$, all choices of specific values for parameters $\alpha_1, \ldots, \alpha_m$ and $\beta_1, \ldots, \beta_n$ satisfying Eq. (3.1) yield the same optimal win probability at a given level of allowed correlations Σ. We unambiguously refer to this value as $\omega_\Sigma(m, n)$ and show in Corollary 3.10 the symmetry $\omega_\Sigma(m, n) = \omega_\Sigma(n, m)$. We show in Corollary 3.12 that $\omega_\Sigma(m, n)$ is independently increasing in both m and n (with an explicit lower bound given in Lemma 3.11 in terms of that for smaller magic rectangle games). Finally, the correlation hierarchy of Eq. (2.28) implies for any particular game

$$\omega_N \geq \omega_1 \geq \omega_{1+AB} \geq \omega_2 \geq \cdots \geq \omega_Q \geq \omega_L. \tag{3.6}$$

Combining these facts leads us to the path we will take towards a characterization, as stated in the following theorem.

Theorem 3.2. *In order to fully characterize quantum (or weaker) optimal strategies for magic rectangle games of arbitrary dimension, it is sufficient to consider only* $1 \times n$ *games,* $2 \times n$ *games with* $n \geq 2$*, and* 3×3 *games. Moreover, only a single example game for each different dimension need be considered.*

Proof. Postponed until the end of this section, after we have shown some general properties of magic rectangle games. □

Definition 3.3 (Equivalence of games)**.** We will call two games G and G' *equivalent*, and write $G \sim G'$, if there exist bijections $f : \mathscr{A} \to \mathscr{A}'$ and $g : \mathscr{B} \to \mathscr{B}'$ taking the natural alphabets of G to those of G', such that the winning events are equal. That is, such that $(X', \boldsymbol{A}') = f(X, \boldsymbol{A})$ and $(Y', \boldsymbol{B}') = g(Y, \boldsymbol{B})$ imply $W = W'$, where W and W' are the events that each game is won (the sets of underlying outcomes corresponding to a win are requested to be identical, so that the bijections are simply relabeling inputs and outputs while preserving win conditions).

Remark. Under Definition 3.3, given a fixed allowed level for correlations, all equivalent games have the same optimal win probability; strategies are identified with others of equal win probabilities.

Lemma 3.4. *Let* $b, b' \in \{0, 1\}^n$ *be binary sequences of length* $n \geq 2$ *with the same parity (that is their Hamming weights are either both odd or both even). Consider the operations* $\varphi_{i,j}$ *on binary sequences, which have the effect of flipping the bits in both the* i*th and* j*th positions. Then, there exists an involutory composition of these operations* $\varphi = \varphi_{i_m, j_m} \circ \ldots \circ \varphi_{i_1, j_1}$ *such that* $b' = \varphi(b)$.

Proof. Starting with a binary sequence, we can apply operations $\varphi_{i,j}$ one-by-one in the following way: if there are two or more 1's in the sequence, apply the operation which replaces two of the 1's with 0's. If the initial binary sequence had even parity, repeating this process will eventually yield the sequence of zeros. Else, we will eventually have exactly one nonzero element in position k of the sequence. If it is not already the case, we can apply $\varphi_{1,k}$ to take this to the sequence with exactly one nonzero element occurring in the first position. Hence, we can apply a sequence of these operations, taking each binary sequence to a canonical form depending only on its parity. Since each operation $\varphi_{i,j}$ is involutory, and the operations commute, any sequence of these operations is also involutory and thus invertible. Therefore we may apply some sequence of the operations $\varphi_{i_m,j_m} \circ \ldots \circ \varphi_{i_1,j_1}$ taking b to its canonical form, and from its canonical form to b'. □

Lemma 3.5. *Let G be an $m \times n$ magic rectangle game specified by the parameters $\alpha_1, \ldots, \alpha_m$ and $\beta_1, \ldots, \beta_n$ satisfying Eq.* (3.1)*, and let G' be a magic rectangle game of identical dimension specified by $\alpha'_1, \ldots, \alpha'_m$ and $\beta'_1, \ldots, \beta'_n$ also satisfying Eq.* (3.1)*. Then $G \sim G'$ and, moreover, there exists an involution F on the set of $m \times n$ games such that $G' = F(G)$.*

Proof. Consider the operations $F_{i,j}$ which act on a game with parameters $\alpha_1, \ldots, \alpha_m$ and $\beta_1, \ldots, \beta_n$ to produce an identical game with exception that the sign of both α_i and β_j have been flipped (this is a valid game as Eq. (3.1) is still satisfied). Correspondingly, let $f_{i,j}$ and $g_{i,j}$ act on the natural alphabets of the game to produce identical alphabets with the exceptions that each player changes the sign of their output corresponding to the (i, j)th cell of the table. That is, $f_{i,j}(X, \boldsymbol{A})$ differs from $(X, \boldsymbol{A})$ in that Alice flips the sign of A_j if her input is $X = i$; similarly, in $g_{i,j}(Y, \boldsymbol{B})$, Bob flips the sign of $\boldsymbol{B}_i$ if his input is $Y = j$. Upon applying $F_{i,j}$ to a game, the corresponding functions $f_{i,j}$ and $g_{i,j}$ leave the winning event Eq. (3.5) unchanged for all possible inputs. Moreover, the $f_{i,j}$ and $g_{i,j}$ are bijective when considered as maps to the natural alphabets of the game produced by $F_{i,j}$. Hence, $F_{i,j}$ takes games to equivalent games. We will now show that we can apply some sequence of these operations $F = F_{i_k,j_k} \circ \ldots \circ F_{i_1,j_1}$ such that $G' = F(G)$. Transitivity of $\sim$ then shows the desired equivalence.

Consider the parameters of G as a binary sequence $b = (\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n)$ containing an odd number of negative elements. The operation $F_{i,j}$ applied to G acts to flip the sign of α_i and β_j. Furthermore, we can always construct an operation $F_{i_2,j} \circ F_{i_1,j}$ which flips the sign of α_{i_1} and α_{i_2}, and similarly an operation $F_{i,j_2} \circ F_{i,j_1}$ which flips

the sign of β_{j_1} and β_{j_2}. Thus, by applying a sequence of these operations to G, we can flip the sign of any pair of its parameters in b. Therefore applying Lemma 3.4 shows the existence of a sequence of these operations $F = F_{i_k,j_k} \circ \ldots \circ F_{i_1,j_1}$ such that the game $F(G)$ has parameters given by the binary sequence (also containing an odd number of negative elements) $b' = (\alpha'_1, \ldots, \alpha'_m, \beta'_1, \ldots, \beta'_n)$. That is, $G' = F(G)$. Finally, since the $F_{i,j}$ are involutory and commute with one another, F is involutory. □

Corollary 3.6. *Given a fixed correlation level Σ, all magic rectangle games of dimension $m \times n$ have equal optimal win probability, which we denote $\omega_\Sigma(m, n)$.*

Proof. As a direct consequence of Definition 3.3, equivalent games have equal optimal win probabilities at any given level of correlations. In Lemma 3.5, any two valid magic rectangle games G and G' of the same size $m \times n$ are shown to be equivalent $G \sim G'$. Since G and G' may be chosen arbitrarily from all valid $m \times n$ games, all games of size $m \times n$ are equivalent to one another, and so must have equal optimal win probabilities. □

Definition 3.7 (Transpose game)**.** We define the *transpose* of an $m \times n$ game G (with parameters $\alpha_1, \ldots, \alpha_m$ and $\beta_1, \ldots, \beta_n$), denoted by G^T, to be the $n \times m$ game specified by the parameters $\alpha_i^T = \beta_i$ and $\beta_j^T = \alpha_j$ for all $i \in \{1, \ldots, n\}$ and $j \in \{1, \ldots, m\}$.

Lemma 3.8. *Let G be an $m \times n$ magic rectangle game, and fix an allowed level Σ for correlations. If S_Σ is a strategy for G that wins with probability p, then there exists a strategy S_Σ^T for the transpose game G^T that also wins with probability p.*

Proof. We let S_Σ^T be the strategy with the roles of the players exchanged relative to S_Σ, so that Bob's former strategy is now played by Alice, and vice versa. In particular, Alice in the transpose strategy S_Σ^T outputs Bob's columns of the strategy S_Σ as rows. Similarly, Bob in S_Σ^T outputs Alice's rows of S_Σ as columns. Since the values of shared cells remain unchanged by transposing rows and columns, S_Σ^T thus wins with probability p. □

Lemma 3.9. *Let G be an $m \times n$ magic rectangle game, and let G' be an $n \times m$ magic rectangle game. Fix an allowed level Σ for correlations. If S_Σ is a strategy for G that wins with probability p, then there exists a strategy S'_Σ for G' that also wins with probability p.*

Proof. Let S_Σ^T be the *transpose* strategy of S_Σ, obtained from Lemma 3.8. Then, S_Σ^T is a valid strategy for G^T that wins with probability p. By Lemma 3.5, $G' \sim G^T$,

and so there exists a strategy S'_Σ for G' that also wins with probability p, formed by performing S_Σ^T but with alphabets relabeled according to the equivalence between the games (Definition 3.3). □

Corollary 3.10. *Optimal win probability is symmetric in the sense that*

$$\omega_\Sigma(m,n) = \omega_\Sigma(n,m). \tag{3.7}$$

Proof. Let S_Σ be an optimal strategy for an $m \times n$ game G, winning with probability p. Suppose that S'_Σ found from Lemma 3.9 for some $n \times m$ game G' (also winning with probability p) is not optimal. Then, there exists a strategy for G' that wins with probability $q > p$. Again by Lemma 3.9, this implies the existence of a strategy for G that also wins with probability $q > p$, contradicting the optimality of S_Σ. Hence, S'_Σ is an optimal strategy for G'. Since G and G' were arbitrary, optimal strategies for all $m \times n$ and $n \times m$ games win with equal probability $p = \omega_\Sigma(m,n) = \omega_\Sigma(n,m)$. □

Lemma 3.11. *Fix a level of allowed correlation Σ. Let the optimal win probability of $m \times n$ magic rectangle games be given by $\omega_\Sigma(m,n)$. If $m' \geq m$ and $n' \geq n$, then the optimal win probability of $m' \times n'$ games satisfies*

$$\omega_\Sigma(m',n') \geq 1 - \frac{mn}{m'n'}[1 - \omega_\Sigma(m,n)]. \tag{3.8}$$

Proof. Let G be an $m \times n$ magic rectangle game specified by the parameters $\alpha_1, \ldots, \alpha_m$ and $\beta_1, \ldots, \beta_n$. From this, define an $m' \times n'$ game G' such that its parameters are

$$\alpha'_i = \begin{cases} \alpha_i & \text{if } 1 \leq i \leq m, \\ 1 & \text{if } m < i \leq m', \end{cases} \tag{3.9a}$$

$$\beta'_j = \begin{cases} \beta_j & \text{if } 1 \leq j \leq n, \\ 1 & \text{if } n < j \leq n'. \end{cases} \tag{3.9b}$$

Note that G' is indeed a valid game, as its parameters automatically satisfy Eq. (3.1). Let S_Σ be an optimal strategy for G, winning with probability $\omega_\Sigma(m,n)$, in which Alice outputs according to the random row vector $\boldsymbol{A} = (A_1, \ldots, A_n)$ and Bob according to the random column vector $\boldsymbol{B} = (B_1, \ldots, B_m)^T$. Construct a strategy S'_Σ for G' in which Alice and Bob play their part of the strategy S_Σ upon inputs $1 \leq X' \leq m$ and $1 \leq Y' \leq n$ respectively, but deterministically append 1's to their outputs to make up

the required output length; upon other inputs, the players output only 1's. That is,

$$\boldsymbol{A}' = \begin{cases} (A_1, \ldots, A_n, 1, \ldots, 1) & \text{if } 1 \leq X' \leq m, \\ (1, \ldots, 1) & \text{if } m < X' \leq m', \end{cases} \tag{3.10a}$$

$$\boldsymbol{B}' = \begin{cases} (B_1, \ldots, B_m, 1, \ldots, 1)^T & \text{if } 1 \leq Y' \leq n, \\ (1, \ldots, 1)^T & \text{if } n < Y' \leq n'. \end{cases} \tag{3.10b}$$

It is clear that these outputs always satisfy the rules given in Definition 3.1 for the parameters of G' defined in Eq. (3.9). Moreover, by using strategy S'_Σ, the players succeed at G' with probability $\omega_\Sigma(m,n)$ upon mn of the $m'n'$ possible inputs, and with certainty upon the remaining inputs. By Corollary 3.6, the win probability of S'_Σ at the $m' \times n'$ game G' is at most the optimal win probability for $m' \times n'$ games $\omega_\Sigma(m', n')$. Hence, since the inputs are chosen uniformly at random,

$$\omega_\Sigma(m', n') \geq \frac{mn}{m'n'}\omega_\Sigma(m,n) + \frac{m'n' - mn}{m'n'}, \tag{3.11}$$

which is exactly Eq. (3.8). □

Corollary 3.12. *Fix a correlation level Σ, and let $m' \geq m$ and $n' \geq n$. Then*

$$\omega_\Sigma(m', n') \geq \omega_\Sigma(m,n). \tag{3.12}$$

Proof. Immediate from Eq. (3.8) upon noting $\frac{mn}{m'n'} \leq 1$ and $\omega_\Sigma(m,n) \leq 1$. □

Having stated and proven the preceding properties of magic rectangle games, it is now easy to see that Theorem 3.2 holds as follows.

Proof of Theorem 3.2. The second part of the claim (that only a single example game for each different dimension need be considered) is shown by Lemma 3.5 and Corollary 3.6, which state that all games of the same dimension are equivalent.

For the first part of the claim, we first choose to examine optimal strategies for $1 \times n$ games. Then, by Lemma 3.9 and Corollary 3.10, there are maps between optimal strategies for $n \times 1$ games and $1 \times n$ games. We next examine $2 \times n$ games (without the need to consider the 2×1 case already covered). Again, due to Lemma 3.9 and Corollary 3.10, we find we need not consider $n \times 2$ cases. Finally, considering the following observations, we will see that all $m \times n$ games where both $m \geq 3$ and $n \geq 3$ can be won with certainty for quantum (or weaker) behaviors. It was pointed out in Section 2.2 that quantum strategies for the standard 3×3 magic square game that win with certainty are already known. As the Rules S1 to S3 for the standard 3×3 magic

square game are a special case of our magic rectangle games given in Definition 3.1, the existence of quantum winning strategies for all general 3×3 games is guaranteed by Corollary 3.6. Therefore, since by Corollary 3.12 the quantum value $\omega_Q(m,n)$ is increasing in m and n, and noting the inequalities of Eq. (3.6), all magic rectangle games with $m \geq 3$ and $n \geq 3$ satisfy $\omega_\Sigma(m,n) = 1$, where Σ is any nonsignaling correlation level at most as strong as the quantum set. Furthermore, the proof of Lemma 3.11 combined with Lemma 3.5 shows how to construct winning strategies for all such games from a winning 3×3 strategy. Hence, the 3×3 games already studied are the final case required to complete the characterization of magic rectangle games. □

3.3 Characterization of magic rectangles

Following Theorem 3.2, we characterize magic rectangle games of all sizes by considering those of dimension $1\times n$ for $n \geq 1$ and $2\times n$ for $n \geq 2$. The final 3×3 case was already discussed in Section 2.2.

Theorem 3.13. *The optimal success probabilities of all magic rectangle games can be characterized as follows.*

1. *Games of dimension $1\times n$ cannot exhibit superclassical behavior:*

$$\omega_N(1,n) = \omega_L(1,n) = 1 - \frac{1}{n}. \tag{3.13}$$

2. *Games of dimension $2\times n$ for $n \geq 2$ satisfy*

$$1 - \frac{2-\sqrt{2}}{2n} \leq \omega_Q(2,n) \leq \omega_{1+AB}(2,n) = \frac{1}{2}\left(1+\sqrt{1-\frac{1}{n}}\right), \tag{3.14}$$

   where the final equality is conjectured, with strong numerical evidence for $n \leq 6$. Such games can be won with certainty in the general nonsignaling regime:

$$\omega_N(2,n) = 1. \tag{3.15}$$

   Moreover, for NPA hierarchy level 1 (or weaker) correlations and $n \geq 3$,

$$\omega_1(2,n) = 1. \tag{3.16}$$

3. *For all quantum or weaker correlations, games of dimension $m\times n$ where both $m \geq 3$ and $n \geq 3$ can be won with certainty:*

$$\omega_Q(m,n) = 1. \tag{3.17}$$

Proof. The content of Item 1 is Theorem 3.14. The discussion in Section 3.3.2 covers Item 2. Item 3 was discussed as part of the proof of Theorem 3.2, and can be seen by combining Corollary 3.12 with the fact that $\omega_Q(3,3) = 1$ by Corollary 3.6. □

3.3.1 1-by-n magic rectangles

Theorem 3.14. *Under any set of nonsignaling correlations, the optimal win probability of* $1 \times n$ *games coincides with the classical value,*

$$\omega_N(1,n) = \omega_L(1,n) = 1 - \frac{1}{n}. \tag{3.18}$$

Proof. For all possible inputs $Y = j$ for Bob, his single output value is deterministically equal to β_j according to Rule R3 of Definition 3.1. However, recalling Eq. (3.1) and denoting the product of Alice's single output row by α, we require any valid $1 \times n$ game to satisfy $\alpha \neq \beta_1 \ldots \beta_n$. That is, Alice's output row must contain at least one element, in position k say, which differs from the output value β_k Bob would give if his input was $Y = k$. By the assumption of no-signaling, Alice cannot have any knowledge about which of n possible uniform inputs was provided to Bob. Thus the probability of the losing event that $A_k \neq \beta_k$ (the element of Alice's output corresponding to Bob's input differs from Bob's output) is at least n^{-1}. Therefore $\omega_N(1,n) \leq 1 - n^{-1} = \omega_L(1,n)$. Since trivially also $\omega_N(1,n) \geq \omega_L(1,n)$ by Eq. (3.6), we have the result. □

3.3.2 2-by-n magic rectangles

Before discussing the general case of $2 \times n$ magic rectangle games, let us first examine the special case of 2×2 magic square games.

3.3.2.1 2-by-2 magic squares

In this case, Eq. (3.1) states that either exactly one of the possible rows or columns is required to have a negative product, or exactly one is required to have a positive product. In fact, any such 2×2 magic square game can be identified with the well-known CHSH game, in which Alice and Bob are provided binary inputs $X_{\text{CHSH}} \in \{0,1\}$ and $Y_{\text{CHSH}} \in \{0,1\}$ uniformly at random, and win by returning binary outputs $A_{\text{CHSH}} \in \{0,1\}$ and $B_{\text{CHSH}} \in \{0,1\}$ which satisfy [9]

$$A_{\text{CHSH}} \oplus B_{\text{CHSH}} = X_{\text{CHSH}} \wedge Y_{\text{CHSH}}. \tag{3.19}$$

We will now explicitly construct this equivalence, whereupon we note the statement $\omega_L(2,2) = \frac{3}{4}$ defines the unique nontrivial facet of the local polytope in the $(2,2,2)$ Bell scenario (which corresponds also to the CHSH inequality) [58, 82].

Theorem 3.15. *Any* 2×2 *magic square game is equivalent (in the sense of Definition 3.3) to the CHSH game.*

Proof. Consider the 2×2 magic square with specified row products $(\alpha_1, \alpha_2) = (+,+)$ and column products $(\beta_1, \beta_2) = (+,-)$. We first show that this game is equivalent to the CHSH game. Then, since all 2×2 games are equivalent (Lemma 3.5), the desired result follows by transitivity.

We can identify the input events of the two games as

$$X_{\text{CHSH}} = 0 \longleftrightarrow X = 1, \tag{3.20a}$$
$$X_{\text{CHSH}} = 1 \longleftrightarrow X = 2 \tag{3.20b}$$

for Alice, and for Bob

$$Y_{\text{CHSH}} = 0 \longleftrightarrow Y = 1, \tag{3.21a}$$
$$Y_{\text{CHSH}} = 1 \longleftrightarrow Y = 2. \tag{3.21b}$$

Alice identifies her two possible outputs as simply

$$A_{\text{CHSH}} = 0 \longleftrightarrow \boldsymbol{A} = (+,+), \tag{3.22a}$$
$$A_{\text{CHSH}} = 1 \longleftrightarrow \boldsymbol{A} = (-,-). \tag{3.22b}$$

Bob identifies his outputs depending on his assigned input. If $Y_{\text{CHSH}} = 0$ (equivalently $Y = 1$), then he makes the identifications

$$\boldsymbol{B}_{\text{CHSH}} = 0 \longleftrightarrow \boldsymbol{B} = (+,+)^T, \tag{3.23a}$$
$$\boldsymbol{B}_{\text{CHSH}} = 1 \longleftrightarrow \boldsymbol{B} = (-,-)^T. \tag{3.23b}$$

However, if $Y_{\text{CHSH}} = 1$ (equivalently $Y = 2$), then he makes alternative identifications

$$\boldsymbol{B}_{\text{CHSH}} = 0 \longleftrightarrow \boldsymbol{B} = (+,-)^T, \tag{3.24a}$$
$$\boldsymbol{B}_{\text{CHSH}} = 1 \longleftrightarrow \boldsymbol{B} = (-,+)^T. \tag{3.24b}$$

These identifications form bijections $f : \mathscr{A}_{\text{CHSH}} \to \mathscr{A}$ and $g : \mathscr{B}_{\text{CHSH}} \to \mathscr{B}$ between the natural alphabets of each game, and are explicitly tabulated in Table 3.1.

Table 3.1: The bijections $f\colon \mathscr{A}_{\text{CHSH}} \to \mathscr{A}$ and $g\colon \mathscr{B}_{\text{CHSH}} \to \mathscr{B}$ used to show the equivalence between the CHSH game and the 2×2 magic square game with parameters $(\alpha_1, \alpha_2) = (+,+)$ and $(\beta_1, \beta_2) = (+,-)$. Elements of the natural alphabets $\mathscr{A}$, $\mathscr{B}$, $\mathscr{A}_{\text{CHSH}}$, and $\mathscr{B}_{\text{CHSH}}$ have the form of possible input/output pairs for each game and player, with the input written first.

f		g	
$\mathscr{A}_{\text{CHSH}}$	$\mathscr{A}$	$\mathscr{B}_{\text{CHSH}}$	$\mathscr{B}$
$(0,0)$	$(1,(+,+))$	$(0,0)$	$(1,(+,+)^T)$
$(0,1)$	$(1,(-,-))$	$(0,1)$	$(1,(-,-)^T)$
$(1,0)$	$(2,(+,+))$	$(1,0)$	$(2,(+,-)^T)$
$(1,1)$	$(2,(-,-))$	$(1,1)$	$(2,(-,+)^T)$

It remains to show that the winning event for the CHSH game, Eq. (3.19), and the winning event for the 2×2 magic rectangle game of Eq. (3.5) over all inputs

$$\bigcup_{x,y\in\{1,2\}} [(A_y = B_x) \cap (X = x) \cap (Y = y)] \tag{3.25}$$

are identical under the functions f and g. We can rewrite these two events to more closely resemble one another as

$$\bigcup_{x,y\in\{0,1\}} [(A_{\text{CHSH}} \oplus B_{\text{CHSH}} = x \wedge y) \cap (X_{\text{CHSH}} = x) \cap (Y_{\text{CHSH}} = y)] \tag{3.26}$$

for Eq. (3.19), and for Eq. (3.25)

$$\bigcup_{x,y\in\{0,1\}} [(A_{y+1} = B_{x+1}) \cap (X = x+1) \cap (Y = y+1)]. \tag{3.27}$$

One can verify from the identifications made (for example by examining Table 3.1) that terms in the first union Eq. (3.26) are pairwise equal to those in the second union Eq. (3.27). For example, for the term where inputs $x = 0$ and $y = 0$, Table 3.1 defines that the relevant ($x = 0$) input/output pairs for Alice relate through bijection $f\colon \mathscr{A}_{\text{CHSH}} \to \mathscr{A}$ by

$$(0,0) \overset{f}{\mapsto} (1,(+,+)), \tag{3.28a}$$

$$(0,1) \overset{f}{\mapsto} (1,(-,-)), \tag{3.28b}$$

and the relevant ($y = 0$) pairs for Bob relate through bijection $g\colon \mathscr{B}_{\text{CHSH}} \to \mathscr{B}$ by

$$(0,0) \overset{g}{\mapsto} (1,(+,+)^T), \tag{3.29a}$$

$$(0,1) \overset{g}{\mapsto} (1,(-,-)^T). \tag{3.29b}$$

We then see that

$$(A_{\mathrm{CHSH}} \oplus B_{\mathrm{CHSH}} = 0) \equiv (A_1 = B_1), \tag{3.30a}$$

$$(X_{\mathrm{CHSH}} = 0) \equiv (X = 1), \tag{3.30b}$$

$$(Y_{\mathrm{CHSH}} = 0) \equiv (Y = 1), \tag{3.30c}$$

and so, combined together into the term in question,

$$\begin{aligned}&[(A_{\mathrm{CHSH}} \oplus B_{\mathrm{CHSH}} = 0) \cap (X_{\mathrm{CHSH}} = 0) \cap (Y_{\mathrm{CHSH}} = 0)] \\ &\quad \equiv [(A_1 = B_1) \cap (X = 1) \cap (Y = 1)].\end{aligned} \tag{3.31}$$

Analogous statements can be made for all terms in Eqs. (3.26) and (3.27), since we have exhibited some f and g that allow it. That is, for all $x, y \in \{0, 1\}$,

$$\begin{aligned}&[(A_{\mathrm{CHSH}} \oplus B_{\mathrm{CHSH}} = x \wedge y) \cap (X_{\mathrm{CHSH}} = x) \cap (Y_{\mathrm{CHSH}} = y)] \\ &\quad \equiv [(A_{y+1} = B_{x+1}) \cap (X = x + 1) \cap (Y = y + 1)].\end{aligned} \tag{3.32}$$

Therefore, the unions Eqs. (3.26) and (3.27) are equal, and thus so are the winning events for the CHSH and 2×2 magic rectangle games of Eqs. (3.19) and (3.25) over all inputs. □

Corollary 3.16. *The maximum probability with which the* 2×2 *magic square game can be won is (i)* $\frac{1}{4}\left(2 + \sqrt{2}\right) \approx 0.854$ *for quantum strategies and (ii) unity for general nonsignaling strategies.*

Proof. The result of Theorem 3.15 means that the maximum attainable win probability for any quantum strategy coincides with that of the CHSH game, namely $\frac{1}{4}\left(2+\sqrt{2}\right) \approx 0.854$. For the same reason, under PR box assumptions [83], the 2×2 magic square game can be won with certainty. □

An example of the identifications made for the 2×2 magic square game considered in the proof of Theorem 3.15 is depicted in Fig. 3.2.

3.3.2.2 General 2-by-n games

As stated in Theorem 3.2, it is enough to consider $n \geq 2$. From Eq. (3.2), the optimal classical win probability for $2 \times n$ games is given by

$$\omega_L(2, n) = 1 - \frac{1}{2n}. \tag{3.33}$$

Using the discussion of Section 3.3.2.1, we can apply Lemma 3.11 to an optimal 2×2 quantum strategy with value $\omega_Q(2, 2) = \frac{1}{4}\left(2 + \sqrt{2}\right)$ as given by Corollary 3.16. The

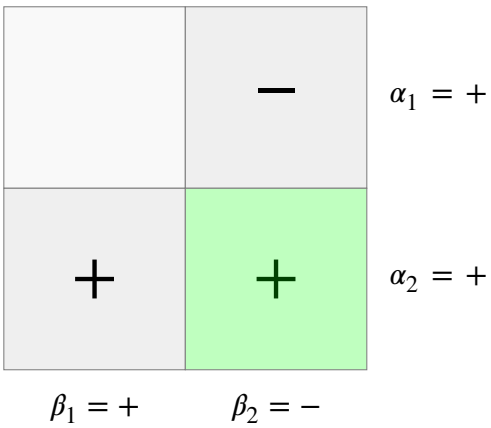


Figure 3.2: Example of the equivalence of the 2×2 magic square and CHSH games. Shown is a filled 2×2 magic square with row products $(\alpha_1, \alpha_2) = (+, +)$ and column products $(\beta_1, \beta_2) = (+, -)$ specified. The input row and column $X = 2$ and $Y = 2$ were chosen for this example. Alice gave output $\boldsymbol{A} = (+, +)$ and Bob gave output $\boldsymbol{B} = (-, +)^T$. The outputs from both players are combined in the single table shown. The game is won since $A_2 = B_2$ (shaded green). The equivalent input and output configuration for the CHSH game, using the identifications of Table 3.1, are $(X_{\text{CHSH}}, A_{\text{CHSH}}) = (1, 0)$ and $(Y_{\text{CHSH}}, B_{\text{CHSH}}) = (1, 1)$. The CHSH win condition of Eq. (3.19) is also satisfied.

win probability of the resulting $2 \times n$ strategy lower bounds the $2 \times n$ quantum value via Eq. (3.8) as

$$\omega_Q(2, n) \geq 1 - \frac{2 - \sqrt{2}}{2n}. \tag{3.34}$$

In order to find an upper bound for this quantum value, we have used the implementation of the NPA hierarchy found in the NCPOL2SDPA [84] package with the MOSEK [85] semidefinite program solver. Optimal values for different $2 \times n$ games and levels of the hierarchy are shown in Table 3.2.

We note that for all levels $1 + AB$ and above that were tested, the optimal value is identical for each $2 \times n$ game, and appears to bound above the quantum value for $n \leq 6$ by the closed-form expression

$$\omega_Q(2, n) \leq \omega_{1+AB}(2, n) = \frac{1}{2}\left(1 + \sqrt{1 - \frac{1}{n}}\right). \tag{3.35}$$

Furthermore, the so-called "intersection graph" of a $2 \times n$ magic rectangle game (obtained by swapping the roles of vertices and edges in a hypergraph whose edges are the different rows and columns of the magic rectangle table) corresponds to the complete bipartite graph $K_{2,n}$. This graph is planar for all n, as can be seen by placing the n vertices of one partition in a straight line in the plane with the two vertices of the other partition above and below the line. Therefore, we know using a result of Arkhipov [80, Theorem 21] that $\omega_Q(2, n) < 1$.

Table 3.2: Optimal win probabilities for $2 \times n$ magic rectangle games under correlations allowed by different levels of the NPA hierarchy. We see that, for the cases tested, the optimal win probabilities are identical at every level beyond the almost quantum $1 + AB$ level. Moreover, these values appear to follow exactly the expression given in Eq. (3.35). For $n \geq 3$, we observe games which can be won with certainty at level 1, but with lower than unit probability at the almost quantum and higher levels. Values were obtained through NCPOL2SDPA [84] with the MOSEK [85] solver. Results were also verified with the QETLAB [86] toolbox, using MOSEK [87] within CVX [88].

	NPA hierarchy level				
n	1	$1 + AB$	2	3	4
2	0.8535533906	0.8535533906	0.8535533906	0.8535533906	0.8535533906
3	1.0000000000	0.9082482905	0.9082482905	0.9082482905	0.9082482905
4	1.0000000000	0.9330127019	0.9330127019		
5	1.0000000000	0.9472135955	0.9472135955		
6	1.0000000000	0.9564354646			

While the output of the semidefinite program solver, say for the $1 + AB$ level, explicitly specifies a behavior that is achievable at that level, a truly quantum strategy of states and measurements implementing these behaviors remains elusive for $2 \times n$ games larger than 2×2. Indeed, a quantum strategy for the behaviors given at the levels examined in Table 3.2 may be unachievable, despite the numerical indication. It is thus unknown precisely where the quantum value of these games sits between the upper and lower bounds discussed. Another open problem is that of finding a general analytic proof of Eq. (3.35) extending to any n (while for small n we can often find this from inspection of the semidefinite program solver output as noted). The classical value given by Eq. (3.33) and the quantum bounds given by Eqs. (3.34) and (3.35) are depicted in Fig. 3.3.

Conjecture 3.17. *The expression for* $\omega_{1+AB}(2, n)$ *given in Eq.* (3.35) *holds for all* $n \geq 1$.

Remark. Using the SDPA-GMP [89–91] semidefinite program solver with arbitrary-precision arithmetic, we have been able to verify agreement of Eq. (3.35) with all but the most computationally intensive entries of Table 3.2 to a much higher precision than printed.

Since under general no-signaling assumptions the 2×2 magic square game can be won with certainty (Corollary 3.16), so too can all $2 \times n$ games with $n \geq 2$ by Corollary 3.12. It is interesting to note that, as far as the authors are aware, those

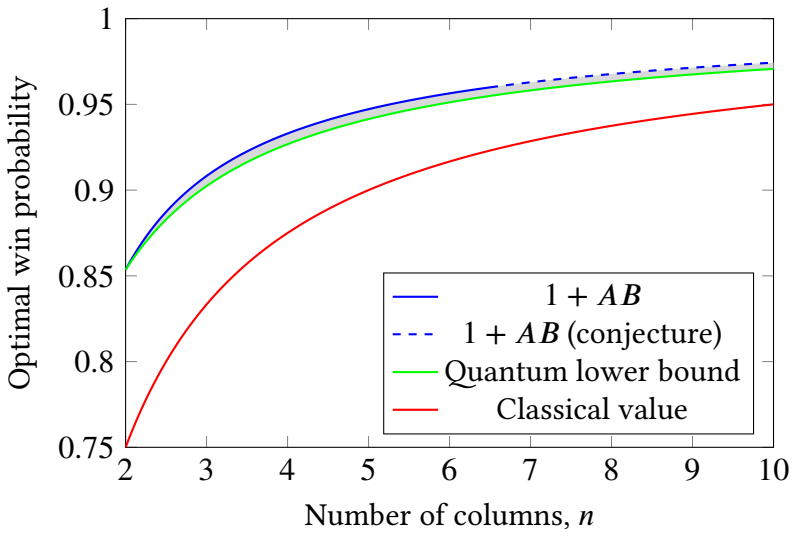


Figure 3.3: Bounds on the optimal quantum win probability of $2 \times n$ magic rectangle games. The lowermost curve is the classical value for each game, given by Eq. (3.33). The middle curve is the lower bound of Eq. (3.34) on the quantum value of each game, resulting from application of Lemma 3.11 to the optimal quantum value for 2×2 games. The solid upper curve shows the maximal almost quantum win probability (see NPA hierarchy level $1 + AB$ of Table 3.2), which provides an upper bound to the quantum value; where the line is dashed corresponds to our conjectured values for large n, given by Eq. (3.35), which have proved to be too computationally intensive to test. The region within which the quantum values could possibly lie is shaded.

$2 \times n$ games for $n \geq 3$ examined in Table 3.2 are the first examples of nonlocal games with the property that they can be won with certainty using NPA hierarchy level 1 correlations, but only with less than unit probability using almost quantum level $1 + AB$ correlations. This hints that it may be fruitful to study these games in the quantum measure theory framework for studying fundamental nonlocality, in which level 1 NPA correlations imply the existence of a strongly positive joint quantum measure, while level $1 + AB$ correlations are equivalent to those satisfying a similar condition [92]. Additionally, when the optimal value of a game is unity, winning individual rounds of that game offers greater statistical significance; losing even a single round would immediately discredit the supposed strategy of (ideal) players. Here, this is the case at level 1 but not at the higher levels of the same underlying game. An explicit strategy for winning the 2×3 game with certainty using NPA hierarchy level 1 correlations is given in Appendix A. Hence, by Corollary 3.12, the result that $\omega_1(2, n) = 1$ for all $n \geq 3$ is exact.

3.4 Discussion

In this chapter, we defined a class of nonlocal games which we called "magic rectangles", since they are natural generalizations of the Mermin [18] and Peres [19] magic square. We obtained a complete characterization of magic rectangle games with respect to the winning probabilities of quantum and classical strategies.

We have shown that $1 \times n$ games cannot exhibit superclassical behavior. Moreover, any magic rectangle game of at least size 3×3 can be won with certainty using quantum or weaker correlations. For these games, the interesting properties of strong contextuality and implementation with only Clifford computations of the regular magic square game are preserved. We have also shown that the special case of dimension 2×2 is identical to the CHSH game, which is well studied and does not exhibit the aforementioned properties.

The class of $2 \times n$ games for $n \geq 3$ is seen to exhibit the richest behavior: there do not exist perfect quantum winning strategies for these games, however, we have shown superclassical lower bounds on their optimal success probabilities using quantum correlations. We have also given numerical upper bounds on quantum win probabilities for these games with small n, and conjectured a closed-form expression extending to all n. An interesting consequence of our analysis of $2 \times n$ magic rectangle games is that they provide examples of nonlocal games that can be won with certainty using NPA level 1 correlations, and yet for which no quantum (or, considering our numerical results, even almost quantum) strategy winning with certainty exists (see also Appendix A for a 2×3 example strategy using NPA level 1 correlations).

Future works As a first point for future work, it would be interesting to further generalize our games to the multipartite scenario, in which players would output by filling $(d-1)$-dimensional slices of a "magic hyperrectangle" of d dimensions. Specific rules for the players of such hyperrectangles games (perhaps resembling the product of rows/columns and win condition imposed in the rectangular case) would need to be found such that the generalization is useful (i.e. a gap between classical and quantum win probabilities exists). By characterizing a suitable generalization of this kind, it may also be possible to identify other well-known multipartite nonlocal games as special cases. Another interesting future direction is to closer examine the special class of $2 \times n$ magic rectangles. The problem of finding optimal quantum values is still an open question, where the possibilities that they coincide with our lower

bounds, upper bounds, or something between all have interesting implications. In the first case, optimal strategies could be implemented using CHSH sub-games. Games of the third case would outperform the CHSH game while also exhibiting a separation between the quantum and almost quantum sets. We believe the second case, in which the quantum and almost quantum sets coincide for each magic rectangle, to be the most likely. This would provide further evidence of the naturality of almost quantum correlations. Once specific strategies (for games beyond CHSH) have been obtained, one could directly see how these perform for various device-independent cryptographic primitives or self-testing.

Chapter 4

Application: Certified private randomness expansion

In this short chapter, we will be concerned with utilizing the Bell inequality violations provided by magic rectangle games (as examined in detail in the previous chapter) to achieve certified randomness expansion using the device-independent spot-checking protocol R_{gen} described in [54, Figure 2]. The main technical result of this chapter is to relate the win probabilities of $m \times n$ magic rectangle games that have a *distinguished input* (that is, a game that instead has deterministic outputs upon a single distinguished choice of input), to those of ordinary $(m-1) \times (n-1)$ games (with no distinguished input). This enables us to get the optimal noise tolerance of such games, as well as to simply obtain rates for randomness expansion using general magic rectangle games. In terms of rates, there are also new techniques that could significantly improve our results [93, 94], however, utilizing these would be more involved, with analysis of each game of interest to be undertaken on a case-by-case basis (see also Section 4.3).

Related works Certified randomness expansion was first introduced by Colbeck and Kent [5], with the idea first appearing in Dec. 2006 as part of the thesis of Colbeck [95, Chapter 5]. Afterwords (2010), renewed attention was brought to this work by Pironio et al. [64], who developed it further with a proof-of-concept experiment. Vazirani and Vidick [96] demonstrated quantum security for an exponential expansion protocol. Subsequently (2016), Miller and Shi [66] obtained cryptographic security and robustness. Acín and Masanes [97] reviewed efforts to design device-independent quantum random number generators (up to 2016), and included a comparison of the

main protocols. In Jan. 2017, Miller and Shi [54] gave the spot-checking protocol that we use for our analysis of certified randomness expansion, and to obtain bounds on expansion rates. Finally, Arnon-Friedman et al. [93] (2019) and Brown et al. [94] (2020) detail more modern techniques, which give better rates for the spot-checking protocol by using the entropy accumulation theorem [98, 99]. These are more involved and case-specific than [54] and, thus, to give a general analysis of certified randomness for all magic rectangle games, we opt to use the results of Miller and Shi [54] (summarized using our notation in Section 2.4) in this chapter. Note, however, that the noise tolerances we obtain for the different magic rectangle games do not depend on the specific technique used to bound the rates, and thus apply in general.

Chapter organization We use the characterization of our games given in the previous chapter (Chapter 3) to analyze the certified randomness expansion achievable using our magic rectangle games. Specifically, we show in Section 4.1 that the win probability of an $m \times n$ game with a distinguished input can be obtained from that of the $(m-1) \times (n-1)$ game (this is Theorem 4.2). This, along with the results of Theorem 3.13 from the previous chapter, allows us in Section 4.2 to determine the noise tolerance (robustness) in the case of each magic rectangle game. Also in Section 4.2, we then follow the analysis of Miller and Shi [54] to get rates for certified randomness expansion using different magic rectangle games (see Table 4.1 for a summary of both noise tolerance and rate results). We discuss the results and possible future works in Section 4.3.

4.1 Win probability with distinguished input

Let us recall from Section 3.1 in the previous chapter the events that the $m \times n$ magic rectangle game with row parameters $\alpha_1, \ldots, \alpha_m$ and column parameters $\beta_1, \ldots, \beta_n$ is won **and** that an input $(X, Y) = (x, y)$ was chosen

$$W_{x,y}^{m,n} \equiv (A_y = B_x) \cap (X = x) \cap (Y = y). \tag{4.1}$$

The inputs to Alice and Bob can take values $x \in \{1, \ldots, m\}$ and $y \in \{1, \ldots, n\}$ due to the $m \times n$ size of magic rectangle game being considered. The random variables A_j and B_i denote values belonging to $\{+, -\}$ for individual cells of the outputs given by Alice and Bob, respectively. Given that the inputs were $X = x$ and $Y = y$, they are

assumed to satisfy

$$\prod_{j=1}^{n} A_j = \alpha_x, \quad \prod_{i=1}^{m} B_i = \beta_y. \tag{4.2}$$

The events in $\left\{W_{x,y}^{m,n}\right\}_{x,y}$ are pairwise disjoint, and the overall event corresponding to winning the game is given by their (disjoint) union

$$W^{m,n} = \bigcup_{x,y} W_{x,y}^{m,n}. \tag{4.3}$$

Since $1 \times n$ magic rectangle games do not exhibit superclassical behavior (see Theorem 3.14), such games cannot be used in randomness expansion. We construct an optimal strategy for arbitrary $m \times n$ magic rectangle games having a distinguished input, where we may henceforth consider only the cases $m, n \geq 2$.

In the proof that follows, we will make use of a simple fact of probabilities, which we state here for convenience.

Lemma 4.1. *Suppose that for some events W, E, and F we have*

$$\Pr(E \mid W \cap F) = 1. \tag{4.4}$$

Then it is true that

$$\Pr(W \mid F) = \Pr(W \cap E \mid F). \tag{4.5}$$

Proof. By the definition of conditional probabilities, the assumption can be rewritten as

$$\frac{\Pr(E \cap W \cap F)}{\Pr(W \cap F)} = 1 \tag{4.6}$$

or, equivalently, $\Pr(W \cap F) = \Pr(E \cap W \cap F)$. Dividing both sides by $\Pr(F)$ gives

$$\frac{\Pr(W \cap F)}{\Pr(F)} = \frac{\Pr(E \cap W \cap F)}{\Pr(F)}. \tag{4.7}$$

After writing both sides of the equality using the definition of conditional probabilities, this is exactly the desired equation. □

We now proceed with the proof of optimal strategies assuming the presence of a distinguished input.

Theorem 4.2. *Fix an allowed level Σ for nonsignaling correlations. The optimal win probability for any $m \times n$ magic rectangle game having a distinguished input, with $m \geq 2$ and $n \geq 2$, is given by*

$$\bar{\omega}_\Sigma(m, n) = 1 - \frac{(m-1)(n-1)}{mn}[1 - \omega_\Sigma(m-1, n-1)]. \tag{4.8}$$

A strategy which attains this value is to play an optimal strategy for $(m-1) \times (n-1)$ games, but with all output strings extended to include one deterministic entry.

Remark. While the similar expression from Lemma 3.11 depicts a similar expression as a lower bound (for the win probability when no distinguished input is assumed), the present result claims that this value is also the greatest achievable win probability when restricted to devices having a distinguished input.

Proof. We will let the event that the game is won and some input $(X, Y) = (x, y)$ chosen be denoted by $W_{x,y} \equiv W^{m,n}_{x,y}$ throughout this proof for brevity, as we have fixed the size of the magic rectangle as $m \times n$. Similarly, we write $W \equiv W^{m,n}$ for the overall event that the game is won.

Without loss of generality, let us choose the distinguished input to be given by the event $(X = 1) \cap (Y = 1)$. By imposing the no-signaling principle, we see that for all inputs $x \in \{1, \dots, m\}$ and $y \in \{1, \dots, n\}$, there exists an output entry $a^x \in \{+1, -1\}$ for Alice such that

$$\begin{aligned} &\Pr(A_1 = a^x \mid W \cap X = x \cap Y = y) \\ &\quad = \Pr(A_1 = a^x \mid W \cap X = x \cap Y = 1) \\ &\quad = \Pr(B_x = a^x \mid W \cap X = x \cap Y = 1) \\ &\quad = \Pr(B_x = a^x \mid W \cap X = 1 \cap Y = 1) \\ &\quad = \Pr(B_x = a^x \mid W \cap Y = 1) = 1, \end{aligned} \tag{4.9}$$

where the second equality uses our conditioning on the event that the game is won; the first, third, and fourth equalities use no-signaling; and the final equality comes from our choice of distinguished input. Similarly, there exists an output b^y for Bob such that

$$\begin{aligned} &\Pr(B_1 = b^y \mid W \cap X = x \cap Y = y) \\ &\quad = \Pr(A_y = b^y \mid W \cap X = 1) = 1. \end{aligned} \tag{4.10}$$

Combining Eqs. (4.9) and (4.10) yields

$$\Pr(A_1 = a^x \cap B_1 = b^y \mid W \cap X = x \cap Y = y) = 1. \tag{4.11}$$

Now, from the fact of probabilities stated in Lemma 4.1 and Eq. (4.11), we can see

$$\Pr(W_{x,y} \mid X = x \cap Y = y) = \Pr(W_{x,y} \cap A_1 = a^x \cap B_1 = b^y \mid X = x \cap Y = y). \tag{4.12}$$

We can now calculate the win probability for a device with a distinguished input. Expanding according to the uniformly distributed input variables and applying the

result of Eq. (4.12) gives

$$\begin{aligned}\Pr(W) &= \frac{1}{mn}\sum_{x,y}\Pr(W_{x,y} \mid X = x \cap Y = y) \\ &= \frac{1}{mn}\sum_{x,y}\Pr(W_{x,y} \cap A_1 = a^x \cap B_1 = b^y \mid X = x \cap Y = y).\end{aligned} \tag{4.13}$$

We shall proceed in cases, bounding above the win probabilities corresponding to different sets of possible deterministic outputs, until we have covered all of those possible.

If $a^1 \neq b^1$, then the first term of Eq. (4.13) vanishes. This is because, by our choice of distinguished input, $\Pr(A_1 = a^x \mid X = 1) = 1$ and $\Pr(B_1 = b^x \mid Y = 1) = 1$. We then have the first term bounded above by $\Pr(A_1 = B_1 \mid X = 1 \cap Y = 1) = 0$. Thus, in this case, $\Pr(W) \leq 1 - (mn)^{-1}$.

Let us now assume instead that $a^1 = b^1$. In the case where $\prod_{j=1}^{n} b^j \neq \alpha_1$, we can bound the terms of Eq. (4.13) where $X = 1$ as

$$\begin{aligned}&\sum_{y=1}^{n}\Pr(W_{1,y} \cap A_1 = a^1 \cap B_1 = b^y \mid X = 1 \cap Y = y) \\ \leq &\sum_{y=1}^{n}\Pr(A_y = b^y \cap \textstyle\prod_{j=1}^{n} A_j = \alpha_1 \mid X = 1) \leq n - 1.\end{aligned} \tag{4.14}$$

Similarly, in the case where $\prod_{i=1}^{m} a^i \neq \beta_1$, we can bound the terms where $Y = 1$ as

$$\begin{aligned}&\sum_{x=1}^{m}\Pr(W_{x,1} \cap A_1 = a^x \cap B_1 = b^1 \mid X = x \cap Y = 1) \\ \leq &\sum_{x=1}^{m}\Pr(B_x = a^x \cap \textstyle\prod_{i=1}^{m} B_i = \beta_1 \mid Y = 1) \leq m - 1.\end{aligned} \tag{4.15}$$

Therefore, we have shown $\Pr(W) \leq 1 - (mn)^{-1} = \omega_L(m, n)$ in all cases other than where

$$\left(a^1 = b^1\right) \cap \left(\prod_{i=1}^{m} a^i = \beta_1\right) \cap \left(\prod_{j=1}^{n} b^j = \alpha_1\right). \tag{4.16}$$

In all such remaining cases of Eq. (4.16), combining this equation with the product condition for the α_i and β_j given by Eq. (3.1), and defining new symbols $\alpha'_i \equiv a^{i+1}\alpha_{i+1}$ and $\beta'_j \equiv b^{j+1}\beta_{j+1}$, yields

$$\alpha'_1 \ldots \alpha'_{m-1} \cdot \beta'_1 \ldots \beta'_{n-1} = \prod_{i=2}^{m} a^i \alpha_i \cdot \prod_{j=2}^{n} b^j \beta_j = -1. \tag{4.17}$$

We will now assume Eq. (4.17) to be true in order to completely bound $\Pr(W)$. Further bounding the win probability expansion of Eq. (4.13) by setting terms conditioned on $X = 1$ or $Y = 1$ to unity, we get

$$\Pr(W) \leq \frac{m+n-1}{mn} + \frac{(m-1)(n-1)}{mn}\left[\frac{1}{(m-1)(n-1)}\sum_{y=2}^{n}\sum_{x=2}^{m}\Pr(W_{x,y} \mid X = x \cap Y = y)\right]. \tag{4.18}$$

Under a relabeling of the input variables, the square-bracketed terms above coincide exactly with the win probability of an $m-1\times n-1$ magic rectangle game, with its rules for row and column products specified by $\alpha'_1, \ldots, \alpha'_{m-1}$ and $\beta'_1, \ldots, \beta'_{n-1}$ respectively. These α'_i and β'_j specify a valid magic rectangle game since they satisfy Eq. (3.1), as shown by Eq. (4.17). Hence, we have the attainable upper bound

$$\frac{1}{(m-1)(n-1)}\sum_{y=2}^{n}\sum_{x=2}^{m}\Pr(W_{x,y} \mid X = x \cap Y = y) \leq \omega_{\Sigma}(m-1, n-1). \tag{4.19}$$

Combining this with Eq. (4.18) gives the bound

$$\Pr(W) \leq \bar{\omega}_{\Sigma}(m, n), \tag{4.20}$$

where $\bar{\omega}_{\Sigma}(m, n)$ is as defined in Eq. (4.8) of the statement of the present theorem.

We have now exhibited (in all possible cases for the values deterministically output by the parties given our distinguished input) bounds that are $\Pr(W) \leq 1-(mn)^{-1}$ and $\Pr(W) \leq \bar{\omega}_{\Sigma}(m, n)$. Thus, since the latter of the two upper bounds is the greatest, it is always the case for our distinguished input that

$$\Pr(W) \leq \bar{\omega}_{\Sigma}(m, n). \tag{4.21}$$

That $\bar{\omega}_{\Sigma}(m, n) \geq 1 - (mn)^{-1}$ follows from inserting the inequality

$$\omega_{\Sigma}(m-1, n-1) \geq \omega_L(m-1, n-1) = 1 - \frac{1}{(m-1)(n-1)}, \tag{4.22}$$

which holds for all levels of correlations Σ, into Eq. (4.8).

We see that the expression defined in Eq. (4.8) for the value of our $\Pr(W) \leq \bar{\omega}_{\Sigma}(m, n)$ upper bound

$$\bar{\omega}_{\Sigma}(m, n) = 1 - \frac{(m-1)(n-1)}{mn}[1 - \omega_{\Sigma}(m-1, n-1)] \tag{4.23}$$

has the same form as the lower bound for Eq. (3.8) on the win probability of a larger magic rectangle game in terms of that of a smaller one (in our present terms, the

smaller game is of size $m-1 \times n-1$ and the larger game of size $m \times n$). The strategy constructed in the proof of Lemma 3.11 attains this bound. It proceeds by the players outputting fixed predetermined values for any entry of theirs that is to be placed overlapping the first row or column of the rectangular grid. In particular, this is an example of a strategy for the $m \times n$ game that is deterministic upon our distinguished input $(X, Y) = (1, 1)$. This means that there exist strategies even using devices with our distinguished input that have win probability $\Pr(W) \geq \bar{\omega}_{\Sigma}(m, n)$. We have already shown in Eq. (4.21) the reverse bound that $\Pr(W) \leq \bar{\omega}_{\Sigma}(m, n)$. Therefore, such a strategy is both optimal and achieves $\Pr(W) = \bar{\omega}_{\Sigma}(m, n)$ as claimed. □

We now outline an alternative proof of Theorem 4.2 that may be more intuitive.

Proof. Let us suppose that $\boldsymbol{a} = (a_1, \ldots, a_n)$ is the deterministic output of Alice upon being given the input $X = 1$. Similarly, let $\boldsymbol{b} = (b_1, \ldots, b_m)^T$ be the deterministic output of Bob upon being given the input $Y = 1$. We may assume that $a_1 = b_1$, otherwise the players would lose with certainty whenever the inputs are $(X, Y) = (1, 1)$, and at best achieve a classical win probability.

Consider a distinguished input strategy with outputs given by random vectors $\boldsymbol{A} = (A_1, \ldots, A_n)$ for Alice and $\boldsymbol{B} = (B_1, \ldots, B_m)^T$ for Bob. From this strategy let us construct another strategy with new outputs for Alice $\boldsymbol{A}' = (A'_1, \ldots, A'_n)$ in which, when provided an input value x', Alice performs some postprocessing on her output. This new strategy is defined as follows.

1. Alice executes her side of the original strategy and obtains values for all the A_j.
2. If both $X = x'$ and $A_1 \neq b_{x'}$ then Alice flips the signs of the first two, setting
$$A'_1 = -A_1, \quad A'_2 = -A_2. \tag{4.24}$$
Otherwise, she leaves them unchanged with $A'_1 = A_1$ and $A'_2 = A_2$.
3. Alice sets all other A'_j (those for all $j > 2$) as in the original strategy $A'_j = A_j$.
4. Alice returns $\boldsymbol{A}' = (A'_1, \ldots, A'_n)$ as her answer to the referee.

The elements of the output $\boldsymbol{A}'$ have the same product as the original $\boldsymbol{A}$, satisfying Rule R2, and so it is also a valid answer to the game. Moreover, the new strategy satisfies the additional property that

$$\Pr(A'_1 = b_{x'} \mid X = x') = 1 \tag{4.25}$$

by construction; whenever the input for Alice takes the value $X = x'$, the first element of her output is deterministic and equal to $b_{x'}$.

We will now argue that the newly defined primed strategy succeeds with at least the probability of the original strategy. We can expand the win probability of the original strategy by the different possible inputs as

$$\Pr(W) = \frac{1}{mn} \sum_{x=1}^{m} \sum_{y=1}^{n} \Pr(A_y = B_x \mid X = x \cap Y = y), \tag{4.26}$$

and similarly for the primed strategy

$$\Pr(W') = \frac{1}{mn} \sum_{x=1}^{m} \sum_{y=1}^{n} \Pr(A'_y = B_x \mid X = x \cap Y = y). \tag{4.27}$$

The only terms inside the summations that may differ between the original and primed strategies are those where both $x = x'$ and $y \in \{1, 2\}$, since otherwise $A'_y = A_y$ by construction of the primed strategy. We can thus compare the two win probabilities by considering their difference

$$\begin{aligned} mn\big[\Pr(W') - \Pr(W)\big] = \Pr(A'_1 = B_{x'} \mid X = x' \cap Y = 1) \\ - \Pr(A_1 = B_{x'} \mid X = x' \cap Y = 1) \\ + \Pr(A'_2 = B_{x'} \mid X = x' \cap Y = 2) \\ - \Pr(A_2 = B_{x'} \mid X = x' \cap Y = 2). \end{aligned} \tag{4.28}$$

Since the first two terms are conditioned on $Y = 1$, we can use Bob's deterministic answer to replace $B_{x'}$ with $b_{x'}$ in them. We can then use the no-signaling principle to remove conditioning on $Y = 1$. Furthermore, by the property of the primed strategy given in Eq. (4.25), we then see that the first term is unity. Overall, this leaves us with

$$\begin{aligned} mn\big[\Pr(W') - \Pr(W)\big] = 1 - \Pr(A_1 = b_{x'} \mid X = x') \\ + \Pr(A'_2 = B_{x'} \mid X = x' \cap Y = 2) \\ - \Pr(A_2 = B_{x'} \mid X = x' \cap Y = 2). \end{aligned} \tag{4.29}$$

Partitioning the final two terms into four terms by whether $A_1 = b_{x'}$ or $A_1 \neq b_{x'}$ affords us further cancellations, since in the former case $A'_2 = A_2$. After canceling the two terms of the former case, we are left with

$$\begin{aligned} mn\big[\Pr(W') - \Pr(W)\big] = 1 - \Pr(A_1 = b_{x'} \mid X = x') \\ + \Pr(A'_2 = B_{x'} \cap A_1 \neq b_{x'} \mid X = x' \cap Y = 2) \\ - \Pr(A_2 = B_{x'} \cap A_1 \neq b_{x'} \mid X = x' \cap Y = 2). \end{aligned} \tag{4.30}$$

Since in the final term we are in the event $A_1 \neq b_{x'}$, we can replace $A_2 = B_{x'}$ with $A_2' = -B_{x'}$ (the complement of $A_2' = B_{x'}$ appearing in the preceding term) due to the construction of the primed strategy. Thus, applying the probability rule

$$\begin{aligned} \Pr(E^{\complement} \cap F) &= \Pr(F \setminus (E \cap F)) \\ &= \Pr(F) - \Pr(E \cap F) \end{aligned} \tag{4.31}$$

to the final term allows us to rewrite the expression as

$$\begin{aligned} mn\big[\Pr(W') - \Pr(W)\big] = 1 &- \Pr(A_1 = b_{x'} \mid X = x') \\ &+ 2\Pr(A_2' = B_{x'} \cap A_1 \neq b_{x'} \mid X = x' \cap Y = 2) \\ &- \Pr(A_1 \neq b_{x'} \mid X = x' \cap Y = 2). \end{aligned} \tag{4.32}$$

Finally, we can apply the no-signaling principle to the final term to remove its conditioning on $Y = 2$. It then cancels with the first two terms, leaving us with

$$\begin{aligned} mn\big[\Pr(W') - \Pr(W)\big] &= 2\Pr(A_2' = B_{x'} \cap A_1 \neq b_{x'} \mid X = x' \cap Y = 2) \\ &\geq 0. \end{aligned} \tag{4.33}$$

So far we have shown that, given any strategy with deterministic input $(X, Y) = (1, 1)$ that wins with probability $\Pr(W)$ and given some x', we can construct another strategy that wins with probability $\Pr(W') \geq \Pr(W)$ and is such that the first element of Alice's output A_1 is equal to the corresponding element of Bob's deterministic first column b_x with certainty whenever she is given the input $X = x'$ (this is the property exhibited in Eq. (4.25)). This implies that any *optimal* strategy must satisfy this property and, therefore, we can rule out those that do not from being optimal strategies. From the remaining strategies, we can perform the same argument with a different x' to rule out those too, and so on until all values of x' have been exhausted. We now know that any optimal strategy must satisfy

$$\Pr(A_1 = b_x \mid X = x) = 1 \text{ for all } x \in \{1, \ldots, m\}. \tag{4.34}$$

Now, going back to the construction of the primed strategy we started with and constructing a similar strategy for Bob, we can then run through an identical argument to that we have performed so far, but this time we find a necessary condition for optimal strategies involving Bob's output. We can thus proceed to rule out further strategies in which the first elements of Bob's outputs are not deterministic. That is, similarly to Eq. (4.34), we find that any optimal strategy must also satisfy

$$\Pr(B_1 = a_y \mid Y = y) = 1 \text{ for all } y \in \{1, \ldots, n\}. \tag{4.35}$$

As we have now shown, it is sufficient to search for optimal distinguished input strategies among those simultaneously satisfying both Eqs. (4.34) and (4.35). That is, among strategies in which both players are forced to deterministically return fixed values for any elements of their outputs that are to be placed in a cell appearing in the first row or first column of the $m \times n$ table. To be clear, this is a more restrictive assumption than that of the distinguished input that we started with: there, Alice was not required to act deterministically to obtain the element A_1 of her answer unless she was given the input $X = 1$, and similarly for Bob. In all the strategies that we need to consider, if $X > 1$ and $Y > 1$ then the optimal win probability is that of an $(m-1) \times (n-1)$ magic rectangle game $\omega_\Sigma(m-1, n-1)$ with row parameters $\alpha'_i = b_{i+1}\alpha_{i+1}$ and column parameters $\beta'_j = a_{j+1}\beta_{j+1}$, where the α_i and β_j are the parameters of the $m \times n$ we started with. Furthermore, if $X = 1$ or $Y = 1$ then the players win with certainty due to Eqs. (4.34) and (4.35). Since there are mn possible inputs, $(m-1)(n-1)$ of which have $X > 1$ and $Y > 1$ and the remaining $m + n - 1$ of which have $X = 1$ or $Y = 1$, we therefore conclude that the overall optimal win probability over all strategies with distinguished input and correlation level Σ is

$$\bar{\omega}_\Sigma(m, n) = \frac{(m-1)(n-1)}{mn}\omega_\Sigma(m-1, n-1) + \frac{m+n-1}{mn}. \tag{4.36}$$

This is the claimed Eq. (4.8). □

4.2 Performance

We first exhibit for which magic rectangle games randomness expansion can be performed using the R_{gen} spot-checking protocol.

Lemma 4.3. *The magic rectangle games that can be used in the R_{gen} protocol are those of sizes $2 \times n$ and $3 \times n$ where $n \geq 2$, along with their transposed counterparts.*

Proof. We know from Theorem 3.14 that $1 \times n$ games do not exhibit superclassical behavior, and so cannot be used for randomness expansion. By Theorem 2.4, then, we seek $m \times n$ games with $m, n \geq 2$ for which $\bar{\omega}_Q(m, n) < \omega_Q(m, n)$. Conversely, if $\bar{\omega}_Q(m, n) = \omega_Q(m, n)$, then it would be impossible to extract randomness in the spot-checking protocol R_{gen}. This is because randomness is extracted from the outputs of generation rounds. In this case, the observed success rate in game rounds cannot distinguish the strategy being employed from a strategy that always returns deterministic outputs (containing no extractable randomness) whenever the input pair used to obtain randomness (in generation rounds) is chosen.

It is clear that $\bar{\omega}_Q(m,n) = \omega_Q(m,n)$ for $m,n > 3$, since $\omega_Q(m,n) = 1$ for $m,n \geq 3$, and substituting this into Eq. (4.8) of Theorem 4.2 yields $\bar{\omega}_Q(m,n) = 1$ for $m,n \geq 3$. Thus $\omega_Q(m,n) = \bar{\omega}_Q(m,n)$ for $m,n > 3$.

It remains to show that $2\times n$ games for $n \geq 2$ and $3\times n$ games for $n \geq 3$ can be used in $\boldsymbol{R}_{gen}$. Then, the symmetry in $\omega_Q(m,n)$ provided by Corollary 3.10 (and inherited by $\bar{\omega}_Q(m,n)$ through Eq. (4.8)) shows that games with transposed dimensions to those may also be used. Consider the $2\times n$ games for $n \geq 2$. Using Theorem 3.14 in Eq. (4.8) gives

$$\bar{\omega}_Q(2,n) = 1 - \frac{1}{n} < \omega_Q(2,n), \tag{4.37}$$

where the final inequality is established by comparing with Eq. (3.34). Now consider the $3 \times n$ games for $n \geq 3$. As in Section 3.3.2.2, from [80] we have the upper bound $\omega_Q(2,n-1) < 1$. Again substituting into Eq. (4.8) of Theorem 4.2, we get

$$\bar{\omega}_Q(3,n) < 1 = \omega_Q(3,n), \tag{4.38}$$

where the final equality uses Corollary 3.12. □

4.2.1 Noise tolerances and rates

For the magic rectangle games which can be used in the protocol $\boldsymbol{R}_{gen}$ (shown in Lemma 4.3), Theorem 2.4 results in a maximum noise tolerance of

$$\rho_{m,n}^{\max} = \omega_Q(m,n) - \bar{\omega}_Q(m,n). \tag{4.39}$$

Furthermore, combining Theorem 2.4 with the universal lower bound of Theorem 2.5 shows that $\boldsymbol{R}_{gen}$ produces (asymptotically in the number of protocol rounds) quantum-secure extractable bits at a rate of at least

$$\pi(\chi) = \frac{2(\log_2 e)(\chi - \bar{\omega})^2}{r-1} \tag{4.40}$$

per round, where $\chi \in (\bar{\omega}, \omega]$, and $r \geq 2$ is the total size of the output alphabet for the game. According to Rules R2 and R3, a magic rectangle game of dimension $m \times n$ has $2^{m-1} \cdot 2^{n-1}$ possible outputs. Substituting the result of Theorem 4.2 for $\bar{\omega}$, this lower bound on the rate can be written for $m \times n$ magic rectangle games as

$$\pi_{m,n}(\chi) = \frac{2(\log_2 e)[\chi - \bar{\omega}_Q(m,n)]^2}{2^{m+n-2} - 1}, \tag{4.41}$$

where $\bar{\omega}_Q(m,n)$ is as given in Eq. (4.8). The maximum possible lower bound that Theorem 2.5 can achieve for the rate then occurs when the score acceptance threshold

is set to its maximum $\chi = \omega_Q(m,n)$, such that there is no tolerance to noise, and is given by

$$\pi^{\max}_{m,n} = \pi_{m,n}(\omega_Q(m,n)) = \frac{2(\log_2 e)(\rho^{\max}_{m,n})^2}{2^{m+n-2}-1}. \tag{4.42}$$

While this lower bound has the advantage that it only depends only on the dimension of the magic rectangle used, it gives rates that are far from optimal. More practical lower bounds on the rate for the spot-checking protocol could, for example, be calculated based on the techniques of [93], or numerically as in [94].

The noise tolerance for the CHSH game, or equivalently the 2×2 magic square game (Theorem 3.15), is already known to be $(\sqrt{2}-1)/4 \approx 10.4\%$, and this is confirmed by Eq. (4.39). Combining our characterization of magic rectangle games from Section 3.3 with the result of Theorem 4.2, we summarize the performance of all viable magic rectangle games in Table 4.1. Since the exact quantum values of the 2×2 and 3×3 games are known, inserting Eq. (4.8) of Theorem 4.2 into Eq. (4.39) gives exactly the optimal noise tolerance for $\boldsymbol{R}_{gen}$ using the 3×3 game. Hence, the 3×3 noise tolerance stated in Table 4.1 is exact.

It is important to note that, in Table 4.1, the upper bounds given for the noise tolerance and rate of $2 \times n$ games where $n \geq 7$ are calculated based on our Conjecture 3.17, that Eq. (3.35) holds for all such n. However, even if this conjecture proved false, by trivially weakening Eq. (3.35) to $\omega_Q(2,n) \leq 1$ we can still find less strict upper bounds for these quantities that must still hold. Inputting this relaxation into Eqs. (4.39) and (4.42), we arrive at

$$\rho^{\max}_{2,n} \leq \frac{1}{2n}, \quad \pi^{\max}_{2,n} \leq \frac{\log_2 e}{2n^2(2^n-1)}. \tag{4.43}$$

These expressions are also strictly decreasing with n and, for the conjectural cases of $n \geq 7$, do not exceed the upper bounds for even the relatively small 2×3 game in the case that the conjecture is true (see the 2×3 row of Table 4.1).

In the non-device-independent case in which privacy of the random string is considered unimportant, one can generate a bit of randomness per qubit of resource consumed by simply measuring in the computational basis. Considering the best of all magic rectangle games found in Table 4.1 (the 2×2 or CHSH game) using the spot-checking protocol of Miller and Shi [54] to the non-device-independent case, we see rates that are approximately 0.01 bits per round (each round consumes two maximally entangled qubits); loss of privacy yields of the order of a hundred times faster randomness generation when compared to the protocol that we considered. The notion of noise tolerance used for device-independent protocols (see Section 2.4) is not

Table 4.1: All $m \times n$ magic rectangle games that can produce quantum-secure extractable bits in the spot-checking protocol. A selection of specific examples are given in the lower half of the table. Bounds shown for the maximum attainable noise tolerance of $2 \times n$ and $3 \times n$ games are given based on upper and lower bounds for the $2 \times n$ quantum value (see Section 3.3.2.2). Corresponding bounds are displayed for the maximal universal lower bound on the rate, as given by Eq. (4.42). For 2×2 and 3×3 games, upper and lower bounds coincide, so their optimal noise tolerance is exact. The $3 \times n$ lower bounds shown for $n \geq 8$ are based on Conjecture 3.17. The $2 \times n$ upper bounds for $n \geq 7$ are also based on Conjecture 3.17, but may be more weakly bound as in Eq. (4.43).

	Noise tolerance $\rho_{m,n}^{\max}$		Rate bound $\pi_{m,n}^{\max}$ (bit/round)[a]	
$m \times n$	Upper bound	Lower bound	Upper bound	Lower bound
2×2	$\frac{1}{4}\left(\sqrt{2}-1\right) \approx 10.4\%$	$\frac{1}{4}\left(\sqrt{2}-1\right) \approx 10.4\%$	≈ 0.01031	≈ 0.01031
3×3	$\frac{1}{9}\left(2-\sqrt{2}\right) \approx 6.5\%$	$\frac{1}{9}\left(2-\sqrt{2}\right) \approx 6.5\%$	≈ 0.00081	≈ 0.00081
$2 \times n$	$\frac{1}{2}\left[\sqrt{1-\frac{1}{n}}-\left(1-\frac{1}{n}\right)\right]$	$\frac{1}{2n}\left(\sqrt{2}-1\right)$	$\frac{\left(\sqrt{n(n-1)}+1-n\right)^2}{2(2^n-1)n^2\ln 2}$	$\frac{3-2\sqrt{2}}{2(2^n-1)n^2\ln 2}$
$3 \times n$	$\frac{1}{3n}\left(2-\sqrt{2}\right)$	$\frac{1}{3}\left(1-\frac{1}{n}\right)\left(1-\sqrt{1-\frac{1}{n-1}}\right)$	$\frac{4(3-2\sqrt{2})}{9(2^{n+1}-1)n^2\ln 2}$	$\frac{2(n-1)\left(\sqrt{n-2}-\sqrt{n-1}\right)^2}{9(2^{n+1}-1)n^2\ln 2}$
2×3	$\frac{1}{6}\left(\sqrt{6}-2\right) \approx 7.5\%$	$\frac{1}{6}\left(\sqrt{2}-1\right) \approx 6.9\%$	≈ 0.00231	≈ 0.00196
2×4	$\frac{1}{8}\left(2\sqrt{3}-3\right) \approx 5.8\%$	$\frac{1}{8}\left(\sqrt{2}-1\right) \approx 5.2\%$	≈ 0.00065	≈ 0.00052
3×4	$\frac{1}{12}\left(2-\sqrt{2}\right) \approx 4.9\%$	$\frac{1}{12}\left(3-\sqrt{6}\right) \approx 4.6\%$	≈ 0.00022	≈ 0.00020
3×5	$\frac{1}{15}\left(2-\sqrt{2}\right) \approx 3.9\%$	$\frac{2}{15}\left(2-\sqrt{3}\right) \approx 3.6\%$	≈ 0.00007	≈ 0.00006

[a] These rates found from Miller and Shi [54] depend only on the dimension of magic rectangle game used. More practical rates could be calculated using the techniques of [93, 94].

comparable to metrics for noise in the non-DI scenario, since it is measured in units of win probability for some nonlocal game being considered. However, in the device-independent space, the CHSH game under spot-checking is known to have the best noise tolerance. This is not contradicted by our findings, as the CHSH game is equivalent to our 2×2 magic rectangle game.

4.3 Discussion

In this chapter, we focused on one possible application for our magic rectangle games of Chapter 3, namely certified randomness expansion. The optimal noise tolerance of an $m \times n$ magic rectangle game for certified randomness expansion in the spot-checking protocol is fully determined by the difference of the optimal quantum win probability $\omega_Q(m,n)$ and the optimal quantum win probability with distinguished input $\bar{\omega}_Q(m,n)$. In Theorem 4.2, we relate $\bar{\omega}_Q(m,n)$ with $\omega_Q(m-1,n-1)$ and, given that we have characterized the quantum win probabilities for magic rectangle games of all dimensions in Theorem 3.13, we can obtain the noise tolerance of all magic rectangle games (Table 4.1). Specifically, the noise tolerance of an $m \times n$ is given as the difference between its quantum value, and the corresponding value of the $(m-1) \times (n-1)$ game extended to dimension $m \times n$ by including in each of its outputs a deterministic entry. It follows that only magic rectangle games of dimension $2 \times n$ and $3 \times n$, with $n \geq 2$, can be used for certified randomness expansion (larger rectangle games fail since the games can be won with certainty even with a distinguished input). Moreover, we can also see from Table 4.1 that the most robust game turns out to be the 2×2 magic square game (which we showed is equivalent to the CHSH game). The values given for general $2 \times n$ and $3 \times n$ games are strictly decreasing with n and, furthermore, of these only the 2×2 and 2×3 games outperform the noise tolerance and rate bound given for the 3×3 game.

From the equivalence with the CHSH game, optimal strategies for the 2×2 game can be implemented using only a single Bell state shared between the players, whereas all known implementations of optimal strategies for the 3×3 game require a system of at least two Bell states. However, implementations of certain winning 3×3 strategies may still be advantageous, for example in cases where physical limitations on the quantum devices dictate certain additional constraints (such as requiring the use of only Clifford gates), or in the context of self-testing (where the use of pairs of Bell states enables parallel self-testing).

Future works An important remaining question is that of the optimal rates that one can achieve with magic rectangle games. Since we showed that, in terms of noise tolerance, the optimal game coincides with the CHSH game, analysis of the rates has already been done extensively. However, it is still an interesting open problem to obtain rates for all the games (whether this is because one is interested in a specific game, or because other games may provide better rates despite their worse noise tolerance—something conceivably possible).

Note that in Table 4.1 we do give some rates for all the different games. Theorem 2.5 directly relates noise tolerance to a lower bound on the rate of randomness expansion, which we used to directly obtain indicative rates (see the last column of Table 4.1). However, we would like to stress that the rates obtained in this way (unlike our noise tolerance analysis) are far from optimal. More practical rates can be calculated, for example, by referring to the techniques outlined in [93] or found numerically as in [94]. To obtain these improved rates requires an involved, case-by-case analysis that treats each magic rectangle game separately, something that is sensible to do if one is interested in a given game, and is left for the future.

Chapter 5

Self-testing via magic rectangle games

Self-tests of quantum states typically arise as the observation of an optimal quantum strategy for a certain nonlocal game. Conversely, exploring how different nonlocal games that appear elsewhere in the literature can be used for self-testing and what (if any) advantages these offer over other self-tests is, in its own right, an interesting endeavor. In this chapter, we examine the rectangular generalization of the magic square game introduced in Chapter 3 to obtain a family of self-tests that compare favorably with other self-tests.

Many of the most important applications for which one may envisage self-testing being used (such as delegated verifiable blind quantum computation [40, 100], to which we return in Chapter 6) exist within a scenario where one party, whom we often call the "client", has minimal quantum technological capabilities. On the other hand, it could also be assumed that the other party (by analogy, the "server") has access to a universal quantum computer. This is a setting with increasing practical relevancy, for example since quantum hardware companies already offer their services in the cloud. Having extra quantum operations being performed on this side as part of a self-test would then come with almost no further practical limitations. Moreover, the two parties should be able to self-test a large number of maximally entangled Bell states in parallel. Taking again our example of delegated computation, this is required in order to perform any interestingly large quantum computation (otherwise the client could simply perform the computation classically on their side). It follows that any natural self-test for such applications will have minimal experimental requirements on one side while also being required to test for many Bell states

in parallel. This is precisely the nature of the self-test we obtain in this chapter.

It is worth mentioning that comparisons between self-tests can be made with respect to a number of different figures of merit; the importance of each depending on the application for which one wishes to use the self-test. We consider several different qualities, and in Section 5.7 analyze what our proposed self-tests achieve and how they compare to other works. The first is the experimental complexity required by our self-test. This depends on the honest strategy and determines the quantum devices and resources required by each party. The second is that of communication complexity (required input and output sizes for the parties involved). Its most important ingredient is that of input question size, as this determines the amount of randomness that must be consumed per round of interaction of the protocol. This can also play an important role in other aspects, e.g., in how much randomness can be generated in possible applications to quantum certified randomness expansion. Finally, the third figure of merit that self-tests can be compared upon is their robustness, i.e., how close to the ideal behavior the observed correlations need to be in order to ensure that the tested quantum state is sufficiently close to the desired reference state. Given that experiments have intrinsic imperfections and correlations cannot be perfectly saturated in a real setting, achieving good robustness is crucial for practical uses of self-testing. While many self-testing protocols are designed to perform well with respect to few particular figures of merit, it is key for the type of applications at hand that a protocol achieves appropriate levels of performance simultaneously across all relevant areas. This is a major consideration of the self-test we present here.

We aim to obtain an improved self-test of multiple Bell states (with respect to different figures of merit). The nonlocal games at the core of our approach belong to the set of magic rectangle games. Our contributions may be summarized specifically as follows.

- We provide a quantum strategy to win the magic square game with certainty. This strategy involves three Bell pairs and, importantly, one side (say Alice) need only ever make local (single-qubit) Pauli measurements.[1] We say this strategy has the "one-side-local" property.

- Based on this quantum strategy, we present a one-side-local self-test of three Bell states. This requires the introduction of some extra "check" rounds. Com-

[1] We refer to a measurement performed on an observer's system of qubits as *local* (as opposed to *entangled*) or *single-qubit* if it can be realized from measurements made on individual qubits independently.

pared to other self-tests using the magic square game, ours requires a simpler experimental setup (one-side-local) and certifies a greater number of Bell states in parallel.

- We also consider the set of $3 \times n$ magic rectangle games, obtaining one-side-local quantum strategies for these (again winning with certainty) involving n Bell states.

- From these strategies, we construct a parallel self-test of n Bell pairs that is one-side-local. This is our main result, as it offers an experimentally simpler parallel self-test that (i) consumes only a small amount of input randomness with respect to the number of Bell states n (a constant number of bits for Alice and $O(\log n)$ bits for Bob), (ii) uses only perfect correlations, and (iii) is robust with robustness $O\left(n^{5/2}\sqrt{\varepsilon}\right)$, where ε is the closeness of the ideal (perfect) correlations to those observed. That the size of the (randomly selected) inputs is small with respect to n is not only useful in applications where randomness is considered an important resource, but it also means that the total number of inputs (polynomial in n) is small enough that measurement statistics over all inputs can be gathered in efficient time. Importantly, all three properties are achieved simultaneously.

Related works The magic square game was first introduced by Mermin [18] and Peres [19]. Aravind [56] gives a nontechnical demonstration of the Mermin–Peres magic square game. In Chapter 3, we examined an extension of the magic square game to arbitrary rectangular dimensions. A family of these games is used as the basis for the self-test presented here.

The concept of self-testing was first introduced by Mayers and Yao [4] in a cryptographic context, with the first mention of the term "self-testing" appearing in [23]. Wu et al. [101] gave the first self-test of two maximally entangled pairs of qubits based on the magic square game, making use of the work of McKague [102] on self-testing in parallel. Coudron and Natarajan [26] and Coladangelo [27] independently gave robust parallel self-tests of arbitrarily many Bell states based on the magic square game. A result of Coladangelo [27], which is in turn based on results of Chao et al. [70], is used in the present chapter (see Theorem 2.8). Natarajan and Vidick [28] gave the first example of a self-test for n Bell states with constant robustness. Subsequent work by the same authors achieved such a test where the number of bits of communication

required is logarithmic in n [103]. A variant of this by Natarajan and Wright [104] called the "Pauli basis test" is presented as part of the work of Ji et al. [105]. Work in another direction is offered by Šupić et al. [106], who exhibit (without consideration of robustness) a constant-input-size parallel self-test for many copies of an arbitrary state given a self-test for a single copy. On self-testing maximally-entangled states of arbitrary local dimension d, the results of Fu [107] and Mančinska et al. [108] provide robust self-tests using constant-sized questions and answers. However, the robustness of the former is exponential in d and in the latter is not constructed. Sarkar et al. [109] also provide such a self-test, however, its robustness is not studied. More details on self-testing can be found in the excellent review by Šupić and Bowles [24].

Chapter organization Section 5.1 contains notes on the notation used in this chapter. An overview of the techniques used in this chapter is given in Section 5.2. In Section 5.3, we rephrase the definition of certain magic rectangles to better suit our self-testing purposes. In Section 5.4 a one-side-local optimal quantum winning strategy for the magic square game is given, and in Section 5.5 this strategy is used as the basis of a parallel, one-side-local self-test of three Bell states. In Section 5.6 a generalization of this one-side-local quantum strategy for $3 \times n$ magic rectangle games is given, and the corresponding self-test for n Bell states is proven. We conclude in Section 5.7.

5.1 Notation

Recall from Section 2.1.10 that in this chapter we let observers Alice and Bob be labeled by the letters A and B respectively. We denote a local Hilbert space of Alice by $\mathcal{H}_A$, and similarly a local Hilbert space of Bob by $\mathcal{H}_B$. Sometimes we will need to talk about different Hilbert spaces local to an observer's subsystem. For this, we will use notation such as $\mathcal{H}'_A$ or $\tilde{\mathcal{H}}_A$ to mean different Hilbert spaces on Alice's side.

All quantum measurements in this chapter will be defined to have two possible outcomes labeled by ± 1. We take all unknown measurements to be projective, with observables of the form $M = M_+ - M_-$. That an operator is not unknown (but is instead a *reference* operator) will be denoted by a hat symbol, for example the Pauli $\hat{X}$ observable.

Since we will be dealing with many noncommutative objects, recall from Eq. (2.5) of Chapter 2 that we unambiguously define the finite product notation to be formed

with indices in ascending order as

$$\prod_{j=1}^{n} M_j = M_1 M_2 \dots M_n. \tag{5.1}$$

We will use this notation to denote the composition of (not necessarily commutative) operators.

Due to our labeling convention in this chapter, we will denote the maximally entangled Bell state shared between Alice and Bob

$$|\Phi^+\rangle_{AB} = \frac{|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B}{\sqrt{2}}. \tag{5.2}$$

In cases where Alice and Bob share multiple such states, we may label each by an additional index so that each qubit of an observer's register can be uniquely identified. That is, we may write

$$|\Phi^+\rangle_{AB}^{(i)} = \frac{|0\rangle_A^i \otimes |0\rangle_B^i + |1\rangle_A^i \otimes |1\rangle_B^i}{\sqrt{2}}. \tag{5.3}$$

To denote the case of n copies of such states, with one half of each being held by Alice and the other by Bob, we will adopt the notation

$$|\Phi^+\rangle_{AB}^{\otimes n} = \bigotimes_{i=1}^{n} |\Phi^+\rangle_{AB}^{(i)}. \tag{5.4}$$

5.2 Overview of techniques

Our two main results are self-testing protocols for three and n Bell states, respectively. Informally, to self-test a quantum state one needs to provide a local isometry that maps an untrusted state (and operators) to a reference state (and operators), which are close to the desired ones. Our proofs proceed in five steps. In the first step, we define a nonlocal game (along with an optimal quantum winning strategy for that game) that will form the basis of the self-test. Importantly, the particular strategy given should involve the states that we are testing. In the second step, we give the honest behavior for the self-test. This fixes the experimental requirements for each side. The honest behavior includes (i) the optimal quantum strategy for the nonlocal game given earlier; and (ii) additional "check" rounds, where some further correlations (that do not need to exhibit nonlocality on their own) are requested.[2] In the

[2]It is precisely these extra checks that allow us to self-test three Bell states using a nonlocal game that is normally used to self-test two Bell states (the magic square game). This is extended later for the n Bell state case with a game whose optimal winning probability could be saturated with a quantum strategy involving just a pair of Bell states.

third step, we define the (untrusted) observables and specify all the correlations that are to be tested. This is the information we have from experiment; it quantifies the proximity of the real experiment to the ideal maximum winning probabilities, and it forms the basis for obtaining the desired isometry. In the fourth step, the above correlations are used to prove that the untrusted single-qubit Pauli operators have commutation and anticommutation relations exactly as the corresponding (trusted) Pauli operators have. This is the hardest step, as it demonstrates that the correlations obtained from the experiment suffice to construct some untrusted operators that behave as the desired trusted operators. The fifth and final step is simply the application of a theorem of Coladangelo [27], wherein the existence of the desired local isometry was reduced to the satisfaction of the commutation and anticommutation relations obtained in the fourth step.

5.2.1 Self-test of three Bell states

Base nonlocal game We introduce a strategy for winning the magic square game with certainty (Section 5.4). This strategy has two interesting features. Firstly, unlike the "standard" strategy that involves two Bell states [56], this strategy involves three Bell states. This means that any self-test based on this would result in self-testing more Bell states in parallel than using the magic square game in the standard way [101]. To succeed in the parallel self-testing of more Bell states requires some extra correlations (obtained from some "check" rounds) to prevent dishonest players from simply following the standard magic square strategy using only two Bell states. The second feature is that this strategy can be realized with Pauli measurements (as in the standard magic square strategy) but with one of the players (say Alice) needing only to perform local (single-qubit) measurements. In the usual magic square strategy, both parties must measure in entangled bases (see Section 2.2). This implies that a self-test based on this strategy would be simpler to execute experimentally and, importantly, impose fewer quantum-technological requirements on Alice's side—something of immediate interest for major applications of self-testing.

Honest run Alice plays the one-side-local magic square strategy (see Section 5.4), with the difference being that she measures locally each of her three qubits and returns these as her answer, allowing the product of pairs to be checked by a referee. Bob has two types of rounds: game rounds, where he plays the modified magic square

game by measuring pairs of qubits in the $\hat{X} \otimes \hat{X}$, $\hat{Y} \otimes \hat{Y}$, and $\hat{Z} \otimes \hat{Z}$ bases simultaneously, and "check" rounds, where he measures his three qubits locally.

Untrusted observables and correlations Alice has only untrusted local Pauli observables, while Bob has different untrusted observables in game and check rounds. Interestingly, Bob's observables in the check rounds are the ones used for the isometry, while the observables of game rounds are used to enforce the suitable commutation and anticommutation relations on Alice's side. The correlations observed are those required for the magic square game along with the (perfect) Einstein–Podolsky–Rosen (EPR) correlations in check rounds.

Commutation and anticommutation The main theorem for this case (Theorem 5.4 of Section 5.5.3) is stated informally here.

Theorem 5.1 (Informal Theorem 5.4)**.** *The game-round observables of Alice and the check-round observables of Bob obey standard commutation and anticommutation relations up to $O(\sqrt{\varepsilon})$, where ε is the distance of the observed correlations from the ideal ones. The observables commute when acting on different qubits; commute when they are of the same type and act on the same qubit; and anticommute when they act on the same qubit and are conjugate (e.g. X and Z).*

Isometry Using the relations provided by the aforementioned theorem and following Coladangelo [27], we obtain a suitable local isometry and complete the self-test.

5.2.2 Self-test of many Bell states

Base nonlocal game We introduce a strategy that wins the $3 \times n$ magic rectangle game with certainty using n Bell states (Section 5.6.1). Note that the $3 \times n$ magic rectangle game can also be won with only two Bell states, but our strategy enables the parallel self-test of n Bell states, having the same one-side-locality as our previous result.

Honest run Alice plays the magic rectangle strategy (see Section 5.6.1) described by measuring all of her qubits in one of the three Pauli bases (all in the same basis). Suitable products of her outcomes can be checked for consistency in the magic rectangle game by a referee. Bob now has three round types: game rounds, *local* check

rounds (in which single-qubit correlations are checked), and *pair* check rounds (in which correlations of pairs of qubits are checked).

Untrusted observables and correlations Alice has only untrusted local Pauli observables, while Bob has untrusted observables for all three round types. The local-check-round observables are used to construct the subsequent local isometry, while the other observables are used to obtain suitable commutation and anticommutation relations.

Commutation and anticommutation The main theorem (Theorem 5.11 of Section 5.6.4) contains the same type of relations as in the case with three Bell states, where obtaining the anticommutation relations is considerably more complicated (and requires the extra set of rounds). This is stated informally as follows:

Theorem 5.2 (Informal Theorem 5.11)**.** *The game-round observables of Alice and the local-check-round observables of Bob obey standard commutation relations up to* $O\left(\sqrt{\varepsilon}\right)$ *and anticommutation relations up to* $O\left(n\sqrt{\varepsilon}\right)$*, where* ε *is the distance of the observed correlations from the ideal ones. The observables commute when acting on different qubits; commute when they are of the same type and act on the same qubit; and anti-commute when they act on the same qubit and are conjugate (e.g.* X *and* Z*).*

Isometry Again following Coladangelo [27] and using the relations provided by Theorem 5.11, we recover the desired local isometry that results in a self-test of n Bell states.

5.3 Magic rectangle games (redefinition)

As we have seen in Chapter 3, the magic square game can be generalized to be played on an $m \times n$ table. Such a *magic rectangle* game corresponds to m possible questions for Alice and n for Bob. To avoid trivially winning strategies, the game rules are generalized accordingly in Definition 3.1, which we restate here.

Definition 3.1 (Magic rectangle games)**.** An $m \times n$ game is specified by fixing some $\alpha_1, \ldots, \alpha_m$ and $\beta_1, \ldots, \beta_n$ each belonging to $\{+1, -1\}$, such that their product satisfies

$$\alpha_1 \ldots \alpha_m \cdot \beta_1 \ldots \beta_n = -1. \tag{3.1}$$

The rules of the given game are then:

R1. Each filled cell must belong to the set $\{+1, -1\}$.

R2. Upon being assigned the ith row, the product of Alice's entries must be α_i.

R3. Upon being assigned the jth column, the product of Bob's entries must be β_j.

As before, the game is won if both players enter the same value into their shared cell.

We will later be concerned specifically with $3 \times n$ games in which entries to rows must all have positive products and entries to columns must all have negative products. Such games are defined by $\alpha_i = 1$ and $\beta_j = -1$ for all i and j and must have odd n due to Eq. (3.1). A particular class of winning strategies for these games will be used to build part of our self-test of n Bell states. In the case of these particular games, we can rephrase the definition of magic rectangles in a way that will prove more useful for our self-testing purposes. If $(p_1, \dots, p_n) \in \{+1, -1\}^n$ is any possible output row of Alice (whose product is required to be $+1$), then there exists an assignment of $a_1, \dots, a_n \in \{+1, -1\}$ such that $p_j = \prod_{k \neq j} a_k$ for all j. To see this, simply take $a_k = p_k$ for all k. Conversely then, we may ask that Alice outputs some $a_1, \dots, a_n \in \{+1, -1\}$ and leave it to the game referees to check whether the appropriate products $p_j = \prod_{k \neq j} a_k$ form a winning row. Notice in our special case of n odd, such p_j automatically satisfy the rule for Alice's rows $\prod_{j=1}^{n} p_j = +1$ for any assignment of the a_k. We now rephrase the definition of $3 \times n$ magic rectangle games in this special case.

Definition 5.3 ($3 \times n$ magic games)**.** Given n odd, Alice and Bob receive inputs $x \in \{1, 2, 3\}$ and $y \in \{1, \dots, n\}$, respectively. Alice outputs n bits $a_1, \dots, a_n \in \{+1, -1\}$. Bob outputs $(b_1, b_2, b_3) \in \{+1, -1\}^3$ required to satisfy $b_1 b_2 b_3 = -1$. The game is won if $\prod_{k \neq y} a_k = b_x$.

Remark. While Bob's output here is column y of a magic rectangle, Alice's output corresponds to filling row x as $(p_1, \dots, p_n)$ where $p_j = \prod_{k \neq j} a_k$. The win condition is then equivalent to the familiar case when both players enter the same value into the shared cell $p_y = b_x$.

5.4 One-side-local magic square strategy

Recall that the usual quantum winning strategy for the magic square game requires some measurements of both Alice and Bob to be performed in entangled bases (see

the discussion of Section 2.2). We now propose a quantum strategy for the magic square game, also winning with certainty, which can be realized under the additional constraint that Alice may only make measurements localized to single qubits of her quantum system. Each round begins by allowing Alice and Bob to share three Bell states

$$|\psi\rangle = |\Phi^+\rangle_{AB}^{(1)} \otimes |\Phi^+\rangle_{AB}^{(2)} \otimes |\Phi^+\rangle_{AB}^{(3)}. \tag{5.5}$$

Half of each Bell state is given to Alice, and the other half to Bob. The proposed measurement strategy is depicted in Fig. 5.1.

$I \otimes \hat{X} \otimes \hat{X}$	$\hat{X} \otimes I \otimes \hat{X}$	$\hat{X} \otimes \hat{X} \otimes I$
$I \otimes \hat{Y} \otimes \hat{Y}$	$\hat{Y} \otimes I \otimes \hat{Y}$	$\hat{Y} \otimes \hat{Y} \otimes I$
$I \otimes \hat{Z} \otimes \hat{Z}$	$\hat{Z} \otimes I \otimes \hat{Z}$	$\hat{Z} \otimes \hat{Z} \otimes I$

Figure 5.1: The proposed "one-side-local" magic square strategy. To realize any particular row, Alice is only required to measure each of her qubits locally, as the observables to be measured for any individual one of her three qubits commute within each row.

Notice in Fig. 5.1 that each row is formed out of commuting observables whose product is equal to the identity operator. Similarly, the observables in each column commute and have a product equal to minus the identity operator. Moreover, the eigenvalues of each observable are $+1$ and -1. These facts combined show that Rules S1 to S3 in Section 2.2 are automatically satisfied by the outcomes of measuring a full row or column. If M_A is any observable for Alice's system contained in Fig. 5.1, and if M_B is the observable of the same cell for Bob's system, then it is easy to show the correlation

$$\langle\psi| M_A M_B |\psi\rangle = 1. \tag{5.6}$$

This can be seen, for example, by writing the Bell states comprising the shared state

of Eq. (5.5) in terms of eigenstates of the $\hat{X}$, $\hat{Y}$, and $\hat{Z}$ operators respectively

$$\begin{aligned} |\Phi^+\rangle &= \frac{|+\rangle \otimes |+\rangle + |-\rangle \otimes |-\rangle}{\sqrt{2}} \\ &= \frac{|+i\rangle \otimes |-i\rangle + |-i\rangle \otimes |+i\rangle}{\sqrt{2}} \\ &= \frac{|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle}{\sqrt{2}}. \end{aligned} \tag{5.7}$$

Alice, therefore, always measures the same outcome as Bob for the shared cell (either both $+1$ or both -1), and so they win the game with certainty.

For any particular row assigned to Alice, it is clear from inspection of Fig. 5.1 that she need only make single-qubit measurements; for any given qubit of her system, the single-qubit observables she is required to measure with respect to that qubit of her register mutually commute within the row. That is, it is always possible for Alice to realize the required observables by recording the measurement outcomes of a particular Pauli operator ($\hat{X}$, $\hat{Y}$, or $\hat{Z}$ depending on the row) on each one of her three qubits. This strategy can thus be phrased naturally for the magic square game in the sense of Definition 5.3 with $n = 3$. Bob generates his outputs according to the columns of Fig. 5.1 as usual. The jth output bit a_j of Alice, however, results from the outcome of the single-qubit Pauli measurement $\hat{X}_A^j$, $\hat{Y}_A^j$, or $\hat{Z}_A^j$ on Alice's jth qubit depending on whether the first, second, or third row was assigned, respectively.

5.5 Self-test of three Bell states

In the quantum strategy for the magic square game introduced in Section 5.4, the players share three EPR pairs, while in the standard quantum strategy they share two EPR pairs. Indeed, from observing perfect statistics in the magic square game alone, it is only possible to extract (under some local isometry) the existence of two EPR pairs. That is, attaining the quantum value of the magic square game can only self-test two EPR pairs, even if the players in fact shared three (since they could easily cheat by only making use of two of their three pairs and implementing the standard quantum strategy). Nonetheless, we can introduce some simple further questioning of the players, in addition to asking them to play the magic square game, such that enough information is gathered about their measurement strategy to assert the existence of three EPR pairs of entanglement. The exact additional questions are inspired by the form of the one-side-local strategy we gave in Section 5.4. Furthermore, the

one-side-local strategy is the honest strategy for the magic square game part of the modified questioning.

By augmenting the correlations arising from a winning magic square strategy by certain additional correlations that ensure Alice implements her side of the strategy locally, it is possible to self-test three copies of the Bell state $|\Phi^+\rangle$. These additional correlations are obtained from Bob making single-qubit Pauli measurements of his qubits in some rounds of the test, which we will call "check" rounds. Rounds that are not check rounds will be called "game" rounds. We now describe the structure of the self-test and specify its honest behavior. Afterwards, we exhibit explicitly the correlations of unknown observables used in the test. Finally, we show how these correlations can be used to prove the relevant commutation and anticommutation relations required for a self-testing proof.

5.5.1 Structure and honest behavior

Alice receives an input $x \in \{1,2,3\}$ and Bob an input $y \in \{1,2,3\}$. Additionally, Bob receives an input $c \in \{0,1\}$ controlling whether the round is a game or check round. If the round is a game round ($c = 0$), then it is the goal of the players to win at the magic square game (in the sense of Definition 5.3) with the row and column assigned to Alice and Bob given by x and y, respectively. Otherwise, if the round is a check round ($c = 1$), then the players are required to perfectly correlate certain combinations of their output bits (which will be convenient to state after our description of the honest behavior). Notice, however, that Alice is not directly provided with the information of whether the round is to be considered a game or check round. The protocol is summarized in Protocol 5.1.

In an honest round of the experiment, the players share three Bell states, so that $|\psi\rangle = |\Phi^+\rangle_{AB}^{\otimes 3}$ as in the magic square strategy of Section 5.4. Alice always performs her side of this magic square strategy, providing each of her output bits a_j to the referees (as in Definition 5.3) by measuring

$$\hat{X}_A^j \quad \text{if } x = 1, \tag{5.8a}$$

$$\hat{Y}_A^j \quad \text{if } x = 2, \tag{5.8b}$$

$$\hat{Z}_A^j \quad \text{if } x = 3. \tag{5.8c}$$

The honest behavior of Bob depends on the type of round c. If $c = 0$, then Bob also performs his side of our one-side-local magic square strategy, returning outputs according to measuring the observables in column y of Fig. 5.1 so that the magic square

Protocol 5.1: A protocol for certifying three Bell states. Strategies in which Alice uses entangled measurements are ruled out by *local check* rounds. The protocol is phrased in terms of the parameter n, as it will be extended in Section 5.6.2 in order to self-test n Bell states.

Let $n = 3$ be the number of Bell states to be certified. In each round, a verifier chooses $c \in \{0, 1\}$ and $y \in \{1, \ldots, n\}$. The verifier sends Bob (c, y) and, depending on c, runs one of the following subprotocols:

0. *Magic game*: Send Alice $x \in \{1, 2, 3\}$. Alice and Bob answer with $a_1, \ldots, a_n$ and b_1, b_2, b_3 in $\{+1, -1\}$ satisfying $b_1 b_2 b_3 = -1$. Accept if and only if $\prod_{k \neq y} a_k = b_x$.

1. *Local check*: Send Alice $x \in \{1, 3\}$. Alice and Bob answer with $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$ in $\{+1, -1\}$.

   (a) If $x = 1$, accept if and only if $a_y = b_y$.

   (b) If $x = 3$, accept if and only if $a_j = b_j$ for all $j \neq y$.

---

game is won with certainty. Otherwise, if $c = 1$, then the input y determines which one of three sets of single-qubit Pauli measurements he performs. Specifically, Bob's output bits are generated as the measurement outcomes of the set of Pauli observables,

$$\left\{\hat{X}_B^1, \hat{Z}_B^2, \hat{Z}_B^3\right\} \quad \text{if } y = 1, \tag{5.9a}$$

$$\left\{\hat{Z}_B^1, \hat{X}_B^2, \hat{Z}_B^3\right\} \quad \text{if } y = 2, \tag{5.9b}$$

$$\left\{\hat{Z}_B^1, \hat{Z}_B^2, \hat{X}_B^3\right\} \quad \text{if } y = 3. \tag{5.9c}$$

It is convenient at this point to call attention to the perfect correlations of output bits expected in honest check rounds. These are all the single-qubit quantum correlations $\langle\psi| \hat{X}_A^j \hat{X}_B^j |\psi\rangle = 1$ and $\langle\psi| \hat{Z}_A^j \hat{Z}_B^j |\psi\rangle = 1$. Observation of a version of these correlations using *untrusted* observables (which will not be assumed to be identical for Bob upon his different inputs) will become a requirement for our protocol to certify the desired reference state.

5.5.2 Unknown observables and correlations

We will now denote the unknown state shared by the players by $|\psi\rangle$, and the expectation value of an unknown observable M with respect to this state by $\langle M \rangle =$

$\langle\psi| M |\psi\rangle$. We now describe the unknown observables which will be used by Alice and Bob in our self-testing proof. Recall that, in contrast to the honest Pauli observables used in the previous Section 5.5.1, such unknown observables are denoted without a hat symbol (using X for the corresponding unknown version of the Pauli $\hat{X}$ observable). We may not assume a priori, in the potentially dishonest case of the self-testing protocol, that the players measure any of the same observables upon being given different inputs. For this reason, we introduce notation in such a way that the observer and their input can always be deduced from the label of an unknown observable. This choice of notation will be seen in Eqs. (5.10), (5.11) and (5.13).

It is important to note that all unknown observables that are to be measured as part of the same local input commute by definition. For example, from the observables defined immediately below, it can always be assumed that $\left[X_A^1, X_A^2\right] = 0$, since both observables correspond to the input $x = 1$ for Alice. Furthermore, it can always be assumed that any two observables defined for different players commute. These two properties will be exploited frequently in proofs throughout the rest of the chapter.

Alice's observables We define sets of mutually commuting unknown observables on Alice's side to be measured depending on her input x as

$$\left\{X_A^1, X_A^2, X_A^3\right\} \quad \text{if } x = 1, \tag{5.10a}$$

$$\left\{Y_A^1, Y_A^2, Y_A^3\right\} \quad \text{if } x = 2, \tag{5.10b}$$

$$\left\{Z_A^1, Z_A^2, Z_A^3\right\} \quad \text{if } x = 3. \tag{5.10c}$$

Each of these unknown observables corresponds to a single-qubit Pauli observable, which acts on the qubit of Alice indicated by its superscript.

Bob's observables (game rounds) For game rounds ($c = 0$), we will denote the sets of unknown observables to be measured by Bob, depending on his input y, by

$$\left\{X_B^{\overline{1}}, Y_B^{\overline{1}}, Z_B^{\overline{1}}\right\} \quad \text{if } y = 1, \tag{5.11a}$$

$$\left\{X_B^{\overline{2}}, Y_B^{\overline{2}}, Z_B^{\overline{2}}\right\} \quad \text{if } y = 2, \tag{5.11b}$$

$$\left\{X_B^{\overline{3}}, Y_B^{\overline{3}}, Z_B^{\overline{3}}\right\} \quad \text{if } y = 3. \tag{5.11c}$$

Figure 5.2 clarifies the meaning of our unknown observables for game rounds.

The overline notation used in each superscript reflects that these observables correspond to the product of single-qubit Pauli observables acting on all qubits of Bob

$X_A^2 X_A^3$	$X_A^1 X_A^3$	$X_A^1 X_A^2$
$Y_A^2 Y_A^3$	$Y_A^1 Y_A^3$	$Y_A^1 Y_A^2$
$Z_A^2 Z_A^3$	$Z_A^1 Z_A^3$	$Z_A^1 Z_A^2$

(a) Alice's strategy.

$X_B^{\bar{1}}$	$X_B^{\bar{2}}$	$X_B^{\bar{3}}$
$-X_B^{\bar{1}} Z_B^{\bar{1}}$	$-X_B^{\bar{2}} Z_B^{\bar{2}}$	$-X_B^{\bar{3}} Z_B^{\bar{3}}$
$Z_B^{\bar{1}}$	$Z_B^{\bar{2}}$	$Z_B^{\bar{3}}$

(b) Bob's strategy.

Figure 5.2: The layout of unknown observables in a magic square strategy for (a) Alice and (b) Bob.

other than that indicated. For example, here the unknown observable $X_B^{\bar{1}}$ corresponds to $\hat{X}_B^2 \hat{X}_B^3$ in the honest case. Note also that Rule S3 of the magic square game requires columns to have negative products. In terms of unknown observables, that is $\langle X_B^{\bar{y}} Y_B^{\bar{y}} Z_B^{\bar{y}} \rangle = -1$ for all y. Thus we need not have defined one observable in each set, say $Y_B^{\bar{y}}$, since this implies

$$Y_B^{\bar{y}} |\psi\rangle = -X_B^{\bar{y}} Z_B^{\bar{y}} |\psi\rangle. \tag{5.12}$$

We will, however, choose to keep all of these observables for notational convenience, referring to Eq. (5.12) when necessary.

Bob's observables (check rounds) For check rounds ($c = 1$), Bob's unknown observables correspond to single-qubit Pauli X and Z observables acting on his system. These will be denoted as follows, with an additional subscript to distinguish unknown observables of different inputs:

$$\left\{ X_{B,1}^1, Z_{B,1}^2, Z_{B,1}^3 \right\} \quad \text{if } y = 1, \tag{5.13a}$$
$$\left\{ Z_{B,2}^1, X_{B,2}^2, Z_{B,2}^3 \right\} \quad \text{if } y = 2, \tag{5.13b}$$
$$\left\{ Z_{B,3}^1, Z_{B,3}^2, X_{B,3}^3 \right\} \quad \text{if } y = 3. \tag{5.13c}$$

Correlations The correlations of unknown observables amounting to a uniformly ε_0-close to perfect strategy for the magic square game (i.e. correlations obtained in

game rounds) are, for all distinct $i, j, k \in \{1, 2, 3\}$,

$$\langle X_A^i X_A^j X_B^{\overline{k}} \rangle \geq 1 - \varepsilon_0, \tag{5.14a}$$

$$-\langle Y_A^i Y_A^j X_B^{\overline{k}} Z_B^{\overline{k}} \rangle \geq 1 - \varepsilon_0, \tag{5.14b}$$

$$\langle Z_A^i Z_A^j Z_B^{\overline{k}} \rangle \geq 1 - \varepsilon_0. \tag{5.14c}$$

The correlations constituting uniformly ε_1-close to perfect check rounds are, again for all distinct $i, j \in \{1, 2, 3\}$,

$$\langle X_A^i X_{B,i}^i \rangle \geq 1 - \varepsilon_1, \tag{5.15a}$$

$$\langle Z_A^i Z_{B,j}^i \rangle \geq 1 - \varepsilon_1. \tag{5.15b}$$

5.5.3 Commutation and anticommutation relations

In this section, we prove commutation and anticommutation relations (acting on our unknown state) for those unknown observables of Alice and Bob corresponding to single-qubit Pauli measurements. To do this, we use the correlations of Section 5.5.2. The results of this section are summarized in the following theorem:

Theorem 5.4. *Let $i, j, k, l \in \{1, 2, 3\}$ be such that $i \neq k$ and $j \neq l$. We have correlations between each unknown observable of Alice with each of the corresponding observables on Bob's side*

$$\left\| \left(X_A^i - X_{B,i}^i \right) |\psi\rangle \right\| \leq \sqrt{2\varepsilon_1}, \tag{5.16}$$

$$\left\| \left(Z_A^i - Z_{B,k}^i \right) |\psi\rangle \right\| \leq \sqrt{2\varepsilon_1}. \tag{5.17}$$

We have the state-dependent anticommutativity of all unknown X observables with all unknown Z observables corresponding to the same qubit

$$\left\| \left\{ X_A^i, Z_A^i \right\} |\psi\rangle \right\| \leq 9\sqrt{2\varepsilon_0} + 16\sqrt{2\varepsilon_1}, \tag{5.18}$$

$$\left\| \left\{ X_{B,i}^i, Z_{B,k}^i \right\} |\psi\rangle \right\| \leq 9\sqrt{2\varepsilon_0} + 20\sqrt{2\varepsilon_1}. \tag{5.19}$$

Finally, we have the state-dependent commutativity of unknown X and Z observables. On Bob's side we have

$$\left\| \left[X_{B,i}^i, X_{B,j}^j \right] |\psi\rangle \right\| \leq 4\sqrt{2\varepsilon_1}, \tag{5.20}$$

$$\left\| \left[Z_{B,k}^i, Z_{B,l}^j \right] |\psi\rangle \right\| \leq 4\sqrt{2\varepsilon_1}; \tag{5.21}$$

and moreover restricting to observables corresponding to different qubits $i \neq j$

$$\left\| \left[X^i_{B,i}, Z^j_{B,l} \right] |\psi\rangle \right\| \leq 8\sqrt{2\varepsilon_1}. \tag{5.22}$$

On Alice's side, for different qubits $i \neq j$, we have

$$\left\| \left[M^i_A, N^j_A \right] |\psi\rangle \right\| \leq 4\sqrt{2\varepsilon_1}, \tag{5.23}$$

where M and N can be either of X and Z.

Proof. Combine Propositions 5.5, 5.6 and 5.8. □

Proposition 5.5 (Correlation)**.** *For all distinct $i, j \in \{1, 2, 3\}$ we have the correlation estimates*

$$\left\| \left(X^i_A - X^i_{B,i} \right) |\psi\rangle \right\| \leq \sqrt{2\varepsilon_1}, \tag{5.24a}$$
$$\left\| \left(Z^i_A - Z^i_{B,j} \right) |\psi\rangle \right\| \leq \sqrt{2\varepsilon_1}. \tag{5.24b}$$

Proof. Apply Lemma 2.2 to the correlations given in Eq. (5.15). □

The following proposition shows the commutation of unknown observables which we expect to correspond to local measurements on different qubits. Since observables defined for different players are assumed to commute, we show commutation for the observables of each player separately.

Proposition 5.6 (Commutation)**.** *For all $i, j, k, l \in \{1, 2, 3\}$ such that $i \neq k$ and $j \neq l$ we have*

$$\left\| \left[X^i_{B,i}, X^j_{B,j} \right] |\psi\rangle \right\| \leq 4\sqrt{2\varepsilon_1}, \tag{5.25a}$$
$$\left\| \left[Z^i_{B,k}, Z^j_{B,l} \right] |\psi\rangle \right\| \leq 4\sqrt{2\varepsilon_1}. \tag{5.25b}$$

Moreover if $i \neq j$ we have commutation relations for Bob

$$\left\| \left[X^i_{B,i}, Z^j_{B,l} \right] |\psi\rangle \right\| \leq 8\sqrt{2\varepsilon_1} \tag{5.26}$$

and for Alice

$$\left\| \left[M^i_A, N^j_A \right] |\psi\rangle \right\| \leq 4\sqrt{2\varepsilon_1}, \tag{5.27}$$

where M and N can be either of X and Z.

Proof. Using the triangle inequality with the estimates of Proposition 5.5, and the commutation of Alice's observables corresponding to the same input, we can write

$$\begin{aligned}\left\|\left[X^i_{B,l}, X^j_{B,j}\right]|\psi\rangle\right\| &\leq 4\sqrt{2\varepsilon_1} + \left\|\left[X^j_A, X^i_A\right]|\psi\rangle\right\| \\ &= 4\sqrt{2\varepsilon_1},\end{aligned} \tag{5.28}$$

showing Eq. (5.25a). Similarly, to obtain Eq. (5.25b),

$$\begin{aligned}\left\|\left[Z^i_{B,k}, Z^j_{B,l}\right]|\psi\rangle\right\| &\leq 4\sqrt{2\varepsilon_1} + \left\|\left[Z^j_A, Z^i_A\right]|\psi\rangle\right\| \\ &= 4\sqrt{2\varepsilon_1}.\end{aligned} \tag{5.29}$$

We now assume $i \neq j$. From the definition of Bob's check-round observables [Eq. (5.13)] we have $\left[X^i_{B,i}, Z^j_{B,i}\right] = 0$. We use this and Proposition 5.5 to get

$$\begin{aligned}\left\|\left[X^i_A, Z^j_A\right]|\psi\rangle\right\| &= \left\|X^i_A Z^j_A|\psi\rangle - Z^j_A X^i_A|\psi\rangle\right\| \\ &\leq 2\sqrt{2\varepsilon_1} + \left\|X^i_A Z^j_A|\psi\rangle - X^i_{B,i} Z^j_{B,i}|\psi\rangle\right\| \\ &= 2\sqrt{2\varepsilon_1} + \left\|X^i_A Z^j_A|\psi\rangle - Z^j_{B,i} X^i_{B,i}|\psi\rangle\right\| \\ &\leq 4\sqrt{2\varepsilon_1} + \left\|X^i_A Z^j_A|\psi\rangle - X^i_A Z^j_A|\psi\rangle\right\| \\ &= 4\sqrt{2\varepsilon_1}.\end{aligned} \tag{5.30}$$

Combining this with the definition of Alice's observables [Eq. (5.10)], from which we have $\left[X^i_A, X^j_A\right] = 0$ and $\left[Z^i_A, Z^j_A\right] = 0$, yields Eq. (5.27). To obtain Eq. (5.26), we again use Proposition 5.5 to write

$$\left\|\left[X^i_{B,i}, Z^j_{B,l}\right]|\psi\rangle\right\| \leq 4\sqrt{2\varepsilon_1} + \left\|\left[Z^j_A, X^i_A\right]|\psi\rangle\right\| \leq 8\sqrt{2\varepsilon_1}, \tag{5.31}$$

where the final inequality uses Eq. (5.27) just proved. □

We now show an intermediate result that will allow us to prove the anticommutativity of unknown local X and Z observables. The lemma shows that Alice's unknown observables for pairs of X and Z operators not acting on the same qubits anticommute (cf. the observables used in the magic square strategy of Section 5.4). The proof follows a similar line to [101].

Lemma 5.7. *For all distinct $i, j, k \in \{1, 2, 3\}$ we have anticommutation relations for Bob's game round observables*

$$\left\|\left\{X^i_A X^j_A, Z^i_A Z^k_A\right\}|\psi\rangle\right\| \leq 9\sqrt{2\varepsilon_0}. \tag{5.32}$$

Proof. By estimating the game-round correlations of Eq. (5.14) using Lemma 2.2, and repeatedly applying the triangle inequality,

$$\begin{aligned}
\left\|\left\{X_A^i X_A^j, Z_A^i Z_A^k\right\}|\psi\rangle\right\| &\leq 4\sqrt{2\varepsilon_0} + \left\|Z_B^{\bar{j}} X_B^{\bar{k}}|\psi\rangle + X_B^{\bar{j}} X_B^{\bar{i}} Z_A^i Z_A^k|\psi\rangle\right\| \\
&= 4\sqrt{2\varepsilon_0} + \left\|X_B^{\bar{j}} Z_B^{\bar{j}} X_B^{\bar{k}} Z_A^i Z_A^j|\psi\rangle + X_B^{\bar{i}} Z_A^j Z_A^k|\psi\rangle\right\| \\
&\leq 6\sqrt{2\varepsilon_0} + \left\|\left(X_B^{\bar{j}} Z_B^{\bar{j}}\right)\left(X_B^{\bar{k}} Z_B^{\bar{k}}\right)|\psi\rangle + X_B^{\bar{i}} Z_B^{\bar{i}}|\psi\rangle\right\| \\
&\leq 8\sqrt{2\varepsilon_0} + \left\|\left(Y_A^i Y_A^j\right)\left(Y_A^i Y_A^k\right)|\psi\rangle + X_B^{\bar{i}} Z_B^{\bar{i}}|\psi\rangle\right\| \\
&= 8\sqrt{2\varepsilon_0} + \left\|Y_A^j Y_A^k|\psi\rangle + X_B^{\bar{i}} Z_B^{\bar{i}}|\psi\rangle\right\| \\
&\leq 9\sqrt{2\varepsilon_0},
\end{aligned} \tag{5.33}$$

where the first equality results from applying unitary operators $Z_A^i Z_A^j$ and $X_B^{\bar{j}}$ inside the norm. □

We are now in a position to prove the required anticommutativity of unknown X observables with Z observables which act on the same qubits of the unknown state.

Proposition 5.8 (Anticommutation)**.** *For all $i \in \{1,2,3\}$ we have anticommutation relations for Alice's unknown observables*

$$\left\|\left\{X_A^i, Z_A^i\right\}|\psi\rangle\right\| \leq 9\sqrt{2\varepsilon_0} + 16\sqrt{2\varepsilon_1}. \tag{5.34}$$

Furthermore, for all $j \in \{1,2,3\}$ distinct from i we have anticommutation relations for Bob's check-round observables

$$\left\|\left\{X_{B,i}^i, Z_{B,j}^i\right\}|\psi\rangle\right\| \leq 9\sqrt{2\varepsilon_0} + 20\sqrt{2\varepsilon_1}. \tag{5.35}$$

Proof. Let $k \in \{1,2,3\}$ be distinct from i and j, then

$$\begin{aligned}
\left\|\left\{X_A^i, Z_A^i\right\}|\psi\rangle\right\| &= \left\|X_{B,j}^j Z_{B,i}^k \left\{X_A^i, Z_A^i\right\}|\psi\rangle\right\| \\
&= \left\|X_A^i Z_A^i X_{B,j}^j Z_{B,i}^k|\psi\rangle + Z_A^i X_A^i X_{B,j}^j Z_{B,i}^k|\psi\rangle\right\| \\
&\leq \left\|X_A^i Z_A^i Z_{B,i}^k X_{B,j}^j|\psi\rangle + Z_A^i X_A^i X_{B,j}^j Z_{B,i}^k|\psi\rangle\right\| + 8\sqrt{2\varepsilon_1} \\
&\leq \left\|X_A^i Z_{B,i}^k X_{B,j}^j Z_{B,j}^i|\psi\rangle + Z_A^i X_{B,j}^j Z_{B,i}^k X_{B,i}^i|\psi\rangle\right\| + 10\sqrt{2\varepsilon_1} \\
&= \left\|X_A^i Z_{B,i}^k Z_{B,j}^i X_{B,j}^j|\psi\rangle + Z_A^i X_{B,j}^j X_{B,i}^i Z_{B,i}^k|\psi\rangle\right\| + 10\sqrt{2\varepsilon_1} \\
&\leq \left\|\left\{X_A^i X_A^j, Z_A^i Z_A^k\right\}|\psi\rangle\right\| + 16\sqrt{2\varepsilon_1} \\
&\leq 9\sqrt{2\varepsilon_0} + 16\sqrt{2\varepsilon_1}.
\end{aligned} \tag{5.36}$$

For the first inequality, we commuted Bob's check-round observables using Eq. (5.26) of Proposition 5.6. For the final inequality, we applied Lemma 5.7 to bound the anti-commutator norm. All other inequalities were found from the correlation estimates of Proposition 5.5.

To obtain Eq. (5.35) we use Proposition 5.5 to write

$$\begin{aligned} \left\| \left\{ X_{B,i}^i, Z_{B,j}^i \right\} |\psi\rangle \right\| &\leq 4\sqrt{2\varepsilon_1} + \left\| \left\{ X_A^i, Z_A^i \right\} |\psi\rangle \right\| \\ &\leq 9\sqrt{2\varepsilon_0} + 20\sqrt{2\varepsilon_1}, \end{aligned} \tag{5.37}$$

where the final inequality follows from Eq. (5.34) just proved. □

5.6 Self-test of many Bell states

We can use similar techniques to Section 5.5 to self-test $n > 3$ Bell states, provided $n \equiv 3 \pmod 4$ (which we will assume throughout this section). In this case, the honest strategy is played using a $3 \times n$ magic game, as described by Definition 5.3. The strategy for this game upon which we base our self-test will be explained in Section 5.6.1. The structure and honest behavior of the self-test will simultaneously be described in Section 5.6.2, with all general unknown observables for Alice and Bob and their required correlations then defined in Section 5.6.3. All commutation and anticommutation relations required to construct a local self-testing isometry will finally be shown in Section 5.6.4. From this, we have the final self-testing statement for many Bell states.

Theorem 5.9. *Let $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ be an unknown state shared by Alice and Bob and let $n \equiv 3 \pmod 4$ with $n > 3$ be the number of Bell states to be self-tested. Let sets of pairwise commutative, ± 1-valued, unknown observables in $\mathcal{L}(\mathcal{H}_A)$ for Alice be given as in Eq. (5.46), and in $\mathcal{L}(\mathcal{H}_B)$ for Bob as in Eqs. (5.47), (5.49) and (5.50). Suppose that these observables satisfy all correlations given in Eqs. (5.51) to (5.53) and let $\varepsilon = \max\{\varepsilon_0, \varepsilon_1, \varepsilon_2\}$. Then, for any choice $(k_i)_{i=1}^n$ of elements in $\{1, \ldots, n\}$ where each $k_i \neq i$, there exists a junk state $|\xi\rangle$ and isometries V_A and V_B defining the local isometry $V =$*

$V_A \otimes V_B$ *such that, for all* $i \in \{1, \dots, n\}$,

$$\left\| V|\psi\rangle - |\Phi^+\rangle_{AB}^{\otimes n} \otimes |\xi\rangle \right\| = O\left(n^{\frac{5}{2}}\sqrt{\varepsilon}\right), \tag{5.38a}$$

$$\left\| V X_A^i|\psi\rangle - \hat{X}_A^i|\Phi^+\rangle_{AB}^{\otimes n} \otimes |\xi\rangle \right\| = O\left(n^{\frac{5}{2}}\sqrt{\varepsilon}\right), \tag{5.38b}$$

$$\left\| V Z_A^i|\psi\rangle - \hat{Z}_A^i|\Phi^+\rangle_{AB}^{\otimes n} \otimes |\xi\rangle \right\| = O\left(n^{\frac{5}{2}}\sqrt{\varepsilon}\right), \tag{5.38c}$$

$$\left\| V X_{B,i}^i|\psi\rangle - \hat{X}_B^i|\Phi^+\rangle_{AB}^{\otimes n} \otimes |\xi\rangle \right\| = O\left(n^{\frac{5}{2}}\sqrt{\varepsilon}\right), \tag{5.38d}$$

$$\left\| V Z_{B,k_i}^i|\psi\rangle - \hat{Z}_B^i|\Phi^+\rangle_{AB}^{\otimes n} \otimes |\xi\rangle \right\| = O\left(n^{\frac{5}{2}}\sqrt{\varepsilon}\right). \tag{5.38e}$$

Proof. Take the observables $\{X_A^i, Z_A^i\}_{i=1}^n$ of Eq. (5.46) and $\{X_{B,i}^i, Z_{B,k_i}^i\}_{i=1}^n$ of Eq. (5.49) to be the (extended if necessary) reflections assumed by Theorem 2.8, with δ given by the largest upper bound appearing in Theorem 5.11. □

Relatively few of the unknown observables defined as part of the self-test are actually used to construct the isometry, with most only serving in the proofs of necessary commutation and anticommutation relations. The total number of observables defined in Eqs. (5.46), (5.47), (5.49) and (5.50) is $2n^2 + 4n$, while only $4n$ of these are required for the isometry of Theorem 2.8. In particular, we are free to use any n of the $Z_{B,y}^i$ of Eq. (5.49) provided that we cover all qubits (denoted by the superscript index). This freedom is expressed in Theorem 5.9 above by choice of the k_i. In the honest case, many of the unknown observables are in fact identical to one another.

For this self-test, Bob must make Pauli measurements on pairs of qubits to ensure their commutation. This was not explicitly required in the self-test of three Bell states, since Bob's game-round observables (corresponding to products of Pauli observables on all but one of his qubits) automatically served this purpose. We would thus like a way to subdivide all possible pairs of (an odd number of) qubits into as few disjoint sets of disjoint pairs as possible. This is equivalent to finding an optimal edge coloring for the complete graph K_n where n is odd. The following lemma constructs such a coloring.

Lemma 5.10. *Consider the complete graph* K_n *for* n *odd, whose vertices are labeled by* $V = \{1, \dots, n\}$. *For each* $v \in V$, *color the edges* $\{v - i, v + i\}$ *by color* v *for all* $i \in \left\{1, \dots, \frac{n-1}{2}\right\}$, *where addition is performed modulo* n. *This is a proper* n*-edge-coloring for* K_n *and is optimal in the sense that it uses as few colors as possible.*

Proof. Define the color of each edge $\{a, b\}$ to be $\frac{a+b}{2} \pmod{n}$, where the multiplicative inverse of 2 modulo n always exists since 2 is coprime to any odd n. Suppose that

two edges $\{x, i\}$ and $\{x, j\}$ have the same color under this definition. Then $\frac{x+i}{2} \equiv \frac{x+j}{2}$ (mod n), and thus $i = j$. Therefore no two distinct adjacent edges can have the same color. That is, we defined a proper edge coloring. Notice that all edges of the same color v here take the form $\{v - i, v + i\}$ for $i \in \left\{1, \ldots, \frac{n-1}{2}\right\}$. Hence our coloring is identical to that given in the statement. Optimality results from the fact that the chromatic index of K_n is n when n is odd. □

Remark. If the graph is depicted by straight lines drawn between the vertices of a regular n-gon, the given construction assigns a different color to each of n sets of parallel edges.

5.6.1 Magic game strategy

A simple winning strategy for $3 \times n$ magic games, in which players share three Bell states and Alice need only make single-qubit measurements, can be constructed by appending deterministic columns to the 3×3 strategy of Section 5.4. However, we will base our self-test on an alternative strategy, which will be described here.

Let Alice and Bob share the n Bell states

$$|\psi\rangle = \bigotimes_{j=1}^{n} |\Phi^+\rangle_{AB}^{(j)}. \tag{5.39}$$

Figure 5.3 depicts the $3 \times n$ measurement strategy that our self-test will be based upon.

$\prod_{j \neq 1} \hat{X}^j$	$\prod_{j \neq 2} \hat{X}^j$	…	$\prod_{j \neq n} \hat{X}^j$
$\prod_{j \neq 1} \hat{Y}^j$	$\prod_{j \neq 2} \hat{Y}^j$	…	$\prod_{j \neq n} \hat{Y}^j$
$\prod_{j \neq 1} \hat{Z}^j$	$\prod_{j \neq 2} \hat{Z}^j$	…	$\prod_{j \neq n} \hat{Z}^j$

Figure 5.3: The $3 \times n$ magic game strategy that our self-test is based upon. Pauli observables which act on qubit j of a player's register are denoted by $\hat{X}^j$, $\hat{Y}^j$, and $\hat{Z}^j$.

Since $n \equiv 3 \pmod 4$, the observable for each square of the strategy is composed of $2 \pmod 4$ single-qubit Pauli observables. Hence the three observables in each column mutually commute and satisfy Bob's negative product rule

$$\left(\prod_{j\neq y} \hat{X}^j\right)\left(\prod_{j\neq y} \hat{Y}^j\right)\left(\prod_{j\neq y} \hat{Z}^j\right) = \prod_{j\neq y} \hat{X}^j\hat{Y}^j\hat{Z}^j = i^{n-1}I = i^2 I = -I. \tag{5.40}$$

Since the Pauli observables appearing in each row are all of the same type, the squares in each row mutually commute. Moreover, since Pauli observables are involutory and there are an even number of such observables corresponding to each qubit in each row, every row has product $+I$. There is also perfect correlation between Alice's and Bob's observables for each square of the strategy. That is, letting $\hat{S}$ stand for $\hat{X}$, $\hat{Y}$, or $\hat{Z}$, and for all y,

$$\langle\psi| \prod_{j\neq y} \hat{S}_A^j \prod_{j\neq y} \hat{S}_B^j |\psi\rangle = \prod_{j\neq y} \langle\Phi^+| \hat{S}_A^j \hat{S}_B^j |\Phi^+\rangle_{AB}^{(j)} = (\pm 1)^{n-1} = 1. \tag{5.41}$$

This strategy can again be naturally phrased as a winning strategy for magic games in the sense of Definition 5.3. Alice generates her outputs a_j as the outcomes of measurements of $\hat{X}_A^j$, $\hat{Y}_A^j$, or $\hat{Z}_A^j$ depending on whether the first, second, or third row was assigned respectively. Bob generates his outputs (b_1, b_2, b_3) according to the outcomes of observables in Fig. 5.3 for the column he was assigned. By Eq. (5.40), Bob's outputs always satisfy the rule $b_1 b_2 b_3 = -1$. By Eq. (5.41), for input row and columns x and y, respectively, the outputs always satisfy $\prod_{j\neq y} a_j = b_x$. Therefore, in the strategy described, the players win with certainty.

In terms of experimental implementation, note that Alice need only make single-qubit Pauli measurements for her side of the strategy. On Bob's side, making the required compatible measurements of $\prod_{j\neq y} \hat{X}_B^j$, $\prod_{j\neq y} \hat{Y}_B^j$, and $\prod_{j\neq y} \hat{Z}_B^j$ may seem impractical for systems with large n. Note, however, that since the pairs of Pauli observables $\hat{X}\otimes\hat{X}$, $\hat{Y}\otimes\hat{Y}$, and $\hat{Z}\otimes\hat{Z}$ mutually commute, Bob need only measure $\frac{3}{2}(n-1)$ such pairs to construct measurements of all three required observables.

5.6.2 Structure and honest behavior

As in our self-test for three Bell states, Alice receives an input $x \in \{1, 2, 3\}$. However, Bob now receives an input $y \in \{1, \ldots, n\}$. Furthermore, Bob's input controlling the type of round is now a trit $c \in \{0, 1, 2\}$. The additional value $c = 2$ determines that the players are requested to check correlations between certain pairs of Pauli observables. As such, we will call such rounds where $c = 2$ *pair check* rounds, and

rename those rounds where $c = 1$ to *local check* rounds to avoid ambiguity. Alice must always output n bits, whereas the number of output bits of Bob depends on the type of round c. The protocol is summarized in Protocol 5.2.

Protocol 5.2: Protocol for certifying n Bell states. Intuitively, *pair check* rounds rule out those single-qubit $3 \times n$ magic rectangle game strategies found by extending strategies for smaller $3 \times n'$ games using deterministic entries. Otherwise, the required correlations could be satisfied by provers sharing fewer Bell states.

Let $n = 3 \pmod 4$ be the number of Bell states to be certified. The verifier chooses $c \in \{0, 1, 2\}$ and performs Protocol 5.1 with an additional subprotocol if $c = 2$ is chosen:

2. *Pair check*: Send Alice $x \in \{1, 3\}$. Alice answers with $a_1, \ldots, a_n$. Bob answers with $n - 1$ bits $b_{y-k,y+k}$ and $b'_{y-k,y+k}$ in $\{+1, -1\}$ (with addition taken modulo n) for all $k \in \{1, \ldots, \frac{n-1}{2}\}$.
   (a) If $x = 1$, accept if and only if $a_i a_j = b_{i,j}$ for all i, j.
   (b) If $x = 3$, accept if and only if $a_i a_j = b'_{i,j}$ for all i, j.

Honest rounds consist of the players sharing n Bell states,

$$|\psi\rangle = \bigotimes_{j=1}^{n} |\Phi^+\rangle_{AB}^{(j)}. \tag{5.42}$$

Alice always provides each of her output bits a_j by measuring the n observables of our $3 \times n$ magic game strategy (Section 5.6.1),

$$\hat{X}_A^j \quad \text{if } x = 1, \tag{5.43a}$$
$$\hat{Y}_A^j \quad \text{if } x = 2, \tag{5.43b}$$
$$\hat{Z}_A^j \quad \text{if } x = 3. \tag{5.43c}$$

This is structurally identical to Eq. (5.8) in the previous self-test of three Bell states, with the exception that n measurements are now made upon each input.

Once again the honest behavior of Bob depends on c. If it is a game round ($c = 0$), then Bob must output three bits, as usual with the goal of winning the $3 \times n$ magic game. In the case of a local check round ($c = 1$), Bob proceeds similarly to Eq. (5.9) of the previous self-test, but now generates his jth of n output bits depending on the

input y as the measurement outcomes of Pauli observables $\hat{S}_B^j$, where

$$\hat{S}_B^j = \begin{cases} \hat{X}_B^j & \text{if } y = j, \\ \hat{Z}_B^j & \text{otherwise.} \end{cases} \tag{5.44}$$

Finally, if it is a pair check round ($c = 2$), Bob measures $n - 1$ Pauli observables of the form $\hat{X} \otimes \hat{X}$ and $\hat{Z} \otimes \hat{Z}$ on disjoint pairs of qubits. Depending on the input y, the observables he measures are

$$\left\{ \hat{X}_B^{y-j} \hat{X}_B^{y+j} \right\}_{j=1}^{(n-1)/2} \cup \left\{ \hat{Z}_B^{y-j} \hat{Z}_B^{y+j} \right\}_{j=1}^{(n-1)/2}, \tag{5.45}$$

where addition is taken modulo n. Notice that all observables in the set of Eq. (5.45) mutually commute, and by the construction given in Lemma 5.10 the combination of all n such sets covers every possible pair of n qubits.

The correlations that we expect to be satisfied from honest check rounds are the appropriate perfect correlations between Alice and Bob. For local check rounds, these are (as before) all the single-qubit correlations $\langle\psi| \hat{X}_A^j \hat{X}_B^j |\psi\rangle = 1$ and $\langle\psi| \hat{Z}_A^j \hat{Z}_B^j |\psi\rangle = 1$. For pair check rounds, these are the correlations between all pairs of observables $\langle\psi| \hat{X}_A^j \hat{X}_A^k \hat{X}_B^j \hat{X}_B^k |\psi\rangle = 1$ and $\langle\psi| \hat{Z}_A^j \hat{Z}_A^k \hat{Z}_B^j \hat{Z}_B^k |\psi\rangle = 1$.

5.6.3 Unknown observables and correlations

We will again now denote the unknown state shared by the players by $|\psi\rangle$. Recall that, as in Section 5.5.2 for the previous self-test of three Bell states, all unknown observables must be labeled uniquely with respect to each observer's possible input questions in order to avoid assumptions about their measurements in this potentially dishonest case.

Alice's observables We define sets of mutually commuting unknown observables on Alice's side to be measured depending on her input x as

$$\left\{ X_A^j \right\}_{j=1}^n \quad \text{if } x = 1, \tag{5.46a}$$

$$\left\{ Y_A^j \right\}_{j=1}^n \quad \text{if } x = 2, \tag{5.46b}$$

$$\left\{ Z_A^j \right\}_{j=1}^n \quad \text{if } x = 3. \tag{5.46c}$$

Each of these unknown observables corresponds in the honest case to a single-qubit Pauli observable that acts on the qubit of Alice indicated by its superscript. However, it should be noted that no such assumption is made about the qubit locality of the untrusted observables defined here.

Bob's observables (game rounds) For game rounds ($c = 0$), we will denote the sets of unknown observables to be measured by Bob, depending on his input y, by

$$\left\{X_B^{\overline{y}}, Y_B^{\overline{y}}, Z_B^{\overline{y}}\right\}. \tag{5.47}$$

It should once again be noted that one of the observables for each input is redundant, as

$$Y_B^{\overline{y}}|\psi\rangle = -X_B^{\overline{y}} Z_B^{\overline{y}}|\psi\rangle \tag{5.48}$$

by the rule for the product of Bob's outputs (see Definition 5.3). We will, however, keep all for notational convenience.

Bob's observables (local check rounds) For local check rounds ($c = 1$), Bob's unknown observables correspond to single-qubit Pauli $\hat{X}$ and $\hat{Z}$ observables acting on his system. The set of observables for input y is defined by

$$\left\{X_{B,y}^{y}\right\} \cup \left\{Z_{B,y}^{j} : 1 \leq j \leq n, j \neq y\right\}. \tag{5.49}$$

Bob's observables (pair check rounds) For pair check rounds ($c = 2$), we define sets of $n - 1$ observables for each input y as

$$\left\{X_B^{y-j,y+j}\right\}_{j=1}^{(n-1)/2} \cup \left\{Z_B^{y-j,y+j}\right\}_{j=1}^{(n-1)/2} \tag{5.50}$$

where addition is taken modulo n. In contrast to the honest case of Eq. (5.45), we have not assumed that Bob's outputs arise as the product of multiple other observables. The two superscript indices denote that these observables correspond to the product of Pauli observables on pairs of qubits. For example, the unknown observable $X_B^{1,2}$ corresponds to $\hat{X}_B^1 \hat{X}_B^2$ in the honest case. In the notation we have introduced, the order of superscript indices for an unknown observable is unimportant. Thus, for convenience, we also introduce labels with reversed ordering of superscripts and identify these with observables appearing in Eq. (5.50). Specifically, let the labels $X_B^{i,j} \equiv X_B^{j,i}$ and $Z_B^{i,j} \equiv Z_B^{j,i}$. This is consistent with the honest case, in which the corresponding pairs of observables commute. By Lemma 5.10, the pairs of indices $(y - j, y + j)$ appearing in Eq. (5.50) for a given input y are pairwise disjoint and the combination of these pairs over every input gives every possible index pair (up to ordering of the indices). Thus the n sets of $n - 1$ pair check observables defined account for measurements of $\hat{X} \otimes \hat{X}$ and $\hat{Z} \otimes \hat{Z}$ on every possible pair of n qubits and, moreover, the observables for a given input mutually commute in the honest case as expected.

Correlations The correlations of unknown observables amounting to a uniformly ε_0-close to perfect strategy for the $3 \times n$ magic game (i.e. correlations obtained in game rounds) are, with reference to the winning strategy described in Section 5.6.1,

$$\Big\langle \Big(\prod_{j \neq k} X_A^j \Big) X_B^{\bar{k}} \Big\rangle \geq 1 - \varepsilon_0, \tag{5.51a}$$

$$-\Big\langle \Big(\prod_{j \neq k} Y_A^j \Big) X_B^{\bar{k}} Z_B^{\bar{k}} \Big\rangle \geq 1 - \varepsilon_0, \tag{5.51b}$$

$$\Big\langle \Big(\prod_{j \neq k} Z_A^j \Big) Z_B^{\bar{k}} \Big\rangle \geq 1 - \varepsilon_0. \tag{5.51c}$$

The correlations constituting uniformly ε_1-close to perfect local check rounds are, for all distinct $i, j \in \{1, \dots, n\}$,

$$\langle X_A^i X_{B,i}^i \rangle \geq 1 - \varepsilon_1, \tag{5.52a}$$

$$\langle Z_A^i Z_{B,j}^i \rangle \geq 1 - \varepsilon_1. \tag{5.52b}$$

The correlations describing uniformly ε_2-close to perfect pair check rounds are, for all distinct $i, j \in \{1, \dots, n\}$,

$$\langle X_A^i X_A^j X_B^{i,j} \rangle \geq 1 - \varepsilon_2, \tag{5.53a}$$

$$\langle Z_A^i Z_A^j Z_B^{i,j} \rangle \geq 1 - \varepsilon_2. \tag{5.53b}$$

From the assumption that all of these correlations are satisfied for our unknown observables, we will deduce appropriate commutation and anticommutation relations which imply the existence of a local self-testing isometry by Theorem 2.8.

5.6.4 Commutation and anticommutation relations

Here we will deduce the appropriate state-dependent commutation and anticommutation relations of our unknown reflections from which a local self-testing isometry can be constructed. The results of this section are summarized in the following theorem.

Theorem 5.11. *Let $i, j, k, l \in \{1, \dots, n\}$ be such that $i \neq k$ and $j \neq l$. We have correlations between each unknown observable of Alice with each of the corresponding observables on Bob's side*

$$\big\| (X_A^i - X_{B,i}^i) |\psi\rangle \big\| \leq \sqrt{2\varepsilon_1}, \tag{5.54}$$

$$\big\| (Z_A^i - Z_{B,k}^i) |\psi\rangle \big\| \leq \sqrt{2\varepsilon_1}. \tag{5.55}$$

We have the state-dependent anticommutativity of all unknown X observables with all unknown Z observables corresponding to the same qubit

$$\left\|\left\{X_A^i, Z_A^i\right\}|\psi\rangle\right\| \leq 3n\sqrt{2\varepsilon_0} + 2(n-1)\sqrt{2\varepsilon_2} + \left(\frac{13(n-1)}{2} + 17\right)\sqrt{2\varepsilon_1}, \quad (5.56)$$

$$\left\|\left\{X_{B,i}^i, Z_{B,k}^i\right\}|\psi\rangle\right\| \leq 3n\sqrt{2\varepsilon_0} + 2(n-1)\sqrt{2\varepsilon_2} + \left(\frac{13(n-1)}{2} + 21\right)\sqrt{2\varepsilon_1}. \quad (5.57)$$

Finally, we have the state-dependent commutativity of unknown X and Z observables. On Bob's side we have

$$\left\|\left[X_{B,i}^i, X_{B,j}^j\right]|\psi\rangle\right\| \leq 4\sqrt{2\varepsilon_1}, \quad (5.58)$$

$$\left\|\left[Z_{B,k}^i, Z_{B,l}^j\right]|\psi\rangle\right\| \leq 4\sqrt{2\varepsilon_1}; \quad (5.59)$$

and moreover restricting to observables corresponding to different qubits $i \neq j$

$$\left\|\left[X_{B,i}^i, Z_{B,l}^j\right]|\psi\rangle\right\| \leq 8\sqrt{2\varepsilon_1}. \quad (5.60)$$

On Alice's side, for different qubits $i \neq j$, we have

$$\left\|\left[M_A^i, N_A^j\right]|\psi\rangle\right\| \leq 4\sqrt{2\varepsilon_1}, \quad (5.61)$$

where M and N can be either of X and Z.

Proof. Combine Propositions 5.12 to 5.14. □

We begin by expressing the correlations of Eq. (5.52), between those observables of the players corresponding to local Pauli observables acting on the same qubit, in terms of norms.

Proposition 5.12 (Correlation)**.** *For all distinct $i, j \in \{1, \ldots, n\}$ we have the correlation estimates*

$$\left\|\left(X_A^i - X_{B,i}^i\right)|\psi\rangle\right\| \leq \sqrt{2\varepsilon_1}, \quad (5.62a)$$

$$\left\|\left(Z_A^i - Z_{B,j}^i\right)|\psi\rangle\right\| \leq \sqrt{2\varepsilon_1}. \quad (5.62b)$$

Proof. Apply Lemma 2.2 to the correlations given in Eq. (5.52). □

We now show the required state-dependent commutation relations for observables that correspond to local Pauli observables acting on different qubits. Since observables of Alice are defined to commute exactly with those of Bob, it is only necessary to consider state-dependent commutation relations on each side separately.

Proposition 5.13 (Commutation). *For all $i, j, k, l \in \{1, \dots, n\}$ such that $i \neq k$ and $j \neq l$ we have*

$$\left\| \left[X^i_{B,i}, X^j_{B,j} \right] |\psi\rangle \right\| \leq 4\sqrt{2\varepsilon_1}, \tag{5.63a}$$

$$\left\| \left[Z^i_{B,k}, Z^j_{B,l} \right] |\psi\rangle \right\| \leq 4\sqrt{2\varepsilon_1}. \tag{5.63b}$$

Moreover if $i \neq j$ we have commutation relations for Bob

$$\left\| \left[X^i_{B,i}, Z^j_{B,l} \right] |\psi\rangle \right\| \leq 8\sqrt{2\varepsilon_1} \tag{5.64}$$

and for Alice

$$\left\| \left[M^i_A, N^j_A \right] |\psi\rangle \right\| \leq 4\sqrt{2\varepsilon_1}, \tag{5.65}$$

where M and N can be either of X and Z.

Proof. As the proof of Proposition 5.6, but using the correlations of Eq. (5.52) instead of Eq. (5.15). □

The following proposition states the robust state-dependent anticommutation relations between each pair of unknown X and Z observables corresponding to the same qubit, depending on the correlation errors ε_0, ε_1, and ε_2. A sketch proof is given below for the ideal case with vanishing errors, with the more lengthy, full proof being the contents of Appendix B.

Proposition 5.14 (Anticommutation). *For all $i \in \{1, \dots, n\}$ we have state-dependent anticommutation relations for unknown observables of Alice*

$$\left\| \left\{ X^i_A, Z^i_A \right\} |\psi\rangle \right\| \leq 3n\sqrt{2\varepsilon_0} + 2(n-1)\sqrt{2\varepsilon_2} + \left(\frac{13(n-1)}{2} + 17 \right) \sqrt{2\varepsilon_1}. \tag{5.66}$$

Furthermore, for all $j \in \{1, \dots, n\}$ distinct from i we have state-dependent anticommutation relations for Bob's check-round observables

$$\left\| \left\{ X^i_{B,i}, Z^i_{B,j} \right\} |\psi\rangle \right\| \leq 3n\sqrt{2\varepsilon_0} + 2(n-1)\sqrt{2\varepsilon_2} + \left(\frac{13(n-1)}{2} + 21 \right) \sqrt{2\varepsilon_1}. \tag{5.67}$$

Sketch proof. For the sake of sketching the proof, take correlation errors to vanish $\varepsilon_0 = \varepsilon_1 = \varepsilon_2 = 0$. We will show the state-dependent anticommutation relation $\left\{ X^1_A, Z^1_A \right\} |\psi\rangle = 0$. The relations for observables corresponding to the other qubits follow similarly.

From the game correlations Eq. (5.51b) we have

$$\left(\prod_{k=2}^{n} Z^{\bar{k}}_B X^{\bar{k}}_B \right) |\psi\rangle + Z^{\bar{1}}_B X^{\bar{1}}_B |\psi\rangle = 0, \tag{5.68}$$

where the sign of the first term uses that n is odd. Swapping to Alice's side those observables acting immediately on the state and multiplying on the left by appropriate unitary operators gives

$$X_B^{\overline{2}}\Big(\prod_{k=3}^{n-1} Z_B^{\overline{k}} X_B^{\overline{k}}\Big) Z_B^{\overline{n}}|\psi\rangle + Z_B^{\overline{2}} Z_B^{\overline{1}} X_A^n X_A^1|\psi\rangle = 0. \tag{5.69}$$

Rewriting this by commuting those X and Z observables within each term of the product with k odd results in

$$\Big(\prod_{k=1}^{(n-3)/2} X_B^{\overline{2k}} X_B^{\overline{2k+1}} Z_B^{\overline{2k+1}} Z_B^{\overline{2k+2}}\Big) X_B^{\overline{n-1}} Z_B^{\overline{n}}|\psi\rangle + Z_B^{\overline{2}} Z_B^{\overline{1}} X_A^n X_A^1|\psi\rangle = 0. \tag{5.70}$$

Using the correlations of Eqs. (5.51a) and (5.51c) to swap Bob's observables to Alice's side (and freely inserting the identity operator as $X_A^{n-1} X_A^{n-1}$ into the resulting first term) yields

$$\Big(\prod_{k\neq n} Z_A^k\Big)\Big(\prod_k X_A^k\Big)\Big(\prod_{k=1}^{(n-3)/2} X_A^{n-2k+1} Z_A^{n-2k+1} Z_A^{n-2k} X_A^{n-2k}\Big) X_A^2|\psi\rangle + X_A^n X_A^1 Z_A^1 Z_A^2|\psi\rangle = 0. \tag{5.71}$$

From the correlations of Eq. (5.52) we have

$$X_A^2 Z_{B,n}^1 Z_{B,n}^2 X_{B,n}^n X_{B,1}^1|\psi\rangle = X_{B,n}^n Z_B^{1,2} X_B^{1,2}|\psi\rangle. \tag{5.72}$$

Hence multiplying Eq. (5.71) on the left by $Z_{B,n}^1 Z_{B,n}^2 X_{B,n}^n X_{B,1}^1$, applying Eq. (5.72) via the triangle inequality in its first term (commuting the resulting observables for Bob with the existing observables of Alice), and in its second term using the correlations of Eq. (5.52),

$$X_{B,n}^n Z_B^{1,2} X_B^{1,2}\Big(\prod_{k\neq n} Z_A^k\Big)\Big(\prod_k X_A^k\Big)\Big(\prod_{k=1}^{(n-3)/2} X_A^{n-2k+1} Z_A^{n-2k+1} Z_A^{n-2k} X_A^{n-2k}\Big)|\psi\rangle + \big(X_A^n X_A^1 Z_A^1 Z_A^2\big)^2|\psi\rangle = 0. \tag{5.73}$$

Lemma B.1 shows for all $k \in \big\{1, \ldots, \frac{n-3}{4}\big\}$ that in particular

$$\begin{aligned}&\big(X_A^{4k+2} Z_A^{4k+2} Z_A^{4k+1} X_A^{4k+1}\big)\big(X_A^{4k} Z_A^{4k} Z_A^{4k-1} X_A^{4k-1}\big)|\psi\rangle \\ &\quad = X_B^{4k-1,4k+1} Z_B^{4k-1,4k+1} Z_B^{4k,4k+2} X_B^{4k,4k+2}|\psi\rangle.\end{aligned} \tag{5.74}$$

Since $n \equiv 3 \pmod 4$, we can consider successive pairs of terms in the final product of Eq. (5.73). We can replace each pair of these terms using pair check observables by

repeatedly applying Eq. (5.74) and commuting the resulting observables of Bob with those of Alice. This gives

$$X_{B,n}^{n} Z_B^{1,2} X_B^{1,2} \Bigg(\prod_{k=1}^{(n-3)/4} X_B^{4k-1,4k+1} Z_B^{4k-1,4k+1} Z_B^{4k,4k+2} X_B^{4k,4k+2} \Bigg) \Bigg(\prod_{k\neq n} Z_A^k \Bigg) \Bigg(\prod_k X_A^k \Bigg) |\psi\rangle + \left(X_A^n X_A^1 Z_A^1 Z_A^2\right)^2 |\psi\rangle = 0. \quad (5.75)$$

Lemma B.2 with $\sigma = \mathrm{id}$ chosen to be the identity permutation shows

$$\Bigg(\prod_{k\neq n} Z_A^k \Bigg) \Bigg(\prod_k X_A^k \Bigg) |\psi\rangle = X_A^n X_B^{1,2} \Bigg(\prod_{k=1}^{(n-3)/4} X_B^{4k-1,4k+1} X_B^{4k,4k+2} \Bigg) Z_B^{1,2} \Bigg(\prod_{k=1}^{(n-3)/4} Z_B^{4k-1,4k+1} Z_B^{4k,4k+2} \Bigg) |\psi\rangle. \quad (5.76)$$

If we assume that all pair check observables appearing in Eq. (5.75) are measured as part of the same (pair check round) input for Bob (which is compatible with an honest strategy since all of these observables have either disjoint or identical superscript index pairs to all others), then all such observables mutually commute. Thus applying Eq. (5.76) to Eq. (5.75) and using the involutory property of all pair check observables to achieve many cancellations, we get

$$X_A^n X_{B,n}^n |\psi\rangle + \left(X_A^n X_A^1 Z_A^1 Z_A^2\right)^2 |\psi\rangle = 0. \quad (5.77)$$

It should be noted that, for the simplicity of this sketch, the set of mutually commuting pair check observables used as an input here does not necessarily match one of the inputs defined in Eq. (5.50). Nonetheless, it is still the case that only n such sets must be used to complete the proof for all anticommutation relations of Alice's observables, and (with the proof essentially unchanged) the set used here matches one of those in Eq. (5.50) under a suitable permutation of the qubit labels.

Applying the correlations of Eq. (5.52a) once in the first term of Eq. (5.77) and then multiplying on the left by $Z_A^2 Z_A^1 X_A^1 X_A^n$ gives

$$\left\{X_A^1 X_A^n, Z_A^1 Z_A^2\right\} |\psi\rangle = 0. \quad (5.78)$$

By identical argument to the proof of Proposition 5.8, but using Propositions 5.12 and 5.13 instead of Propositions 5.5 and 5.6 and using Eq. (5.78) in place of Lemma 5.7, this implies the desired state-dependent anticommutation relation $\left\{X_A^1, Z_A^1\right\} |\psi\rangle = 0$ for Alice's observables.

The state-dependent anticommutation relations for Bob can all be obtained by simple application of Proposition 5.12, given those just proved for Alice's observables. □

5.7 Discussion

In this chapter we introduced one-side-local quantum strategies for the magic square and $3 \times n$ magic rectangle games that win with certainty. We then supplemented these strategies with some extra correlations obtained via "check" rounds to obtain the desired self-tests. Our final result is a parallel self-test for n maximally entangled Bell states which has several practical advantages over other protocols. Being a parallel self-test of n Bell states, our protocol makes no assumptions within the n single-qubit systems of each side.

We examine first the experimental requirements of realizing our self-test: something that is determined by the honest runs. All observables used in the honest strategy for our self-test can be implemented as the tensor product of at most two Pauli operators (of the same type) acting on different pairs of qubits. Moreover, an advantage of our work is that Alice need only ever make local measurements of single-qubit Pauli observables in the honest case. This is especially important for uses of self-testing in which the level of quantum technology available to the parties is asymmetric. For example, in the context of delegated quantum computation, the "client" could have very limited quantum capabilities. It suffices that they are able to measure single qubits in Pauli bases.

Another interesting property of our self-test concerns its communication complexity. Of particular importance is the size of input questions, which quantify how much randomness must be consumed by the protocol in each round of interaction. If the input size is too large (for example linear in n), then estimation of probability distributions of outcomes for each question becomes unfeasible (exponentially many questions would take exponential time). Our test requires constant size (1 trit) input questions for Alice, and for Bob requires $O(\log n)$ bit inputs. With a few very recent exceptions [106–109] (in all of which robustness is either not explicitly constructed or doubly exponential in n), other works have achieved at best logarithmic input complexities (see for example [70, 103]). In our protocol, one of the players need only receive questions of a constant size. Players must each output $O(n)$ bit answers, except for in game rounds, in which Bob need only return 2 bit outputs.

Our protocol also has the practical advantage that it makes use of solely perfect correlations; any optimal strategy succeeds with certainty, thus requiring fewer rounds of experiment to achieve a desired statistical confidence.

The final figure of merit that we consider is robustness to noise. Given correlations that are at worst ε-close to perfect, using a self-testing theorem that can be found in [27], our results achieve a robustness that is $O\left(n^{5/2}\sqrt{\varepsilon}\right)$ for the collection of Bell states and all single-qubit Pauli observables. That is, to achieve a robustness δ it is sufficient that $\varepsilon(n,\delta) = \Omega(n^{-5}\delta^2)$. The self-testing works of Coladangelo [27] and Coudron and Natarajan [26] using instead the parallel repetition of the magic square game as a basis perform slightly better in this regard, with $\varepsilon(n,\delta) = \Omega(n^{-3}\delta^2)$ and $\varepsilon(n,\delta) = \Omega(n^{-4}\delta^4)$ being sufficient for robustness δ, respectively. The work of Coudron and Natarajan [26] achieves robustness for observables acting on all qubits simultaneously, however, both works are examples of strictly parallel self-tests and thus necessarily require $O(n)$ bit inputs. A protocol of Natarajan and Vidick [28] exhibits the interesting property that its robustness does not depend explicitly on n. The same authors later extended this work to have communication complexity only logarithmic in the number of entangled states to be certified. The protocol, however, instead self-tests N maximally entangled *qudit* states and corresponding single-*qudit* Pauli observables defined over a finite field $\mathbb{F}_q$, where q increases with N [103]. It is unclear whether the honest strategy provided can be realized with local measurements with respect to Bell states.[3]

Our protocol is unique in that it achieves several desirable properties simultaneously. The prover with minimal quantum-technological capabilities (the client) need only make local single-qubit measurements in Pauli bases upon accepting questions all of constant size. Despite this, our protocol relies entirely on perfect correlations, maintains a noise tolerance comparable with that of most others, and requires questions provided to the server to be of size at most logarithmic in the number of Bell states tested. Sample comparisons with some other protocols can be found in Table 5.1. The list of works included is not exhaustive, and other figures of merit could also be considered depending on intended applications.

[3]While maximally-entangled qudit states and generalized qudit Pauli measurement projectors are isomorphic to tensor products of $|\Phi^+\rangle$ and *qubit* Pauli measurement projectors respectively (as shown in a lemma of [105]), it is not clear that all of the measurements used in the qudit honest strategy of [103] can be mapped under such an isomorphism to local measurements with respect to each two-dimensional register (in general they may become entangled measurements).

Table 5.1: Comparison between certain protocols capable of self-testing n EPR pairs in parallel. Cells highlighted in green depict favorable comparisons within the property being considered. Those in red compare unfavorably and those in yellow neutrally. Whether the honest strategy of each protocol uses only local (single-qubit) measurements, is constructed entirely from measurements of the Pauli group (on standard Bell states), and makes use of only perfect correlations (so that the strategy wins with certainty) are considered. The error tolerance $\varepsilon(n, \delta)$ is a sufficient maximum error in observed correlations so that the states and measurements (up to local isometry) are a distance at most δ from ideal. Input question sizes (the amounts of randomness consumed) are given in units of information.

Protocol	Local	Pauli	Perf. corr.	Error tol.	Input size	
				$\varepsilon(n, \delta)$	Alice	Bob
$3 \times n$ protocol (**this work**)	Alice	Yes	Yes	$\Omega(n^{-5}\delta^2)$	$O(1)$	$O(\log n)$
Šupić et al. [106]	Depends on base self-tests			N/A	$O(1)$	
Chao et al. [70]	Yes	No	No	$\Omega(n^{-5}\delta^2)$	$O(\log n)$	
Natarajan and Vidick [103]	No	No	Yes	$\Omega(\text{poly}(\delta))$	$\text{poly}(\log n)$	
Natarajan and Vidick [28]	No	As CHSH or MS		$\Omega(\delta^{16})$	$O(n)$	
Coladangelo [27] (magic square)	No	Yes	Yes	$\Omega(n^{-3}\delta^2)$	$O(n)$	
Coladangelo [27] (CHSH)	Yes	No	No	$\Omega(n^{-3}\delta^2)$	$O(n)$	
Coudron and Natarajan [26]	No	Yes	Yes	$\Omega(n^{-4}\delta^4)$	$O(n)$	
McKague [102] (Mayers–Yao)	Yes	No	No	$\Omega(n^{-8}\delta^8)$	$O(\log \log n)$	

Future works Aside from our self-testing result, all self-tests whose honest strategies rely solely on the magic square game (such as those of [26, 27]) can of course be implemented using our one-side-local strategy if desired. It may also be possible to use our one-side-local strategy as a direct replacement for honest subroutines in other protocols (such as the CHSH game in the protocol of Chao et al. [70] or for the anticommutation test of Natarajan and Vidick [28]), allowing them to function with the additional benefits of local Pauli measurements and perfect correlations at the same time.

It may also be possible to devise magic square strategies that makes use of even more Bell states (four or more) in a nontrivial way. In this case, we could also study any additional properties of these strategies (similar to the one-side-locality of the strategy we gave). Additional check rounds would likely need to be used to form a self-testing statement inspired by such a strategy. However, with ever more kinds of check rounds being required, it may become difficult to simultaneously preserve any advantageous properties that are found from the larger magic square strategy.

In our work, we made use of a theorem of Coladangelo [27] to translate our main state-dependent commutation/anticommutation results into a proper self-testing state-

ment on the existence of a desired local isometry. Other choices of isometry could equally-well have been made. On the one hand, other results based on the relevant commutativity and anticommutativity of untrusted observables exist. For example, a result of McKague [102, Lemma 6] could be directly substituted for that used here, offering the additional property of simultaneously testing multiple Pauli measurements at the cost of poorer robustness scaling: requiring $\varepsilon(n, \delta) = \Omega(n^{-6}\delta^4)$. On the other hand, it would be interesting to examine the plausibility of more robust isometries for our self-test. Such isometries could arise either as improved general techniques for the construction of self-testing isometries given certain relations between the untrusted observables (similar to [27, 102]), or alternatively in the form of specially-constructed isometries making use of features unique to the testing scenario. Another possible future direction is to study the robustness of our protocol experimentally (or numerically under the semidefinite-programming characterization of quantum correlations [59, 60, 110, 111]).

Adaptation of our results for device-independent versions of delegated quantum computation protocols, or other secure quantum computation protocols [112, 113], could be explored. The utility of our protocol for device-independent quantum key distribution could also be examined. We hope that our self-test will be of retroactive use in new applications of self-testing with asymmetric quantum technological requirements that may be developed in the future.

Chapter 6

Parallel remote state preparation for device-independent VBQC

In this chapter, we exhibit a two-prover parallel self-testing-based scheme in which a classical verifier is able to delegate a quantum computation to an untrusted quantum server Bob (who is assumed to be in possession of a powerful universal quantum computer) using only a simple untrusted measurement device (which may only perform single-qubit measurements) and shared entanglement. In our context, Alice acts both as the verifier and the client who is in possession of the measurement device. The computation is performed blindly by the server and its correctness is verifiable by the client. The protocol proceeds for the verifier in the following way:

1. Certify n EPR pairs of entanglement shared between Alice and Bob, and measurements of each in the XY-plane and computational bases.

2. Prepare a suitable n-qubit state on Bob's side by measurements performed on Alice's side.

3. Perform with Bob the unconditionally secure interactive protocol of Fitzsimons and Kashefi [40] (or another FK-type protocol).

The blindness and verifiability properties of our protocol are inherited from the FK protocol, since using an entanglement-based approach to the remote state preparation ensures that blindness is not compromised [7, 114]. Our main result is the parallel device-independent certification of remotely prepared states that can be used for the first two steps of the protocol.

Theorem 6.1 (Informal Theorem 6.11)**.** *Suppose that the maximal quantum expectation values of all given Bell expressions are approximately attained by the measurement statistics collected from provers Alice and Bob, i.e., Alice and Bob pass all requested Bell tests with high probability (this is achievable by using the honest strategy of Section 6.5.3). Then, with high probability, the state on Bob's side upon Alice performing a measurement is close (up to some isometry that is independent of the measurement or its outcome) in trace distance to an ideal valid input to the FK protocol or that with all dummy qubits flipped. The prepared state is known only to Alice.*

The self-testing protocol that we base Theorem 6.1 on (whose resulting statement is given in Theorem 6.16) simultaneously exhibits many properties desirable for the VBQC application we consider. The rationale behind all of these properties is discussed in further detail in Section 6.2.

1. Our self-test is parallel, meaning that n Bell states are certified at once with no prior assumption on the tensor product structure of the underlying state space.

2. Permutations of n single-qubit measurements on Alice's side, each either in the computational basis or one of the four bases of the eight canonical states of the XY-plane (those corresponding to all cardinal and intercardinal directions) are also certified.

3. The possible correlated complex conjugation freedom that arises for measurement operators of this kind is accounted for and, moreover, is limited to measurements in the computational basis (so as only to affect the preparation of dummy qubits for the VBQC protocol).

4. The number of possible input questions in the test is small. The client side measurement device is asked questions of size logarithmic in n, while questions of only a constant size need be communicated to the server.

5. In the honest case, Alice need only perform single-qubit measurements local to each of the EPR pairs she shares with Bob. This reflects the minimal quantum capabilities she is given access to. Moreover, despite Bob being assumed to possess a powerful universal quantum computer, he need only perform two-qubit Bell measurements in the self-testing protocol, and most of the time only measures single qubits.

6. The isometry on Bob's subsystem (and resulting reduced junk state) guaranteed by the self-test is independent of any string of n measurement bases selected for state preparation. This ensures composability with the FK protocol.

7. Classical processing of the gathered raw experimental data required for the self-test scales efficiently in n.

While the parallel self-test based on magic rectangles of Chapter 5 may be useful in a general variety of client–server applications, it does not quite exhibit all these properties required for the application of the current chapter. In particular, it is not clear how it could be adapted to satisfy both Items 2 and 7 (we need the client to be capable of performing all possible sets of different measurements on n individual qubits, while we also want not to spend time estimating the probabilities for all possible outcomes of these).

While we do not explicitly attempt to derive robustness bounds for our self-testing statement, we believe that our derivations are compatible with the many standard techniques that have been developed and used successfully for this purpose in other works [27, 70, 102, 115, 116]. Nevertheless, we do phrase all of the subtests comprising our full self-test in terms of an error tolerance ε, and derive all relations between operators in terms of this quantity. We therefore expect that our self-testing statement would exhibit analytic robustness at worst $O(\sqrt{\varepsilon}n^2)$, thereby giving a trace distance that is $O(\varepsilon^{1/3}n^{4/3})$ in Theorem 6.1. Large improvements in robustness having been shown achievable using numerical optimization techniques such as semidefinite programming [25, 59–61, 101, 106, 110, 111, 117, 118].

The information aggregated from experimental outcomes that is used in each subtest is *local* in the sense that it corresponds to measurements of only individual or pairs of the n Bell states in the honest strategy (despite being conditioned on the measurements that are asked for at other positions). The quantity ε for each subtest then does not refer to the noise and statistical uncertainty present over all n Bell states, but rather for constant sized chunks of the experimental resources. Thus, in a (possibly noisy) physical implementation of the honest strategy, the error estimate ε would not typically increase with the number of qubits being prepared n. It is also for this reason that the exponential number of possible outcomes in n associated with each question does not lead to the estimation of probabilities requiring exponential time; local consideration of outcomes effectively transforms exponentially many probabilities with one distribution per question to a linear number of distributions per question each

with a constant number of probabilities to estimate.

Many of our results are not specific to VBQC alone. In particular, our self-test and remote state preparation protocol have properties that may be desirable for other quantum delegation applications. Furthermore, due to the range of measurements we are able to certify, our tests could be easily adapted to the remote preparation of other states.

Related works General composability of delegated quantum computation was studied by Dunjko et al. [119]. The original two-prover protocol for VBQC that we make use of is that of Fitzsimons and Kashefi [40], which is a verifiable extension to the blind protocol of Broadbent et al. [120]. Other forms of resource states and repetition schemes have since been devised in order to improve the practicality and overhead of the protocol [44, 45, 121]. This VBQC protocol was proven to be robust and composable with device-independent state preparation protocols by Gheorghiu et al. [7]. In this work, they also used the CHSH rigidity results of Reichardt et al. [122, 123] to achieve such preparation sequentially, resulting in a device-independent VBQC protocol using total resources scaling like g^{2048}, where g is the number of gates in the circuit to be delegated. A more efficient scheme (again with sequential preparation but this time based on self-testing) was given by Hajdušek et al. [30] and uses $\Theta(g^4 \log g)$ resources. This, however, requires that the server party is in possession of n spacelike separated provers, which is difficult to achieve in practice and cannot be verified to be the case by the client. Another many-prover protocol was presented by McKague [29] based on self-testing graph states. A more recent approach is the so-called "verifier-on-a-leash" protocol of Coladangelo et al. [53]. This device-independent protocol is based on the verifiable delegation approach of Broadbent [49] rather than the FK protocol, with the blindness property a result of its combination with self-testing. The efficient resource usage $\Theta(g \log g)$ is primarily a result of the self-testing protocol used: a modified version of the "Pauli braiding test" of Natarajan and Vidick [28]. However, this protocol requires that the client possesses a more powerful quantum measuring device (being able to perform joint measurements of multiple qubits), has exponentially many questions of size $O(n)$ bits, and is not fault-tolerant. The robustness guarantee given by the underlying self-testing protocol is poly(ϵ), where ϵ is the overall rejection probability in the test (a quantity that is not directly comparable with the local error tolerances ε used in many other self-testing statements including our own). The quantum steering scenario, in which the device of one party is

entirely trusted, was considered in the context of VBQC by Gheorghiu et al. [31]. In the setting of *computational* security, there exist recent single-prover protocols such as those of Mahadev [124], Gheorghiu and Vidick [125], and Gheorghiu et al. [126], the latter of which perform remote state preparation in this setting.

The concept of self-testing was first introduced by Mayers and Yao [4] in a cryptographic context, with the first mention of the term "self-testing" appearing in [23]. The question of which states can be self-tested was answered by Coladangelo et al. [127] in the bipartite case and later for the multipartite case [128]. Arbitrary parallel self-testing of EPR pairs was first introduced by McKague [102] and a host of self-tests for entangled states of arbitrary local dimension have now been proposed [26–28, 70, 71, 102–104, 106–109, 115, 116, 127, 129–131]. Complex conjugation ambiguity in self-testing complex measurements was first recognized by McKague and Mosca [68]. The triple CHSH inequality was first introduced by Acín et al. [132] and subsequently used for self-testing by Bowles et al. [116], whose results we make use of in the present work. It was also used by Renou et al. [133] to devise an experiment to rule out quantum theory with real numbers. Commutation-based measures were introduced by Kaniewski [69] and also used to certify multiple anticommuting observables. Works of McKague [102] and [27] gave general theorems for converting certain sets of approximate commutation relations between observables to robust self-testing statements (with real measurements). The latter is based on work by Chao et al. [70] and also gives self-testing statements for parallel repeated CHSH games, while the former was later used as such by the same author [115]. The possibility of self-testing with just a single prover by replacing nonlocal correlations by computational assumptions was examined by Metger and Vidick [134]. More details on self-testing can be found in the excellent review by Šupić and Bowles [24].

Chapter organization An overview of our techniques is given in Section 6.1. In Section 6.2, we explain in further detail the desirable properties required of self-testing protocols that are to be used for remote state preparation in the context of VBQC. The triple CHSH inequality of Acín et al. [132] is exhibited in Section 6.3, and we use it to show a single-copy self-testing statement that is used as a building block in later results. Section 6.4 contains our results linking the existence of certain operator relations to a self-testing statement with desired properties, as well as a result for lifting parallel self-testing statements certifying only single-qubit observables to those with arbitrary tensor products of observables. Our main protocol is outlined in

Section 6.5, where we give some intuition behind our self-testing protocol, state our main remote state preparation result (Theorem 6.11), detail the construction of Alice's question set in Section 6.5.1, define the measurement scenario and tests required in Section 6.5.2, and give the honest strategy in Section 6.5.3. We prove in Section 6.6 that approximate acceptance in our tests yields approximate operator relations, and thus give our formal self-testing statements of Theorem 6.16 and Corollary 6.17. We finish in Section 6.7 with some discussion and possible future directions.

Notation The usual notation introduced in Section 2.1 for Hilbert spaces will be used in this chapter. That is, different Hilbert spaces local to Alice will be denoted by calligraphic variants such as $\mathcal{A}$, $\mathcal{A}'$, and $\tilde{\mathcal{A}}$ (and similarly for Bob). A hat symbol placed above an operator in this chapter will always mean the regularized version of a corresponding operator labeled without the hat. For example, $\hat{X}$ will refer to the regularized version of some operator X, rather than referring to the Pauli observable that will unambiguously be written using the notation σ_{x} or σ_1 (and similarly for other Pauli observables).

Recall also from Section 2.1 that, for a string $\boldsymbol{x} = (x_1, \ldots, x_n)$, we adopt the notation that x_i is the ith element of $\boldsymbol{x}$, while $\boldsymbol{x}_i$ denotes $\boldsymbol{x}$ with its ith element removed.

6.1 Overview of techniques

The basis for our self-testing is a careful consideration of the statistics one would expect to find from parallel Clauser–Horne–Shimony–Holt (CHSH) measurements of n maximally entangled Bell states shared between provers Alice and Bob [9]. We take Alice to be the one performing measurements of Pauli observables from the standard strategy for the CHSH game. By appropriately chunking the raw data received by the verifier into outcomes for the different questions of a local CHSH inequality conditioned on the different possible fixed input questions asked at other position, it is possible to construct sets of CHSH-type inequalities for each of the individual Bell states, all of which would be saturated with honest behavior. We proceed to show the opposite of this—that the saturation of these inequalities is sufficient to prove all operator relations required and achieve a self-testing statement for the Bell states and CHSH measurements. Moreover, we show that after removing many of the requested inequalities, the remaining tests are still sufficient. Enough of the tests can be removed that the total number of remaining tests (and thus input questions) is

reduced to scale quadratically (rather than exponentially) in n, and there are only a constant number of possible actions that Bob need take. Intuitively, the players cannot cheat in the tests by sharing fewer than n Bell states since Alice cannot be sure which of n positions of Bob she is being tested against, while at the same time Bob does not know how correlated different positions in Alice's input question are with one another. The reduction in the number of our questions comes from the fact that only pairwise correlations in Alice's question strings must be hidden (see Section 6.5 for further details).

We show that the "triple CHSH" inequalities introduced by Acín et al. [132] can be used to extend our technique to include certification of all Pauli observables σ_x, σ_y, and σ_z. We construct our isometry such that the complex conjugation ambiguity appears in σ_z rather than the usual σ_y measurements. We then introduce further tests (also efficient), based on perfect correlations between further measurements for Alice and those present already for Bob, that ensure that these additional untrusted measurements for Alice certify reference measurements of the intercardinal directions of the XY-plane, as required to generate input states to the FK VBQC protocol. Finally, we augment our self-test thus far with a test that expects Bob to perform Bell measurements on two sets of pairs of his qubits, in order to ensure that any possible correlated complex conjugation of the provers' measurement operators occurs globally across all n of their registers (this is similar to techniques used in [53, 116] for the same purpose).

One drawback of the technique we use to reduce Alice's questions to quadratic order is that the resulting local isometry is only able to certify the measurement operators for a constant number of choices of bases for Alice's measurement of the n EPR pairs. The greater structure present in her restricted set of possible inputs may leak some information about this choice of bases, which in turn would allow Bob to gain some knowledge of the states prepared for him and cheat in the subsequent VBQC interactive protocol. To remedy this, we instead use polynomially many different sets of our quadratically many questions (polynomially many questions in n overall) and perform the certification for each of these. This results in a polynomial-sized subset $\mathcal{S}$ of questions for Alice (which we call "special" questions), for each of which a different local isometry certifies a different string of bases measured on Alice's reference system. In order for our remote state preparation protocol to be composable with the FK interactive protocol, it must be the case that states are prepared up to an isometry that is independent of the choice of bases in $\mathcal{S}$ (otherwise one could not assume that

the physical state of Bob originates from local quantum operations applied to his ideal reference state without also assuming that he has knowledge of the bases chosen [7]). This does not present a problem for the use of our self-test as, despite each question in $\mathcal{S}$ requiring a different local isometry, we show that the isometry local to Bob's subsystem is the same in all of these cases. While it is the case that the resulting security parameter for the FK protocol will go as the reciprocal of $|\mathcal{S}|$, which is inverse polynomial in n for our choice of questions, this trade-off between question size and security scaling is an inescapable feature of any remote state preparation protocol used for FK-type protocols.

Since our protocol must perform remote state preparation, we are interested in self-testing statements estimate the closeness of (normalized) physical post-measurement states from their (normalized) ideal counterparts. The robustness guarantees usually given by self-testing statements estimate this distance for observables acting on states, which naively lead to similar estimates for (subnormalized) measurement projectors acting on states. This is acceptable for protocols that prepare states sequentially (such as in [7, 30, 122, 123]), however, for parallel protocols of n states (which have exponentially many outcomes per measurement) would lead to robustness estimates that scale exponentially in n for post-measurement states. We overcome this using Lemma 6.2 and Theorem 6.4 of Section 6.2.1 at the cost of relaxing the estimate by a factor that is polynomial in the original robustness and allowing acceptance with high probability.

6.2 Efficient parallel self-testing for DIVBQC

Standard VBQC protocols (such as the original Fitzsimons–Kashefi protocol [40] we will consider) require that n qubits be prepared on the server side, each in one of the states $|\pm_\theta\rangle$, or the states $|0\rangle$ or $|1\rangle$ (for dummy qubits). A self-test appropriate for device-independently preparing states for practical VBQC should satisfy the following properties.

1. The self-test should certify the presence of n copies of the Bell state $|\Phi^+\rangle$ shared between Alice and Bob. That is, the state $|\Phi^+\rangle^{\otimes n}$ should be self-tested.

2. Denote by $|\sigma_\chi^\lambda\rangle$ the eigenstate of σ_χ with eigenvalue $\lambda \in \{+1, -1\}$ and $\chi \in \{\mathrm{x}, \mathrm{y}, \mathrm{z}, \mathrm{x}+\mathrm{y}, \mathrm{x}-\mathrm{y}\}$ (see notation in Section 2.1). For n-tuples of Pauli bases $\boldsymbol{\chi} = (\chi_1, \ldots, \chi_n) \in \{\mathrm{x}, \mathrm{y}, \mathrm{z}, \mathrm{x}+\mathrm{y}, \mathrm{x}-\mathrm{y}\}^n$, the self-test should certify the projective

measurement of the certified state $|\Phi^+\rangle^{\otimes n}$ on Alice's side

$$\left\{ \bigotimes_{j=1}^{n} \left|\sigma_{\chi_j}^{\lambda_j}\right\rangle\!\left\langle\sigma_{\chi_j}^{\lambda_j}\right| \right\}_{\lambda\in\{+1,-1\}^n} \tag{6.1}$$

with each measurement operator composed of the tensor product of n projectors. We will refer to these as *special* or *preparation* measurements for reasons that will become clear.

3. The number of possible input questions, and hence the number of different measurements required, should be small. Specifically, questions should be of size at most logarithmic in n.

4. The self-test should be robust to the observation of nonideal statistics.

5. All measurements performed on Alice's subsystem (the client side) must be local to one of her qubits in the honest case.

6. Classical processing of the gathered experimental outcomes should scale efficiently in n.

7. Possible complex conjugation of measurement operators should occur only in the preparation of dummy qubits $|0\rangle$ and $|1\rangle$ (i.e. measurement of Pauli σ_z).

8. The isometry on Bob's subsystem and reduced junk state guaranteed by the self-test should be independent of the choice of preparation question χ.

Together, Properties 1 and 2 allow Alice to remotely prepare n qubit states on Bob's subsystem (up to the freedoms allowed by self-testing), each in one of the two states comprising a prechosen basis for the purpose of VBQC (any of the bases corresponding to observables σ_x, σ_y, σ_z, σ_{x+y}, or σ_{x-y}). The outcome Alice receives allows her to determine the state that has been prepared on Bob's subsystem. Meanwhile, Bob is aware of neither the state that was prepared on his side, nor the specific bases chosen.

Property 3 means that it is experimentally feasible to gather outcome statistics upon all possible questions. If, instead, questions had size linear in n, then the time required to achieve good statistical confidence would scale exponentially with the number of qubits to be prepared. At first glance, Properties 2 and 3 may appear slightly contradictory, since the number of possible n-tuples of bases is exponential in n. We avoid this issue by requiring that only a single *special* one of these exponentially

many measurements be among those self-tested. We still require, however, that this special measurement may be freely defined using any of the possible basis tuples, prior to the initiation of the self-testing protocol. The reason for this is that the special measurement will later be used by Alice to prepare the n server-side qubits in the suitable bases to perform an arbitrary computation (that is prechosen by Alice), for which the ability to prepare each qubit in an arbitrary basis is desirable. In this sense, we must in fact define a whole class of self-testing protocols—one for each choice of special measurement—all of which satisfy the other properties.

The robustness included as Property 4 is important to allow for experimental noise and imperfections. The connection between the level of robustness guaranteed by a self-testing statement and that which can be achieved in remote state preparation is examined in more detail in Section 6.2.1.

Property 5 is included to ensure that it is sufficient for the client to possess only a simple quantum device. Such a device may only be capable of performing single-qubit measurements and, thus, we must ensure that all measurements included as part of the honest strategy for the self-test (even those that are not used for preparation) can be performed by the client.

Property 6 means that the experimental data that is collected may be combined and processed such that the conditions of the self-test are shown to be true in a reasonable time. This may not necessarily be the case if, for example, the Bell expressions which must be evaluated in order to perform the certification have exponentially many terms in n [106].

Property 7 preserves the verifiability property of the FK protocol while still allowing states to be prepared in all required bases. This is discussed further in Section 6.2.2 (see also [7]).

Property 8 is a slight restriction on isometries found in self-testing protocols, allowing the physical states prepared using an untrusted strategy to be used as resource states for VBQC. In the FK protocol, the possibly deviating server of Bob is allowed to apply any unitary (or, more generally, quantum channel) to the reference qubits that are received, but has no knowledge of the bases in which these qubits have been prepared [40]. We would thus like to interpret the physical state prepared on Bob's side due to a self-testing protocol as originating solely from such a process [7]. This can be done be "undoing" Bob's self-testing isometry, provided that his junk state (ancillary to the reference qubits) and isometry do not depend on any information about the choice of bases (i.e. the preparation question chosen).

6.2.1 Post-measurement states

Robust parallel self-tests for n-qubit states and measurements typically guarantee estimates for observables acting on the states of the form

$$V M^{\boldsymbol{s}} |\psi\rangle \overset{\delta}{\approx} M'^{\boldsymbol{s}} |\psi'\rangle \otimes |\xi\rangle \tag{6.2}$$

for all $\boldsymbol{s} \in \{0,1\}^n$ (or in expectation over all $\boldsymbol{s}$ in some cases [28, 103]). This naively leads to statements for individual outcomes $\boldsymbol{a} \in \{+,-\}^n$ of the form

$$V M_{\boldsymbol{a}} |\psi\rangle \overset{\delta}{\approx} M'_{\boldsymbol{a}} |\psi'\rangle \otimes |\xi\rangle, \tag{6.3}$$

where the $M_{\boldsymbol{a}}$ and $M'_{\boldsymbol{a}}$ are projection operators (cf. Eqs. (2.39) and (2.40) and Definitions 2.6 and 2.7). For most practical applications (including the present one), however, one is instead interested in characterizing the physical and reference post-measurement states

$$\frac{M_{\boldsymbol{a}} |\psi\rangle}{\sqrt{\langle\psi| M_{\boldsymbol{a}} |\psi\rangle}}, \quad \frac{M'_{\boldsymbol{a}} |\psi'\rangle}{\sqrt{\langle\psi| M'_{\boldsymbol{a}} |\psi'\rangle}}. \tag{6.4}$$

Since there are 2^n possible outcomes $\boldsymbol{a}$ (and assuming they occur approximately uniformly), their respective probabilities $\langle\psi| M_{\boldsymbol{a}} |\psi\rangle$ must all be approximately 2^{-n}. Therefore, self-testing guarantees of the form of Eq. (6.3) typically lead to vector norm distances $\delta\sqrt{2^n}$ of physical post-measurement states from their reference counterparts, which blow up exponentially in n.

In the following, we will overcome this impracticality by slightly relaxing the distance guaranteed by a factor polynomial in δ, and also allowing that this guarantee fails to be satisfied with some probability that is polynomially small in δ. In the noiseless honest case, δ is written in terms of some error ε that (as is typical of the statistical tools used to analyze data for self-testing protocols [135]) can be experimentally saturated with statistical confidence exponentially close to unity in the number of experimental trials performed.

We first exhibit in Lemma 6.2 a general result on the trace distance between pure states that is compatible with distances that are expressed in expectation (as is the case for some self-testing statements). We then use a special case of this to show in Theorem 6.4 that, given certain self-testing guarantees of the form that will be derived in our context later (see Theorems 6.11 and 6.16 and Corollary 6.17), the post-measurement states of the physical experiment must be close in trace distance to those of the reference experiment most of the time.

Lemma 6.2. *Let $\Sigma \times \Omega$ be some finite sample space. Let π be some probability mass function on Σ for the random variable $S\colon\ \Sigma \times \Omega \to \Sigma$ defined by $S(\sigma, \omega) = \sigma$. For all $\sigma \in \Sigma$ and $\omega \in \Omega$, let $|u_\sigma^\omega\rangle$ be vectors satisfying*

$$\sum_{\omega \in \Omega} \| |u_\sigma^\omega\rangle \|^2 = 1. \tag{6.5}$$

For each $\sigma \in \Sigma$, let p_σ be the function on Ω defined by

$$p_\sigma(\omega) = \| |u_\sigma^\omega\rangle \|^2. \tag{6.6}$$

Define the probability mass function p on $\Sigma \times \Omega$ by

$$p(\sigma, \omega) = p_\sigma(\omega)\pi(\sigma). \tag{6.7}$$

For each $\sigma \in \Sigma$ and $\omega \in \Omega$ satisfying $p(\sigma, \omega) > 0$, let $|v_\sigma^\omega\rangle$ be nonzero vectors. Denote normalized versions of all the vectors (when they are defined) by

$$|\hat{u}_\sigma^\omega\rangle = \frac{|u_\sigma^\omega\rangle}{\| |u_\sigma^\omega\rangle \|}, \quad |\hat{v}_\sigma^\omega\rangle = \frac{|v_\sigma^\omega\rangle}{\| |v_\sigma^\omega\rangle \|}. \tag{6.8}$$

Let D be a random variable on $\Sigma \times \Omega$ defined by the trace distance between these normalized states

$$D(\sigma, \omega) = \begin{cases} \frac{1}{2} \| |\hat{u}_\sigma^\omega\rangle\langle\hat{u}_\sigma^\omega| - |\hat{v}_\sigma^\omega\rangle\langle\hat{v}_\sigma^\omega| \|_1 & \text{if } p(\sigma, \omega) > 0, \\ 0 & \text{if } p(\sigma, \omega) = 0. \end{cases} \tag{6.9}$$

Suppose that for some $\delta \geq 0$ we have

$$\sum_{\sigma \in \Sigma} \pi(\sigma) \sum_{\omega \in \Omega} \| |u_\sigma^\omega\rangle - |v_\sigma^\omega\rangle \|^2 \leq \delta^2. \tag{6.10}$$

Then, for any $c > 0$,

$$\Pr(D \leq \delta^c) \geq 1 - 4\delta^{2(1-c)} \tag{6.11}$$

for all $\sigma \in \Sigma$ for which $\pi(\sigma) > 0$.

Proof. See Appendix D. □

The proof of Lemma 6.2 relies on the following elementary lemma, which gives a useful bound on the trace distance between operators of the form $|v\rangle\langle v|$, where vectors $|v\rangle$ may be subnormalized.

Lemma 6.3. *Let vectors $|u\rangle$ and $|v\rangle$ belonging to the same Hilbert space satisfy $\||u\rangle\| \leq 1$ and $\||v\rangle\| \leq 1$. The trace distance is then bounded as*

$$\frac{1}{2}\||u\rangle\langle u| - |v\rangle\langle v|\|_1 \leq 2\||u\rangle - |v\rangle\|. \tag{6.12}$$

If the vectors have unit length then the bound can be tightened to

$$\frac{1}{2}\||u\rangle\langle u| - |v\rangle\langle v|\|_1 \leq \||u\rangle - |v\rangle\|. \tag{6.13}$$

Proof. See Appendix C for a proof of the general bound. For unit vectors, a simpler proof suffices, with the result immediately following from the inequality

$$|\langle u|v\rangle| \geq \mathfrak{Re}\,\langle u|v\rangle = 1 - \frac{1}{2}\||u\rangle - |v\rangle\|^2 \tag{6.14}$$

applied to the Fuchs–van de Graaf expression

$$\frac{1}{2}\||u\rangle\langle u| - |v\rangle\langle v|\|_1 = \sqrt{1 - |\langle u|v\rangle|^2} \tag{6.15}$$

for pure states. □

We now proceed to use a special case of Lemma 6.2 to state a similar result for the context of self-testing with robustness guarantees given for all possible observables that can be formed from measurement operators for parallel binary outcomes.

Theorem 6.4. *Let $V\colon \mathcal{H} \to \mathcal{H}'$ be an isometry. Define the probability mass function p for outcomes $\boldsymbol{a} \in \{0,1\}^n$ of a projective measurement $\{M_{\boldsymbol{a}}\}_{\boldsymbol{a}} \subset \mathcal{L}(\mathcal{H})$ on a state $|\psi\rangle \in \mathcal{H}$ by $p(\boldsymbol{a}) = \langle\psi| M_{\boldsymbol{a}} |\psi\rangle$. Let $|\psi'\rangle \in \mathcal{H}'$ be a state and let $\{M'_{\boldsymbol{a}}\}_{\boldsymbol{a}} \subset \mathcal{L}(\mathcal{H}')$ be a projective measurement such that $M'_{\boldsymbol{a}}|\psi'\rangle \neq 0$ for all $\boldsymbol{a}$. For all $\boldsymbol{s} \in \{0,1\}^n$, define observables*

$$M^{\boldsymbol{s}} = \sum_{\boldsymbol{a}} (-1)^{\boldsymbol{a}\cdot\boldsymbol{s}} M_{\boldsymbol{a}}, \quad M'^{\boldsymbol{s}} = \sum_{\boldsymbol{a}} (-1)^{\boldsymbol{a}\cdot\boldsymbol{s}} M'_{\boldsymbol{a}}. \tag{6.16}$$

Suppose that for all $\boldsymbol{s}$ we have

$$V M^{\boldsymbol{s}} |\psi\rangle \overset{\delta}{\approx} M'^{\boldsymbol{s}} |\psi'\rangle. \tag{6.17}$$

Defining a random variable D for the trace distance between post-measurement states

$$D(\boldsymbol{a}) = \frac{1}{2}\left\| \frac{V M_{\boldsymbol{a}} |\psi\rangle\langle\psi| M_{\boldsymbol{a}} V^\dagger}{p(\boldsymbol{a})} - \frac{M'_{\boldsymbol{a}} |\psi'\rangle\langle\psi'| M'_{\boldsymbol{a}}}{\langle\psi'| M'_{\boldsymbol{a}} |\psi'\rangle} \right\|_1 \tag{6.18}$$

we then have (with respect to the probability distribution p) that

$$\Pr\left(D \leq \delta^{2/3}\right) \geq 1 - 4\delta^{2/3}. \tag{6.19}$$

Remark. We assume without loss of generality that all outcomes satisfy $p(\boldsymbol{a}) > 0$, since values of $\boldsymbol{D}$ that could never be observed would not contribute towards the resulting probability.

Proof. Let us denote

$$|w_{\boldsymbol{a}}\rangle = V M_{\boldsymbol{a}}|\psi\rangle - M'_{\boldsymbol{a}}|\psi'\rangle. \tag{6.20}$$

Combining Eqs. (6.16) and (6.17), we can write

$$\begin{aligned}
\delta^2 &\geq \frac{1}{2^n}\sum_{\boldsymbol{s}} \left\| V M^{\boldsymbol{s}}|\psi\rangle - M'^{\boldsymbol{s}}|\psi'\rangle \right\|^2 \\
&= \frac{1}{2^n}\sum_{\boldsymbol{s}} \left\| \sum_{\boldsymbol{a}} (-1)^{\boldsymbol{a}\cdot\boldsymbol{s}} |w_{\boldsymbol{a}}\rangle \right\|^2 \\
&= \frac{1}{2^n}\sum_{\boldsymbol{a},\boldsymbol{b},\boldsymbol{s}} (-1)^{(\boldsymbol{a}\oplus\boldsymbol{b})\cdot\boldsymbol{s}} \langle w_{\boldsymbol{b}}|w_{\boldsymbol{a}}\rangle \\
&= \sum_{\boldsymbol{a}} \|V M_{\boldsymbol{a}}|\psi\rangle - M'_{\boldsymbol{a}}|\psi'\rangle\|^2,
\end{aligned} \tag{6.21}$$

where we have used the fact that

$$\sum_{\boldsymbol{s}} (-1)^{\boldsymbol{c}\cdot\boldsymbol{s}} = \begin{cases} 2^n & \text{if } \boldsymbol{c} = \boldsymbol{0}, \\ 0 & \text{otherwise.} \end{cases} \tag{6.22}$$

Note that $\|V M_{\boldsymbol{a}}|\psi\rangle\|^2 = \langle\psi|\, M_{\boldsymbol{a}}\, |\psi\rangle$ and $\|M'_{\boldsymbol{a}}|\psi'\rangle\|^2 = \langle\psi'|\, M'_{\boldsymbol{a}}\, |\psi'\rangle$. Finally, apply Lemma 6.2 with sample spaces $\Sigma = \{\sigma\}$ for some σ (so that $\pi(\sigma) = 1$) and $\Omega = \{0,1\}^n$, vectors $|u_{\boldsymbol{a}}\rangle = V M_{\boldsymbol{a}}|\psi\rangle$ and $|v_{\boldsymbol{a}}\rangle = M'_{\boldsymbol{a}}|\psi'\rangle$, and choosing $c = 2/3$. □

6.2.2 Correlated complex conjugation

As we have already seen in Section 2.5, it is impossible to distinguish a reference strategy from that with its measurement operators replaced by their complex conjugates (performed in some fixed local orthonormal bases for which the reference state may be assumed to have real matrix elements). Since there is no basis in which all of σ_{x}, σ_{y}, and σ_{z} simultaneously have real matrix representations, some complex conjugation ambiguity must necessarily be included in our self-testing statement in order that we certify measurements of all σ_{x}, σ_{y}, σ_{z}, $\sigma_{\mathrm{x+y}}$, and $\sigma_{\mathrm{x-y}}$ on Alice's side, as required to satisfy Property 2.

Note that there exist a pair of local orthonormal bases for which the matrix representations of the state $|\Phi^+\rangle$ and observables σ_{x} and σ_{y} are all real, while $\sigma_{\mathrm{z}}^* = -\sigma_{\mathrm{z}}$ (with $*$ denoting complex conjugation performed in the aforementioned basis). The

observable $-\sigma_z$ has eigenstate $|1\rangle$ for the eigenvalue $+1$ and eigenstate $|0\rangle$ for the eigenvalue -1. With this choice of complex conjugation basis, the only ambiguity introduced in the preparation of qubits on Bob's side is that a qubit supposedly prepared by the measurement of σ_z in a state $|0\rangle$ or $|1\rangle$ may in fact be prepared in the opposite state $|1\rangle$ or $|0\rangle$, respectively. States prepared by measurements of any of the other observables σ_x, σ_y, σ_{x+y}, or σ_{x-y} remain unambiguous.

The FK protocol correctly handles input states in which all of the "dummy" qubits of the honest input $|0\rangle$ or $|1\rangle$ are unknowingly (with some unknown probability) flipped to $|1\rangle$ and $|0\rangle$, respectively. Hence, for the remainder of this work, we take complex conjugation to be performed in the local orthonormal bases described in this section, unless otherwise stated.

Proposition 6.5 (Gheorghiu et al. [7, Lemma 10])**.** *If the initial input state of the FK protocol is close to the ideal input state with all dummy qubits* $|0\rangle$ *and* $|1\rangle$ *replaced with* $|1\rangle$ *and* $|0\rangle$*, respectively, the protocol will reject it with high probability.*

Proof sketch. Given a trap that has an odd number of dummy qubit neighbors, the verifier expects to apply a Z correction based on the parity of the number of $|1\rangle$ neighbors. With all $|0\rangle$ and $|1\rangle$ qubits of the input flipped with respect to the ideal input, the number of $|1\rangle$ neighbors of the trap has opposite parity to what the verifier expects. In this case, the verifier will always get the opposite result from the trap to that which is expected. Therefore, as long as the verifier makes sure that at least one trap has an odd number of dummy neighbors (which is easily achievable), the state is rejected in the protocol. □

We require that possible flipping of the dummy qubits in the input state occurs *globally*: either all such states are flipped or none are flipped. Note that this is in correspondence with Definition 2.7 of complex self-testing, in which complex conjugation is possibly performed on the whole reference measurement operator without any mention of its structure (in our case the many-qubit tensor product structure). One may otherwise imagine a weaker statement of self-testing for the special case of n-fold product states, in which the reference experiment is certified up to complex conjugation at any combination of the n positions. It is possible to construct tests that enforce global complex conjugation from some such statements [116].

In previous works lifting the FK protocol to the device-independent scenario, that complex conjugation must be accounted for in a global fashion was not a considera-

tion, since state preparation was performed sequentially (self-testing single EPR pairs as in [30] or based on the rigidity of the CHSH game [122, 123] as in [7]).

6.3 Triple CHSH inequality

Let us first consider the well-known problem of self-testing a single Bell state and single-qubit Pauli observables in the following scenario. In each round, Alice is provided with one of three possible input questions $x \in \{1,2,3\}$ and answers with $a \in \{+1,-1\}$. These are denoted by the ± 1-outcome observables acting on Alice's subsystem A_1, A_2, and A_3 respectively. Meanwhile, Bob is provided with one of six possible input questions $y \in \{1,\ldots,6\}$ and answers with $b \in \{+1,-1\}$. These are denoted by the ± 1-outcome observables acting on Bob's subsystem $D_{\mathrm{z,x}}$, $E_{\mathrm{z,x}}$, $D_{\mathrm{z,y}}$, $E_{\mathrm{z,y}}$, $D_{\mathrm{x,y}}$, and $E_{\mathrm{x,y}}$ respectively.

Consider the triple CHSH operator [116, 132] defined as

$$\begin{aligned} C = {} & A_3 \otimes (D_{\mathrm{z,x}} + E_{\mathrm{z,x}}) + A_1 \otimes (D_{\mathrm{z,x}} - E_{\mathrm{z,x}}) \\ & + A_3 \otimes (D_{\mathrm{z,y}} + E_{\mathrm{z,y}}) + A_2 \otimes (D_{\mathrm{z,y}} - E_{\mathrm{z,y}}) \\ & + A_1 \otimes (D_{\mathrm{x,y}} + E_{\mathrm{x,y}}) + A_2 \otimes (D_{\mathrm{x,y}} - E_{\mathrm{x,y}}). \end{aligned} \tag{6.23}$$

This operator is the sum of three CHSH operators, with each of A_1, A_2, and A_3 contained in two of them. The expectation value satisfies $\langle\psi| C |\psi\rangle \leq 6\sqrt{2}$ for any state $|\psi\rangle$ shared between Alice and Bob, since each of the three CHSH operators has expectation upper bounded by $2\sqrt{2}$. We can saturate this bound by taking the shared state to be

$$|\psi\rangle = |\Phi^+\rangle \equiv \frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{6.24}$$

and the observables to be

$$A_1 = \sigma_{\mathrm{x}}, \quad A_2 = -\sigma_{\mathrm{y}}, \quad A_3 = \sigma_{\mathrm{z}}, \quad D_{j,k} = \frac{\sigma_j + \sigma_k}{\sqrt{2}}, \quad E_{j,k} = \frac{\sigma_j - \sigma_k}{\sqrt{2}}. \tag{6.25}$$

In the classical case, we have the triple CHSH inequality $\langle C \rangle \leq 6$. The minus sign preceding σ_{y} in Eq. (6.25) is due to the perfect anticorrelation of σ_{y} between the subsystems of Alice and Bob in the state $|\Phi^+\rangle$. We could just as easily saturate the quantum bound instead taking $A_2 = \sigma_{\mathrm{y}}$ by changing the sign of each A_2 in Eq. (6.23).

It has previously been shown (see [116, 132]) that a maximal violation $\langle\psi| C |\psi\rangle = 6\sqrt{2}$ self-tests the reference state $|\Phi^+\rangle$ and the reference observables $\{\sigma_{\mathrm{x}}, \sigma_{\mathrm{y}}, \sigma_{\mathrm{z}}\}$ or their complex conjugates (in the computational basis) $\{\sigma_{\mathrm{x}}, -\sigma_{\mathrm{y}}, \sigma_{\mathrm{z}}\}$, acting on Alice's

subsystem (with the complex measurement σ_y self-tested in the sense of McKague and Mosca [68]). Specifically, the following theorem was previously shown.

Theorem 6.6 (Bowles et al. [116])**.** *Suppose the state $|\psi\rangle \in \mathcal{A} \otimes \mathcal{B}$ and the observables $A_j \in \mathcal{L}(\mathcal{A})$ and $D_{j,k}, E_{j,k} \in \mathcal{L}(\mathcal{B})$ satisfy*

$$\langle \psi | C | \psi \rangle = 6\sqrt{2} - \varepsilon. \tag{6.26}$$

Then there exist linear isometries $V_{\mathcal{A}} : \mathcal{A} \to \mathcal{A} \otimes \mathcal{A}' \otimes \mathcal{A}''$ and $V_{\mathcal{B}} : \mathcal{B} \to \mathcal{B} \otimes \mathcal{B}' \otimes \mathcal{B}''$ defining the local isometry $V = V_{\mathcal{A}} \otimes V_{\mathcal{B}}$ such that

$$V|\psi\rangle \overset{c\sqrt{\varepsilon}}{\approx} |\Phi^+\rangle_{\mathcal{A}'\mathcal{B}'} \otimes |\xi\rangle, \tag{6.27a}$$

$$VA_1|\psi\rangle \overset{c\sqrt{\varepsilon}}{\approx} \sigma_x^{\mathcal{A}'} |\Phi^+\rangle_{\mathcal{A}'\mathcal{B}'} \otimes |\xi\rangle, \tag{6.27b}$$

$$VA_2|\psi\rangle \overset{c\sqrt{\varepsilon}}{\approx} -\sigma_y^{\mathcal{A}'} |\Phi^+\rangle_{\mathcal{A}'\mathcal{B}'} \otimes \sigma_z^{\mathcal{A}''} |\xi\rangle, \tag{6.27c}$$

$$VA_3|\psi\rangle \overset{c\sqrt{\varepsilon}}{\approx} \sigma_z^{\mathcal{A}'} |\Phi^+\rangle_{\mathcal{A}'\mathcal{B}'} \otimes |\xi\rangle, \tag{6.27d}$$

where c is a nonnegative constant and the state $|\xi\rangle \in \mathcal{A} \otimes \mathcal{A}'' \otimes \mathcal{B} \otimes \mathcal{B}''$ has the form

$$|\xi\rangle = |00\rangle_{\mathcal{A}''\mathcal{B}''} \otimes |\xi_0\rangle_{\mathcal{A}\mathcal{B}} + |11\rangle_{\mathcal{A}''\mathcal{B}''} \otimes |\xi_1\rangle_{\mathcal{A}\mathcal{B}} \tag{6.28}$$

for some subnormalized $|\xi_0\rangle_{\mathcal{A}\mathcal{B}}$ and $|\xi_1\rangle_{\mathcal{A}\mathcal{B}}$ satisfying $\langle \xi_0 | \xi_0 \rangle_{\mathcal{A}\mathcal{B}} + \langle \xi_1 | \xi_1 \rangle_{\mathcal{A}\mathcal{B}} = 1$.

The appearance of the additional σ_z observable in Eq. (6.27c) acting on the ancilla space $\mathcal{A}''$ can be explained as performing a measurement of Alice's junk state ancilla in the computational basis, the outcome of which controls whether σ_y or $-\sigma_y$ is applied to Alice's half of $|\Phi^+\rangle$. The probability of applying the complex conjugate observable is given by $\langle \xi_1 | \xi_1 \rangle_{\mathcal{A}\mathcal{B}}$.

We show a variant of this result that is instead consistent with complex conjugation being performed in a basis in which the state $|\Phi^+\rangle$ and observables σ_x and σ_y have real matrices, while σ_z satisfies $\sigma_z^* = -\sigma_z$. The isometry used to do this is depicted in Fig. 6.1 as a circuit acting on the state $|\psi\rangle_{AB}$. This circuit is similar to the usual partial *swap* isometry (used for self-testing in [136]) followed by phase kickback unitaries controlled by additional ancilla qubits [68]. It is modified to use physical operators corresponding to Pauli X and Y in the first "swap" stage, and Pauli Z in the second "phase kickback" stage. The unitary operators $\hat{X}_{\mathcal{B}}$, $\hat{Y}_{\mathcal{B}}$, and $\hat{Z}_{\mathcal{B}}$ contained on

Bob's side of the circuit are regularized versions of

$$X_{\mathcal{B}} = \frac{D_{\mathrm{x,y}} + E_{\mathrm{x,y}}}{\sqrt{2}}, \tag{6.29a}$$

$$Y_{\mathcal{B}} = \frac{D_{\mathrm{x,y}} - E_{\mathrm{x,y}}}{\sqrt{2}}, \tag{6.29b}$$

$$Z_{\mathcal{B}} = \frac{D_{\mathrm{z,x}} + E_{\mathrm{z,x}}}{\sqrt{2}}. \tag{6.29c}$$

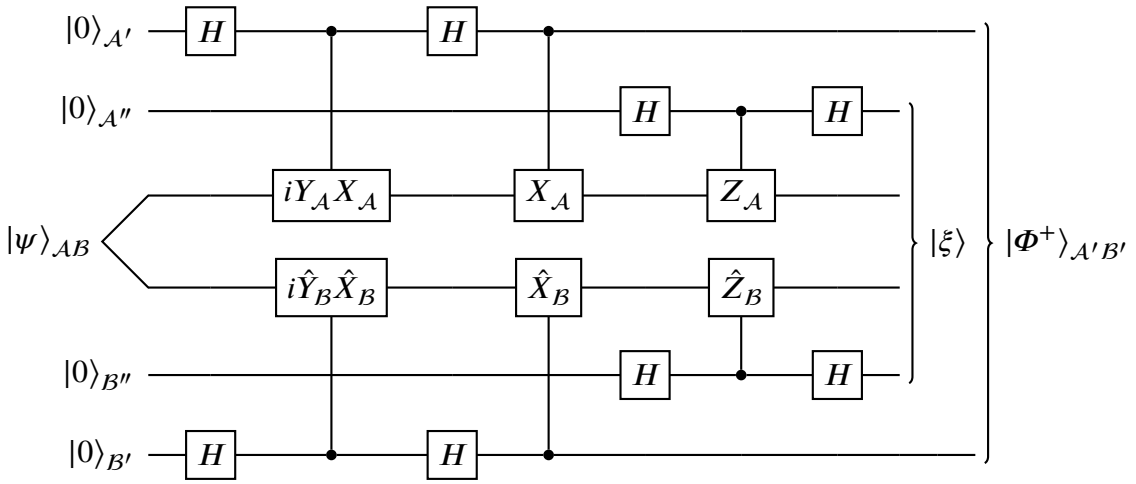


Figure 6.1: A modified partial swap isometry followed by phase kickback unitaries, acting on the state $|\psi\rangle_{\mathcal{AB}}$, which is used to self-test the state $|\Phi^+\rangle$ and measurements of $\{\sigma_{\mathrm{x}}, \sigma_{\mathrm{y}}, \sigma_{\mathrm{z}}\}$ or $\{\sigma_{\mathrm{x}}, \sigma_{\mathrm{y}}, -\sigma_{\mathrm{z}}\}$, given a maximal violation of the triple CHSH inequality. The unitary operators on Alice's subsystem are simply $X_{\mathcal{A}} = A_1$, $Y_{\mathcal{A}} = -A_2$, and $Z_{\mathcal{A}} = A_3$. The unitary operators $\hat{X}_{\mathcal{B}}$, $\hat{Y}_{\mathcal{B}}$, and $\hat{Z}_{\mathcal{B}}$ are regularized versions of $X_{\mathcal{B}}$, $Y_{\mathcal{B}}$, and $Z_{\mathcal{B}}$ respectively, which are each defined in terms of the operators $D_{j,k}$ and $E_{j,k}$.

We will state the result in a more explicit form than that of Definition 2.7, as doing so will later prove useful in the proof of our parallel version of the self-test (see Appendix G). In order to write the result, we introduce the notation $W\colon \mathcal{A} \otimes \mathcal{B} \to \mathcal{A} \otimes \mathcal{A}' \otimes \mathcal{B} \otimes \mathcal{B}'$ and $K\colon \mathcal{A} \otimes \mathcal{B} \to \mathcal{A} \otimes \mathcal{A}'' \otimes \mathcal{B} \otimes \mathcal{B}''$ for the local "swap" and "phase kickback" isometries, respectively, that are constructed in Fig. 6.2.

Proposition 6.7. *Let $|\psi\rangle_{\mathcal{AB}} \in \mathcal{A} \otimes \mathcal{B}$. Suppose for each $q \in \{1, 2, 3\}$ that there exist ± 1-outcome observables S_q on $\mathcal{A}$ and T_q on $\mathcal{B}$ satisfying (for some $\eta \geq 0$) the following relations:*

1. $(S_q - T_q)|\psi\rangle_{\mathcal{AB}} \overset{\eta}{\approx} 0$ *for all* q.
2. $\{S_q, S_r\}|\psi\rangle_{\mathcal{AB}} \overset{\eta}{\approx} 0$ *and* $\{T_q, T_r\}|\psi\rangle_{\mathcal{AB}} \overset{\eta}{\approx} 0$ *for all* q *and* r *such that* $q \neq r$.

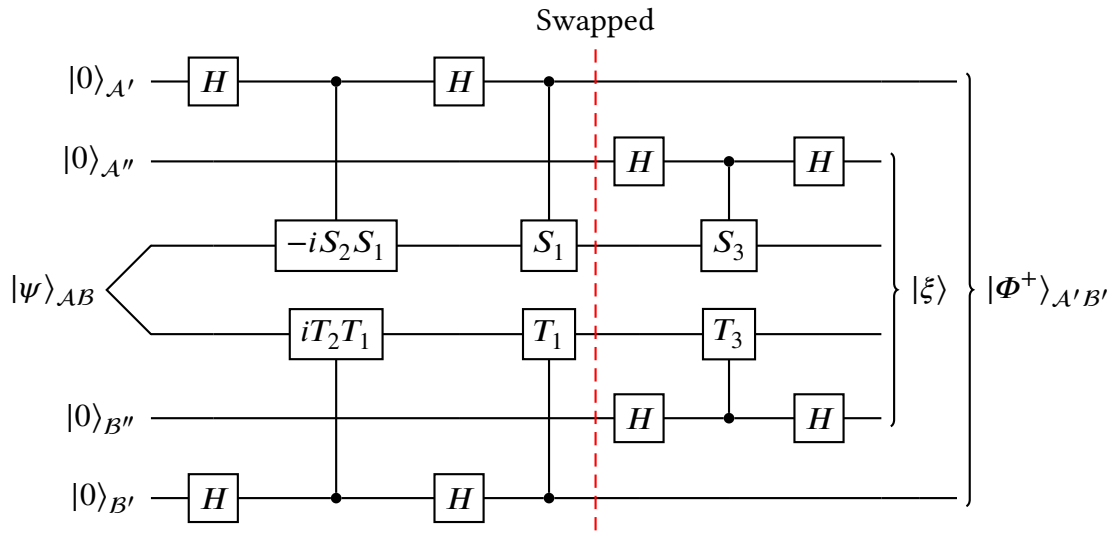


Figure 6.2: The circuit describing the action of the local isometry $V = KW$ on the state $|\psi\rangle_{AB}$. The isometries $W_A : \mathcal{A} \to \mathcal{A} \otimes \mathcal{A}'$ and $W_B : \mathcal{B} \to \mathcal{B} \otimes \mathcal{B}'$ and the local isometry $W = W_A \otimes W_B$ are defined by the first "swap" stage of the circuit (preceding the dotted line), in which a maximally entangled state is extracted. In the second "phase kickback" stage (succeeding the dotted line), denoted by $K = K_A \otimes K_B$ for isometries $K_A : \mathcal{A} \to \mathcal{A} \otimes \mathcal{A}''$ and $K_B : \mathcal{B} \to \mathcal{B} \otimes \mathcal{B}''$, possible complex conjugation in the presence of a Pauli σ_z operator is accounted for.

Construct the local "swap" isometry $W : \mathcal{A} \otimes \mathcal{B} \to \mathcal{A} \otimes \mathcal{A}' \otimes \mathcal{B} \otimes \mathcal{B}'$ *and the local "phase kickback" isometry* $K : \mathcal{A} \otimes \mathcal{B} \to \mathcal{A} \otimes \mathcal{A}'' \otimes \mathcal{B} \otimes \mathcal{B}''$ *as in Fig. 6.2. Then*

$$W|\psi\rangle_{AB} \overset{c_0\eta}{\approx} |\Phi^+\rangle_{A'B'} \otimes |\varphi\rangle_{AB}, \tag{6.30a}$$

$$WS_1|\psi\rangle_{AB} \overset{c_1\eta}{\approx} \sigma_x^{B'}|\Phi^+\rangle_{A'B'} \otimes |\varphi\rangle_{AB}, \tag{6.30b}$$

$$WS_2|\psi\rangle_{AB} \overset{c_2\eta}{\approx} \sigma_y^{B'}|\Phi^+\rangle_{A'B'} \otimes |\varphi\rangle_{AB}, \tag{6.30c}$$

$$WS_3|\psi\rangle_{AB} \overset{c_3\eta}{\approx} \sigma_z^{B'}|\Phi^+\rangle_{A'B'} \otimes S_3|\varphi\rangle_{AB}, \tag{6.30d}$$

where $|\varphi\rangle_{AB} \in \mathcal{A} \otimes \mathcal{B}$ *is defined as*

$$|\varphi\rangle_{AB} = \frac{1}{\sqrt{2}}(I + iT_2T_1)|\psi\rangle_{AB} \tag{6.31}$$

and nonnegative constants c_0, c_1, c_2, *and* c_3 *are defined as*

$$c_0 = \frac{1}{4}\left(18 + 5\sqrt{2}\right), \tag{6.32a}$$

$$c_1 = \frac{1}{4}\left(26 + 5\sqrt{2}\right), \tag{6.32b}$$

$$c_2 = \frac{1}{4}\left(34 + 5\sqrt{2}\right), \tag{6.32c}$$

$$c_3 = \frac{1}{4}\left(66 + 5\sqrt{2}\right). \tag{6.32d}$$

Moreover,

$$K|\varphi\rangle_{\mathcal{AB}} \overset{6\sqrt{2}\eta}{\approx} |\xi\rangle, \tag{6.33a}$$

$$KS_3|\varphi\rangle_{\mathcal{AB}} \overset{6\sqrt{2}\eta}{\approx} \sigma_{\mathrm{z}}^{\mathcal{B}''}|\xi\rangle. \tag{6.33b}$$

where the state $|\xi\rangle \in \mathcal{A}\otimes\mathcal{A}''\otimes\mathcal{B}\otimes\mathcal{B}''$ *has the form*

$$|\xi\rangle = |0\rangle_{\mathcal{A}''}|0\rangle_{\mathcal{B}''}\otimes|\xi_0\rangle_{\mathcal{AB}} + |1\rangle_{\mathcal{A}''}|1\rangle_{\mathcal{B}''}\otimes|\xi_1\rangle_{\mathcal{AB}}, \tag{6.34}$$

and the subnormalized $|\xi_0\rangle_{\mathcal{AB}}$ *and* $|\xi_1\rangle_{\mathcal{AB}}$ *are given by*

$$|\xi_0\rangle_{\mathcal{AB}} = \frac{I+T_3}{2}|\varphi\rangle_{\mathcal{AB}}, \tag{6.35a}$$

$$|\xi_1\rangle_{\mathcal{AB}} = \frac{I-T_3}{2}|\varphi\rangle_{\mathcal{AB}}. \tag{6.35b}$$

Proof. See Appendix E for the ideal case. Robustness is discussed in Appendix F. □

The operators $X_{\mathcal{A}}$, $-Y_{\mathcal{A}}$, and $Z_{\mathcal{A}}$ for Alice, and $\hat{X}_{\mathcal{B}}$, $\hat{Y}_{\mathcal{B}}$, and $\hat{Z}_{\mathcal{B}}$ for Bob satisfy the conditions of Proposition 6.7. This can be seen from the SOS decomposition (see Section 2.6) of the triple CHSH operator of Eq. (6.23)

$$\begin{aligned} 6\sqrt{2} - C = {} & \frac{1}{\sqrt{2}}\left(A_3 - \frac{D_{\mathrm{z,x}}+E_{\mathrm{z,x}}}{\sqrt{2}}\right)^2 + \frac{1}{\sqrt{2}}\left(A_1 - \frac{D_{\mathrm{z,x}}-E_{\mathrm{z,x}}}{\sqrt{2}}\right)^2 \\ & + \frac{1}{\sqrt{2}}\left(A_3 - \frac{D_{\mathrm{z,y}}+E_{\mathrm{z,y}}}{\sqrt{2}}\right)^2 + \frac{1}{\sqrt{2}}\left(A_2 - \frac{D_{\mathrm{z,y}}-E_{\mathrm{z,y}}}{\sqrt{2}}\right)^2 \\ & + \frac{1}{\sqrt{2}}\left(A_1 - \frac{D_{\mathrm{x,y}}+E_{\mathrm{x,y}}}{\sqrt{2}}\right)^2 + \frac{1}{\sqrt{2}}\left(A_2 - \frac{D_{\mathrm{x,y}}-E_{\mathrm{x,y}}}{\sqrt{2}}\right)^2. \end{aligned} \tag{6.36}$$

Considering the ideal case for simplicity, a maximal violation $\langle\psi|\, C\,|\psi\rangle = 6\sqrt{2}$ then implies that

$$A_1|\psi\rangle = \frac{D_{\mathrm{x,y}}+E_{\mathrm{x,y}}}{\sqrt{2}}|\psi\rangle = \frac{D_{\mathrm{z,x}}-E_{\mathrm{z,x}}}{\sqrt{2}}|\psi\rangle, \tag{6.37a}$$

$$A_2|\psi\rangle = \frac{D_{\mathrm{x,y}}-E_{\mathrm{x,y}}}{\sqrt{2}}|\psi\rangle = \frac{D_{\mathrm{z,y}}-E_{\mathrm{z,y}}}{\sqrt{2}}|\psi\rangle, \tag{6.37b}$$

$$A_3|\psi\rangle = \frac{D_{\mathrm{z,x}}+E_{\mathrm{z,x}}}{\sqrt{2}}|\psi\rangle = \frac{D_{\mathrm{z,y}}+E_{\mathrm{z,y}}}{\sqrt{2}}|\psi\rangle. \tag{6.37c}$$

Since operators $D+E$ and $D-E$ anticommute for any ±1-outcome observables D and E, the state-dependent anticommutation relations for Alice's observables $X_{\mathcal{A}}$,

$-Y_{\mathcal{A}}$, and $Z_{\mathcal{A}}$ are satisfied. Similarly, since Alice's operators commute with Bob's observables, state-dependent anticommutation relations for $X_{\mathcal{B}}$, $Y_{\mathcal{B}}$, and $Z_{\mathcal{B}}$ are also satisfied. Applying Lemma 2.9 shows the required state-dependent anticommutation relations for $\hat{X}_{\mathcal{B}}$, $\hat{Y}_{\mathcal{B}}$, and $\hat{Z}_{\mathcal{B}}$ (which are also unitary as required by Proposition 6.7). Similar arguments apply in the robust case, resulting in the following counterpart to Theorem 6.6, which has possible complex conjugation appearing in the certification of σ_{z} rather than σ_{y}.

Corollary 6.8. *Suppose the state $|\psi\rangle \in \mathcal{A} \otimes \mathcal{B}$ and the observables $A_j \in \mathcal{L}(\mathcal{A})$ and $D_{j,k}, E_{j,k} \in \mathcal{L}(\mathcal{B})$ satisfy*

$$\langle\psi| C |\psi\rangle = 6\sqrt{2} - \varepsilon. \tag{6.38}$$

Then there exist linear isometries $V_{\mathcal{A}} : \mathcal{A} \to \mathcal{A} \otimes \mathcal{A}' \otimes \mathcal{A}''$ and $V_{\mathcal{B}} : \mathcal{B} \to \mathcal{B} \otimes \mathcal{B}' \otimes \mathcal{B}''$ defining the local isometry $V = V_{\mathcal{A}} \otimes V_{\mathcal{B}}$ such that

$$V|\psi\rangle \overset{c\sqrt{\varepsilon}}{\approx} |\Phi^+\rangle_{\mathcal{A}'\mathcal{B}'} \otimes |\xi\rangle, \tag{6.39a}$$

$$VA_1|\psi\rangle \overset{c\sqrt{\varepsilon}}{\approx} \sigma_{\mathrm{x}}^{\mathcal{A}'} |\Phi^+\rangle_{\mathcal{A}'\mathcal{B}'} \otimes |\xi\rangle, \tag{6.39b}$$

$$VA_2|\psi\rangle \overset{c\sqrt{\varepsilon}}{\approx} -\sigma_{\mathrm{y}}^{\mathcal{A}'} |\Phi^+\rangle_{\mathcal{A}'\mathcal{B}'} \otimes |\xi\rangle, \tag{6.39c}$$

$$VA_3|\psi\rangle \overset{c\sqrt{\varepsilon}}{\approx} \sigma_{\mathrm{z}}^{\mathcal{A}'} |\Phi^+\rangle_{\mathcal{A}'\mathcal{B}'} \otimes \sigma_{\mathrm{z}}^{\mathcal{A}''} |\xi\rangle, \tag{6.39d}$$

where c is a nonnegative constant and the state $|\xi\rangle \in \mathcal{A} \otimes \mathcal{A}'' \otimes \mathcal{B} \otimes \mathcal{B}''$ has the form

$$|\xi\rangle = |00\rangle_{\mathcal{A}''\mathcal{B}''} \otimes |\xi_0\rangle_{\mathcal{A}\mathcal{B}} + |11\rangle_{\mathcal{A}''\mathcal{B}''} \otimes |\xi_1\rangle_{\mathcal{A}\mathcal{B}} \tag{6.40}$$

for some subnormalized $|\xi_0\rangle_{\mathcal{A}\mathcal{B}}$ and $|\xi_1\rangle_{\mathcal{A}\mathcal{B}}$ satisfying $\langle\xi_0|\xi_0\rangle_{\mathcal{A}\mathcal{B}} + \langle\xi_1|\xi_1\rangle_{\mathcal{A}\mathcal{B}} = 1$.

6.4 A parallel self-testing isometry (including complex measurements)

We will state in Section 6.5 a measurement scenario and Bell observations for which any valid measurement strategy results in the existence of observables which satisfy certain natural state-dependent relations, as though they are Pauli operators acting on Bell states. Typically, one can use such relations to construct a self-testing isometry. For example, as is often done in the case of real Pauli measurements [27, 70, 101, 102, 115, 136]. We require such a result which can, in the complex sense of Definition 2.7, certify Bell states and all (possibly complex) Pauli operators from similar

relations. Such a construction was also discussed in [116]. In Fig. 6.3, we exhibit a robust isometry of this form, which also captures the effect of complex conjugation in σ_z measurements (as desired for VBQC), instead of in σ_y as is standard.

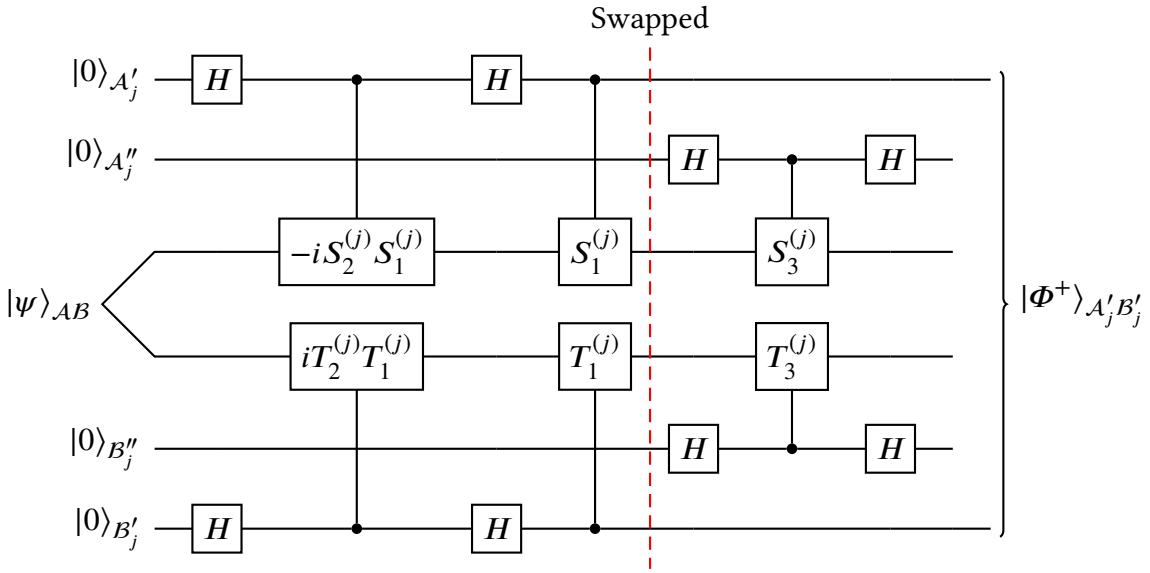


Figure 6.3: The circuit describing the action of the local isometry $V^{(j)} = K^{(j)}W^{(j)}$ on the state $|\psi\rangle_{\mathcal{AB}}$. In the first "swap" stage (preceding the dotted line), denoted by $W^{(j)} = W_{\mathcal{A}}^{(j)} \otimes W_{\mathcal{B}}^{(j)}$, a maximally entangled state is extracted. In the second "phase kickback" stage (succeeding the dotted line), denoted by $K^{(j)} = K_{\mathcal{A}}^{(j)} \otimes K_{\mathcal{A}}^{(j)}$, possible complex conjugation in the presence of a Pauli σ_z operator is accounted for. The full isometry $V = V^{(n)} \dots V^{(1)}$ is a parallel version of this circuit. It is defined by applying the circuit for each j successively, appending ancillae states in $\mathcal{A}'_j$ and $\mathcal{B}'_j$ for each swap stage, and $\mathcal{A}''_j$ and $\mathcal{B}''_j$ for each phase kickback stage. Each isometry $V^{(k)}$ is defined to act trivially on all ancilla spaces with $j < k$.

The following result shows (by application of the isometry defined in Fig. 6.3) the existence of a local isometry with self-testing properties, given natural relations that we will find for our protocol in Section 6.6.

Theorem 6.9. *There exists a function $\delta : \mathbb{R}_{\geq 0} \times \mathbb{N}^* \to \mathbb{R}_{\geq 0}$ satisfying $\delta(0, n) = 0$ for all n such that the following holds. Let $n \in \mathbb{N}^*$ and let $|\psi\rangle_{\mathcal{AB}}$ be a state. Suppose for each $q \in \{1, 2, 3\}$ and $j \in \{1, \dots, n\}$ that there exist ± 1-outcome observables $S_q^{(j)}$ on $\mathcal{A}$ and $T_q^{(j)}$ on $\mathcal{B}$ satisfying (for some $\eta \geq 0$) the following relations:*

1. $\left(S_q^{(j)} - T_q^{(j)}\right)|\psi\rangle_{\mathcal{AB}} \overset{\eta}{\approx} 0$ *for all q and j.*
2. $\left\{S_q^{(j)}, S_r^{(j)}\right\}|\psi\rangle_{\mathcal{AB}} \overset{\eta}{\approx} 0$ *and* $\left\{T_q^{(j)}, T_r^{(j)}\right\}|\psi\rangle_{\mathcal{AB}} \overset{\eta}{\approx} 0$ *for all q, r and j such that $q \neq r$.*

3. $\left[S_q^{(j)}, S_r^{(k)}\right] |\psi\rangle_{\mathcal{AB}} \overset{\eta}{\approx} 0$ *and* $\left[T_q^{(j)}, T_r^{(k)}\right] |\psi\rangle_{\mathcal{AB}} \overset{\eta}{\approx} 0$ *for all* q, r *and* j, k *such that* $j \neq k$.

4. $\left(I + S_1^{(j)} S_1^{(j+1)} S_2^{(j)} S_2^{(j+1)} S_3^{(j)} S_3^{(j+1)}\right) |\psi\rangle_{\mathcal{AB}} \overset{\eta}{\approx} 0$ *for all* $j < n$.

Then there exist subnormalized $|\xi_0\rangle_{\mathcal{AB}}$ *and* $|\xi_1\rangle_{\mathcal{AB}}$ *satisfying* $\langle\xi_0|\xi_0\rangle_{\mathcal{AB}} + \langle\xi_1|\xi_1\rangle_{\mathcal{AB}} = 1$ *that do not depend on any of the* $S_q^{(j)}$*, an isometry* $V_{\mathcal{A}} : \mathcal{A} \to \mathcal{A} \otimes \mathcal{A}' \otimes \mathcal{A}''$*, and an isometry* $V_{\mathcal{B}} : \mathcal{B} \to \mathcal{B} \otimes \mathcal{B}' \otimes \mathcal{B}''$ *that does not depend on any of the* $S_q^{(j)}$ *such that for all* $q \in \{1, 2, 3\}$ *and* $k \in \{1, \ldots, n\}$ *we have*

$$V|\psi\rangle_{\mathcal{AB}} \overset{\delta(\eta,n)}{\approx} \bigotimes_{j=1}^{n} |\Phi^+\rangle_{\mathcal{A}'_j\mathcal{B}'_j} \otimes |\xi\rangle, \tag{6.41a}$$

$$V S_q^{(k)} |\psi\rangle_{\mathcal{AB}} \overset{\delta(\eta,n)}{\approx} \sigma_q^{\mathcal{B}'_k} \bigotimes_{j=1}^{n} |\Phi^+\rangle_{\mathcal{A}'_j\mathcal{B}'_j} \otimes \sigma_{3[q=3]}^{\mathcal{B}''} |\xi\rangle, \tag{6.41b}$$

where $V = V_{\mathcal{A}} \otimes V_{\mathcal{B}}$ *and the junk state* $|\xi\rangle \in \mathcal{A} \otimes \mathcal{A}'' \otimes \mathcal{B} \otimes \mathcal{B}''$ *is defined as*

$$|\xi\rangle = |0\rangle_{\mathcal{A}''}|0\rangle_{\mathcal{B}''} \otimes |\xi_0\rangle_{\mathcal{AB}} + |1\rangle_{\mathcal{A}''}|1\rangle_{\mathcal{B}''} \otimes |\xi_1\rangle_{\mathcal{AB}}. \tag{6.42}$$

Remark. In the statement, the untrusted observables are treated so that the $T_2^{(j)}$ represent Pauli σ_{y} operators acting on Bob's side, while the $S_2^{(j)}$ represent $-\sigma_{\mathrm{y}}$ operators acting on Alice's side.

That $V_{\mathcal{B}}$, $|\xi_0\rangle$, and $|\xi_1\rangle$ do not depend on $S_q^{(j)}$ means that if we replaced this observable with some $\tilde{S}_q^{(j)}$ such that all assumptions were still satisfied, then the same $V_{\mathcal{B}}$, $|\xi_0\rangle$, and $|\xi_1\rangle$ would still be sufficient to meet the conditions of the result.

We will prove that the robustness $\delta(\eta, n)$ satisfies $\delta(0, n) = 0$ for all n, which is the ideal, noiseless case. For the case where $\eta > 0$, we expect that standard existing techniques [27, 70, 102, 115, 116] can be applied to achieve polynomial robustness bounds in the sense $\delta(\eta, n) = O(\eta n^2)$ as $\eta \to 0$ or $n \to \infty$.

Proof sketch. See Appendix G for full details. As noted, here we consider only the ideal case with $\eta = 0$. We show that a sufficient local isometry is $V = V^{(n)} \ldots V^{(1)}$, where each $V^{(j)} = K^{(j)} W^{(j)}$, and $K^{(j)} = K_{\mathcal{A}}^{(j)} \otimes K_{\mathcal{B}}^{(j)}$ and $W^{(j)} = W_{\mathcal{A}}^{(j)} \otimes W_{\mathcal{B}}^{(j)}$ are as defined in Fig. 6.3. We could also have considered the isometry constructed by first applying all swap isometries, followed by applying all phase kickback isometries. However, applying $K^{(j)}$ immediately after the corresponding $W^{(j)}$ reduces the number of terms that must be manipulated at a time. This, along with the usage of Relation 4 (via Lemma G.1) at each step, allows us to keep the number of terms constant after the application of each $V^{(j)}$.

The isometry $V_{\mathcal{B}} = V_{\mathcal{B}}^{(n)} \dots V_{\mathcal{B}}^{(1)}$, where each $V_{\mathcal{B}}^{(j)} = K_{\mathcal{B}}^{(j)} W_{\mathcal{B}}^{(j)}$, is immediately seen from the construction given in Fig. 6.3 not to depend on any of the observables $S_q^{(j)}$. Let us define, for all $1 \leq k \leq n$, the vectors

$$\left|\xi_{\pm}^{k}\right\rangle = \frac{1}{\left(2\sqrt{2}\right)^{k}} \prod_{j=1}^{k} \left(I \pm T_3^{(j)}\right)\left(I + iT_2^{(j)}T_1^{(j)}\right)|\psi\rangle. \tag{6.43}$$

With this notation, Proposition 6.7 gives that

$$V^{(1)}|\psi\rangle = |\Phi^+\rangle_{\mathcal{A}_1'\mathcal{B}_1'} \otimes \left(|0\rangle_{\mathcal{A}_1''}|0\rangle_{\mathcal{B}_1''} \otimes \left|\xi_+^1\right\rangle + |1\rangle_{\mathcal{A}_1''}|1\rangle_{\mathcal{B}_1''} \otimes \left|\xi_-^1\right\rangle\right), \tag{6.44a}$$

$$V^{(1)}S_q^{(1)}|\psi\rangle = \sigma_q^{\mathcal{B}_1'}|\Phi^+\rangle_{\mathcal{A}_1'\mathcal{B}_1'} \otimes \left(|0\rangle_{\mathcal{A}_1''}|0\rangle_{\mathcal{B}_1''} \otimes \left|\xi_+^1\right\rangle + (-1)^{[q=3]}|1\rangle_{\mathcal{A}_1''}|1\rangle_{\mathcal{B}_1''} \otimes \left|\xi_-^1\right\rangle\right). \tag{6.44b}$$

For all $1 < k \leq n$, we have the following properties. Firstly,

$$V^{(k)}\left|\xi_+^{k-1}\right\rangle = |\Phi^+\rangle_{\mathcal{A}_k'\mathcal{B}_k'} \otimes |0\rangle_{\mathcal{A}_k''}|0\rangle_{\mathcal{B}_k''} \otimes \left|\xi_+^k\right\rangle, \tag{6.45a}$$

$$V^{(k)}\left|\xi_-^{k-1}\right\rangle = |\Phi^+\rangle_{\mathcal{A}_k'\mathcal{B}_k'} \otimes |1\rangle_{\mathcal{A}_k''}|1\rangle_{\mathcal{B}_k''} \otimes \left|\xi_-^k\right\rangle. \tag{6.45b}$$

That is, $V^{(k)}$ extracts a Bell state from $\left|\xi_{\pm}^{k-1}\right\rangle$, raises its superscript index from $k-1$ to k, and appends the appropriate ancilla states depending on the sign in subscript. Secondly,

$$V^{(1)}S_q^{(k)}|\psi\rangle = S_q^{(k)}V^{(1)}|\psi\rangle. \tag{6.46}$$

Thirdly, whenever $j \neq k$,

$$V^{(k)}S_q^{(j)}\left|\xi_{\pm}^{k-1}\right\rangle = S_q^{(j)}V^{(k)}\left|\xi_{\pm}^{k-1}\right\rangle. \tag{6.47}$$

Finally,

$$V^{(k)}S_q^{(k)}\left|\xi_+^{k-1}\right\rangle = \sigma_q^{\mathcal{B}_k'}|\Phi^+\rangle_{\mathcal{A}_k'\mathcal{B}_k'} \otimes |0\rangle_{\mathcal{A}_k''}|0\rangle_{\mathcal{B}_k''} \otimes \left|\xi_+^k\right\rangle, \tag{6.48a}$$

$$V^{(k)}S_q^{(k)}\left|\xi_-^{k-1}\right\rangle = (-1)^{[q=3]}\sigma_q^{\mathcal{B}_k'}|\Phi^+\rangle_{\mathcal{A}_k'\mathcal{B}_k'} \otimes |1\rangle_{\mathcal{A}_k''}|1\rangle_{\mathcal{B}_k''} \otimes \left|\xi_-^k\right\rangle. \tag{6.48b}$$

After the full application of the isometry $V = V^{(n)} \dots V^{(1)}$, and defining

$$|0\rangle_{\mathcal{A}''} = |0 \dots 0\rangle_{\mathcal{A}''}, \tag{6.49a}$$

$$|1\rangle_{\mathcal{A}''} = |1 \dots 1\rangle_{\mathcal{A}''}, \tag{6.49b}$$

$$|0\rangle_{\mathcal{B}''} = |0 \dots 0\rangle_{\mathcal{B}''}, \tag{6.49c}$$

$$|1\rangle_{\mathcal{B}''} = |1 \dots 1\rangle_{\mathcal{B}''}, \tag{6.49d}$$

Eqs. (6.44a) and (6.45) give

$$V|\psi\rangle = \bigotimes_{j=1}^{n} |\Phi^+\rangle_{\mathcal{A}'_j\mathcal{B}'_j} \otimes \big(|0\rangle_{\mathcal{A}''}|0\rangle_{\mathcal{B}''} \otimes |\xi^n_+\rangle + |1\rangle_{\mathcal{A}''}|1\rangle_{\mathcal{B}''} \otimes |\xi^n_-\rangle\big). \tag{6.50}$$

Similarly, using Eqs. (6.44b) and (6.45), we have

$$\begin{aligned} VS_q^{(1)}|\psi\rangle &= \sigma_q^{\mathcal{B}'_1} |\Phi^+\rangle_{\mathcal{A}'_1\mathcal{B}'_1} \otimes V^{(n)} \dots V^{(2)} \Big(|0\rangle_{\mathcal{A}''_1}|0\rangle_{\mathcal{B}''_1} \otimes \left|\xi^1_+\right\rangle \\ &\qquad + (-1)^{[q=3]} |1\rangle_{\mathcal{A}''_1}|1\rangle_{\mathcal{B}''_1} \otimes \left|\xi^1_-\right\rangle \Big) \\ &= \sigma_q^{\mathcal{B}'_1} \bigotimes_{j=1}^{n} |\Phi^+\rangle_{\mathcal{A}'_j\mathcal{B}'_j} \otimes \big(|0\rangle_{\mathcal{A}''}|0\rangle_{\mathcal{B}''} \otimes |\xi^n_+\rangle \\ &\qquad + (-1)^{[q=3]} |1\rangle_{\mathcal{A}''}|1\rangle_{\mathcal{B}''} \otimes |\xi^n_-\rangle \big) \\ &= \sigma_q^{\mathcal{B}'_1} \bigotimes_{j=1}^{n} |\Phi^+\rangle_{\mathcal{A}'_j\mathcal{B}'_j} \otimes \sigma^{\mathcal{B}''}_{3[q=3]} \big(|0\rangle_{\mathcal{A}''}|0\rangle_{\mathcal{B}''} \otimes |\xi^n_+\rangle + |1\rangle_{\mathcal{A}''}|1\rangle_{\mathcal{B}''} \otimes |\xi^n_-\rangle \big). \end{aligned} \tag{6.51}$$

Furthermore, for $1 < k \leq n$, we can use Eqs. (6.44a) and (6.45) to (6.48) to write

$$\begin{aligned} VS_q^{(k)}|\psi\rangle &= |\Phi^+\rangle_{\mathcal{A}'_1\mathcal{B}'_1} \otimes V^{(n)} \dots V^{(2)} S_q^{(k)} \Big(|0\rangle_{\mathcal{A}''_1}|0\rangle_{\mathcal{B}''_1} \otimes \left|\xi^1_+\right\rangle \\ &\qquad + |1\rangle_{\mathcal{A}''_1}|1\rangle_{\mathcal{B}''_1} \otimes \left|\xi^1_-\right\rangle \Big) \\ &= \bigotimes_{j=1}^{k-1} |\Phi^+\rangle_{\mathcal{A}'_j\mathcal{B}'_j} \otimes V^{(n)} \dots V^{(k)} S_q^{(k)} \big(|0 \dots 0\rangle \otimes \left|\xi^{k-1}_+\right\rangle \\ &\qquad + |1 \dots 1\rangle \otimes \left|\xi^{k-1}_-\right\rangle \big) \\ &= \sigma_q^{\mathcal{B}'_k} \bigotimes_{j=1}^{n} |\Phi^+\rangle_{\mathcal{A}'_j\mathcal{B}'_j} \otimes \big(|0\rangle_{\mathcal{A}''}|0\rangle_{\mathcal{B}''} \otimes |\xi^n_+\rangle \\ &\qquad + (-1)^{[q=3]} |1\rangle_{\mathcal{A}''}|1\rangle_{\mathcal{B}''} \otimes |\xi^n_-\rangle \big) \\ &= \sigma_q^{\mathcal{B}'_k} \bigotimes_{j=1}^{n} |\Phi^+\rangle_{\mathcal{A}'_j\mathcal{B}'_j} \otimes \sigma^{\mathcal{B}''}_{3[q=3]} \big(|0\rangle_{\mathcal{A}''}|0\rangle_{\mathcal{B}''} \otimes |\xi^n_+\rangle + |1\rangle_{\mathcal{A}''}|1\rangle_{\mathcal{B}''} \otimes |\xi^n_-\rangle \big). \end{aligned} \tag{6.52}$$

Together, Eqs. (6.50) to (6.52) have the desired form by taking $|\xi_0\rangle = |\xi^n_+\rangle$ and $|\xi_1\rangle = |\xi^n_-\rangle$. These $|\xi_0\rangle$ and $|\xi_1\rangle$ have the desired properties: the observables $S_q^{(j)}$ are not present in their definition given in Eq. (6.43), and they satisfy $\langle\xi_+|\xi_+\rangle + \langle\xi_-|\xi_-\rangle = 1$ due to Eq. (6.50) together with the fact that the isometry V preserves inner products. □

Theorem 6.9 allows us to certify the action of one Pauli operator at a time. In order to prepare all of Bob's qubits, however, we require that Pauli measurements of all n of Alice's qubits be certified simultaneously. This is not immediate from Theorem 6.9 since, after applying one of the physical operators to $|\psi\rangle$, its conclusion says

nothing about the action of a second physical operator on the new state, even if the two operators commute. Using the symmetry properties of pairs of Pauli operators with respect to $|\Phi^+\rangle$, this limitation can be overcome.

Lemma 6.10. *Let $|\psi\rangle \in \mathcal{A} \otimes \mathcal{B}$ and $|\phi\rangle \in \tilde{\mathcal{A}} \otimes \tilde{\mathcal{B}}$. For some $m > 1$, let $A_j : \mathcal{A} \to \mathcal{A}$ satisfy $\|A_j\| \leq 1$ and $\tilde{A}_j : \tilde{\mathcal{A}} \to \tilde{\mathcal{A}}$ for all $j \in \{1, \dots, m\}$. Let linear isometries $V_{\mathcal{A}} : \mathcal{A} \to \tilde{\mathcal{A}}$ and $V_{\mathcal{B}} : \mathcal{B} \to \tilde{\mathcal{B}}$ defining the local isometry $V : \mathcal{A} \otimes \mathcal{B} \to \tilde{\mathcal{A}} \otimes \tilde{\mathcal{B}}$ by $V = V_{\mathcal{A}} \otimes V_{\mathcal{B}}$ be such that, for all j,*

$$V|\psi\rangle \overset{\delta}{\approx} |\phi\rangle, \tag{6.53a}$$

$$VA_j|\psi\rangle \overset{\delta}{\approx} \tilde{A}_j|\phi\rangle. \tag{6.53b}$$

Suppose that, for all j, there exist $\tilde{B}_j : \tilde{\mathcal{B}} \to \tilde{\mathcal{B}}$ satisfying $\|\tilde{B}_j\| \leq 1$ such that

$$\tilde{A}_j|\phi\rangle = \tilde{B}_j|\phi\rangle. \tag{6.54}$$

Then, the combined action of all operators satisfies

$$V(A_1 \dots A_m)|\psi\rangle \overset{(2m+1)\delta}{\approx} \tilde{A}_1 \dots \tilde{A}_m|\phi\rangle. \tag{6.55}$$

Proof. See Appendix H. □

Remark. In practice, the A_j may represent some physical ± 1-outcome observables or orthogonal projections acting on a physical state $|\psi\rangle$. In both cases, $\|A_j\| \leq 1$ is automatically satisfied. Similarly, the $\tilde{A}_j$ are understood to represent reference measurements, and we may take the reference state $|\phi\rangle = |\Phi^+\rangle^{\otimes n} \otimes |\xi\rangle$.

6.5 The protocol

We consider a scenario in which Alice is provided with one of m^n questions $\boldsymbol{x} \in \mathcal{X} \subset \{1, \dots, m\}^n$ and answers with $\boldsymbol{a} \in \{+1, -1\}^n$. Bob, on the other hand, is provided with a question y and answers with $\boldsymbol{b}$, whose form depends on the input y. Protocol 6.1 exhibits our process for the preparation of n qubits on Bob's side, which together are to act as the initial state in a VBQC protocol. We will soon make all definitions required for this, but first let us introduce some intuition.

The idea is that Alice and Bob should play n triple CHSH games in order achieve n corresponding maximal Bell violations. For the jth game, Alice receives an input basis $x_j \in \{\mathrm{x}, \mathrm{y}, \mathrm{z}\}$ and outputs $a_j \in \{+, -\}$. Bob receives the same input $y \in \{1, \dots, 6\}$

Protocol 6.1: A protocol that performs the blind preparation of n qubits in appropriate bases on the server-side subsystem, followed by VBQC.

The number of qubits to be prepared is $n \in \mathbb{N}^*$. A verifier first performs the initial setup of the protocol as follows:

1. The verifier chooses a random set of "special" questions $\mathcal{S} \subset \{1, \dots, 5\}^n$ with polynomial cardinality $|\mathcal{S}| = \text{poly}(n)$, each element of which represents an n-tuple of bases in which n qubits may be prepared.

2. The verifier expands $\mathcal{S}$ to the full set of input questions for Alice $\mathcal{X} \subset \{1, \dots 5\}^n$ (which has cardinality $|\mathcal{X}| = \text{poly}(n)$ by construction) as in Eq. (6.62).

The verifier then performs the following subprotocols:

1. *Self-test*: In each self-testing round, the verifier chooses questions $\boldsymbol{x} \in \mathcal{X}$ and $y \in \mathcal{Y} = \{1, \dots, 6\} \cup \{\diamondsuit, \blacklozenge\}$. The verifier sends $\boldsymbol{x}$ to Alice and y to Bob, and receives an answer $\boldsymbol{a} \in \{+, -\}^n$ from Alice.

   (a) If $y \in \{1, \dots, 6\}$, Bob answers with $\boldsymbol{b} \in \{+, -\}^n$. For all $j \in \{1, \dots n\}$, this contributes to the correlations

   $$\left\langle A_{\boldsymbol{x}}^{(j)} B_y^{(j)} \right\rangle.$$

   (b) *Conjugation*: The question sent to Bob was $y \in \{\diamondsuit, \blacklozenge\}$.

      i. If $y = \diamondsuit$, Bob answers with $\boldsymbol{b} \in \{1, 2, 3, 4\}^{\left\lfloor \frac{n}{2} \right\rfloor}$.

      ii. If $y = \blacklozenge$, Bob answers with $\boldsymbol{b} \in \{1, 2, 3, 4\}^{\left\lceil \frac{n}{2} \right\rceil - 1}$.

   For all $1 \leq j < n$, letting $k = \left\lceil \frac{j}{2} \right\rceil$, these contribute to the correlations

   $$\left\langle A_{\boldsymbol{x}}^{(j)} A_{\boldsymbol{x}}^{(j+1)} \Gamma_{b_k}^{(j)} \right\rangle. \tag{6.56}$$

   By combining the correlations appropriately, the verifier can estimate all Bell expressions of Eqs. (6.79), (6.81) and (6.82) and check that the experiment satisfies the assumptions of the self-testing statement.

2. *VBQC*: On some round after the desired confidence threshold has been reached, the verifier asks Alice a special question $\chi \in \mathcal{S}$ and then performs an interactive FK-type protocol with the server.

---

for all n games, and outputs $b_j \in \{+,-\}$ for the jth game. To ensure that the players cannot cheat by sharing fewer than n Bell states, we must examine the experimental outcomes in such a way that we can detect that they originated from n independent games. Intuitively this is possible since (round and communication complexities aside) the overall scenario is identical with one in which, instead of reporting the outcomes for all n games simultaneously, Bob's input also contains a specified index of a single one of the games to play and in each round he reports only a single-bit outcome for this game. Alice is unable to be sure which of the n games Bob is instructed to play, while Alice is not necessarily instructed to measure in the same basis in all n games, and so it is possible to check independence between all games.

It will be necessary in order to perform VBQC that the verifier can also choose to prepare qubits in the eigenbases corresponding to observables $\sigma_{\mathrm{x+y}}$ and $\sigma_{\mathrm{x-y}}$. For this purpose, Alice should accept input questions $x_j \in \{\mathrm{x}+\mathrm{y}, \mathrm{x}-\mathrm{y}\}$ to each game, in addition to those already stated. That is, we will take $m = 5$ in our protocol, with the five values $1, \ldots, 5$ forming Alice's inputs used interchangeably to denote input bases x, y, z, $\mathrm{x}+\mathrm{y}$, and $\mathrm{x}-\mathrm{y}$. At positions where $\mathrm{x}+\mathrm{y}$ or $\mathrm{x}-\mathrm{y}$ are chosen in Alice's input, we enforce that relevant perfect correlations between Alice and Bob are observed. This forces the untrusted operations for both inputs $\mathrm{x} \pm \mathrm{y}$ to act consistently with the correct combination of untrusted operations for inputs x and y.

We would like to restrict the possible questions for Alice to a subset $\mathcal{X} \subset \{1, \ldots, m\}^n$ whose cardinality in the worst case scales polynomially in n, which is required in order to satisfy Property 3 discussed in Section 6.2. This must be done in such a way that the possibility of cheating does not arise from possible correlations between different positions of Alice's inputs. It turns out that it is sufficient to keep only inputs with the following two constraints in mind:

1. Given any pair of positions, there are inputs with all pairs of values at those positions.

2. At any given position, there are inputs taking all possible values.

The precise formulation of Alice's question set $\mathcal{X}$ is the subject of Section 6.5.1.

While we attempt to ensure the independence of the outcomes of n triple CHSH games, a certain dependence between the measurements used in the different games is desirable. Namely, in order to satisfy Definition 2.7 of self-testing with complex measurements, it is required that any possible complex conjugation of measurement operators only ever applies simultaneously to measurements at every position. This

global complex conjugation has been achieved previously [53, 116] (and as we do also) by allowing Bob to accept an additional two inputs $y \in \{\diamondsuit, \blacklozenge\}$, each representing Bell measurements being performed on many pairs of qubits.

Relations that we will derive between untrusted observables from the observation of requested Bell values and correlations allow us to make our desired self-testing-based statement for remote state preparation. After exhibiting it here, we will proceed to expand on the details of our discussion thus far.

Theorem 6.11. *There exists a function $\tau : \mathbb{R}_{\geq 0} \times \mathbb{N}^* \to \mathbb{R}_{\geq 0}$ satisfying $\tau(0, n) = 0$ for all n such that the following holds. Let $n \in \mathbb{N}^*$ be the number of qubits to prepare, let $|\psi\rangle$ be a state in $\mathcal{A} \otimes \mathcal{B}$. Choose a set of special questions $\mathcal{S} \subset \{\mathrm{x}, \mathrm{y}, \mathrm{z}, \mathrm{x}+\mathrm{y}, \mathrm{x}-\mathrm{y}\}^n$ and let $\Pi^{\mathcal{A}}_{\boldsymbol{a}|\chi}$ denote the physical projectors on $\mathcal{A}$ corresponding to Alice answering with $\boldsymbol{a} \in \{+,-\}^n$ upon being asked $\chi \in \mathcal{S}$. Define the tensor products of qubits*

$$\left|e_{\boldsymbol{a}|\chi}\right\rangle = \bigotimes_{j=1}^{n} \left|\sigma^{a_j}_{\chi_j}\right\rangle, \tag{6.57a}$$

$$\left|e^*_{\boldsymbol{a}|\chi}\right\rangle = \bigotimes_{j=1}^{n} \left|\sigma^{a_j(-1)^{[\chi_j=\mathrm{z}]}}_{\chi_j}\right\rangle, \tag{6.57b}$$

and denote the reduced physical states on Bob's subsystem after Alice's possible measurements by

$$\rho^{\boldsymbol{a}|\chi}_{\mathcal{B}} = \mathrm{tr}_{\mathcal{A}}\left(\frac{\Pi^{\mathcal{A}}_{\boldsymbol{a}|\chi}|\psi\rangle\langle\psi|\Pi^{\mathcal{A}}_{\boldsymbol{a}|\chi}}{\langle\psi|\,\Pi^{\mathcal{A}}_{\boldsymbol{a}|\chi}\,|\psi\rangle}\right). \tag{6.58}$$

Suppose that all requested Bell inequalities and correlations are ε-approximately saturated (for some $\varepsilon \geq 0$) as in Eqs. (6.79), (6.81) *and* (6.82) *of Section 6.5.2 and let $V_{\mathcal{B}} : \mathcal{B} \to \mathcal{B}' \otimes \mathcal{B}'' \otimes \mathcal{B}$ be the isometry thus constructed from Bob's measurement operators as in Theorem 6.16. Then there exist subnormalized density operators β_0 and β_1 on $\mathcal{B}$ satisfying $\mathrm{tr}(\beta_0) + \mathrm{tr}(\beta_1) = 1$ such that, with probability at least $1 - 4\tau(\varepsilon, n)$ over all possible answers $\boldsymbol{a}$ given any special question χ, we have*

$$\begin{aligned}\frac{1}{2}\Big\| V_{\mathcal{B}}\rho^{\boldsymbol{a}|\chi}_{\mathcal{B}}V^{\dagger}_{\mathcal{B}} - \Big(&\left|e_{\boldsymbol{a}|\chi}\right\rangle\!\left\langle e_{\boldsymbol{a}|\chi}\right| \otimes |0\rangle\langle 0| \otimes \beta_0 \\ &+ \left|e^*_{\boldsymbol{a}|\chi}\right\rangle\!\left\langle e^*_{\boldsymbol{a}|\chi}\right| \otimes |1\rangle\langle 1| \otimes \beta_1\Big)\Big\|_1 \leq \tau(\varepsilon, n).\end{aligned} \tag{6.59}$$

Remark. The robustness of Theorem 6.9 expected using the standard techniques mentioned is inherited here to yield $\tau(\varepsilon, n) = O(\varepsilon^{1/3}n^{4/3})$ as $\varepsilon \to 0$ or $n \to \infty$.

Proof. See Appendix I. □

That all the special questions $\mathcal{S}$ correspond to valid input states to the FK protocol is easily achievable, since the only requirement is that enough dummy qubits (those in the σ_z basis) are prepared from which to create enough traps. For example, using the "dotted triple graph" resource state construction [44], the number of additional physical qubits needed to be prepared for verification is linear in the size of the desired computation (the number of qubits needed without any verification). Thus, to achieve a given level of verifiability, one only needs that a constant fraction of the qubits prepared are dummies. This can clearly be achieved by instead preparing a large enough constant multiple of the number of qubits and then discarding some of those that are not prepared as dummies. The probability that a special question still corresponds to too few dummy qubits is exponentially small.

6.5.1 Alice's question set

We construct the specific subset of questions $\mathcal{X}$ based on a set of possible special input questions $\mathcal{S} \subset \{1, \ldots, m\}^n$, each element of which is chosen to correspond to preparation bases desired by the verifier. Throughout, we will take addition of questions to be performed (componentwise for strings) modulo m.

We first define the set

$$\mathcal{D} = \left\{ k\boldsymbol{e}_i^n + l\boldsymbol{e}_j^n \;\middle|\; k, l \in \{0, \ldots, m-1\} \text{ and } 1 \leq i < j \leq n \right\}, \tag{6.60}$$

where $\boldsymbol{e}_i^n = (\delta_{ij})_{j=1}^n$ denotes the ith standard basis vector with n entries. The possible input set $\mathcal{X}$ for Alice is selected by expanding some choice of $\mathcal{S}$. This is performed as follows. For each $\chi \in \mathcal{S}$, we let

$$\mathcal{X}_\chi = \{\chi + \boldsymbol{d} \mid \boldsymbol{d} \in \mathcal{D}\}. \tag{6.61}$$

Then, we combine all such questions to form

$$\mathcal{X} = \bigcup_{\chi \in \mathcal{S}} \mathcal{X}_\chi. \tag{6.62}$$

For example, if $m = 3$, $n = 3$, and $\mathcal{S} = \{\chi\}$, where $\chi = (1, 1, 1)$, then $\mathcal{X}_\chi$ (and $\mathcal{X}$ in

this case) has elements

$$
\begin{array}{llll}
(1,1,1), & & & \\
(2,1,1), & (3,1,1), & & \\
(1,2,1), & (1,3,1), & & \\
(1,1,2), & (1,1,3), & & \\
(2,2,1), & (3,2,1), & (2,3,1), & (3,3,1), \\
(2,1,2), & (3,1,2), & (2,1,3), & (3,1,3), \\
(1,2,2), & (1,3,2), & (1,2,3), & (1,3,3).
\end{array}
$$

Each expanded special set has cardinality $|\mathcal{X}_\chi| = 1 + (m-1)n + \frac{1}{2}(m-1)^2 n(n-1)$, and so the total number of questions for Alice is bounded by

$$|\mathcal{X}| \leq |S| \cdot \left[1 + (m-1)n + \frac{1}{2}(m-1)^2 n(n-1)\right] \tag{6.63}$$

(quadratic in the number of qubits if the number of special questions is taken to be constant). We can thus choose S to be such that $|S| = \text{poly}(n)$, so that indeed $|\mathcal{X}| = \text{poly}(n)$. The sets $\mathcal{X}_\chi$ are constructed such that starting with any particular special question, for any pair of positions, every possible pair of values from $\{1, \ldots, m\}$ appears. Additionally, at any position, every possible value appears. We formalize this here.

Lemma 6.12. *Fix $m \geq 1$ and let $\chi \in S \subset \{1, \ldots, m\}^n$ for some $n \geq 1$. Define $\mathcal{X}_\chi \subset \{1, \ldots, m\}^n$ as in Eq. (6.61) and $\mathcal{X}$ as in Eq. (6.62). The following properties then hold:*

1. *If $n > 1$ then, for any $1 \leq i < j \leq n$ and $q, r \in \{1, \ldots, m\}$, there exists $\boldsymbol{x} \in \mathcal{X}_\chi \subset \mathcal{X}$ such that $x_i = q$, $x_j = r$, and, moreover, $x_k = \chi_k$ for all $k \in \{1, \ldots, n\} \setminus \{i, j\}$.*

2. *For any $1 \leq i \leq n$ and $q \in \{1, \ldots, m\}$, there exists $\boldsymbol{x} \in \mathcal{X}_\chi \subset \mathcal{X}$ such that $x_i = q$ and, moreover, $x_k = \chi_k$ for all $k \neq i$.*

Furthermore, $|\mathcal{X}_\chi| = O(n^2)$.

Proof. For the first property, take $\boldsymbol{x} = \chi + (q - \chi_i)\boldsymbol{e}_i^n + (r - \chi_j)\boldsymbol{e}_j^n$. The second property is implied by the first for $n > 1$ using the choice $v = \chi_j$, and for $n = 1$ we can take $\boldsymbol{x} = \chi + (q - \chi_1)\boldsymbol{e}_1^n$. Let $\mathcal{D}$ be defined as in Eq. (6.60). The cardinality $|\mathcal{X}_\chi| = |\mathcal{D}|$ since each element of $\mathcal{D}$ is simply shifted by addition with the fixed χ to form $\mathcal{X}_\chi$. Finally, $|\mathcal{D}| = 1 + (m-1)n + \frac{1}{2}(m-1)^2 n(n-1)$. □

Remark. It is clear from Eq. (6.62) that $|\mathcal{X}| \leq |\mathcal{S}| \cdot |\mathcal{X}_\chi| = |\mathcal{S}| \cdot |\mathcal{D}|$.

The set $\mathcal{X}$ of Eq. (6.62) is generated from the many questions in $\mathcal{S}$ (rather than just from a single choice of preparation question) so that Alice has a low chance of guessing which χ is used for the computation from her knowledge of the structure of $\mathcal{X}$ (the elements of which she can deduce from the questions asked of her during self-test rounds of Protocol 6.1).

We will now present another construction of the same set $\mathcal{X}$, which will be useful in Section 6.5.2 to define the Bell expressions we must consider. Recall the notation $\boldsymbol{x}_j = (x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_n)$ for a string $\boldsymbol{x} = (x_1, \ldots, x_n)$ excluding the jth position. For each $\chi \in \mathcal{S}$ and $1 \leq j \leq n$, define

$$\mathcal{R}_\chi^{(j)} = \left\{ \chi_j + k\boldsymbol{e}_i^{n-1} \;\middle|\; 0 \leq k \leq m-1 \text{ and } 1 \leq i \leq n-1 \right\} \tag{6.64}$$

and then use this to define

$$\mathcal{R}^{(j)} = \bigcup_{\chi \in \mathcal{S}} \mathcal{R}_\chi^{(j)}. \tag{6.65}$$

These satisfy $\left|\mathcal{R}_\chi^{(j)}\right| = 1 + (m-1)n$ for all $\chi \in \mathcal{S}$ and thus

$$\left|\mathcal{R}^{(j)}\right| \leq |\mathcal{S}| \cdot [1 + (m-1)n]. \tag{6.66}$$

Define further

$$\mathcal{X}^{(j)} = \left\{ (r_1, \ldots, r_{j-1}, q, r_j, \ldots, r_{n-1}) \;\middle|\; 0 \leq q \leq m-1 \text{ and } \boldsymbol{r} \in \mathcal{R}^{(j)} \right\}. \tag{6.67}$$

We now have the notation to reconstruct $\mathcal{X}$ as follows.

Lemma 6.13. *The set $\mathcal{X}$ of Eq.* (6.62) *can alternatively be written as*

$$\mathcal{X} = \bigcup_{j=1}^{n} \mathcal{X}^{(j)}. \tag{6.68}$$

Proof. We first show that $\mathcal{X}^{(j)} \subset \mathcal{X}$ for all $1 \leq j \leq n$. Let $0 \leq q \leq m-1$ and $\boldsymbol{r} \in \mathcal{R}^{(j)}$. Then there exists $\chi \in \mathcal{S}$ such that $\boldsymbol{r} \in \mathcal{R}_\chi^{(j)}$. Thus, there exists $0 \leq k \leq m-1$ and $1 \leq i \leq n$ such that $\boldsymbol{r} = \chi_j + k\boldsymbol{e}_i^{n-1}$. We can therefore write for some $l \neq j$ that

$$(r_1, \ldots, r_{j-1}, q, r_j, \ldots, r_{n-1}) = \chi + (q - \chi_j)\boldsymbol{e}_j^n + k\boldsymbol{e}_l^n \in \mathcal{X}_\chi \subset \mathcal{X}. \tag{6.69}$$

For the reverse inclusion, take any $\boldsymbol{x} \in \mathcal{X}$. Then there exists $\chi \in \mathcal{S}$ such that $\boldsymbol{x} \in \mathcal{X}_\chi$. For some $k, l \in \{0, \ldots, m-1\}$ and $i, j \in \{1, \ldots, n\}$ satisfying $i < j$, we thus have $\boldsymbol{x} = \chi + k\boldsymbol{e}_i^n + l\boldsymbol{e}_j^n$. Choosing $q = \chi_j + l$ and $\boldsymbol{r} = \chi_j + k\boldsymbol{e}_i^{n-1}$ gives $\boldsymbol{x} = (r_1, \ldots, r_{j-1}, q, r_j, \ldots, r_{n-1})$. Finally, since $\boldsymbol{r} \in \mathcal{R}_\chi^{(j)} \subset \mathcal{R}^{(j)}$, we have $\boldsymbol{x} \in \mathcal{X}^{(j)}$. □

A useful property of certain input questions for switching the local subsystem on which pairs of observables act in Section 6.6.1 is given by the following.

Lemma 6.14. *Let $\chi \in \mathcal{S}$, let $1 \leq i < j \leq n$, and let $q, r \in \{1, \dots, m\}$. Suppose that $\boldsymbol{x} \in \{1, \dots, m\}^n$ is defined such that $x_i = q$, $x_j = r$, and $x_k = \chi_k$ for all $k \in \{1, \dots, n\} \setminus \{i, j\}$. Then $\boldsymbol{x}_i \in \mathcal{R}_\chi^{(i)} \subset \mathcal{R}^{(i)}$ and $\boldsymbol{x}_j \in \mathcal{R}_\chi^{(j)} \subset \mathcal{R}^{(j)}$.*

Proof. It is clear that $\boldsymbol{x}_i = \chi_i + (r - \chi_j)\boldsymbol{e}_{j-1}^{n-1}$ and $\boldsymbol{x}_j = \chi_j + (q - \chi_i)\boldsymbol{e}_i^{n-1}$. □

6.5.2 Bell value observations

Let us model Alice's behavior upon the question $\boldsymbol{x} \in \mathcal{X}$ as projective measurements with projection operators $\Pi_{\boldsymbol{a}|\boldsymbol{x}}^{\mathcal{A}}$, where $\boldsymbol{a} \in \{+, -\}^n$. Similarly, let us model Bob's behavior upon the question $y \in \{1, \dots, 6\} \cup \{\diamondsuit, \blacklozenge\}$ using projections $\Pi_{\boldsymbol{b}|y}^{\mathcal{B}}$. For $y \in \{1, \dots, 6\}$ Bob answers with $\boldsymbol{b} \in \{+, -\}^n$, while for $y = \diamondsuit$ he answers with $\boldsymbol{b} \in \{1, 2, 3, 4\}^{\left\lfloor \frac{n}{2} \right\rfloor}$ and for $y = \blacklozenge$ with $\boldsymbol{b} \in \{1, 2, 3, 4\}^{\left\lceil \frac{n}{2} \right\rceil - 1}$.

For all questions $\boldsymbol{x} \in \mathcal{X}$ for Alice and $y \in \{1, \dots, 6\}$ for Bob, we define projections corresponding to Alice observing a and Bob observing b at the jth positions of their respective answers

$$\Pi_{a|\boldsymbol{x}}^{\mathcal{A},j} = \sum_{\boldsymbol{a}|a_j=a} \Pi_{\boldsymbol{a}|\boldsymbol{x}}^{\mathcal{A}}, \tag{6.70a}$$

$$\Pi_{b|y}^{\mathcal{B},j} = \sum_{\boldsymbol{b}|b_j=b} \Pi_{\boldsymbol{b}|y}^{\mathcal{B}}. \tag{6.70b}$$

In the case of $y \in \{\diamondsuit, \blacklozenge\}$, we similarly define projections corresponding to Bob observing $b \in \{1, 2, 3, 4\}$ at the kth position of $\boldsymbol{b}$ as

$$\Gamma_b^{(2k-1)} = \sum_{\boldsymbol{b}|b_k=b} \Pi_{\boldsymbol{b}|\diamondsuit}^{\mathcal{B}}, \tag{6.71a}$$

$$\Gamma_b^{(2k)} = \sum_{\boldsymbol{b}|b_k=b} \Pi_{\boldsymbol{b}|\blacklozenge}^{\mathcal{B}}. \tag{6.71b}$$

Notice that, due to the form of $\boldsymbol{b}$ in the cases $y = \diamondsuit$ and $y = \blacklozenge$, the projections $\Gamma_b^{(j)}$ are defined for $1 \leq j < n$. In the honest case, such projectors will correspond to an outcome b for the Bell measurement of the jth and $(j+1)$th qubit pair of Bob's subsystem. Performing the measurements $\left\{\Gamma_1^{(j)}, \Gamma_2^{(j)}, \Gamma_3^{(j)}, \Gamma_4^{(j)}\right\}$ for all odd j is equivalent to the original measurement $\left\{\Pi_{\boldsymbol{b}|\diamondsuit}^{\mathcal{B}}\right\}_{\boldsymbol{b}}$, and for all even j is equivalent to the original measurement $\left\{\Pi_{\boldsymbol{b}|\blacklozenge}^{\mathcal{B}}\right\}_{\boldsymbol{b}}$.

We may now define corresponding ± 1-outcome observables for each input $\boldsymbol{x} \in \mathcal{X}$ for Alice and $y \in \{1, \ldots, 6\}$ for Bob, and each position $j \in \{1, \ldots, n\}$, as

$$A_{\boldsymbol{x}}^{(j)} = \Pi_{+|\boldsymbol{x}}^{\mathcal{A},j} - \Pi_{-|\boldsymbol{x}}^{\mathcal{A},j}, \tag{6.72a}$$

$$B_{y}^{(j)} = \Pi_{+|y}^{\mathcal{B},j} - \Pi_{-|y}^{\mathcal{B},j}. \tag{6.72b}$$

Alice's observables commute with Bob's observables since they are defined on separate subsystems. Moreover, for any questions $\boldsymbol{x}$ and y, and any positions j and k, we have commutation relations

$$\left[A_{\boldsymbol{x}}^{(j)}, A_{\boldsymbol{x}}^{(k)}\right] = 0, \tag{6.73a}$$

$$\left[B_{y}^{(j)}, B_{y}^{(k)}\right] = 0. \tag{6.73b}$$

Measuring $A_{\boldsymbol{x}}^{(j)}$ and $B_{y}^{(j)}$ for all j is equivalent to performing the original measurements $\left\{\Pi_{\boldsymbol{a}|\boldsymbol{x}}^{\mathcal{A}}\right\}_{\boldsymbol{a}}$ and $\left\{\Pi_{\boldsymbol{b}|y}^{\mathcal{B}}\right\}_{\boldsymbol{b}}$, respectively.

As mentioned previously, we have that $m = 5$ for constructing $\mathcal{X}$ in our protocol. It will be convenient to assign some alternative labels to the observables defined in Eq. (6.72). We will sometimes use notation defined by

$$A_{x_j,\boldsymbol{x}_j}^{(j)} = A_{\boldsymbol{x}}^{(j)} \tag{6.74}$$

for all $1 \leq j \leq n$ and $\boldsymbol{x} \in \mathcal{X}$. In particular, at any position j, we can write labels for the observables of Alice associated with all input values $1 \leq q \leq 5$ at position j and a fixed question at all other positions

$$A_{q,\boldsymbol{x}_j}^{(j)}, \tag{6.75}$$

provided that this fixed question $\boldsymbol{x} \in \mathcal{X}^{(j)}$. All such observables are well defined due to Eq. (6.67) and Lemma 6.13.

We define $D_{\mathrm{z,x}}^{(j)}$, $E_{\mathrm{z,x}}^{(j)}$, $D_{\mathrm{z,y}}^{(j)}$, $E_{\mathrm{z,y}}^{(j)}$, $D_{\mathrm{x,y}}^{(j)}$, and $E_{\mathrm{x,y}}^{(j)}$ for all $1 \leq j \leq n$ on Bob's side such that

$$B_{y}^{(j)} = \begin{cases} D_{\mathrm{z,x}}^{(j)} & \text{if } y = 1, \\ E_{\mathrm{z,x}}^{(j)} & \text{if } y = 2, \\ D_{\mathrm{z,y}}^{(j)} & \text{if } y = 3, \\ E_{\mathrm{z,y}}^{(j)} & \text{if } y = 4, \\ D_{\mathrm{x,y}}^{(j)} & \text{if } y = 5, \\ E_{\mathrm{x,y}}^{(j)} & \text{if } y = 6. \end{cases} \tag{6.76}$$

We also define on Bob's side the (not necessarily unitary) combinations of these observables

$$X_{\mathrm{x,y}}^{(j)} = \frac{D_{\mathrm{x,y}}^{(j)} + E_{\mathrm{x,y}}^{(j)}}{\sqrt{2}}, \tag{6.77a}$$

$$Y_{\mathrm{x,y}}^{(j)} = \frac{D_{\mathrm{x,y}}^{(j)} - E_{\mathrm{x,y}}^{(j)}}{\sqrt{2}}, \tag{6.77b}$$

$$Z_{\mathrm{z,x}}^{(j)} = \frac{D_{\mathrm{z,x}}^{(j)} + E_{\mathrm{z,x}}^{(j)}}{\sqrt{2}}, \tag{6.77c}$$

$$X_{\mathrm{z,x}}^{(j)} = \frac{D_{\mathrm{z,x}}^{(j)} - E_{\mathrm{z,x}}^{(j)}}{\sqrt{2}}, \tag{6.77d}$$

$$Y_{\mathrm{z,y}}^{(j)} = \frac{D_{\mathrm{z,y}}^{(j)} - E_{\mathrm{z,y}}^{(j)}}{\sqrt{2}}, \tag{6.77e}$$

$$Z_{\mathrm{z,y}}^{(j)} = \frac{D_{\mathrm{z,y}}^{(j)} + E_{\mathrm{z,y}}^{(j)}}{\sqrt{2}}. \tag{6.77f}$$

Finally, we define on Bob's side the observables

$$Q_1^{(j)} = X_{\mathrm{x,y}}^{(j)}, \tag{6.78a}$$

$$Q_2^{(j)} = Y_{\mathrm{x,y}}^{(j)}, \tag{6.78b}$$

$$Q_3^{(j)} = Z_{\mathrm{z,x}}^{(j)}, \tag{6.78c}$$

$$Q_4^{(j)} = D_{\mathrm{x,y}}^{(j)}, \tag{6.78d}$$

$$Q_5^{(j)} = E_{\mathrm{x,y}}^{(j)}. \tag{6.78e}$$

It is from (regularized versions of) the observables defined in Eqs. (6.75) and (6.78) which, after proving the necessary relations between them, we will construct our isometry. In order to prove the relations, we request that certain Bell expressions be observed to take maximal values (within some small ε to account for experimental imperfections).

Commutation structure In order that the observables satisfy the main state-dependent commutativity and anticommutativity properties required, we request that, at all positions $1 \leq j \leq n$, maximal violations

$$\langle\psi|\, C_{\boldsymbol{x}_j}^{(j)} \,|\psi\rangle \geq 6\sqrt{2} - \frac{\varepsilon}{\sqrt{2}} \tag{6.79}$$

are observed of the triple CHSH operators

$$\begin{aligned} C_{\boldsymbol{x}_j}^{(j)} = A_{3,\boldsymbol{x}_j}^{(j)} \otimes \left(D_{\mathrm{z,x}}^{(j)} + E_{\mathrm{z,x}}^{(j)}\right) + A_{1,\boldsymbol{x}_j}^{(j)} \otimes \left(D_{\mathrm{z,x}}^{(j)} - E_{\mathrm{z,x}}^{(j)}\right) \\ + A_{3,\boldsymbol{x}_j}^{(j)} \otimes \left(D_{\mathrm{z,y}}^{(j)} + E_{\mathrm{z,y}}^{(j)}\right) + A_{2,\boldsymbol{x}_j}^{(j)} \otimes \left(D_{\mathrm{z,y}}^{(j)} - E_{\mathrm{z,y}}^{(j)}\right) \\ + A_{1,\boldsymbol{x}_j}^{(j)} \otimes \left(D_{\mathrm{x,y}}^{(j)} + E_{\mathrm{x,y}}^{(j)}\right) + A_{2,\boldsymbol{x}_j}^{(j)} \otimes \left(D_{\mathrm{x,y}}^{(j)} - E_{\mathrm{x,y}}^{(j)}\right) \end{aligned} \tag{6.80}$$

for all inputs for Alice at other positions $\boldsymbol{x}_j \in \mathcal{R}^{(j)}$.

The expectation values of all terms appearing in Eq. (6.80) for $C_{\boldsymbol{x}_j}^{(j)}$ are derivable from the observed statistics. For any $1 \leq j \leq n$, since $\boldsymbol{x}_j \in \mathcal{R}^{(j)}$, the observables for Alice all correspond to questions in $\mathcal{X}^{(j)} \subset \mathcal{X}$ by its definition in Eq. (6.67), and so are well defined. Moreover, for each j there are $12\left|\mathcal{R}^{(j)}\right|$ correlations. Due to the choice $|\mathcal{S}| = \mathrm{poly}(n)$ of special questions, inserting Eq. (6.66) then gives a total of at most $12n[1+4n]|\mathcal{S}| = \mathrm{poly}(n)$ correlations needed to verify these requests.

Additional bases So that qubits may be prepared in the additional bases necessary for VBQC, we incorporate the additional observables of Alice corresponding to inputs where $x_j = \mathrm{x} + \mathrm{y}$ and $x_j = \mathrm{x} - \mathrm{y}$. We request that, for all special questions $\chi \in \mathcal{S}$, perfect correlations

$$\langle\psi| A_{4,\chi_j}^{(j)} \otimes D_{\mathrm{x,y}}^{(j)} |\psi\rangle \geq 1 - \varepsilon, \tag{6.81a}$$

$$\langle\psi| A_{5,\chi_j}^{(j)} \otimes E_{\mathrm{x,y}}^{(j)} |\psi\rangle \geq 1 - \varepsilon \tag{6.81b}$$

are observed for all $1 \leq j \leq n$. This serves to ensure that (in the case of any special question) the untrusted operations corresponding to inputs where $x_j = \mathrm{x} \pm \mathrm{y}$ are consistent with the correct combinations of those for the separate inputs $x_j = \mathrm{x}$ and $x_j = \mathrm{y}$.

All of Alice's observables appearing in Eq. (6.81) are well defined (see Lemma 6.12). There are at most $2n|\mathcal{S}| = \mathrm{poly}(n)$ correlations needed to verify these requests.

Complex conjugation To ensure that possible complex conjugation of measurement operators may only occur across all positions simultaneously, we enforce certain correlations that include (commuting) pairs of Alice's observables. This has also been achieved previously by similar methods [53, 116]. Fix any choice of $\chi \in \mathcal{S}$. We request for all $1 \leq j < n$ and $q \in \{1,2,3\}$ that

$$\langle\psi| A_{\boldsymbol{w}}^{(j)} A_{\boldsymbol{w}}^{(j+1)} \otimes \left[(-1)^{[q=2]} \Gamma_1^{(j)} + (-1)^{[q=1]} \Gamma_2^{(j)} + (-1)^{[q=3]} \Gamma_3^{(j)} - \Gamma_4^{(j)}\right] |\psi\rangle \geq 1 - \frac{\varepsilon}{2}, \tag{6.82}$$

where $\boldsymbol{w} = (\chi_1, \ldots, \chi_{j-1}, q, q, \chi_{j+2}, \ldots, \chi_n)$.

All of Alice's observables appearing in Eq. (6.82) are well defined since $\boldsymbol{w} \in \mathcal{X}_\chi \subset \mathcal{X}$, as can be seen from Eqs. (6.61) and (6.62). The observables $A^{(j)}_{\boldsymbol{w}}$ and $A^{(j+1)}_{\boldsymbol{w}}$ are chosen so that they both correspond to the same question $\boldsymbol{w}$, and thus commute with one another. This ensures that the correlations being considered are derivable from observed statistics, since $A^{(j)}_{\boldsymbol{w}} A^{(j+1)}_{\boldsymbol{w}}$ is then a valid observable corresponding to restricting measurement to the product of entries $a_j a_{j+1} \in \{+, -\}$ in the outcome $\boldsymbol{a}$. There are a total of $O(n)$ probabilities involved in verifying these requests.

Classical processing Overall, the total amount of classical processing required to check all of the Bell values and correlations requested in this section grows at worst as $O(n^2)|S| = \text{poly}(n)$. It is thus efficient to perform these checks; the desirable Property 6 discussed in Section 6.2 is satisfied.

6.5.3 Completeness (honest strategy)

The ideal values of Bell expressions and correlations given at the end of Section 6.5.2 can be satisfied using an honest strategy. We take the shared state to be

$$|\psi\rangle = \bigotimes_{j=1}^{n} |\Phi^+\rangle_{\mathcal{A}_j \mathcal{B}_j}, \tag{6.83}$$

where $\mathcal{A}_j$ and $\mathcal{B}_j$ denote the jth reference qubit registers of Alice and Bob, respectively. For all $1 \leq j \leq n$ and all $\boldsymbol{r}$ for which they are defined, we take Alice's observables to be

$$A^{(j)}_{1,\boldsymbol{r}} = \sigma_1^{\mathcal{A}_j}, \tag{6.84a}$$
$$A^{(j)}_{2,\boldsymbol{r}} = -\sigma_2^{\mathcal{A}_j}, \tag{6.84b}$$
$$A^{(j)}_{3,\boldsymbol{r}} = \sigma_3^{\mathcal{A}_j}, \tag{6.84c}$$
$$A^{(j)}_{4,\boldsymbol{r}} = \sigma_5^{\mathcal{A}_j}, \tag{6.84d}$$
$$A^{(j)}_{5,\boldsymbol{r}} = \sigma_4^{\mathcal{A}_j}, \tag{6.84e}$$

where σ_4 and σ_5 are defined as stated in Section 2.1. We take Bob's observables for the questions $y \in \{1, \ldots, 6\}$ to be

$$D_{k,l}^{(j)} = \frac{\sigma_k^{\mathcal{B}_j} + \sigma_l^{\mathcal{B}_j}}{\sqrt{2}}, \tag{6.85a}$$

$$E_{k,l}^{(j)} = \frac{\sigma_k^{\mathcal{B}_j} - \sigma_l^{\mathcal{B}_j}}{\sqrt{2}}, \tag{6.85b}$$

where $k, l \in \{1, 2, 3\}$. In the case $k = 1$ and $l = 2$, these are σ_4 and σ_5, respectively. As for the inputs $y \in \{\diamondsuit, \blacklozenge\}$, the correlations of Eq. (6.82) can be achieved by performing a Bell measurement of pairs of qubits on Bob's subsystem. The projections $\Gamma_b^{(j)}$ denote the projective measurement operator with outcome $b \in \{1, 2, 3, 4\}$ for such a measurement performed on Bob's jth and $(j+1)$th qubits. Specifically, at any position $1 \leq j < n$, we take

$$\Gamma_1^{(j)} = |\Phi^+\rangle\langle\Phi^+|_{\mathcal{B}_j\mathcal{B}_{j+1}}, \tag{6.86a}$$

$$\Gamma_2^{(j)} = |\Phi^-\rangle\langle\Phi^-|_{\mathcal{B}_j\mathcal{B}_{j+1}}, \tag{6.86b}$$

$$\Gamma_3^{(j)} = |\Psi^+\rangle\langle\Psi^+|_{\mathcal{B}_j\mathcal{B}_{j+1}}, \tag{6.86c}$$

$$\Gamma_4^{(j)} = |\Psi^-\rangle\langle\Psi^-|_{\mathcal{B}_j\mathcal{B}_{j+1}}, \tag{6.86d}$$

and perform the projective measurement specified by $\{\Gamma_1^{(j)}, \Gamma_2^{(j)}, \Gamma_3^{(j)}, \Gamma_4^{(j)}\}$.

6.6 Operator relations in the self-test subprotocol

In this section, we demonstrate that the values for Bell expressions and correlations requested as part of Protocol 6.1 (detailed at the end of Section 6.5.2) imply the existence of unitary observables satisfying Theorem 6.9. That is, the observed experimental probabilities self-test (in the sense of Definition 2.7) n Bell states, and also Pauli measurements for Alice. We go on to state this self-testing result in Theorem 6.16 and Corollary 6.17. The following theorem summarizes the relations derived between observables, which are shown in individual detail subsequently in Section 6.6.1.

Theorem 6.15. *Suppose that the values of Bell expressions and correlations requested in Section 6.5.2 are attained (within the tolerance specified in terms of ε). Then the ± 1-outcome observables $\hat{Q}_q^{(j)}$ (regularized versions of the observables $Q_q^{(j)}$) defined by Eqs.* (6.78a) *to* (6.78c) *and, for any choice of special question $\chi \in \mathcal{S} \subset \{1, \ldots, 5\}^n$, the*

± 1-outcome observables $A^{(j)}_{q,\chi_j}$ defined for $q \in \{1,2,3\}$ and $1 \leq j \leq n$ by Eq. (6.75), satisfy the assumptions of Theorem 6.9 with $\eta \leq 21\sqrt{\varepsilon}$.

Proof. For any given $\chi \in \mathcal{S}$, take $S^{(j)}_q = A^{(j)}_{q,\chi_j}$ and $T^{(j)}_q = \hat{Q}^{(j)}_q$ for Theorem 6.9. Proposition 6.18 shows Relation 1. Relation 3 on the commutativity of observables is shown by Propositions 6.19 and 6.20. Relation 2 on anticommutativity is shown by Propositions 6.21 and 6.22. Finally, Relation 4 (which ensures global complex conjugation) is shown by Proposition 6.23. All relations are shown to within a maximum of $21\sqrt{\varepsilon}$ from the ideal, and thus we may choose $\eta \leq 21\sqrt{\varepsilon}$. □

Each of the triple CHSH operators of Eq. (6.80) has an SOS decomposition

$$\begin{aligned} 6\sqrt{2} - C^{(j)}_{\boldsymbol{x}_j} = &\frac{1}{\sqrt{2}}\left(A^{(j)}_{3,\boldsymbol{x}_j} - \frac{D^{(j)}_{\mathrm{z,x}} + E^{(j)}_{\mathrm{z,x}}}{\sqrt{2}}\right)^2 + \frac{1}{\sqrt{2}}\left(A^{(j)}_{1,\boldsymbol{x}_j} - \frac{D^{(j)}_{\mathrm{z,x}} - E^{(j)}_{\mathrm{z,x}}}{\sqrt{2}}\right)^2 \\ &+ \frac{1}{\sqrt{2}}\left(A^{(j)}_{3,\boldsymbol{x}_j} - \frac{D^{(j)}_{\mathrm{z,y}} + E^{(j)}_{\mathrm{z,y}}}{\sqrt{2}}\right)^2 + \frac{1}{\sqrt{2}}\left(A^{(j)}_{2,\boldsymbol{x}_j} - \frac{D^{(j)}_{\mathrm{z,y}} - E^{(j)}_{\mathrm{z,y}}}{\sqrt{2}}\right)^2 \\ &+ \frac{1}{\sqrt{2}}\left(A^{(j)}_{1,\boldsymbol{x}_j} - \frac{D^{(j)}_{\mathrm{x,y}} + E^{(j)}_{\mathrm{x,y}}}{\sqrt{2}}\right)^2 + \frac{1}{\sqrt{2}}\left(A^{(j)}_{2,\boldsymbol{x}_j} - \frac{D^{(j)}_{\mathrm{x,y}} - E^{(j)}_{\mathrm{x,y}}}{\sqrt{2}}\right)^2 \end{aligned} \tag{6.87}$$

Thus, for all j, Eq. (6.79) implies (see Section 2.6) for all $\boldsymbol{x}_j \in \mathcal{R}^{(j)}$ specified that

$$\left(A^{(j)}_{1,\boldsymbol{x}_j} - X^{(j)}_{\mathrm{x,y}}\right)|\psi\rangle \overset{\sqrt{\varepsilon}}{\approx} 0, \tag{6.88a}$$

$$\left(A^{(j)}_{2,\boldsymbol{x}_j} - Y^{(j)}_{\mathrm{x,y}}\right)|\psi\rangle \overset{\sqrt{\varepsilon}}{\approx} 0, \tag{6.88b}$$

$$\left(A^{(j)}_{3,\boldsymbol{x}_j} - Z^{(j)}_{\mathrm{z,x}}\right)|\psi\rangle \overset{\sqrt{\varepsilon}}{\approx} 0, \tag{6.88c}$$

$$\left(A^{(j)}_{1,\boldsymbol{x}_j} - X^{(j)}_{\mathrm{z,x}}\right)|\psi\rangle \overset{\sqrt{\varepsilon}}{\approx} 0, \tag{6.88d}$$

$$\left(A^{(j)}_{2,\boldsymbol{x}_j} - Y^{(j)}_{\mathrm{z,y}}\right)|\psi\rangle \overset{\sqrt{\varepsilon}}{\approx} 0, \tag{6.88e}$$

$$\left(A^{(j)}_{3,\boldsymbol{x}_j} - Z^{(j)}_{\mathrm{z,y}}\right)|\psi\rangle \overset{\sqrt{\varepsilon}}{\approx} 0. \tag{6.88f}$$

Due to the definitions made in Eq. (6.78), Bob's observables in Eqs. (6.88a) to (6.88c) may also be replaced with $Q^{(j)}_1$, $Q^{(j)}_2$, and $Q^{(j)}_3$, respectively. Since Alice's observables in Eq. (6.88) are unitary, regularization can be applied to Bob's observables (see

Section 2.7). This results in expressions involving only unitary operators

$$\left(A^{(j)}_{1,\boldsymbol{x}_j} - \hat{X}^{(j)}_{\mathrm{x,y}}\right)|\psi\rangle \overset{2\sqrt{\varepsilon}}{\approx} 0, \tag{6.89a}$$

$$\left(A^{(j)}_{2,\boldsymbol{x}_j} - \hat{Y}^{(j)}_{\mathrm{x,y}}\right)|\psi\rangle \overset{2\sqrt{\varepsilon}}{\approx} 0, \tag{6.89b}$$

$$\left(A^{(j)}_{3,\boldsymbol{x}_j} - \hat{Z}^{(j)}_{\mathrm{z,x}}\right)|\psi\rangle \overset{2\sqrt{\varepsilon}}{\approx} 0, \tag{6.89c}$$

$$\left(A^{(j)}_{1,\boldsymbol{x}_j} - \hat{X}^{(j)}_{\mathrm{z,x}}\right)|\psi\rangle \overset{2\sqrt{\varepsilon}}{\approx} 0, \tag{6.89d}$$

$$\left(A^{(j)}_{2,\boldsymbol{x}_j} - \hat{Y}^{(j)}_{\mathrm{z,y}}\right)|\psi\rangle \overset{2\sqrt{\varepsilon}}{\approx} 0, \tag{6.89e}$$

$$\left(A^{(j)}_{3,\boldsymbol{x}_j} - \hat{Z}^{(j)}_{\mathrm{z,y}}\right)|\psi\rangle \overset{2\sqrt{\varepsilon}}{\approx} 0. \tag{6.89f}$$

Similarly to before, Bob's observables in Eqs. (6.89a) to (6.89c) may also be replaced with $\hat{Q}^{(j)}_1$, $\hat{Q}^{(j)}_2$, and $\hat{Q}^{(j)}_3$, respectively.

Additionally to the relations required for Theorem 6.9, we have from Eqs. (6.77a) and (6.77b) that, for all positions $1 \leq j \leq n$,

$$D^{(j)}_{\mathrm{x,y}} = \frac{X^{(j)}_{\mathrm{x,y}} + Y^{(j)}_{\mathrm{x,y}}}{\sqrt{2}}, \quad E^{(j)}_{\mathrm{x,y}} = \frac{X^{(j)}_{\mathrm{x,y}} - Y^{(j)}_{\mathrm{x,y}}}{\sqrt{2}}. \tag{6.90}$$

The required observation of the correlations in Eq. (6.81) then implies (via Lemma 2.2) that

$$A^{(j)}_{4,\chi_j}|\psi\rangle \overset{\sqrt{2\varepsilon}}{\approx} \frac{X^{(j)}_{\mathrm{x,y}} + Y^{(j)}_{\mathrm{x,y}}}{\sqrt{2}}|\psi\rangle, \tag{6.91a}$$

$$A^{(j)}_{5,\chi_j}|\psi\rangle \overset{\sqrt{2\varepsilon}}{\approx} \frac{X^{(j)}_{\mathrm{x,y}} - Y^{(j)}_{\mathrm{x,y}}}{\sqrt{2}}|\psi\rangle. \tag{6.91b}$$

From the relations of Eqs. (6.88a) and (6.88b) inferred from the triple CHSH inequalities (in the special case $\boldsymbol{x}_j = \chi_j$), we then have for all $\chi \in \mathcal{S}$ that

$$A^{(j)}_{4,\chi_j}|\psi\rangle \overset{2\sqrt{2\varepsilon}}{\approx} \frac{A^{(j)}_{1,\chi_j} + A^{(j)}_{2,\chi_j}}{\sqrt{2}}|\psi\rangle, \tag{6.92a}$$

$$A^{(j)}_{5,\chi_j}|\psi\rangle \overset{2\sqrt{2\varepsilon}}{\approx} \frac{A^{(j)}_{1,\chi_j} - A^{(j)}_{2,\chi_j}}{\sqrt{2}}|\psi\rangle. \tag{6.92b}$$

We may now write a version of Theorem 6.9 for the experimental observations required by our protocol which also incorporates certification of σ_4 and σ_5. This, along with Lemma 6.10, will allow us to prove Theorem 6.11.

Theorem 6.16. *There exists $\delta(\varepsilon, n) \geq 0$ satisfying $\delta(0, n) = 0$ such that the following holds. Suppose that values of Bell expressions and correlations requested in Section 6.5.2 are attained (within the tolerance specified in terms of ε). Then there exist subnormalized $|\xi_0\rangle_{\mathcal{AB}}$ and $|\xi_1\rangle_{\mathcal{AB}}$ satisfying $\langle\xi_0|\xi_0\rangle_{\mathcal{AB}} + \langle\xi_1|\xi_1\rangle_{\mathcal{AB}} = 1$, isometries $V_{\mathcal{A}}^{\chi} : \mathcal{A} \to \mathcal{A} \otimes \mathcal{A}' \otimes \mathcal{A}''$ for all $\chi \in \mathcal{S}$, and an isometry $V_{\mathcal{B}} : \mathcal{B} \to \mathcal{B} \otimes \mathcal{B}' \otimes \mathcal{B}''$ such that for all $q \in \{1, \ldots, 5\}$, $k \in \{1, \ldots, n\}$, and $\chi \in \mathcal{S}$ we have*

$$V^{\chi}|\psi\rangle_{\mathcal{AB}} \overset{\delta(\varepsilon,n)}{\approx} \bigotimes_{j=1}^{n} |\Phi^+\rangle_{\mathcal{A}'_j\mathcal{B}'_j} \otimes |\xi\rangle, \tag{6.93a}$$

$$V^{\chi} A^{(k)}_{q,\chi_j} |\psi\rangle_{\mathcal{AB}} \overset{\delta(\varepsilon,n)}{\approx} \sigma_q^{\mathcal{B}'_k} \bigotimes_{j=1}^{n} |\Phi^+\rangle_{\mathcal{A}'_j\mathcal{B}'_j} \otimes \sigma_{3[q=3]}^{\mathcal{B}''} |\xi\rangle, \tag{6.93b}$$

where $V^{\chi} = V_{\mathcal{A}}^{\chi} \otimes V_{\mathcal{B}}$ and the junk state $|\xi\rangle \in \mathcal{A} \otimes \mathcal{A}'' \otimes \mathcal{B} \otimes \mathcal{B}''$ is defined as

$$|\xi\rangle = |0\rangle_{\mathcal{A}''}|0\rangle_{\mathcal{B}''} \otimes |\xi_0\rangle_{\mathcal{AB}} + |1\rangle_{\mathcal{A}''}|1\rangle_{\mathcal{B}''} \otimes |\xi_1\rangle_{\mathcal{AB}}. \tag{6.94}$$

Proof. For $q \in \{1, 2, 3\}$, Theorem 6.9 can be applied for each $\chi \in \mathcal{S}$ due to Theorem 6.15, giving an appropriate function δ, junk state $|\xi\rangle$, and isometries $V_{\mathcal{A}}^{\chi}$ and $V_{\mathcal{B}}$. To get the remaining cases $q \in \{4, 5\}$, note the linearity of V^{χ} and use Eq. (6.92).

The isometry on Bob's subsystem $V_{\mathcal{B}}$ given by each application of Theorem 6.9 to Theorem 6.15 (once for each $\chi \in \mathcal{S}$) is that of Fig. 6.3. For each $\chi \in \mathcal{S}$ it is constructed from the same set of Bob's observables, as stated in Theorem 6.15. Thus, given any choice of measurement strategy for Bob as in Eqs. (6.70b) and (6.71), Theorem 6.9 guarantees that the isometry $V_{\mathcal{B}}$ remains unchanged under all different choices of special question $\chi \in \mathcal{S}$. That the same $|\xi\rangle$ is sufficient for all χ can be seen from the fact that the junk states in Theorem 6.9 do not depend on any of Alice's observables. □

Remark. That $V_{\mathcal{B}}$ does not depend on the choice of special question χ leads to the required Property 8 of self-tests applicable to our DIVBQC protocol.

The local isometries V^{χ} in Theorem 6.16 are constructed such that the actions of all observables $A^{(k)}_{q,\chi_k}$ on $|\psi\rangle_{\mathcal{AB}}$ under V^{χ} are shown (in a slightly different form) to be

$$V^{\chi} A^{(k)}_{q,\chi_k} |\psi\rangle_{\mathcal{AB}} \overset{\delta(\varepsilon,n)}{\approx} \left(\sigma_q^{\mathcal{B}'_k} \otimes |0\rangle\langle 0|_{\mathcal{B}''} + \sigma_q^{\mathcal{B}'^{*}_k} \otimes |1\rangle\langle 1|_{\mathcal{B}''} \right) \bigotimes_{j=1}^{n} |\Phi^+\rangle_{\mathcal{A}'_j\mathcal{B}'_j} \otimes |\xi\rangle. \tag{6.95}$$

In particular (by looking at the case $q = \chi_k$ for each k), it is constructed so that the actions of all $A^{(k)}_{\chi} = A^{(k)}_{\chi_k,\chi_k}$ (corresponding to special questions $\chi \in \mathcal{S}$) are shown. The following statement is then immediate.

Corollary 6.17. *For some $\gamma(\varepsilon, n) \geq 0$ satisfying $\gamma(0, n) = 0$, the isometries $V^{\chi} = V_{\mathcal{A}}^{\chi} \otimes V_{\mathcal{B}}$ resulting from Theorem 6.16 act for all $\boldsymbol{s} \in \{0,1\}^n$ as*

$$V^{\chi} A_{\chi}^{\boldsymbol{s}} |\psi\rangle_{\mathcal{A}\mathcal{B}} \overset{\gamma(\varepsilon,n)}{\approx} \left[\bigotimes_{j=1}^{n} \left(\sigma_{\chi_j}^{\mathcal{B}'_j} \right)^{s_j} \otimes |0\rangle\langle 0|_{\mathcal{B}''} + \bigotimes_{j=1}^{n} \left(\sigma_{\chi_j}^{\mathcal{B}'_j *} \right)^{s_j} \otimes |1\rangle\langle 1|_{\mathcal{B}''} \right] \bigotimes_{j=1}^{n} |\Phi^+\rangle_{\mathcal{A}'_j \mathcal{B}'_j} \otimes |\xi\rangle. \quad (6.96)$$

Proof. For each $\chi \in \mathcal{S}$, apply Lemma 6.10 to Eq. (6.95) with $|\phi\rangle = \bigotimes_{j=1}^{n} |\Phi^+\rangle_{\mathcal{A}'_j \mathcal{B}'_j} \otimes |\xi\rangle$. □

As discussed after the statement of Theorem 6.9, for which Theorem 6.15 guarantees $\eta \leq 21\sqrt{\varepsilon}$, we expect standard techniques to yield $\delta(\varepsilon, n) = O\left(\sqrt{\varepsilon} n^2\right)$ and $\gamma(\varepsilon, n) = O\left(\sqrt{\varepsilon} n^2\right)$ in the previous Theorem 6.16 and Corollary 6.17.

6.6.1 Individual relations

We now show each relation that forms Theorem 6.15 in individual detail. We will take it as given throughout this section that the values of all Bell expressions and correlations requested in Section 6.5.2 are attained (within the tolerance specified in terms of ε).

Proposition 6.18 (Symmetry, Alice and Bob)**.** *For any $\chi \in \mathcal{S}$,*

$$\left(A_{q,\chi_j}^{(j)} - \hat{Q}_q^{(j)} \right) |\psi\rangle \overset{2\sqrt{\varepsilon}}{\approx} 0 \quad (6.97)$$

for any position j and for all $q \in \{1,2,3\}$.

Proof. The relations are special cases of those of Eq. (6.89) with $\boldsymbol{x}_j = \chi_j$. □

Proposition 6.19 (Commutativity, Bob)**.** *For any distinct positions j and k such that $j \neq k$, and for all $q, r \in \{1,2,3\}$,*

$$\left[\hat{Q}_q^{(j)}, \hat{Q}_r^{(k)} \right] |\psi\rangle \overset{8\sqrt{\varepsilon}}{\approx} 0. \quad (6.98)$$

Proof. By construction (see Lemma 6.12), there exists $\chi \in \mathcal{S}$ and an input $\boldsymbol{x} \in \mathcal{X}$ such that $x_j = q$, $x_k = r$, and $x_i = \chi_i$ for all $i \in \{1, \ldots, n\} \setminus \{j, k\}$. For this $\boldsymbol{x}$, consider the observables $A_{\boldsymbol{x}}^{(j)}$ and $A_{\boldsymbol{x}}^{(k)}$ which commute by construction as in Eq. (6.73a). Since $x_j = q$ and $x_k = r$, we have $A_{\boldsymbol{x}}^{(j)} = A_{q,\boldsymbol{x}_j}^{(j)}$ and $A_{\boldsymbol{x}}^{(k)} = A_{r,\boldsymbol{x}_k}^{(k)}$, respectively. Lemma 6.14

ensures that $\boldsymbol{x}_j \in \mathcal{R}^{(j)}$ and $\boldsymbol{x}_k \in \mathcal{R}^{(k)}$, and thus from Eq. (6.89) we have $A^{(j)}_{q,\boldsymbol{x}_j}|\psi\rangle \overset{2\sqrt{\varepsilon}}{\approx} \hat{Q}^{(j)}_q|\psi\rangle$ and $A^{(k)}_{r,\boldsymbol{x}_k}|\psi\rangle \overset{2\sqrt{\varepsilon}}{\approx} \hat{Q}^{(k)}_r|\psi\rangle$. Therefore,

$$\left[\hat{Q}^{(j)}_q, \hat{Q}^{(k)}_r\right]|\psi\rangle \overset{8\sqrt{\varepsilon}}{\approx} \left[A^{(k)}_{r,\boldsymbol{x}_k}, A^{(j)}_{q,\boldsymbol{x}_j}\right]|\psi\rangle = \left[A^{(k)}_{\boldsymbol{x}}, A^{(j)}_{\boldsymbol{x}}\right]|\psi\rangle = 0 \tag{6.99}$$

as required. □

Proposition 6.20 (Commutativity, Alice)**.** *For any $\chi \in S$,*

$$\left[A^{(j)}_{q,\chi_j}, A^{(k)}_{r,\chi_k}\right]|\psi\rangle \overset{16\sqrt{\varepsilon}}{\approx} 0 \tag{6.100}$$

for any distinct positions j and k such that $j \neq k$, and all $q, r \in \{1,2,3\}$.

Proof. The observables $A^{(j)}_{q,\chi_j}$ and $A^{(k)}_{r,\chi_k}$ are valid due to Lemma 6.12. One out of the six commutation relations has both its observables coincide with χ, and so also holds exactly and state-independently. Let us suppose q and r are chosen such that this is not the case. By Eqs. (6.64) and (6.65), $\chi_j \in \mathcal{R}^{(j)}$ and $\chi_k \in \mathcal{R}^{(k)}$, and so we may use Eq. (6.89) to see that

$$A^{(j)}_{q,\chi_j}|\psi\rangle \overset{2\sqrt{\varepsilon}}{\approx} \hat{Q}^{(j)}_q|\psi\rangle, \quad A^{(k)}_{r,\chi_k}|\psi\rangle \overset{2\sqrt{\varepsilon}}{\approx} \hat{Q}^{(k)}_r|\psi\rangle. \tag{6.101}$$

Therefore,

$$\left[A^{(j)}_{q,\chi_j}, A^{(k)}_{r,\chi_k}\right]|\psi\rangle \overset{8\sqrt{\varepsilon}}{\approx} \left[\hat{Q}^{(k)}_r, \hat{Q}^{(j)}_q\right]|\psi\rangle \overset{8\sqrt{\varepsilon}}{\approx} 0, \tag{6.102}$$

where the final equality is simply Eq. (6.98). □

Proposition 6.21 (Anticommutativity, Alice)**.** *For any $\chi \in S$,*

$$\left\{A^{(j)}_{q,\chi_j}, A^{(j)}_{r,\chi_j}\right\}|\psi\rangle \overset{2\left(1+\sqrt{2}\right)\sqrt{\varepsilon}}{\approx} 0 \tag{6.103}$$

for any position j and for all distinct $q, r \in \{1,2,3\}$ such that $q \neq r$.

Proof. The observables $A^{(j)}_{q,\chi_j}$ and $A^{(j)}_{r,\chi_j}$ are valid due to Lemma 6.12. Note that if D and E are ± 1-outcome observables, then $\{D+E, D-E\} = 0$. It follows from the definitions made in Eq. (6.77) that

$$\left\{X^{(j)}_{\mathrm{x,y}}, Y^{(j)}_{\mathrm{x,y}}\right\} = 0, \tag{6.104a}$$

$$\left\{X^{(j)}_{\mathrm{z,x}}, Z^{(j)}_{\mathrm{z,x}}\right\} = 0, \tag{6.104b}$$

$$\left\{Y^{(j)}_{\mathrm{z,y}}, Z^{(j)}_{\mathrm{z,y}}\right\} = 0. \tag{6.104c}$$

Since $\chi_j \in \mathcal{R}^{(j)}$ by Eqs. (6.64) and (6.65), we can use Eq. (6.88) to exchange the observables $A^{(j)}_{q,\chi_j}$ and $A^{(j)}_{r,\chi_j}$ with the appropriate two of Bob's observables from one of Eqs. (6.104a) to (6.104c), matching the values of q and r. Let us denote these two observables here by R_q and R_r. Since $\{R_q, R_r\} = 0$, we have

$$\begin{aligned}\left\| \left\{ A^{(j)}_{q,\chi_j}, A^{(j)}_{r,\chi_j} \right\} |\psi\rangle \right\| &= \left\| \left\{ A^{(j)}_{q,\chi_j}, A^{(j)}_{r,\chi_j} \right\} |\psi\rangle - \{R_q, R_r\}|\psi\rangle \right\| \\ &\leq (2 + \|R_q\| + \|R_r\|)\sqrt{\varepsilon},\end{aligned} \tag{6.105}$$

where the inequality follows from Eq. (6.88), the triangle inequality, unitarity of $A^{(j)}_q$ and $A^{(j)}_r$, and the definition of the operator norm. Applying the triangle inequality to Eq. (6.77) to get

$$\|R_q\| \leq \sqrt{2}, \quad \|R_r\| \leq \sqrt{2} \tag{6.106}$$

yields the desired expression. □

Proposition 6.22 (Anticommutativity, Bob)**.** *For any position j,*

$$\left\{ \hat{Q}^{(j)}_1, \hat{Q}^{(j)}_2 \right\} |\psi\rangle \overset{2\left(3+\sqrt{2}\right)\sqrt{\varepsilon}}{\approx} 0, \tag{6.107a}$$

$$\left\{ \hat{Q}^{(j)}_1, \hat{Q}^{(j)}_3 \right\} |\psi\rangle \overset{2\left(4+\sqrt{2}\right)\sqrt{\varepsilon}}{\approx} 0, \tag{6.107b}$$

$$\left\{ \hat{Q}^{(j)}_2, \hat{Q}^{(j)}_3 \right\} |\psi\rangle \overset{2\left(5+\sqrt{2}\right)\sqrt{\varepsilon}}{\approx} 0. \tag{6.107c}$$

Proof. Since $Q^{(j)}_1 = X^{(j)}_{\mathrm{x,y}}$ and $Q^{(j)}_2 = Y^{(j)}_{\mathrm{x,y}}$, we have as before that $Q^{(j)}_1$ and $Q^{(j)}_2$ anticommute by construction. Furthermore, applying the triangle inequality to the operator norms of Eqs. (6.77a) and (6.77b) shows that

$$\left\| Q^{(j)}_1 \right\| \leq \sqrt{2}, \quad \left\| Q^{(j)}_2 \right\| \leq \sqrt{2}. \tag{6.108}$$

Thus, Lemma 2.9 applied using Eqs. (6.88a) and (6.88b) immediately gives the first desired relation for the regularized operators $\hat{Q}^{(j)}_1$ and $\hat{Q}^{(j)}_2$.

We also know, as before, that $X^{(j)}_{\mathrm{z,x}}$ anticommutes with $Z^{(j)}_{\mathrm{z,x}}$. Our strategy is thus to write the state-dependent anticommutator of the regularized operators $\hat{Q}^{(j)}_1 = \hat{X}^{(j)}_{\mathrm{x,y}}$ and $\hat{Q}^{(j)}_3 = \hat{Z}^{(j)}_{\mathrm{z,x}}$ in terms of $X^{(j)}_{\mathrm{z,x}}$ and $Z^{(j)}_{\mathrm{z,x}}$ (note the differing subscripts between $\hat{X}^{(j)}_{\mathrm{x,y}}$ and $X^{(j)}_{\mathrm{z,x}}$). Taking any $\chi \in \mathcal{S}$ (which satisfies $\chi_j \in \mathcal{R}^{(j)}$ by definition), we have

$$\hat{X}^{(j)}_{\mathrm{x,y}} \hat{Z}^{(j)}_{\mathrm{z,x}} |\psi\rangle \overset{4\sqrt{\varepsilon}}{\approx} A^{(j)}_{3,\chi_j} A^{(j)}_{1,\chi_j} |\psi\rangle \overset{\left(1+\sqrt{2}\right)\sqrt{\varepsilon}}{\approx} X^{(j)}_{\mathrm{z,x}} Z^{(j)}_{\mathrm{z,x}} |\psi\rangle, \tag{6.109}$$

where the first estimate uses Eqs. (6.89a) and (6.89c), and the second estimate uses Eqs. (6.88c) and (6.88d) along with the triangle inequality applied to the operator norm of Eq. (6.77d). We can also write

$$\hat{Z}^{(j)}_{\mathrm{z,x}}\hat{X}^{(j)}_{\mathrm{x,y}}|\psi\rangle \overset{3\sqrt{\varepsilon}}{\approx} Z^{(j)}_{\mathrm{z,x}}A^{(j)}_{1,\chi_j}|\psi\rangle \overset{\sqrt{2\varepsilon}}{\approx} Z^{(j)}_{\mathrm{z,x}}X^{(j)}_{\mathrm{z,x}}|\psi\rangle, \tag{6.110}$$

where this time for the first estimate (since we do not need to change the subscripts on the first operator) we use the property of regularization that gives

$$\hat{Z}^{(j)}_{\mathrm{z,x}}|\psi\rangle \overset{\sqrt{\varepsilon}}{\approx} Z^{(j)}_{\mathrm{z,x}}|\psi\rangle \tag{6.111}$$

in light of Eq. (6.88c) (see Section 2.7). Therefore, we can now combine Eqs. (6.109) and (6.110) conclude the second desired relation

$$\left\{\hat{Q}^{(j)}_1, \hat{Q}^{(j)}_3\right\}|\psi\rangle = \left\{\hat{X}^{(j)}_{\mathrm{x,y}}, \hat{Z}^{(j)}_{\mathrm{z,x}}\right\}|\psi\rangle \overset{2\left(4+\sqrt{2}\right)\sqrt{\varepsilon}}{\approx} \left\{X^{(j)}_{\mathrm{z,x}}, Z^{(j)}_{\mathrm{z,x}}\right\}|\psi\rangle = 0. \tag{6.112}$$

To derive the third and final relation, we know that $Y^{(j)}_{\mathrm{z,y}}$ anticommutes with $Z^{(j)}_{\mathrm{z,y}}$. Now we can perform the same process as in deriving Eq. (6.109) to write both

$$\hat{Y}^{(j)}_{\mathrm{x,y}}\hat{Z}^{(j)}_{\mathrm{z,x}}|\psi\rangle \overset{4\sqrt{\varepsilon}}{\approx} A^{(j)}_{3,\chi_j}A^{(j)}_{2,\chi_j}|\psi\rangle \overset{\left(1+\sqrt{2}\right)\sqrt{\varepsilon}}{\approx} Y^{(j)}_{\mathrm{z,y}}Z^{(j)}_{\mathrm{z,y}}|\psi\rangle, \tag{6.113a}$$

$$\hat{Z}^{(j)}_{\mathrm{z,x}}\hat{Y}^{(j)}_{\mathrm{x,y}}|\psi\rangle \overset{4\sqrt{\varepsilon}}{\approx} A^{(j)}_{2,\chi_j}A^{(j)}_{3,\chi_j}|\psi\rangle \overset{\left(1+\sqrt{2}\right)\sqrt{\varepsilon}}{\approx} Z^{(j)}_{\mathrm{z,y}}Y^{(j)}_{\mathrm{z,y}}|\psi\rangle. \tag{6.113b}$$

Finally, we conclude that

$$\left\{\hat{Q}^{(j)}_2, \hat{Q}^{(j)}_3\right\}|\psi\rangle = \left\{\hat{Y}^{(j)}_{\mathrm{x,y}}, \hat{Z}^{(j)}_{\mathrm{z,x}}\right\}|\psi\rangle \overset{2\left(5+\sqrt{2}\right)\sqrt{\varepsilon}}{\approx} \left\{Y^{(j)}_{\mathrm{z,y}}, Z^{(j)}_{\mathrm{z,y}}\right\}|\psi\rangle = 0 \tag{6.114}$$

and have now shown all desired anticommutation relations for Bob. □

Proposition 6.23 (Complex conjugation relation)**.** *For any $\chi \in \mathcal{S}$ and $1 \leq j < n$ we have*

$$|\psi\rangle + A^{(j)}_{1,\chi_j}A^{(j+1)}_{1,\chi_{j+1}}A^{(j)}_{2,\chi_j}A^{(j+1)}_{2,\chi_{j+1}}A^{(j)}_{3,\chi_j}A^{(j+1)}_{3,\chi_{j+1}}|\psi\rangle \overset{21\sqrt{\varepsilon}}{\approx} 0. \tag{6.115}$$

Proof. Suppose that $\chi' \in \mathcal{S}$ is the special question for which Eq. (6.82) is satisfied. For all $q \in \{1,2,3\}$, we can see immediately from the definitions in Eqs. (6.64) and (6.65) that $\boldsymbol{w}_j \in \mathcal{R}^{(j)}_{\chi} \subset \mathcal{R}^{(j)}$ and $\boldsymbol{w}_{j+1} \in \mathcal{R}^{(j+1)}_{\chi} \subset \mathcal{R}^{(j+1)}$, where

$$\boldsymbol{w} = (\chi'_1, \ldots, \chi'_{j-1}, q, q, \chi'_{j+2}, \ldots, \chi'_n).$$

Similarly, we can see for all $\chi \in \mathcal{S}$ that $\chi_i \in \mathcal{R}^{(i)}_{\chi} \subset \mathcal{R}^{(i)}$ for all i.

We can thus write for all χ and q that

$$A^{(j)}_{q,\chi_j} A^{(j+1)}_{q,\chi_{j+1}} |\psi\rangle \overset{3\sqrt{\varepsilon}}{\approx} \hat{Q}^{(j+1)}_q Q^{(j)}_q |\psi\rangle \overset{3\sqrt{\varepsilon}}{\approx} A^{(j)}_{\boldsymbol{w}} A^{(j+1)}_{\boldsymbol{w}} |\psi\rangle, \tag{6.116}$$

where both estimates use Eqs. (6.88) and (6.89), and again

$$\boldsymbol{w} = (\chi'_1, \ldots, \chi'_{j-1}, q, q, \chi'_{j+2}, \ldots, \chi'_n).$$

Notice now that the operators

$$\Gamma^{(j)}_1 - \Gamma^{(j)}_2 + \Gamma^{(j)}_3 - \Gamma^{(j)}_4, \tag{6.117a}$$
$$-\Gamma^{(j)}_1 + \Gamma^{(j)}_2 + \Gamma^{(j)}_3 - \Gamma^{(j)}_4, \tag{6.117b}$$
$$\Gamma^{(j)}_1 + \Gamma^{(j)}_2 - \Gamma^{(j)}_3 - \Gamma^{(j)}_4, \tag{6.117c}$$

are unitary, since the $\Gamma^{(j)}_b$ as defined in Eq. (6.71) form a projective measurement for each j. Alice's operators appearing in Eq. (6.82) are also unitary by definition in Eq. (6.72a). We can thus apply Lemma 2.2 to Eq. (6.82). Together with Eq. (6.116) holding for all q, this implies

$$A^{(j)}_{1,\chi_j} A^{(j+1)}_{1,\chi_{j+1}} |\psi\rangle \overset{7\sqrt{\varepsilon}}{\approx} \left(\Gamma^{(j)}_1 - \Gamma^{(j)}_2 + \Gamma^{(j)}_3 - \Gamma^{(j)}_4\right) |\psi\rangle, \tag{6.118a}$$
$$A^{(j)}_{2,\chi_j} A^{(j+1)}_{2,\chi_{j+1}} |\psi\rangle \overset{7\sqrt{\varepsilon}}{\approx} \left(-\Gamma^{(j)}_1 + \Gamma^{(j)}_2 + \Gamma^{(j)}_3 - \Gamma^{(j)}_4\right) |\psi\rangle, \tag{6.118b}$$
$$A^{(j)}_{3,\chi_j} A^{(j+1)}_{3,\chi_{j+1}} |\psi\rangle \overset{7\sqrt{\varepsilon}}{\approx} \left(\Gamma^{(j)}_1 + \Gamma^{(j)}_2 - \Gamma^{(j)}_3 - \Gamma^{(j)}_4\right) |\psi\rangle. \tag{6.118c}$$

Therefore,

$$\begin{aligned} &A^{(j)}_{1,\chi_j} A^{(j+1)}_{1,\chi_{j+1}} A^{(j)}_{2,\chi_j} A^{(j+1)}_{2,\chi_{j+1}} A^{(j)}_{3,\chi_j} A^{(j+1)}_{3,\chi_{j+1}} |\psi\rangle \\ &\quad \overset{7\sqrt{\varepsilon}}{\approx} \left(\Gamma^{(j)}_1 + \Gamma^{(j)}_2 - \Gamma^{(j)}_3 - \Gamma^{(j)}_4\right) A^{(j)}_{1,\chi_j} A^{(j+1)}_{1,\chi_{j+1}} A^{(j)}_{2,\chi_j} A^{(j+1)}_{2,\chi_{j+1}} |\psi\rangle \\ &\quad \overset{7\sqrt{\varepsilon}}{\approx} \left(-\Gamma^{(j)}_1 + \Gamma^{(j)}_2 - \Gamma^{(j)}_3 + \Gamma^{(j)}_4\right) A^{(j)}_{1,\chi_j} A^{(j+1)}_{1,\chi_{j+1}} |\psi\rangle \\ &\quad \overset{7\sqrt{\varepsilon}}{\approx} -\left(\Gamma^{(j)}_1 + \Gamma^{(j)}_2 + \Gamma^{(j)}_3 + \Gamma^{(j)}_4\right) |\psi\rangle. \end{aligned} \tag{6.119}$$

Since $\sum_b \Gamma^{(j)}_b = I$, the result follows. □

6.7 Discussion

We have shown that the self-testing protocol given in this chapter exhibits all of the requirements to be combined with Fitzsimons–Kashefi-type verifiable blind quantum computation delegation schemes to achieve fully device-independent security.

Furthermore, our protocol achieves several properties that are desirable for future practical implementations. Of particular note is that, despite being able to certify the remote preparation of a wide variety of states in parallel, only a rudimentary quantum measurement device is needed by the client party. The input randomness required for generating questions is also small, scaling logarithmically in the number of qubits for the client and with constant-sized questions being sent to the remote server. Our combined protocol would also enjoy many of the benefits brought by further developments in VBQC protocols. It can already be optimized, for example, by starting with different resource state structures [44, 45, 121], and can be made fault-tolerant as in [7]. Many of the properties shown of our self-test are also desirable in other applications (especially those involving device-independent state preparation), and as such our work is not restricted to use in delegated quantum computation. In such cases, it may not be necessary to use as many possible input questions as we have done, and simpler special cases of our tests could be used as is necessary.

Resource consumption Let us comment on the resources used by our protocol by first focusing on the self-testing and remote state preparation components. Using standard statistical techniques, achieving a fixed statistical confidence (of say 99%) for a given error tolerance ε in our protocol is possible in $O(1/\varepsilon^2)$ experimental trials of each of $O(n^2)|S|$ questions. Using the conservative self-testing robustness estimate we expect to be achievable, some fixed constant distance between physical and reference states in our self-testing and remote state preparation statements (Theorems 6.11 and 6.16 and Corollary 6.17) would require an error tolerance $\varepsilon = \Omega(1/n^4)$. Thus, a given fixed robustness can be achieved (with 99% confidence) in $O(n^8)$ experimental trials per question. For the sake of argument, let us take our number of special questions to be $|S| = O(n)$, resulting in $O(n^3)$ questions overall and a total of $O(n^{11})$ trials. Since each of our questions consume $O(\log n)$ bits of randomness, the total self-testing cost is $O(n^{11} \log n)$ bits in this case.

A circuit with g gates may be delegated using $N = O(g)$ qubits [40, 120, 137]. Starting with the dotted triple graph version of the brickwork resource state used for composability in the robust FK protocol of [7], it is possible to achieve exponential security with a number of repetitions that is constant in the size of the computation, all the while conserving the composability and fault tolerance properties of the protocol [44, Appendix F]. In this case, the overhead due to verification for a fixed level of security is $O(N)$ additional qubits prepared and $O(N)$ bits of total commu-

nication (thanks to the constant number of repetitions). The total number of qubits that must be prepared is then $n = O(g)$ and the *total* computation cost also scales as $O(g)$. Errors in soundness and completeness of the robust FK protocol due to a nonideal input state depend only of the trace distance of this state from the ideal [7]. Therefore, to obtain a correct answer with some fixed high probability is estimated to cost $O(g^{11} \log g)$ bits of self-testing resources and $O(g)$ total computation resources, resulting in an overall resource cost estimate for our composite device-independent VBQC protocol that is $O(g^{11} \log g)$.

Clearly, despite outperforming a number of previous works in this metric, this is not ideal (the state-of-the-art is $\Theta(g \log g)$ [53]). It should be noted, however, that while our extra nonlinear cost enters entirely from self-testing, resource estimation is performed under the assumption of noiseless and honest provers, with errors originating only from statistical analysis. In a more realistic setting with non-adversarial provers contending with depolarizing experimental noise local to each of their n EPR pairs, the comparison is less transparent. The error tolerance ϵ we can achieve would only be worsened by a constant factor (depending on the level of noise), as it refers to outcomes for fixed-sized chunks of registers (one or two EPR pairs each). Meanwhile, self-testing protocols with robustness depending on an ϵ that instead represents global failure rate in its tests would see ϵ increasing to some nonzero constant exponentially quickly in n due to such noise. In this case, even with robustness guarantees scaling polynomially (as $\epsilon \to 0$) in ϵ alone, it would be extraordinarily difficult to achieve the fidelities required in such an experiment as the number of qubits grows. Further discussion of this point can be found in [138].

Future works While we believe that the robustness bounds used for our estimation are conservative and achievable using standard existing techniques, we have opted to wait for techniques yielding improved bounds to be developed (perhaps using techniques such as in [28, 69, 103, 106, 139–142]) that are applicable to local error tolerances. Any analytic improvements on results of the form of our Theorem 6.9 or Lemma 6.10 would be of direct consequence to our resource costs. For practical applicability, numerical optimization approaches such as those using semidefinite programming have yielded much better robustness values (and apparent scaling) than those analytically derived [25, 59–61, 101, 106, 110, 111, 117, 118]. Advances of the computational efficiency of such techniques are, thus, also of great interest.

In case a much more technologically capable client device is acceptable, it may be

possible to adapt the rigidity results conceived by Coladangelo et al. [53] to prepare input states to FK-type VBQC protocols. This would likely lead to a protocol whose total resources scale as $O(g)$ in the noiseless case, an improvement by a logarithmic factor over the state-of-the-art. Whether the more recent self-testing protocol of Natarajan and Vidick [103] with smaller communication could also be used for the required state preparation is an open question. Device-independent "one-shot" tests in the spirit of [138, 143] could also be studied in the context of state preparation.

Chapter 7

Conclusion

The narrative we have presented in this thesis was composed of three main phases. Firstly, we united for the first time arguably the two most famous two-player nonlocal games (the CHSH and magic square games) under a single framework, inspired as a generalization to the rules of the magic square game of Mermin [18], Peres [19], and Aravind [77] to be played on rectangular tables of arbitrary sizes. Secondly, armed with the additional structure brought by these nonlocal games and guided by our results, we embarked on a search for exciting contexts within which they could be put to work in the form of cryptographic applications. The particular tasks that we chose to focus upon were those of certified private randomness expansion and the self-testing of quantum systems, although any number of other applications could also have been considered. As an aside, whether or not self-testing should fall under the umbrella of quantum cryptography is often debated, however, we are comfortable in regarding it as such due to its usefulness in many specifically cryptographic applications and also the inherently low level of trust afforded to devices in the device-independent regime of which it forms a part. Thirdly, having already exhibited a protocol certifying the presence of arbitrarily many maximally entangled Bell states with many properties appropriate for simple-client tasks in the device-independent scenario, we turned our attention to arguably one of the most crucial of such applications: universal verifiable blind delegated quantum computation (VBQC). We constructed another self-test tailored specifically for (but certainly not limited to) lifting existing VBQC protocols into the fully device-independent security setting. This scheme satisfies an extensive list of properties that allow for the efficiency and composability achieved. We now comment on some of the implications of each part of the thesis.

In Chapter 3, we studied optimal winning probabilities for our magic rectangle

games, considering various levels of correlations characterized by the NPA hierarchy. As mentioned, we would like to see whether a useful definition for the multipartite case of "magic hyperrectangles" could be made. It may be possible to then incorporate further well-known (say, tripartite examples of) nonlocal games under the same framework, as we already say for the 2×2 case of the CHSH game. In these cases, the multipartite extension to the usual techniques of the NPA hierarchy could be applied [60]. Also, in any case, the open question as to the optimal quantum values for all $2\times n$ games is an interesting one. That our 2×3 game exhibits a separation between the NPA level 1 and almost quantum sets (with the former having a perfect winning strategy) may indicate some usefulness in quantum measure theory (a generalization of measure theory in which the σ-additivity property of probability measures is weakened to a similar condition that allows for interference between pairs of alternative histories for a system, but not triples) [92, 144]. Since being presented, our magic rectangle games have also been studied as a special case of *graph incidence games* by Paddock et al. [145].

The applications that we considered for our magic rectangles were those of certified private randomness (Chapter 4) and self-testing (Chapter 5). For randomness expansion, we found that the smallest games perform the best in terms of noise tolerance, starting with the CHSH game (the 2×2 case). In terms of rates, while we have used very weak general bounds (resulting in quite suboptimal rates), we also find that smaller games perform better. This is somewhat expected, since the smaller magic rectangles exhibit a larger classical–quantum gap (the classical win probability tends to unity as the rectangles grow larger). The smaller games also require fewer input questions, leading to lower consumption of randomness in the required Bell tests of expansion protocols (although performing spot checking as is usually done significantly reduces the impact of this). Even so, it may be worthwhile to examine some of our games using the recent techniques based on entropy accumulation [94], with the smallest nonstandard 2×3 magic rectangle game being an ideal first candidate. As a starting point for our self-testing application, we gave a perfectly winning "one-side-local" strategy for the Mermin–Peres magic square game in which one of the parties requires only to perform single-qubit Pauli measurements. This strategy would also be of practicality in any existing (or future) scenario employing the magic square game in which the cost of sharing three EPR pairs of entanglement does not exceed in magnitude the benefit of measurement simplicity for one side. Our protocol was particularly suited for certifying many Bell states in the client–server setting, per-

forming favorably with respect to some of the properties it simultaneously exhibits in this case.

Finally, we gave in Chapter 6 a self-testing protocol instead based primarily on (triple) CHSH statistics that allows (by parallel remote state preparation via teleportation) existing VBQC schemes of the Fitzsimons–Kashefi type to be brought into the realm of fully device-independent security. This scheme provides an alternative in the measurement-based quantum computation model to that of Coladangelo et al. [53], which instead makes use of the verifiability scheme of Broadbent [49]. Our scheme is also designed to be efficient (e.g. in terms of communication complexity and classical postprocessing) as well as practical in terms of the technological simplicity required of client devices. It is an open problem as to whether the rigidity results of Coladangelo et al. [53] (that are in turn based on the "Pauli braiding test" of Natarajan and Vidick [28]) could also be adapted for use with FK-type VBQC protocols. If this could be done, it would likely yield a further improved protocol with total resource consumption scaling linearly in the number of gates in the delegated circuit (although it would still require entangled measurements for both parties). Since first presenting the work of this chapter, progress has been made on verification whereby qubits need only be prepared in a single plane of the Bloch sphere [146]. We also note that, while we did not choose to explicitly analyze exact robustness guarantees for our protocol (although they certainly could be derived using standard techniques), such bounds are very simple to derive in this exact special case, since complex conjugation of measurements need not be considered, and are of the form indicated in the relevant results of the chapter.

We hope that through the work that has been presented in this thesis, it has become even more apparent that the study of nonlocal games and of device-independent protocols can form a largely symbiotic relationship, with developments taking place in one often giving rise to interesting developments in the other. This type of rapid and accelerating evolution is taking place across the whole domain of quantum science and technology, and the full potential of such advances is only just beginning to come to fruition.

Appendix A

Winning 2-by-3 games at NPA hierarchy level 1

Consider the 2×3 magic rectangle game in which entries to the first column are required to have a negative product, and all other row and column products are required to be positive. That is, the 2×3 game specified by the parameters $(\beta_1, \beta_2, \beta_3) = (-,+,+)$ and $(\alpha_1, \alpha_2) = (+,+)$ satisfying Definition 3.1. In order to write our strategy more easily, in Table A.1 we introduce a more concise alphabet for the inputs and outputs of the game.

Table A.1: The natural alphabets $\mathscr{A}$ and $\mathscr{B}$ defined here denote new notation for the natural alphabets of the 2×3 magic rectangle game under consideration, with parameters $(\alpha_1, \alpha_2) = (+,+)$ and $(\beta_1, \beta_2, \beta_3) = (-,+,+)$. Elements of each alphabet have the form of input/output pairs for each player, with the input written first.

$\mathscr{A}_{2\times3}$	$\mathscr{A}$	$\mathscr{B}_{2\times3}$	$\mathscr{B}$
$(1,(+,+,+))$	$(1,1)$	$(1,(+,-)^T)$	$(1,1)$
$(1,(+,-,-))$	$(1,2)$	$(1,(-,+)^T)$	$(1,2)$
$(1,(-,+,-))$	$(1,3)$	$(2,(+,+)^T)$	$(2,1)$
$(1,(-,-,+))$	$(1,4)$	$(2,(-,-)^T)$	$(2,2)$
$(2,(+,+,+))$	$(2,1)$	$(3,(+,+)^T)$	$(3,1)$
$(2,(+,-,-))$	$(2,2)$	$(3,(-,-)^T)$	$(3,2)$
$(2,(-,+,-))$	$(2,3)$		
$(2,(-,-,+))$	$(2,4)$		

Under the new notation defined in Table A.1, the success probability of a behavior

$P(a, b \mid x, y)$ where $(x, a) \in \mathscr{A}$ and $(y, b) \in \mathscr{B}$ is

$$\begin{aligned} p = \tfrac{1}{6}[&P(1,1 \mid 1,1) + P(2,1 \mid 1,1) + P(3,2 \mid 1,1) + P(4,2 \mid 1,1) \\ &+ P(1,1 \mid 1,2) + P(2,2 \mid 1,2) + P(3,1 \mid 1,2) + P(4,2 \mid 1,2) \\ &+ P(1,1 \mid 1,3) + P(2,2 \mid 1,3) + P(3,2 \mid 1,3) + P(4,1 \mid 1,3) \\ &+ P(1,2 \mid 2,1) + P(2,2 \mid 2,1) + P(3,1 \mid 2,1) + P(4,1 \mid 2,1) \\ &+ P(1,1 \mid 2,2) + P(2,2 \mid 2,2) + P(3,1 \mid 2,2) + P(4,2 \mid 2,2) \\ &+ P(1,1 \mid 2,3) + P(2,2 \mid 2,3) + P(3,2 \mid 2,3) + P(4,1 \mid 2,3)]. \end{aligned} \tag{A.1}$$

We now state a behavior, achievable using NPA level 1 correlations, for which the win probability p of Eq. (A.1) is unity. This behavior is defined via the matrices

$$(P(a, b \mid 1, 1))_{a,b} = \frac{1}{4}\begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \\ 0 & 1 \end{pmatrix}, \tag{A.2a}$$

$$(P(a, b \mid 2, 1))_{a,b} = \frac{1}{4}\begin{pmatrix} 0 & 1 \\ 0 & 1 \\ 1 & 0 \\ 1 & 0 \end{pmatrix}, \tag{A.2b}$$

$$(P(a, b \mid 1, 2))_{a,b} = (P(a, b \mid 2, 2))_{a,b} = \frac{1}{4}\begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}, \tag{A.2c}$$

$$(P(a, b \mid 1, 3))_{a,b} = (P(a, b \mid 2, 3))_{a,b} = \frac{1}{4}\begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 1 \\ 1 & 0 \end{pmatrix}. \tag{A.2d}$$

Indeed, the behavior defined by Eq. (A.2) admits an NPA hierarchy level 1 certificate,

given by the matrix

$$\Gamma = \frac{1}{8}\begin{pmatrix} 8 & 2 & 2 & 2 & 2 & 2 & 2 & 4 & 4 & 4 \\ 2 & 2 & 0 & 0 & 1 & -1 & 1 & 2 & 2 & 2 \\ 2 & 0 & 2 & 0 & -1 & 1 & 1 & 2 & 0 & 0 \\ 2 & 0 & 0 & 2 & 1 & 1 & 1 & 0 & 2 & 0 \\ 2 & 1 & -1 & 1 & 2 & 0 & 0 & 0 & 2 & 2 \\ 2 & -1 & 1 & 1 & 0 & 2 & 0 & 0 & 0 & 0 \\ 2 & 1 & 1 & 1 & 0 & 0 & 2 & 2 & 2 & 0 \\ 4 & 2 & 2 & 0 & 0 & 0 & 2 & 4 & 2 & 2 \\ 4 & 2 & 0 & 2 & 2 & 0 & 2 & 2 & 4 & 2 \\ 4 & 2 & 0 & 0 & 2 & 0 & 0 & 2 & 2 & 4 \end{pmatrix}. \tag{A.3}$$

By Corollary 3.6, we thus have that $\omega_1(2,3) = 1$. Therefore, by Corollary 3.12, $\omega_1(2,n) = 1$ for all $n \geq 3$.

Appendix B

Robust anticommutation relations

Lemma B.1. *For all distinct $i, j, k, l \in \{1, \dots, n\}$ we have the estimate between Alice's observables and Bob's pair check observables,*

$$\left\| \left(X_A^l Z_A^l Z_A^k X_A^k\right)\left(X_A^j Z_A^j Z_A^i X_A^i\right)|\psi\rangle - X_B^{i,k} Z_B^{i,k} Z_B^{j,l} X_B^{j,l}|\psi\rangle \right\| \leq 18\sqrt{2\varepsilon_1} + 4\sqrt{2\varepsilon_2}. \tag{B.1}$$

Proof. First, commuting X_A^j with X_A^k (as they correspond to the same input) and then using Proposition 5.12 and the triangle inequality to swap four of Alice's observables to Bob's side, we have

$$\begin{aligned}\Big\| \left(X_A^l Z_A^l Z_A^k X_A^k\right)\left(X_A^j Z_A^j Z_A^i X_A^i\right)|\psi\rangle \\ - X_A^l Z_A^l Z_A^k X_A^j X_{B,i}^i Z_{B,k}^i Z_{B,k}^j X_{B,k}^k |\psi\rangle \Big\| \leq 4\sqrt{2\varepsilon_1}.\end{aligned} \tag{B.2}$$

Commuting $X_{B,k}^k$ with observables of the same input ($Z_{B,k}^i$ and $Z_{B,k}^j$) and then again using the correlations to swap observables back to Alice's side gives

$$\left\| \left(X_A^l Z_A^l Z_A^k X_A^k\right)\left(X_A^j Z_A^j Z_A^i X_A^i\right)|\psi\rangle - X_A^l Z_A^l Z_A^k X_A^j Z_A^j Z_A^i X_A^k X_A^i |\psi\rangle \right\| \leq 8\sqrt{2\varepsilon_1}. \tag{B.3}$$

Applying Eq. (5.53a) correlations between Alice's observables and Bob's pair check observables once followed by swapping five of Alice's observables to Bob's side gives

$$\begin{aligned}\Big\| \left(X_A^l Z_A^l Z_A^k X_A^k\right)\left(X_A^j Z_A^j Z_A^i X_A^i\right)|\psi\rangle \\ - X_B^{i,k} X_A^l Z_{B,l}^i Z_{B,l}^j X_{B,j}^j Z_{B,j}^k Z_{B,j}^l |\psi\rangle \Big\| \leq 13\sqrt{2\varepsilon_1} + \sqrt{2\varepsilon_2}.\end{aligned} \tag{B.4}$$

Commuting $X_{B,j}^j$ with observables of the same input ($Z_{B,j}^k$ and $Z_{B,j}^l$) and again swapping local check observables back to Alice's side yields

$$\begin{aligned}\Big\| \left(X_A^l Z_A^l Z_A^k X_A^k\right)\left(X_A^j Z_A^j Z_A^i X_A^i\right)|\psi\rangle \\ - X_B^{i,k} X_A^l X_A^j Z_A^l Z_A^k Z_A^j Z_A^i |\psi\rangle \Big\| \leq 18\sqrt{2\varepsilon_1} + \sqrt{2\varepsilon_2}.\end{aligned} \tag{B.5}$$

Finally, commuting Z_A^j with Z_A^k and applying three correlations of Eq. (5.53) to switch all observables of Alice with pair check observables of Bob gives the result. □

Lemma B.2. *For any permutation σ of $\{1, \dots, n\}$, letting $\sigma_k = \sigma(k)$ for each k, we have the estimate*

$$\Bigg\| \Bigg(\prod_{k \neq n} Z_A^{\sigma_k} \Bigg) \Bigg(\prod_{k} X_A^{\sigma_k} \Bigg) |\psi\rangle - X_A^{\sigma_n} X_B^{\sigma_1,\sigma_2} \Bigg(\prod_{k=1}^{(n-3)/4} X_B^{\sigma_{4k-1},\sigma_{4k+1}} X_B^{\sigma_{4k},\sigma_{4k+2}} \Bigg) Z_B^{\sigma_1,\sigma_2} \Bigg(\prod_{k=1}^{(n-3)/4} Z_B^{\sigma_{4k-1},\sigma_{4k+1}} Z_B^{\sigma_{4k},\sigma_{4k+2}} \Bigg) |\psi\rangle \Bigg\| \leq 2n\sqrt{2\varepsilon_1} + (n-1)\sqrt{2\varepsilon_2}. \quad \text{(B.6)}$$

Proof. Noting that all the X_A^k pairwise commute and using the correlations of Eq. (5.53a) to swap Alice's observables with Bob's pair check observables,

$$\Bigg\| \Bigg(\prod_{k \neq n} Z_A^{\sigma_k} \Bigg) \Bigg(\prod_{k} X_A^{\sigma_k} \Bigg) |\psi\rangle - X_B^{\sigma_1,\sigma_2} \Bigg(\prod_{k=1}^{(n-3)/4} X_B^{\sigma_{4k-1},\sigma_{4k+1}} X_B^{\sigma_{4k},\sigma_{4k+2}} \Bigg) \Bigg(\prod_{k \neq n} Z_A^{\sigma_k} \Bigg) X_A^{\sigma_n} |\psi\rangle \Bigg\| \leq \frac{n-1}{2} \sqrt{2\varepsilon_2}. \quad \text{(B.7)}$$

Consider only the final part of the second term in Eq. (B.7). We can repeatedly apply the triangle inequality with Proposition 5.12 to write

$$\Bigg\| \Bigg(\prod_{k \neq n} Z_A^{\sigma_k} \Bigg) X_A^{\sigma_n} |\psi\rangle - X_{B,\sigma_n}^{\sigma_n} \Bigg(\prod_{k \neq n} Z_{B,\sigma_n}^{\sigma_k} \Bigg) |\psi\rangle \Bigg\| \leq n\sqrt{2\varepsilon_1}. \quad \text{(B.8)}$$

Since all of Bob's observables in this equation correspond to the same input, we can commute $X_{B,\sigma_n}^{\sigma_n}$ with the product to its right and then use Proposition 5.12 again to give

$$\Bigg\| \Bigg(\prod_{k \neq n} Z_A^{\sigma_k} \Bigg) X_A^{\sigma_n} |\psi\rangle - X_A^{\sigma_n} \Bigg(\prod_{k \neq n} Z_A^{\sigma_k} \Bigg) |\psi\rangle \Bigg\| \leq 2n\sqrt{2\varepsilon_1}. \quad \text{(B.9)}$$

Combining this with Eq. (B.7) via the triangle inequality yields

$$\Bigg\| \Bigg(\prod_{k \neq n} Z_A^{\sigma_k} \Bigg) \Bigg(\prod_{k} X_A^{\sigma_k} \Bigg) |\psi\rangle - X_A^{\sigma_n} X_B^{\sigma_1,\sigma_2} \Bigg(\prod_{k=1}^{(n-3)/4} X_B^{\sigma_{4k-1},\sigma_{4k+1}} X_B^{\sigma_{4k},\sigma_{4k+2}} \Bigg) \Bigg(\prod_{k \neq n} Z_A^{\sigma_k} \Bigg) |\psi\rangle \Bigg\| \leq 2n\sqrt{2\varepsilon_1} + \frac{n-1}{2} \sqrt{2\varepsilon_2}. \quad \text{(B.10)}$$

Finally, since all the Z_A^k pairwise commute, the correlations of Eq. (5.53b) imply

$$\left\| \left(\prod_{k\neq n} Z_A^{\sigma_k} \right) |\psi\rangle - Z_B^{\sigma_1,\sigma_2} \left(\prod_{k=1}^{(n-3)/4} Z_B^{\sigma_{4k-1},\sigma_{4k+1}} Z_B^{\sigma_{4k},\sigma_{4k+2}} \right) |\psi\rangle \right\| \leq \frac{n-1}{2} \sqrt{2\varepsilon_2}. \quad \text{(B.11)}$$

Combining this with the previous Eq. (B.10) using the triangle inequality yields the result. □

We now exhibit the full proof of Proposition 5.14 with nonzero correlation errors.

Proposition 5.14 (Anticommutation)**.** *For all $i \in \{1, \dots, n\}$ we have state-dependent anticommutation relations for unknown observables of Alice*

$$\left\| \left\{ X_A^i, Z_A^i \right\} |\psi\rangle \right\| \leq 3n\sqrt{2\varepsilon_0} + 2(n-1)\sqrt{2\varepsilon_2} + \left(\frac{13(n-1)}{2} + 17 \right) \sqrt{2\varepsilon_1}. \quad (5.66)$$

Furthermore, for all $j \in \{1, \dots, n\}$ distinct from i we have state-dependent anticommutation relations for Bob's check-round observables

$$\left\| \left\{ X_{B,i}^i, Z_{B,j}^i \right\} |\psi\rangle \right\| \leq 3n\sqrt{2\varepsilon_0} + 2(n-1)\sqrt{2\varepsilon_2} + \left(\frac{13(n-1)}{2} + 21 \right) \sqrt{2\varepsilon_1}. \quad (5.67)$$

Proof. Let $i \in \{1, \dots, n\}$ and let $\sigma_k = \sigma(k)$ for each $k \in \{1, \dots, n\}$, where σ is some permutation of $\{1, \dots, n\}$. Assume that σ is such that $\sigma_1 = i$. From the game correlations Eq. (5.51b) we have

$$\left\| \left(\prod_{k=2}^{n} Y_A^{\sigma_k} \right) |\psi\rangle + Z_B^{\overline{\sigma_1}} X_B^{\overline{\sigma_1}} |\psi\rangle \right\| \leq \sqrt{2\varepsilon_0}. \quad \text{(B.12)}$$

Again, from the same correlations,

$$\left\| \left(\prod_{k=2}^{n} Z_B^{\overline{\sigma_k}} X_B^{\overline{\sigma_k}} \right) |\psi\rangle + Z_B^{\overline{\sigma_1}} X_B^{\overline{\sigma_1}} |\psi\rangle \right\| \leq n\sqrt{2\varepsilon_0}, \quad \text{(B.13)}$$

where the sign of the first term uses that n is odd. Now using the game correlations Eq. (5.51a),

$$\left\| \left(\prod_{k=2}^{n-1} Z_B^{\overline{\sigma_k}} X_B^{\overline{\sigma_k}} \right) Z_B^{\overline{\sigma_n}} \left(\prod_{k\neq n} X_A^{\sigma_k} \right) |\psi\rangle + Z_B^{\overline{\sigma_1}} \left(\prod_{k\neq 1} X_A^{\sigma_k} \right) |\psi\rangle \right\| \leq (n+2)\sqrt{2\varepsilon_0}. \quad \text{(B.14)}$$

Multiplying on the left by the unitary operators $\prod_{k\neq n} X_A^{\sigma_k}$ and $Z_B^{\overline{\sigma_2}}$ leaves the norm unchanged and gives

$$\left\| X_B^{\overline{\sigma_2}} \left(\prod_{k=3}^{n-1} Z_B^{\overline{\sigma_k}} X_B^{\overline{\sigma_k}} \right) Z_B^{\overline{\sigma_n}} |\psi\rangle + Z_B^{\overline{\sigma_2}} Z_B^{\overline{\sigma_1}} X_A^{\sigma_n} X_A^{\sigma_1} |\psi\rangle \right\| \leq (n+2)\sqrt{2\varepsilon_0}. \quad \text{(B.15)}$$

Rewriting this by commuting those X and Z observables within each term of the product with k odd results in

$$\left\| \left(\prod_{k=1}^{(n-3)/2} X_B^{\overline{\sigma_{2k}}} X_B^{\overline{\sigma_{2k+1}}} Z_B^{\overline{\sigma_{2k+1}}} Z_B^{\overline{\sigma_{2k+2}}} \right) X_B^{\overline{\sigma_{n-1}}} Z_B^{\overline{\sigma_n}} |\psi\rangle \right. \\ \left. + Z_B^{\overline{\sigma_2}} Z_B^{\overline{\sigma_1}} X_A^{\sigma_n} X_A^{\sigma_1} |\psi\rangle \right\| \leq (n+2)\sqrt{2\varepsilon_0}. \quad \text{(B.16)}$$

Using the correlations of Eqs. (5.51a) and (5.51c) to swap Bob's observables to Alice's side (and freely inserting the identity operator as $X_A^{\sigma_{n-1}} X_A^{\sigma_{n-1}}$ into the resulting first term) yields

$$\left\| \left(\prod_{k \neq n} Z_A^{\sigma_k} \right) \left(\prod_k X_A^{\sigma_k} \right) \left(\prod_{k=1}^{(n-3)/2} X_A^{\sigma_{n-2k+1}} Z_A^{\sigma_{n-2k+1}} Z_A^{\sigma_{n-2k}} X_A^{\sigma_{n-2k}} \right) X_A^{\sigma_2} |\psi\rangle \right. \\ \left. + X_A^{\sigma_n} X_A^{\sigma_1} Z_A^{\sigma_1} Z_A^{\sigma_2} |\psi\rangle \right\| \leq 3n\sqrt{2\varepsilon_0}. \quad \text{(B.17)}$$

Now notice from the correlations of Eq. (5.52) we have the estimate

$$\left\| X_A^{\sigma_2} Z_{B,\sigma_n}^{\sigma_1} Z_{B,\sigma_n}^{\sigma_2} X_{B,\sigma_n}^{\sigma_n} X_{B,\sigma_1}^{\sigma_1} |\psi\rangle - X_{B,\sigma_n}^{\sigma_n} Z_B^{\sigma_1,\sigma_2} X_B^{\sigma_1,\sigma_2} |\psi\rangle \right\| \leq 3\sqrt{2\varepsilon_1} + 2\sqrt{2\varepsilon_2}, \quad \text{(B.18)}$$

where we achieved this by commuting $X_{B,\sigma_n}^{\sigma_n}$ with other observables of the same input and converting local check observables to observables of Alice and then to pair check observables. Hence multiplying Eq. (B.17) on the left by $Z_{B,\sigma_n}^{\sigma_1} Z_{B,\sigma_n}^{\sigma_2} X_{B,\sigma_n}^{\sigma_n} X_{B,\sigma_1}^{\sigma_1}$, applying Eq. (B.18) via the triangle inequality in its first term (commuting the resulting observables for Bob with the existing observables of Alice), and in its second term using the correlations of Eq. (5.52),

$$\left\| X_{B,\sigma_n}^{\sigma_n} Z_B^{\sigma_1,\sigma_2} X_B^{\sigma_1,\sigma_2} \left(\prod_{k \neq n} Z_A^{\sigma_k} \right) \left(\prod_k X_A^{\sigma_k} \right) \right. \\ \left(\prod_{k=1}^{(n-3)/2} X_A^{\sigma_{n-2k+1}} Z_A^{\sigma_{n-2k+1}} Z_A^{\sigma_{n-2k}} X_A^{\sigma_{n-2k}} \right) |\psi\rangle + \left(X_A^{\sigma_n} X_A^{\sigma_1} Z_A^{\sigma_1} Z_A^{\sigma_2} \right)^2 |\psi\rangle \Big\| \\ \leq 3n\sqrt{2\varepsilon_0} + 7\sqrt{2\varepsilon_1} + 2\sqrt{2\varepsilon_2}. \quad \text{(B.19)}$$

Since $n \equiv 3 \pmod 4$, we can consider successive pairs of terms in the final product of Eq. (B.19). We can estimate each pair of terms using pair check observables by repeatedly applying the estimate of Lemma B.1 in the first term and commuting the

resulting observables of Bob with those of Alice. This gives

$$\Bigg\| X_{B,\sigma_n}^{\sigma_n} Z_B^{\sigma_1,\sigma_2} X_B^{\sigma_1,\sigma_2} \Bigg(\prod_{k=1}^{(n-3)/4} X_B^{\sigma_{4k-1},\sigma_{4k+1}} Z_B^{\sigma_{4k-1},\sigma_{4k+1}} Z_B^{\sigma_{4k},\sigma_{4k+2}} X_B^{\sigma_{4k},\sigma_{4k+2}} \Bigg) \Bigg(\prod_{k\neq n} Z_A^{\sigma_k} \Bigg) \Bigg(\prod_{k} X_A^{\sigma_k} \Bigg) |\psi\rangle + \left(X_A^{\sigma_n} X_A^{\sigma_1} Z_A^{\sigma_1} Z_A^{\sigma_2}\right)^2 |\psi\rangle \Bigg\| \leq 3n\sqrt{2\varepsilon_0} + \left(\frac{9(n-3)}{2} + 7\right)\sqrt{2\varepsilon_1} + (n-1)\sqrt{2\varepsilon_2}. \quad \text{(B.20)}$$

We may assume the permutation σ to in fact be such that all pair check observables appearing in Eq. (B.6) of Lemma B.2 and Eq. (B.20) correspond to the same (pair check round) input for Bob. This is compatible with an honest behavior (in which pair check observables correspond to pairs of Pauli observables) since all of these observables $M_B^{l,m}$ (where M represents either X or Z) have either disjoint or identical indices to all others. Specifically, referring to the definition [see Eq. (5.45)] of Bob's observables to be measured upon an input y when $c = 2$, we may assume they all correspond to the input $y = \sigma_n$, in which qubit σ_n is not to be tested. Therefore, after applying the estimate of Lemma B.2 to the first term in Eq. (B.20), we may freely commute all pair check observables and use their involutory property to achieve many cancellations. This yields

$$\left\| X_A^{\sigma_n} X_{B,\sigma_n}^{\sigma_n} |\psi\rangle + \left(X_A^{\sigma_n} X_A^{\sigma_1} Z_A^{\sigma_1} Z_A^{\sigma_2}\right)^2 |\psi\rangle \right\| \leq 3n\sqrt{2\varepsilon_0} + \frac{13(n-1)}{2}\sqrt{2\varepsilon_1} + 2(n-1)\sqrt{2\varepsilon_2}. \quad \text{(B.21)}$$

Applying the correlations of Eq. (5.52a) once in the first term and then multiplying on the left by $Z_A^{\sigma_2} Z_A^{\sigma_1} X_A^{\sigma_1} X_A^{\sigma_n}$ gives

$$\left\| \left\{ X_A^{\sigma_1} X_A^{\sigma_n}, Z_A^{\sigma_1} Z_A^{\sigma_2} \right\} |\psi\rangle \right\| \leq 3n\sqrt{2\varepsilon_0} + \left(\frac{13(n-1)}{2} + 1\right)\sqrt{2\varepsilon_1} + 2(n-1)\sqrt{2\varepsilon_2}. \quad \text{(B.22)}$$

By identical argument to the proof of Proposition 5.8, but using Propositions 5.12 and 5.13 instead of Propositions 5.5 and 5.6 and using the bound of Eq. (B.22) in place of Lemma 5.7, this implies

$$\left\| \left\{ X_A^{\sigma_1}, Z_A^{\sigma_1} \right\} |\psi\rangle \right\| \leq 3n\sqrt{2\varepsilon_0} + \left(\frac{13(n-1)}{2} + 17\right)\sqrt{2\varepsilon_1} + 2(n-1)\sqrt{2\varepsilon_2}. \quad \text{(B.23)}$$

That $\sigma_1 = i$ yields the result of Eq. (5.66).

To obtain Eq. (5.67) we use Proposition 5.12 to write

$$\begin{aligned} \left\| \left\{ X_{B,i}^i, Z_{B,j}^i \right\} |\psi\rangle \right\| &\leq 4\sqrt{2\varepsilon_1} + \left\| \left\{ X_A^i, Z_A^i \right\} |\psi\rangle \right\| \\ &\leq 3n\sqrt{2\varepsilon_0} + \left(\frac{13(n-1)}{2} + 21\right)\sqrt{2\varepsilon_1} + 2(n-1)\sqrt{2\varepsilon_2}, \end{aligned} \quad \text{(B.24)}$$

where the final equality follows from Eq. (5.66) just proved. □

Appendix C

Estimation lemma

Proof of Lemma 6.3. First note that for any trace-class operator T we have $\|T\|_1 \leq \sqrt{\operatorname{rank}(T)}\|T\|_2$, where $\|T\|_2 = \sqrt{\operatorname{tr}(T^\dagger T)}$ denotes the Hilbert–Schmidt norm. Since $\operatorname{rank}(|u\rangle\langle u| - |v\rangle\langle v|) \leq 2$, we thus have

$$\||u\rangle\langle u| - |v\rangle\langle v|\|_1 \leq \sqrt{2}\||u\rangle\langle u| - |v\rangle\langle v|\|_2. \tag{C.1}$$

We then evaluate

$$\begin{aligned} 2\||u\rangle\langle u| - |v\rangle\langle v|\|_2^2 &= 2\operatorname{tr}\left[(|u\rangle\langle u| - |v\rangle\langle v|)^2\right] \\ &= 2\||u\rangle\|^4 + 2\||v\rangle\|^4 - 4|\langle u|v\rangle|^2. \end{aligned} \tag{C.2}$$

Using the definition of the norm induced by the inner product,

$$2|\langle u|v\rangle| \geq 2\,\mathfrak{Re}\,\langle u|v\rangle = \||u\rangle\|^2 + \||v\rangle\|^2 - \||u\rangle - |v\rangle\|^2. \tag{C.3}$$

For simplicity, let us adopt the notation

$$\delta = \||u\rangle - |v\rangle\|, \tag{C.4a}$$

$$M = \max\{\||u\rangle\|, \||v\rangle\|\}. \tag{C.4b}$$

Inserting Eq. (C.3) into Eq. (C.2) and using that $\||u\rangle\|^2 + \||v\rangle\|^2 \leq 2M^2$, we have

$$2\||u\rangle\langle u| - |v\rangle\langle v|\|_2^2 \leq \left(\||u\rangle\|^2 - \||v\rangle\|^2\right)^2 + 4M^2\delta^2 - \delta^4. \tag{C.5}$$

It can be seen (similarly to the reverse triangle inequality) that

$$\left|\||u\rangle\|^2 - \||v\rangle\|^2\right| \leq \||u\rangle - |v\rangle\|^2 + 2\max(\||u\rangle\|, \||v\rangle\|)\||u\rangle - |v\rangle\|. \tag{C.6}$$

Inserting this into the previous equation gives

$$2\||u\rangle\langle u| - |v\rangle\langle v|\|_2^2 \leq 8M^2\delta^2 + 4M\delta^3. \tag{C.7}$$

Since $\||u\rangle\| \leq 1$ and $\||v\rangle\| \leq 1$, the triangle inequality implies $\delta \leq 2$, and so $\delta^3 \leq 2\delta^2$. We thus have

$$2\||u\rangle\langle u| - |v\rangle\langle v|\|_2^2 \leq 8\big(M^2 + M\big)\delta^2. \tag{C.8}$$

Combining this with Eq. (C.1) gives

$$\||u\rangle\langle u| - |v\rangle\langle v|\|_1 \leq \delta\sqrt{8\big(M^2 + M\big)}. \tag{C.9}$$

Finally, since by assumption $0 \leq M \leq 1$, we get

$$\||u\rangle\langle u| - |v\rangle\langle v|\|_1 \leq 4\delta \tag{C.10}$$

as required. □

Appendix D

Post-measurement robustness probability

Proof of Lemma 6.2. For the case where $\delta = 0$, it is clear from Eq. (6.10) that for all $\sigma \in \Sigma$ satisfying $\pi(\sigma) > 0$ we have $|u_\sigma^\omega\rangle = |v_\sigma^\omega\rangle$ for all $\omega \in \Omega$, and thus we have that $\Pr(D \leq 0) = 1$. We may henceforth assume that $\delta > 0$. First, let us introduce a new random variable N on $\Sigma \times \Omega$ defined as

$$N(\sigma,\omega) = \begin{cases} \| |\hat{u}_\sigma^\omega\rangle - |\hat{v}_\sigma^\omega\rangle \| & \text{if } p(\sigma,\omega) > 0, \\ 0 & \text{if } p(\sigma,\omega) = 0. \end{cases} \tag{D.1}$$

Let $a > 0$. By Lemma 6.3 we have $D(\sigma,\omega) \leq N(\sigma,\omega)$ for all $\sigma \in \Sigma$ and $\omega \in \Omega$, and thus

$$\Pr(D \geq a) \leq \Pr(N \geq a). \tag{D.2}$$

We now bound the expected value of N^2. We evaluate

$$\begin{aligned} \mathbb{E}\left(N^2\right) &= \sum_{\sigma\in\Sigma} \pi(\sigma) \sum_{\omega\in\Omega} p_\sigma(\omega) N(\sigma,\omega)^2 \\ &= \sum_{\sigma\in\Sigma} \pi(\sigma) \sum_{\omega\in\Omega} \| |u_\sigma^\omega\rangle \|^2 \cdot N(\sigma,\omega)^2 \\ &= \sum_{\sigma\in\Sigma} \pi(\sigma) \sum_{\omega\in\Omega} \left\| |u_\sigma^\omega\rangle - \| |u_\sigma^\omega\rangle \| |\hat{v}_\sigma^\omega\rangle \right\|^2 \end{aligned} \tag{D.3}$$

Now note that

$$\begin{aligned} \left\| \| |u_\sigma^\omega\rangle \| |\hat{v}_\sigma^\omega\rangle - |v_\sigma^\omega\rangle \right\| &= \left| \| |u_\sigma^\omega\rangle \| - \| |v_\sigma^\omega\rangle \| \right| \\ &\leq \| |u_\sigma^\omega\rangle - |v_\sigma^\omega\rangle \|, \end{aligned} \tag{D.4}$$

where we have used the reverse triangle inequality. Starting with the triangle inequality, we can then write for the terms of Eq. (D.3) that

$$\begin{aligned}\left\| |u_\sigma^\omega\rangle - \| |u_\sigma^\omega\rangle \| |\hat{v}_\sigma^\omega\rangle \right\| &\leq \| |u_\sigma^\omega\rangle - |v_\sigma^\omega\rangle \| + \left\| |v_\sigma^\omega\rangle - \| |u_\sigma^\omega\rangle \| |\hat{v}_\sigma^\omega\rangle \right\| \\ &\leq 2 \| |u_\sigma^\omega\rangle - |v_\sigma^\omega\rangle \|,\end{aligned} \tag{D.5}$$

where the final inequality uses Eq. (D.4). We thus have

$$\mathbb{E}\left(N^2\right) \leq 4 \sum_{\sigma \in \Sigma} \pi(\sigma) \sum_{\omega \in \Omega} \| |u_\sigma^\omega\rangle - |v_\sigma^\omega\rangle \|^2 \leq 4\delta^2, \tag{D.6}$$

where the final inequality comes from the assumption of Eq. (6.10). Markov's inequality states that

$$\begin{aligned}\Pr(N \geq a) &= \Pr\left(N^2 \geq a^2\right) \\ &\leq \frac{1}{a^2} \mathbb{E}\left(N^2\right).\end{aligned} \tag{D.7}$$

Combining this with Eqs. (D.2) and (D.6) gives

$$\Pr(\boldsymbol{D} \geq a) \leq \frac{4\delta^2}{a^2}. \tag{D.8}$$

Taking complements yields

$$\Pr(\boldsymbol{D} \leq a) \geq \Pr(\boldsymbol{D} < a) \geq 1 - \frac{4\delta^2}{a^2}. \tag{D.9}$$

Finally, choosing the parameter $a = \delta^c$ gives the desired result. □

Appendix E

Single-copy self-test

Here, we exhibit a proof of Proposition 6.7 in the ideal case that $\eta = 0$. The robust case of $\eta > 0$ is discussed in Appendix F.

Proof of Proposition 6.7 (ideal case). We first consider the isometry applied to the state $|\psi\rangle_{\mathcal{AB}}$. After the "swap" stage of the circuit, given by W, we have the state

$$\begin{aligned} W|\psi\rangle = \frac{1}{4}[&|00\rangle_{\mathcal{A}'\mathcal{B}'} \otimes (I - iS_2S_1)(I + iT_2T_1)|\psi\rangle \\ &+ |01\rangle_{\mathcal{A}'\mathcal{B}'} \otimes (I - iS_2S_1)T_1(I - iT_2T_1)|\psi\rangle \\ &+ |10\rangle_{\mathcal{A}'\mathcal{B}'} \otimes S_1(I + iS_2S_1)(I + iT_2T_1)|\psi\rangle \\ &+ |11\rangle_{\mathcal{A}'\mathcal{B}'} \otimes S_1(I + iS_2S_1)T_1(I - iT_2T_1)|\psi\rangle]. \end{aligned} \tag{E.1}$$

We now simplify this expression. Using the relations of the statement we can write

$$(I \pm iS_2S_1)(I \pm iT_2T_1)|\psi\rangle = 0. \tag{E.2}$$

Thus, the terms corresponding to ancilla states $|01\rangle_{\mathcal{A}'\mathcal{B}'}$ and $|10\rangle_{\mathcal{A}'\mathcal{B}'}$ vanish, and we are left with

$$\begin{aligned} W|\psi\rangle = \frac{1}{4}[&|00\rangle_{\mathcal{A}'\mathcal{B}'} \otimes (I - iS_2S_1)(I + iT_2T_1)|\psi\rangle \\ &+ |11\rangle_{\mathcal{A}'\mathcal{B}'} \otimes S_1(I + iS_2S_1)T_1(I - iT_2T_1)|\psi\rangle]. \end{aligned} \tag{E.3}$$

Using Relation 2, we have that

$$S_1(I + iS_2S_1)|\psi\rangle = (I - iS_2S_1)S_1|\psi\rangle, \tag{E.4a}$$

$$T_1(I - iT_2T_1)|\psi\rangle = (I + iT_2T_1)T_1|\psi\rangle. \tag{E.4b}$$

Thus, using these in addition to Relation 1 and the fact that our observables are involutory results in

$$W|\psi\rangle = |\Phi^+\rangle_{\mathcal{A}'\mathcal{B}'} \otimes \frac{1}{2\sqrt{2}}(I - iS_2S_1)(I + iT_2T_1)|\psi\rangle. \tag{E.5}$$

Using the relations, and again that our observables are involutory, the state simplifies to

$$W|\psi\rangle = |\Phi^+\rangle_{\mathcal{A}'\mathcal{B}'} \otimes |\varphi\rangle. \tag{E.6}$$

With this, we have now extracted the desired maximally entangled state from our initial unknown state. In a similar fashion, it can be shown that

$$WS_1|\psi\rangle = \sigma_{\mathrm{x}}^{\mathcal{B}'}|\Phi^+\rangle_{\mathcal{A}'\mathcal{B}'} \otimes |\varphi\rangle, \tag{E.7a}$$

$$WS_2|\psi\rangle = \sigma_{\mathrm{y}}^{\mathcal{B}'}|\Phi^+\rangle_{\mathcal{A}'\mathcal{B}'} \otimes |\varphi\rangle. \tag{E.7b}$$

Furthermore, although with a little more work (as this is the case where complex conjugation will later become relevant), it can be shown that

$$WS_2|\psi\rangle = \sigma_{\mathrm{z}}^{\mathcal{B}'}|\Phi^+\rangle_{\mathcal{A}'\mathcal{B}'} \otimes S_3|\varphi\rangle. \tag{E.8}$$

We now apply the "phase kickback" stage of the isometry, given by K, to the above simplified states. We suppress the extracted state of the primed ancillae in our notation, as it is entirely unaffected by K. When the state is $|\varphi\rangle$, this gives

$$\begin{aligned} K|\varphi\rangle = \frac{1}{4\sqrt{2}}[&|0\rangle_{\mathcal{A}''}|0\rangle_{\mathcal{B}''} \otimes (I+S_3)(I+T_3)(I+iT_2T_1)|\psi\rangle \\ &+ |0\rangle_{\mathcal{A}''}|1\rangle_{\mathcal{B}''} \otimes (I+S_3)(I-T_3)(I+iT_2T_1)|\psi\rangle \\ &+ |1\rangle_{\mathcal{A}''}|0\rangle_{\mathcal{B}''} \otimes (I-S_3)(I+T_3)(I+iT_2T_1)|\psi\rangle \\ &+ |1\rangle_{\mathcal{A}''}|1\rangle_{\mathcal{B}''} \otimes (I-S_3)(I-T_3)(I+iT_2T_1)|\psi\rangle]. \end{aligned} \tag{E.9}$$

We now simplify this expression. Since $S_3(I+iT_2T_1)|\psi\rangle = T_3(I+iT_2T_1)|\psi\rangle$ by Relations 1 and 2, and using that $(I\pm T_3)(I\pm T_3) = 2(I\pm T_3)$ and $(I\pm T_3)(I\mp T_3) = 0$, we get

$$K|\varphi\rangle = |0\rangle_{\mathcal{A}''}|0\rangle_{\mathcal{B}''} \otimes \frac{I+T_3}{2}|\varphi\rangle + |1\rangle_{\mathcal{A}''}|1\rangle_{\mathcal{B}''} \otimes \frac{I-T_3}{2}|\varphi\rangle. \tag{E.10}$$

Otherwise, when the state is $S_3|\varphi\rangle$, we have

$$\begin{aligned} KS_3|\varphi\rangle = \frac{1}{4\sqrt{2}}[&|0\rangle_{\mathcal{A}''}|0\rangle_{\mathcal{B}''} \otimes (I+S_3)S_3(I+T_3)(I+iT_2T_1)|\psi\rangle \\ &+ |0\rangle_{\mathcal{A}''}|1\rangle_{\mathcal{B}''} \otimes (I+S_3)S_3(I-T_3)(I+iT_2T_1)|\psi\rangle \\ &+ |1\rangle_{\mathcal{A}''}|0\rangle_{\mathcal{B}''} \otimes (I-S_3)S_3(I+T_3)(I+iT_2T_1)|\psi\rangle \\ &+ |1\rangle_{\mathcal{A}''}|1\rangle_{\mathcal{B}''} \otimes (I-S_3)S_3(I-T_3)(I+iT_2T_1)|\psi\rangle]. \end{aligned} \tag{E.11}$$

Since S_3 is involutory, we have $(I+S_3)S_3 = (I+S_3)$ and $(I-S_3)S_3 = -(I-S_3)$. By the same argument as before, we arrive at

$$KS_3|\varphi\rangle = |0\rangle_{\mathcal{A}''}|0\rangle_{\mathcal{B}''} \otimes \frac{I+T_3}{2}|\varphi\rangle - |1\rangle_{\mathcal{A}''}|1\rangle_{\mathcal{B}''} \otimes \frac{I-T_3}{2}|\varphi\rangle. \tag{E.12}$$

Upon defining $|\xi_0\rangle$ and $|\xi_1\rangle$ as in the statement, we have now finished applying the isometries. □

Appendix F

Robustness of single-copy self-test

Here, we expand upon the proof of the ideal case in which $\eta = 0$ discussed in Appendix E. We fill in details concerning the robustness of that proof, extending it to handle also cases where $\eta > 0$, and thus achieving the full claim of Proposition 6.7.

Proof of Proposition 6.7 (robustness). Expanding the left-hand side of Eq. (E.2) and taking its norm gives

$$\begin{aligned}\|(I \pm iS_2S_1)(I \pm iT_2T_1)|\psi\rangle\| &= \|(I - S_2S_1T_2T_1)|\psi\rangle \pm i(S_2S_1 + T_2T_1)|\psi\rangle\| \\ &\leq \||\psi\rangle - S_2S_1T_2T_1|\psi\rangle\| + \|S_2S_1|\psi\rangle + T_2T_1|\psi\rangle\|.\end{aligned} \tag{F.1}$$

Using Relation 1 and that the observables are both unitary and involutory, we have

$$S_qT_q|\psi\rangle \overset{\eta}{\approx} S_qS_q|\psi\rangle = |\psi\rangle. \tag{F.2}$$

Since norms are preserved under unitary operations, we can then bound the norm of all the expressions

$$\begin{aligned}\||\psi\rangle - S_2S_1T_2T_1|\psi\rangle\| &= \|S_2S_1|\psi\rangle - T_1T_2|\psi\rangle\| \\ &= \|S_1T_1|\psi\rangle - S_2T_2|\psi\rangle\| \\ &\leq 2\eta.\end{aligned} \tag{F.3}$$

Now we have bounded the first term of Eq. (F.1). For the second term, using Relation 2 gives

$$S_2S_1|\psi\rangle + T_2T_1|\psi\rangle \overset{\eta}{\approx} S_2S_1|\psi\rangle - T_1T_2|\psi\rangle, \tag{F.4}$$

for which we have already bounded the norm. Thus,

$$\|S_2S_1|\psi\rangle + T_2T_1|\psi\rangle\| \leq 3\eta. \tag{F.5}$$

Combining Eqs. (F.1), (F.3) and (F.5), we arrive at a robust version of Eq. (E.2). That is

$$(I \pm iS_2S_1)(I \pm iT_2T_1)|\psi\rangle \overset{5\eta}{\approx} 0. \tag{F.6}$$

This immediately allows us to write a robust version of Eq. (E.3)

$$\begin{aligned} W|\psi\rangle \overset{5\eta/2}{\approx} \frac{1}{4}[&|00\rangle_{\mathcal{A}'\mathcal{B}'} \otimes (I - iS_2S_1)(I + iT_2T_1)|\psi\rangle \\ &+ |11\rangle_{\mathcal{A}'\mathcal{B}'} \otimes S_1(I + iS_2S_1)T_1(I - iT_2T_1)|\psi\rangle]. \end{aligned} \tag{F.7}$$

We now examine the second term of Eq. (F.7). We can write Eq. (E.4) robustly as

$$S_1(I + iS_2S_1)|\psi\rangle \overset{\eta}{\approx} (I - iS_2S_1)S_1|\psi\rangle, \tag{F.8a}$$

$$T_1(I - iT_2T_1)|\psi\rangle \overset{\eta}{\approx} (I + iT_2T_1)T_1|\psi\rangle. \tag{F.8b}$$

Now, since $\|S_1(I + iS_2S_1)\| \leq 2$, Eq. (F.8b) implies that

$$S_1(I + iS_2S_1)T_1(I - iT_2T_1)|\psi\rangle \overset{2\eta}{\approx} S_1(I + iS_2S_1)(I + iT_2T_1)T_1|\psi\rangle. \tag{F.9}$$

Similarly, since $\|(I + iT_2T_1)T_1\| \leq 2$, Eq. (F.8a) implies that

$$S_1(I + iS_2S_1)(I + iT_2T_1)T_1|\psi\rangle \overset{2\eta}{\approx} (I - iS_2S_1)S_1(I + iT_2T_1)T_1|\psi\rangle. \tag{F.10}$$

Finally, since $\|(I - iS_2S_1)(I + iT_2T_1)\| \leq 4$, Relation 1 implies that

$$(I - iS_2S_1)S_1(I + iT_2T_1)T_1|\psi\rangle \overset{4\eta}{\approx} (I - iS_2S_1)(I + iT_2T_1)|\psi\rangle. \tag{F.11}$$

Combining Eqs. (F.9) to (F.11) through the triangle inequality gives

$$S_1(I + iS_2S_1)T_1(I - iT_2T_1)|\psi\rangle \overset{8\eta}{\approx} (I - iS_2S_1)(I + iT_2T_1)|\psi\rangle. \tag{F.12}$$

We can now apply this to Eq. (F.7) to estimate $W|\psi\rangle$ by

$$W|\psi\rangle \overset{9\eta/2}{\approx} |\Phi^+\rangle_{\mathcal{A}'\mathcal{B}'} \otimes \frac{1}{2\sqrt{2}}(I - iS_2S_1)(I + iT_2T_1)|\psi\rangle. \tag{F.13}$$

Since $\|I + iT_2T_1\| \leq 2$, we have

$$\begin{aligned} (I - iS_2S_1)(I + iT_2T_1)|\psi\rangle &\overset{4\eta}{\approx} (I + iT_2T_1)(I - iT_1T_2)|\psi\rangle \\ &= (2I + iT_2T_1 - iT_1T_2)|\psi\rangle \\ &\overset{\eta}{\approx} 2(I + iT_2T_1)|\psi\rangle \\ &= 2\sqrt{2}|\varphi\rangle, \end{aligned} \tag{F.14}$$

where for the first line we used Eq. (F.3) and for the third line we used Relation 2. Thus, we can apply this to Eq. (F.13) to estimate $W|\psi\rangle$ by

$$\left\| W|\psi\rangle - |\Phi^+\rangle_{\mathcal{A}'\mathcal{B}'} \otimes |\varphi\rangle \right\| \leq \frac{1}{4}\left(18 + 5\sqrt{2}\right)\eta. \tag{F.15}$$

To estimate $WS_1|\psi\rangle$, we note that

$$(I - iS_2S_1)(I + iT_2T_1)S_1|\psi\rangle \overset{2\eta}{\approx} S_1(I + iS_2S_1)(I + iT_2T_1)|\psi\rangle, \tag{F.16a}$$

$$(I - iS_2S_1)T_1(I - iT_2T_1)S_1|\psi\rangle \overset{2\eta}{\approx} S_1(I + iS_2S_1)T_1(I - iT_2T_1)|\psi\rangle, \tag{F.16b}$$

$$S_1(I + iS_2S_1)(I + iT_2T_1)S_1|\psi\rangle \overset{2\eta}{\approx} (I - iS_2S_1)(I + iT_2T_1)|\psi\rangle, \tag{F.16c}$$

$$S_1(I + iS_2S_1)T_1(I - iT_2T_1)S_1|\psi\rangle \overset{2\eta}{\approx} (I - iS_2S_1)T_1(I - iT_2T_1)|\psi\rangle. \tag{F.16d}$$

Therefore, we have

$$\begin{aligned} W S_1|\psi\rangle \overset{2\eta}{\approx} \frac{1}{4}[&|00\rangle_{\mathcal{A}'\mathcal{B}'} \otimes S_1(I + iS_2S_1)(I + iT_2T_1)|\psi\rangle \\ &+ |01\rangle_{\mathcal{A}'\mathcal{B}'} \otimes S_1(I + iS_2S_1)T_1(I - iT_2T_1)|\psi\rangle \\ &+ |10\rangle_{\mathcal{A}'\mathcal{B}'} \otimes (I - iS_2S_1)(I + iT_2T_1)|\psi\rangle \\ &+ |11\rangle_{\mathcal{A}'\mathcal{B}'} \otimes (I - iS_2S_1)T_1(I - iT_2T_1)|\psi\rangle]. \end{aligned} \tag{F.17}$$

The right-hand side of this equation is just that of Eq. (E.1) but with different states in $\mathcal{A}' \otimes \mathcal{B}'$ identifying each term of the superposition. Considering this, we can use the same robustness arguments as before to deduce that

$$\left\| W S_1|\psi\rangle - \sigma_{\mathrm{x}}^{\mathcal{B}'} |\Phi^+\rangle_{\mathcal{A}'\mathcal{B}'} \otimes |\varphi\rangle \right\| \leq \frac{1}{4}\left(26 + 5\sqrt{2}\right)\eta. \tag{F.18}$$

To estimate $WS_2|\psi\rangle$, we note that

$$(I - iS_2S_1)(I + iT_2T_1)S_2|\psi\rangle \overset{4\eta}{\approx} iS_1(I + iS_2S_1)(I + iT_2T_1)|\psi\rangle, \tag{F.19a}$$

$$(I - iS_2S_1)T_1(I - iT_2T_1)S_2|\psi\rangle \overset{4\eta}{\approx} iS_1(I + iS_2S_1)T_1(I - iT_2T_1)|\psi\rangle, \tag{F.19b}$$

$$S_1(I + iS_2S_1)(I + iT_2T_1)S_2|\psi\rangle \overset{4\eta}{\approx} -i(I - iS_2S_1)(I + iT_2T_1)|\psi\rangle, \tag{F.19c}$$

$$S_1(I + iS_2S_1)T_1(I - iT_2T_1)S_2|\psi\rangle \overset{4\eta}{\approx} -i(I - iS_2S_1)T_1(I - iT_2T_1)S_2|\psi\rangle. \tag{F.19d}$$

Therefore, we have

$$\begin{aligned} W S_2|\psi\rangle \overset{4\eta}{\approx} \frac{1}{4}[&i|00\rangle_{\mathcal{A}'\mathcal{B}'} \otimes S_1(I + iS_2S_1)(I + iT_2T_1)|\psi\rangle \\ &+ i|01\rangle_{\mathcal{A}'\mathcal{B}'} \otimes S_1(I + iS_2S_1)T_1(I - iT_2T_1)|\psi\rangle \\ &- i|10\rangle_{\mathcal{A}'\mathcal{B}'} \otimes (I - iS_2S_1)(I + iT_2T_1)|\psi\rangle \\ &- i|11\rangle_{\mathcal{A}'\mathcal{B}'} \otimes (I - iS_2S_1)T_1(I - iT_2T_1)|\psi\rangle]. \end{aligned} \tag{F.20}$$

Again, we can use the same robustness arguments as before to deduce that

$$\left\| W S_2|\psi\rangle - \sigma_{\mathrm{y}}^{\mathcal{B}'} |\Phi^+\rangle_{\mathcal{A}'\mathcal{B}'} \otimes |\varphi\rangle \right\| \leq \frac{1}{4}\left(34 + 5\sqrt{2}\right)\eta. \tag{F.21}$$

The final case of estimating $W S_3|\psi\rangle$ requires a little more care. By repeatedly applying Relation 2, it can be shown that

$$(I - iS_2S_1)(I + iT_2T_1)S_3|\psi\rangle \overset{8\eta}{\approx} S_3(I - iS_2S_1)(I + iT_2T_1)|\psi\rangle, \tag{F.22a}$$

$$(I - iS_2S_1)T_1(I - iT_2T_1)S_3|\psi\rangle \overset{8\eta}{\approx} S_3(I - iS_2S_1)T_1(I - iT_2T_1)|\psi\rangle, \tag{F.22b}$$

$$S_1(I + iS_2S_1)(I + iT_2T_1)S_3|\psi\rangle \overset{16\eta}{\approx} -S_3S_1(I + iS_2S_1)(I + iT_2T_1)|\psi\rangle, \tag{F.22c}$$

$$S_1(I + iS_2S_1)T_1(I - iT_2T_1)S_3|\psi\rangle \overset{16\eta}{\approx} -S_3S_1(I + iS_2S_1)T_1(I - iT_2T_1)|\psi\rangle. \tag{F.22d}$$

Therefore, we have

$$\begin{aligned} W S_3|\psi\rangle \overset{12\eta}{\approx} \frac{1}{4}[&|00\rangle_{\mathcal{A}'\mathcal{B}'} \otimes S_3(I - iS_2S_1)(I + iT_2T_1)|\psi\rangle \\ &+ |01\rangle_{\mathcal{A}'\mathcal{B}'} \otimes S_3(I - iS_2S_1)T_1(I - iT_2T_1)|\psi\rangle \\ &- |10\rangle_{\mathcal{A}'\mathcal{B}'} \otimes S_3S_1(I + iS_2S_1)(I + iT_2T_1)|\psi\rangle \\ &- |11\rangle_{\mathcal{A}'\mathcal{B}'} \otimes S_3S_1(I + iS_2S_1)T_1(I - iT_2T_1)|\psi\rangle]. \end{aligned} \tag{F.23}$$

We can use the same robustness arguments as before (but this time being careful to note that each estimate is unaffected by the presence of the observables S_3 as it is unitary) to deduce that

$$\left\| W S_3|\psi\rangle - \sigma_{\mathrm{z}}^{\mathcal{B}'} |\Phi^+\rangle_{\mathcal{A}'\mathcal{B}'} \otimes S_3|\varphi\rangle \right\| \leq \frac{1}{4}\left(66 + 5\sqrt{2}\right)\eta. \tag{F.24}$$

For the robust phase kickback stage, first note that by Relations 1 and 2 we have

$$S_3(I + iT_2T_1)|\psi\rangle \overset{6\eta}{\approx} T_3(I + iT_2T_1)|\psi\rangle. \tag{F.25}$$

Using also that $(I \pm T_3)(I \pm T_3) = 2(I \pm T_3)$ and $(I \pm T_3)(I \mp T_3) = 0$, we get

$$(I \pm S_3)(I \pm T_3)(I + iT_2T_1)|\psi\rangle \overset{12\eta}{\approx} 2(I \pm T_3)(I + iT_2T_1)|\psi\rangle, \tag{F.26a}$$

$$(I \pm S_3)(I \mp T_3)(I + iT_2T_1)|\psi\rangle \overset{12\eta}{\approx} 0. \tag{F.26b}$$

Therefore, in place of Eq. (E.10), we have the robust version

$$K|\varphi\rangle \overset{6\sqrt{2}\eta}{\approx} |0\rangle_{\mathcal{A}''}|0\rangle_{\mathcal{B}''} \otimes \frac{I + T_3}{2}|\varphi\rangle + |1\rangle_{\mathcal{A}''}|1\rangle_{\mathcal{B}''} \otimes \frac{I - T_3}{2}|\varphi\rangle. \tag{F.27}$$

In order to estimate $KS_3|\varphi\rangle$, we use (as in the ideal case) that $(I + S_3)S_3 = (I + S_3)$ and $(I - S_3)S_3 = -(I - S_3)$. A robust version of Eq. (E.12) given by

$$KS_3|\varphi\rangle \overset{6\sqrt{2}\eta}{\approx} |0\rangle_{\mathcal{A}''}|0\rangle_{\mathcal{B}''} \otimes \frac{I + T_3}{2}|\varphi\rangle - |1\rangle_{\mathcal{A}''}|1\rangle_{\mathcal{B}''} \otimes \frac{I - T_3}{2}|\varphi\rangle \tag{F.28}$$

is then immediate by identical argument to before. □

Appendix G

Many-copy self-test

Before exhibiting the proof of Theorem 6.9, we show the following lemma that will be used repeatedly to cancel terms corresponding to correlated complex conjugation of reference measurements at only some (but not all) positions. We note that a similar argument was also used in [116, Appendix E] in part of a proof of an analogous result.

Lemma G.1. *Let $|\psi\rangle \in \mathcal{A} \otimes \mathcal{B}$. Suppose for each $q \in \{1,2,3\}$ and $j \in \{1,\dots,n\}$ that there exist ± 1-outcome observables $S_q^{(j)}$ on $\mathcal{A}$ and $T_q^{(j)}$ on $\mathcal{B}$ satisfying (for some $\eta \geq 0$) the following relations:*

1. $\left(S_q^{(j)} - T_q^{(j)}\right)|\psi\rangle \overset{\eta}{\approx} 0$ *for all q and j.*
2. $\left\{S_q^{(j)}, S_r^{(j)}\right\}|\psi\rangle \overset{\eta}{\approx} 0$ *and* $\left\{T_q^{(j)}, T_r^{(j)}\right\}|\psi\rangle \overset{\eta}{\approx} 0$ *for all q, r and j such that $q \neq r$.*
3. $\left[S_q^{(j)}, S_r^{(k)}\right]|\psi\rangle \overset{\eta}{\approx} 0$ *and* $\left[T_q^{(j)}, T_r^{(k)}\right]|\psi\rangle \overset{\eta}{\approx} 0$ *for all q, r and j, k such that $j \neq k$.*

For all $j < n$, if (emulating the conclusion of Proposition 6.23) it also holds that

$$\left(I + S_1^{(j)} S_1^{(j+1)} S_2^{(j)} S_2^{(j+1)} S_3^{(j)} S_3^{(j+1)}\right)|\psi\rangle \overset{\eta}{\approx} 0, \tag{G.1}$$

then we have

$$\left(I \pm T_3^{(j)}\right)\left(I + iT_2^{(j)}T_1^{(j)}\right)\left(I \mp T_3^{(j+1)}\right)\left(I + iT_2^{(j+1)}T_1^{(j+1)}\right)|\psi\rangle \overset{118\eta}{\approx} 0. \tag{G.2}$$

Proof. The left-hand side of Eq. (G.2) can be expanded and then rewritten by grouping

pairs of terms as

$$\begin{aligned}
&\left(I + T_3^{(j)}T_2^{(j)}T_1^{(j)}T_3^{(j+1)}T_2^{(j+1)}T_1^{(j+1)}\right)|\psi\rangle \\
&\mp \left(T_3^{(j+1)} + T_3^{(j)}T_2^{(j)}T_1^{(j)}T_2^{(j+1)}T_1^{(j+1)}\right)|\psi\rangle \\
&+ i\left(T_2^{(j+1)}T_1^{(j+1)} - T_3^{(j)}T_2^{(j)}T_1^{(j)}T_3^{(j+1)}\right)|\psi\rangle \\
&\pm i\left(T_3^{(j)}T_2^{(j+1)}T_1^{(j+1)} - T_2^{(j)}T_1^{(j)}T_3^{(j+1)}\right)|\psi\rangle \\
&\mp i\left(T_3^{(j+1)}T_2^{(j+1)}T_1^{(j+1)} - T_3^{(j)}T_2^{(j)}T_1^{(j)}\right)|\psi\rangle \\
&- \left(T_2^{(j)}T_1^{(j)}T_2^{(j+1)}T_1^{(j+1)} + T_3^{(j)}T_3^{(j+1)}\right)|\psi\rangle \\
&- i\left(T_3^{(j)}T_3^{(j+1)}T_2^{(j+1)}T_1^{(j+1)} - T_2^{(j)}T_1^{(j)}\right)|\psi\rangle \\
&\pm \left(T_2^{(j)}T_1^{(j)}T_3^{(j+1)}T_2^{(j+1)}T_1^{(j+1)} + T_3^{(j)}\right)|\psi\rangle.
\end{aligned} \tag{G.3}$$

By applying the given relations to Eq. (G.1), it can be seen that each of the eight resulting terms approximately vanishes. Specifically, we have

$$\left(I + T_3^{(j)}T_2^{(j)}T_1^{(j)}T_3^{(j+1)}T_2^{(j+1)}T_1^{(j+1)}\right)|\psi\rangle \overset{15\eta}{\approx} 0, \tag{G.4a}$$

$$\left(T_3^{(j+1)} + T_3^{(j)}T_2^{(j)}T_1^{(j)}T_2^{(j+1)}T_1^{(j+1)}\right)|\psi\rangle \overset{10\eta}{\approx} 0, \tag{G.4b}$$

$$\left(T_2^{(j+1)}T_1^{(j+1)} - T_3^{(j)}T_2^{(j)}T_1^{(j)}T_3^{(j+1)}\right)|\psi\rangle \overset{17\eta}{\approx} 0, \tag{G.4c}$$

$$\left(T_3^{(j)}T_2^{(j+1)}T_1^{(j+1)} - T_2^{(j)}T_1^{(j)}T_3^{(j+1)}\right)|\psi\rangle \overset{17\eta}{\approx} 0, \tag{G.4d}$$

$$\left(T_3^{(j+1)}T_2^{(j+1)}T_1^{(j+1)} - T_3^{(j)}T_2^{(j)}T_1^{(j)}\right)|\psi\rangle \overset{17\eta}{\approx} 0, \tag{G.4e}$$

$$\left(T_2^{(j)}T_1^{(j)}T_2^{(j+1)}T_1^{(j+1)} + T_3^{(j)}T_3^{(j+1)}\right)|\psi\rangle \overset{10\eta}{\approx} 0, \tag{G.4f}$$

$$\left(T_3^{(j)}T_3^{(j+1)}T_2^{(j+1)}T_1^{(j+1)} - T_2^{(j)}T_1^{(j)}\right)|\psi\rangle \overset{17\eta}{\approx} 0, \tag{G.4g}$$

$$\left(T_2^{(j)}T_1^{(j)}T_3^{(j+1)}T_2^{(j+1)}T_1^{(j+1)} + T_3^{(j)}\right)|\psi\rangle \overset{15\eta}{\approx} 0. \tag{G.4h}$$

The triangle inequality then gives Eq. (G.2), as required. □

We now proceed with the main body of proof for Theorem 6.9.

Proof of Theorem 6.9. Consider the isometry and the corresponding notation introduced in Fig. 6.3. We begin by considering, for any $j \in \{1, \dots, n\}$, the action of the isometry $V^{(j)}$. For this, Proposition 6.7 shows that after the "swap" stage of the circuit,

given by $W^{(j)}$, we have that

$$W^{(j)}|\psi\rangle = |\Phi^+\rangle_{\mathcal{A}'_j\mathcal{B}'_j} \otimes \frac{1}{\sqrt{2}}\Big(I + iT_2^{(j)}T_1^{(j)}\Big)|\psi\rangle, \tag{G.5a}$$

$$W^{(j)}S_1^{(j)}|\psi\rangle = \sigma_{\mathrm{x}}^{\mathcal{B}'_j}|\Phi^+\rangle_{\mathcal{A}'_j\mathcal{B}'_j} \otimes \frac{1}{\sqrt{2}}\Big(I + iT_2^{(j)}T_1^{(j)}\Big)|\psi\rangle, \tag{G.5b}$$

$$W^{(j)}S_2^{(j)}|\psi\rangle = \sigma_{\mathrm{y}}^{\mathcal{B}'_j}|\Phi^+\rangle_{\mathcal{A}'_j\mathcal{B}'_j} \otimes \frac{1}{\sqrt{2}}\Big(I + iT_2^{(j)}T_1^{(j)}\Big)|\psi\rangle, \tag{G.5c}$$

$$W^{(j)}S_3^{(j)}|\psi\rangle = \sigma_{\mathrm{z}}^{\mathcal{B}'_j}|\Phi^+\rangle_{\mathcal{A}'_j\mathcal{B}'_j} \otimes \frac{1}{\sqrt{2}}S_3^{(j)}\Big(I + iT_2^{(j)}T_1^{(j)}\Big)|\psi\rangle, \tag{G.5d}$$

We now apply the "phase kickback" stage of the isometry, given by $K^{(j)}$, to the expressions of Eq. (G.5). To make clearer the resulting equations, let us suppress the extracted state of the primed ancillae in our notation for now, as it is entirely unaffected by the remainder of the isometry. For this purpose, let us define (similarly to Proposition 6.7)

$$\big|\varphi^j\big\rangle = \frac{1}{\sqrt{2}}\Big(I + iT_2^{(j)}T_1^{(j)}\Big)|\psi\rangle. \tag{G.6}$$

For Eqs. (G.5a) to (G.5c), Proposition 6.7 gives the action of $K^{(j)}$ as

$$\begin{aligned} K^{(j)}\big|\varphi^j\big\rangle = |0\rangle_{\mathcal{A}''_j}|0\rangle_{\mathcal{B}''_j} \otimes \frac{1}{2\sqrt{2}}\Big(I + T_3^{(j)}\Big)\Big(I + iT_2^{(j)}T_1^{(j)}\Big)|\psi\rangle \\ + |1\rangle_{\mathcal{A}''_j}|1\rangle_{\mathcal{B}''_j} \otimes \frac{1}{2\sqrt{2}}\Big(I - T_3^{(j)}\Big)\Big(I + iT_2^{(j)}T_1^{(j)}\Big)|\psi\rangle. \end{aligned} \tag{G.7}$$

For Eq. (G.5d), Proposition 6.7 gives the action of $K^{(j)}$ as

$$\begin{aligned} K^{(j)}S_3^{(j)}\big|\varphi^j\big\rangle = |0\rangle_{\mathcal{A}''_j}|0\rangle_{\mathcal{B}''_j} \otimes \frac{1}{2\sqrt{2}}\Big(I + T_3^{(j)}\Big)\Big(I + iT_2^{(j)}T_1^{(j)}\Big)|\psi\rangle \\ - |1\rangle_{\mathcal{A}''_j}|1\rangle_{\mathcal{B}''_j} \otimes \frac{1}{2\sqrt{2}}\Big(I - T_3^{(j)}\Big)\Big(I + iT_2^{(j)}T_1^{(j)}\Big)|\psi\rangle. \end{aligned} \tag{G.8}$$

We have now finished examining the action of $V^{(j)}$ on $|\psi\rangle$ and $S_q^{(j)}|\psi\rangle$.

Notice that Eqs. (G.7) and (G.8) have a form consistent with that required by the junk state of Eq. (6.42), however, we have only yet extracted a single copy of $|\Phi^+\rangle$. Suppressing the ancillae once again when convenient, we will examine the action of $V^{(j)}$ on two subnormalized states of a similar form to those contained in the two terms of Eqs. (G.7) and (G.8). Specifically, let us define for all $k \in \{1, \ldots, n\}$ the vectors

$$\big|\xi_{\pm}^k\big\rangle_{\mathcal{AB}} = \frac{1}{\Big(2\sqrt{2}\Big)^k}\prod_{j=1}^{k}\Big(I \pm T_3^{(j)}\Big)\Big(I + iT_2^{(j)}T_1^{(j)}\Big)|\psi\rangle_{\mathcal{AB}} = \prod_{j=1}^{k}J_{\pm}^{(j)}|\psi\rangle_{\mathcal{AB}}, \tag{G.9}$$

where

$$J_{\pm}^{(j)} = \frac{1}{2\sqrt{2}}\Big(I \pm T_3^{(j)}\Big)\Big(I + iT_2^{(j)}T_1^{(j)}\Big). \tag{G.10}$$

We note that, with this notation, we can now combine Eqs. (G.5a) to (G.5c) with Eq. (G.7) and Eq. (G.5d) with Eq. (G.8) to write

$$\begin{aligned} V^{(j)}|\psi\rangle = |\Phi^+\rangle_{\mathcal{A}_j'\mathcal{B}_j'} \otimes \Big(&|0\rangle_{\mathcal{A}_j''}|0\rangle_{\mathcal{B}_j''} \otimes J_+^{(j)}|\psi\rangle \\ &+ |1\rangle_{\mathcal{A}_j''}|1\rangle_{\mathcal{B}_j''} \otimes J_-^{(j)}|\psi\rangle\Big), \end{aligned} \tag{G.11a}$$

$$\begin{aligned} V^{(j)}S_q^{(j)}|\psi\rangle = \sigma_q^{\mathcal{B}_j'}|\Phi^+\rangle_{\mathcal{A}_j'\mathcal{B}_j'} \otimes \Big(&|0\rangle_{\mathcal{A}_j''}|0\rangle_{\mathcal{B}_j''} \otimes J_+^{(j)}|\psi\rangle \\ &+ (-1)^{[q=3]}|1\rangle_{\mathcal{A}_j''}|1\rangle_{\mathcal{B}_j''} \otimes J_-^{(j)}|\psi\rangle\Big). \end{aligned} \tag{G.11b}$$

In the special case of $j = 1$, since $\big|\xi_{\pm}^1\big\rangle = J_{\pm}^{(1)}|\psi\rangle$, we recover

$$V^{(1)}|\psi\rangle = |\Phi^+\rangle_{\mathcal{A}_1'\mathcal{B}_1'} \otimes \Big(|0\rangle_{\mathcal{A}_1''}|0\rangle_{\mathcal{B}_1''} \otimes \big|\xi_+^1\big\rangle + |1\rangle_{\mathcal{A}_1''}|1\rangle_{\mathcal{B}_1''} \otimes \big|\xi_-^1\big\rangle\Big), \tag{G.12a}$$

$$V^{(1)}S_q^{(1)}|\psi\rangle = \sigma_q^{\mathcal{B}_1'}|\Phi^+\rangle_{\mathcal{A}_1'\mathcal{B}_1'} \otimes \Big(|0\rangle_{\mathcal{A}_1''}|0\rangle_{\mathcal{B}_1''} \otimes \big|\xi_+^1\big\rangle + (-1)^{[q=3]}|1\rangle_{\mathcal{A}_1''}|1\rangle_{\mathcal{B}_1''} \otimes \big|\xi_-^1\big\rangle\Big). \tag{G.12b}$$

We now examine $V^{(k)}\big|\xi_{\pm}^{k-1}\big\rangle_{\mathcal{AB}}$, where $1 < k \leq n$. We begin by showing that

$$V_{\mathcal{B}}^{(k)}\big|\xi_{\pm}^{k-1}\big\rangle = \left(\prod_{j=1}^{k-1} J_{\pm}^{(j)}\right) V_{\mathcal{B}}^{(k)}|\psi\rangle. \tag{G.13}$$

To do this, notice by the definition of $V_{\mathcal{B}}^{(k)} = K_{\mathcal{B}}^{(k)}W_{\mathcal{B}}^{(k)}$ given in Fig. 6.3 that

$$\begin{aligned} V_{\mathcal{B}}^{(k)}|\psi\rangle = \frac{1}{4}\Big[&|0\rangle_{\mathcal{B}_k'} \otimes |0\rangle_{\mathcal{B}_k''} \otimes \Big(I + iT_2^{(k)}T_1^{(k)}\Big)|\psi\rangle \\ &+ |0\rangle_{\mathcal{B}_k'} \otimes |1\rangle_{\mathcal{B}_k''} \otimes T_3^{(k)}\Big(I + iT_2^{(k)}T_1^{(k)}\Big)|\psi\rangle \\ &+ |1\rangle_{\mathcal{B}_k'} \otimes |0\rangle_{\mathcal{B}_k''} \otimes T_1^{(k)}\Big(I - iT_2^{(k)}T_1^{(k)}\Big)|\psi\rangle \\ &+ |1\rangle_{\mathcal{B}_k'} \otimes |1\rangle_{\mathcal{B}_k''} \otimes T_3^{(k)}T_1^{(k)}\Big(I - iT_2^{(k)}T_1^{(k)}\Big)|\psi\rangle\Big]. \end{aligned} \tag{G.14}$$

After applying all the $J_{\pm}^{(j)}$ on the left and bringing operators with index k past all operators with other indices to the front via a chain of state-dependent commutation

and swapping operators between Alice and Bob (Relations 1 and 3) we get

$$\begin{aligned}\left(\prod_{j=1}^{k-1} J_{\pm}^{(j)}\right) V_{\mathcal{B}}^{(k)}|\psi\rangle = \frac{1}{4}\Big[&|0\rangle_{\mathcal{B}_k'} \otimes |0\rangle_{\mathcal{B}_k''} \otimes \left(I + iT_2^{(k)}T_1^{(k)}\right) \prod_{j=1}^{k-1} J_{\pm}^{(j)}|\psi\rangle \\ &+ |0\rangle_{\mathcal{B}_k'} \otimes |1\rangle_{\mathcal{B}_k''} \otimes T_3^{(k)}\left(I + iT_2^{(k)}T_1^{(k)}\right) \prod_{j=1}^{k-1} J_{\pm}^{(j)}|\psi\rangle \\ &+ |1\rangle_{\mathcal{B}_k'} \otimes |0\rangle_{\mathcal{B}_k''} \otimes T_1^{(k)}\left(I - iT_2^{(k)}T_1^{(k)}\right) \prod_{j=1}^{k-1} J_{\pm}^{(j)}|\psi\rangle \\ &+ |1\rangle_{\mathcal{B}_k'} \otimes |1\rangle_{\mathcal{B}_k''} \otimes T_3^{(k)}T_1^{(k)}\left(I - iT_2^{(k)}T_1^{(k)}\right) \prod_{j=1}^{k-1} J_{\pm}^{(j)}|\psi\rangle\Big].\end{aligned} \tag{G.15}$$

By Eq. (G.9), and again by the definition of $V_{\mathcal{B}}^{(k)}$, the right-hand side is simply $V_{\mathcal{B}}^{(k)}\left|\xi_{\pm}^{k-1}\right\rangle$. This is the desired Eq. (G.13). Since all $J_{\pm}^{(j)}$ act on Bob's subsystem, they commute with $V_{\mathcal{A}}^{(k)}$. We can then apply $V_{\mathcal{A}}^{(k)}$ to both sides of Eq. (G.13) to get

$$V^{(k)}\left|\xi_{\pm}^{k-1}\right\rangle = \left(\prod_{j=1}^{k-1} J_{\pm}^{(j)}\right) V^{(k)}|\psi\rangle. \tag{G.16}$$

Substituting Eq. (G.11a) for $V^{(k)}|\psi\rangle$ then gives

$$\begin{aligned}V^{(k)}\left|\xi_{\pm}^{k-1}\right\rangle = |\Phi^+\rangle_{\mathcal{A}_k'\mathcal{B}_k'} \otimes \left(\prod_{j=1}^{k-1} J_{\pm}^{(j)}\right)\Big(&|0\rangle_{\mathcal{A}_k''}|0\rangle_{\mathcal{B}_k''} \otimes J_{+}^{(k)}|\psi\rangle \\ &+ |1\rangle_{\mathcal{A}_k''}|1\rangle_{\mathcal{B}_k''} \otimes J_{-}^{(k)}|\psi\rangle\Big).\end{aligned} \tag{G.17}$$

Lemma G.1 implies

$$\left(I \pm T_3^{(k-1)}\right)\left(I + iT_2^{(k-1)}T_1^{(k-1)}\right)\left(I \mp T_3^{(k)}\right)\left(I + iT_2^{(k)}T_1^{(k)}\right)|\psi\rangle = 0 \tag{G.18}$$

which, rewriting in terms of the $J_{\pm}^{(j)}$, then implies

$$J_{\pm}^{(k-1)} J_{\mp}^{(k)}|\psi\rangle = 0. \tag{G.19}$$

Thus, using this to simplify Eq. (G.17), we have

$$V^{(k)}\left|\xi_{+}^{k-1}\right\rangle = |\Phi^+\rangle_{\mathcal{A}_k'\mathcal{B}_k'} \otimes |0\rangle_{\mathcal{A}_k''}|0\rangle_{\mathcal{B}_k''} \otimes \left|\xi_{+}^{k}\right\rangle, \tag{G.20a}$$

$$V^{(k)}\left|\xi_{-}^{k-1}\right\rangle = |\Phi^+\rangle_{\mathcal{A}_k'\mathcal{B}_k'} \otimes |1\rangle_{\mathcal{A}_k''}|1\rangle_{\mathcal{B}_k''} \otimes \left|\xi_{-}^{k}\right\rangle. \tag{G.20b}$$

By definition of $V_{\mathcal{A}}^{(k)}$,

$$\begin{aligned} V_{\mathcal{A}}^{(k)}|\psi\rangle = \frac{1}{4}\Big[& |0\rangle_{\mathcal{A}_k'} \otimes |0\rangle_{\mathcal{A}_k''} \otimes \left(I - iS_2^{(k)}S_1^{(k)}\right)|\psi\rangle \\ & + |0\rangle_{\mathcal{A}_k'} \otimes |1\rangle_{\mathcal{A}_k''} \otimes S_3^{(k)}\left(I - iS_2^{(k)}S_1^{(k)}\right)|\psi\rangle \\ & + |1\rangle_{\mathcal{A}_k'} \otimes |0\rangle_{\mathcal{A}_k''} \otimes S_1^{(k)}\left(I + iS_2^{(k)}S_1^{(k)}\right)|\psi\rangle \\ & + |1\rangle_{\mathcal{A}_k'} \otimes |1\rangle_{\mathcal{A}_k''} \otimes S_3^{(k)}S_1^{(k)}\left(I + iS_2^{(k)}S_1^{(k)}\right)|\psi\rangle\Big]. \end{aligned} \tag{G.21}$$

Therefore, using Relations 1 and 3, whenever $j \neq k$

$$V_{\mathcal{A}}^{(k)}S_q^{(j)}|\psi\rangle = S_q^{(j)}V_{\mathcal{A}}^{(k)}|\psi\rangle. \tag{G.22}$$

From this, it follows by noting $V_{\mathcal{B}}^k$ commutes with $S_q^{(j)}$ that

$$V^{(k)}S_q^{(j)}|\psi\rangle = S_q^{(j)}V^{(k)}|\psi\rangle. \tag{G.23}$$

A special case is (remembering that $1 < k \leq n$)

$$V^{(1)}S_q^{(k)}|\psi\rangle = S_q^{(k)}V^{(1)}|\psi\rangle. \tag{G.24}$$

Furthermore, again since $V_{\mathcal{A}}^k$ and $S_q^{(j)}$ defined on Alice's side commute with $V_{\mathcal{B}}^{(k)}$ and all $J_{\pm}^{(i)}$, and by applying Eq. (G.23),

$$\begin{aligned} V^{(k)}S_q^{(j)}\left|\xi_{\pm}^{k-1}\right\rangle &= \left(V_{\mathcal{B}}^{(k)}\prod_{i=1}^{k-1}J_{\pm}^{(i)}\right)V_{\mathcal{A}}^{(k)}S_q^{(j)}|\psi\rangle \\ &= \left(V_{\mathcal{B}}^{(k)}\prod_{i=1}^{k-1}J_{\pm}^{(i)}\right)S_q^{(j)}V_{\mathcal{A}}^{(k)}|\psi\rangle \\ &= S_q^{(j)}V^{(k)}\left|\xi_{\pm}^{k-1}\right\rangle. \end{aligned} \tag{G.25}$$

Finally, it follows similarly to Eq. (G.20) that

$$V^{(k)}S_q^{(k)}\left|\xi_{+}^{k-1}\right\rangle = \sigma_q^{\mathcal{B}_k'}|\Phi^+\rangle_{\mathcal{A}_k'\mathcal{B}_k'} \otimes |0\rangle_{\mathcal{A}_k''}|0\rangle_{\mathcal{B}_k''} \otimes \left|\xi_{+}^{k}\right\rangle, \tag{G.26a}$$

$$V^{(k)}S_q^{(k)}\left|\xi_{-}^{k-1}\right\rangle = (-1)^{[q=3]}\sigma_q^{\mathcal{B}_k'}|\Phi^+\rangle_{\mathcal{A}_k'\mathcal{B}_k'} \otimes |1\rangle_{\mathcal{A}_k''}|1\rangle_{\mathcal{B}_k''} \otimes \left|\xi_{-}^{k}\right\rangle. \tag{G.26b}$$

This is because acting with $S_q^{(k)}$ followed by $V_{\mathcal{A}}^{(k)}$ on both sides of Eq. (G.13) gives

$$V^{(k)}S_q^{(k)}\left|\xi_{\pm}^{k-1}\right\rangle = \left(\prod_{j=1}^{k-1}J_{\pm}^{(j)}\right)V^{(k)}S_q^{(k)}|\psi\rangle. \tag{G.27}$$

Substituting Eq. (G.11b) for $V^{(k)}S_q^{(k)}|\psi\rangle$ then gives

$$\begin{aligned} V^{(k)}S_q^{(k)}\left|\xi_{\pm}^{k-1}\right\rangle = \sigma_q^{\mathcal{B}_k'}|\Phi^+\rangle_{\mathcal{A}_k'\mathcal{B}_k'} \otimes \left(\prod_{j=1}^{k-1}J_{\pm}^{(j)}\right)\Big(& |0\rangle_{\mathcal{A}_k''}|0\rangle_{\mathcal{B}_k''} \otimes J_{+}^{(k)}|\psi\rangle \\ & + (-1)^{[q=3]}|1\rangle_{\mathcal{A}_k''}|1\rangle_{\mathcal{B}_k''} \otimes J_{-}^{(k)}|\psi\rangle\Big). \end{aligned} \tag{G.28}$$

Thus, using Eq. (G.19) to simplify this, we have the desired Eq. (G.26).

After the full application of the isometry $V = V^{(n)} \dots V^{(1)}$, and defining

$$|0\rangle_{\mathcal{A}''} = |0 \dots 0\rangle_{\mathcal{A}''}, \tag{G.29a}$$

$$|1\rangle_{\mathcal{A}''} = |1 \dots 1\rangle_{\mathcal{A}''}, \tag{G.29b}$$

$$|0\rangle_{\mathcal{B}''} = |0 \dots 0\rangle_{\mathcal{B}''}, \tag{G.29c}$$

$$|1\rangle_{\mathcal{B}''} = |1 \dots 1\rangle_{\mathcal{B}''}, \tag{G.29d}$$

Eqs. (G.12a) and (G.20) together give

$$V|\psi\rangle = \bigotimes_{j=1}^{n} |\Phi^+\rangle_{\mathcal{A}'_j\mathcal{B}'_j} \otimes \left(|0\rangle_{\mathcal{A}''}|0\rangle_{\mathcal{B}''} \otimes |\xi_+^n\rangle + |1\rangle_{\mathcal{A}''}|1\rangle_{\mathcal{B}''} \otimes |\xi_-^n\rangle\right). \tag{G.30}$$

Similarly, we have

$$\begin{aligned} V S_q^{(1)}|\psi\rangle &= \sigma_q^{\mathcal{B}'_1} |\Phi^+\rangle_{\mathcal{A}'_1\mathcal{B}'_1} \otimes V^{(n)} \dots V^{(2)} \Big(|0\rangle_{\mathcal{A}''_1}|0\rangle_{\mathcal{B}''_1} \otimes \left|\xi_+^1\right\rangle \\ &\qquad + (-1)^{[q=3]} |1\rangle_{\mathcal{A}''_1}|1\rangle_{\mathcal{B}''_1} \otimes \left|\xi_-^1\right\rangle \Big) \\ &= \sigma_q^{\mathcal{B}'_1} \bigotimes_{j=1}^{n} |\Phi^+\rangle_{\mathcal{A}'_j\mathcal{B}'_j} \otimes \left(|0\rangle_{\mathcal{A}''}|0\rangle_{\mathcal{B}''} \otimes |\xi_+^n\rangle \right. \\ &\qquad \left. + (-1)^{[q=3]} |1\rangle_{\mathcal{A}''}|1\rangle_{\mathcal{B}''} \otimes |\xi_-^n\rangle\right) \\ &= \sigma_q^{\mathcal{B}'_1} \bigotimes_{j=1}^{n} |\Phi^+\rangle_{\mathcal{A}'_j\mathcal{B}'_j} \otimes \sigma_{3[q=3]}^{\mathcal{B}''} \left(|0\rangle_{\mathcal{A}''}|0\rangle_{\mathcal{B}''} \otimes |\xi_+^n\rangle + |1\rangle_{\mathcal{A}''}|1\rangle_{\mathcal{B}''} \otimes |\xi_-^n\rangle\right). \end{aligned} \tag{G.31}$$

The first equality follows from Eq. (G.12b) and the second equality from Eq. (G.20). Furthermore, for $1 < k \leq n$, we can write

$$\begin{aligned} V S_q^{(k)}|\psi\rangle &= |\Phi^+\rangle_{\mathcal{A}'_1\mathcal{B}'_1} \otimes V^{(n)} \dots V^{(2)} S_q^{(k)} \Big(|0\rangle_{\mathcal{A}''_1}|0\rangle_{\mathcal{B}''_1} \otimes \left|\xi_+^1\right\rangle \\ &\qquad + |1\rangle_{\mathcal{A}''_1}|1\rangle_{\mathcal{B}''_1} \otimes \left|\xi_-^1\right\rangle \Big) \\ &= \bigotimes_{j=1}^{k-1} |\Phi^+\rangle_{\mathcal{A}'_j\mathcal{B}'_j} \otimes V^{(n)} \dots V^{(k)} S_q^{(k)} \left(|0 \dots 0\rangle|0 \dots 0\rangle \otimes \left|\xi_+^{k-1}\right\rangle \right. \\ &\qquad \left. + |1 \dots 1\rangle|1 \dots 1\rangle \otimes \left|\xi_-^{k-1}\right\rangle\right) \\ &= \sigma_q^{\mathcal{B}'_k} \bigotimes_{j=1}^{n} |\Phi^+\rangle_{\mathcal{A}'_j\mathcal{B}'_j} \otimes \left(|0\rangle_{\mathcal{A}''}|0\rangle_{\mathcal{B}''} \otimes |\xi_+^n\rangle + (-1)^{[q=3]} |1\rangle_{\mathcal{A}''}|1\rangle_{\mathcal{B}''} \otimes |\xi_-^n\rangle\right) \\ &= \sigma_q^{\mathcal{B}'_k} \bigotimes_{j=1}^{n} |\Phi^+\rangle_{\mathcal{A}'_j\mathcal{B}'_j} \otimes \sigma_{3[q=3]}^{\mathcal{B}''} \left(|0\rangle_{\mathcal{A}''}|0\rangle_{\mathcal{B}''} \otimes |\xi_+^n\rangle \right. \\ &\qquad \left. + |1\rangle_{\mathcal{A}''}|1\rangle_{\mathcal{B}''} \otimes |\xi_-^n\rangle\right). \end{aligned} \tag{G.32}$$

For the first equality we used Eqs. (G.12a) and (G.24); for the second equality we used Eqs. (G.20) and (G.25); and the third equality used Eqs. (G.20) and (G.26). Together, Eqs. (G.30) to (G.32) have the desired form by taking $|\xi_0\rangle = |\xi_+^n\rangle$ and $|\xi_1\rangle = |\xi_-^n\rangle$. □

Appendix H

Action of many untrusted operators

Proof of Lemma 6.10. Consider some unitary operators $U_{\tilde{\mathcal{A}}} : \tilde{\mathcal{A}} \to \tilde{\mathcal{A}}$ and $U_{\tilde{\mathcal{B}}} : \tilde{\mathcal{B}} \to \tilde{\mathcal{B}}$ which extend the isometries $V_{\mathcal{A}}$ and $V_{\mathcal{B}}$ to have domains $\tilde{\mathcal{A}}$ and $\tilde{\mathcal{B}}$, respectively. This can be achieved by extending orthonormal bases of the images of each isometry to orthonormal bases of each full space. Define the local unitary $U = U_{\tilde{\mathcal{A}}} \otimes U_{\tilde{\mathcal{B}}}$ on $\tilde{\mathcal{A}} \otimes \tilde{\mathcal{B}}$. We may also consider the trivial extension (by appropriate direct sums) of all operators A_j to $\tilde{\mathcal{A}}$ and the state $|\psi\rangle$ to $\tilde{\mathcal{A}} \otimes \tilde{\mathcal{B}}$, each with zero weight in their new components. This preserves the norms of the state and each operator. Reusing the notation of the original state and operators also for their trivial extensions, we can now write that for all j

$$U|\psi\rangle = V|\psi\rangle, \tag{H.1a}$$

$$UA_j|\psi\rangle = VA_j|\psi\rangle. \tag{H.1b}$$

From the assumption of Eq. (6.53a) and that $\|\tilde{B}_j\| \leq 1$, it follows that

$$\tilde{B}_j U|\psi\rangle \overset{\delta}{\approx} \tilde{B}_j|\phi\rangle. \tag{H.2}$$

Using the assumptions of Eqs. (6.53b) and (6.54), we can write

$$\tilde{B}_j|\phi\rangle = \tilde{A}_j|\phi\rangle \overset{\delta}{\approx} UA_j|\psi\rangle. \tag{H.3}$$

Thus, combining Eqs. (H.2) and (H.3) using the triangle inequality yields

$$\tilde{B}_j U|\psi\rangle \overset{2\delta}{\approx} UA_j|\psi\rangle. \tag{H.4}$$

Since $V_{\mathcal{A}}$ is an isometry, $V_{\mathcal{A}}^\dagger V_{\mathcal{A}} = I_{\mathcal{A}}$, where $I_{\mathcal{A}}$ is the identity operator on $\mathcal{A}$. Thus,

$$\begin{aligned} VA_j &= V_{\mathcal{A}} A_j \otimes V_{\mathcal{B}} \\ &= V_{\mathcal{A}} A_j V_{\mathcal{A}}^\dagger V_{\mathcal{A}} \otimes V_{\mathcal{B}} \\ &= V_{\mathcal{A}} A_j V_{\mathcal{A}}^\dagger V. \end{aligned} \tag{H.5}$$

Similarly, $UA_j = U_{\tilde{\mathcal{A}}} A_j U_{\tilde{\mathcal{A}}}^\dagger U$. We can therefore rewrite Eq. (H.4) as

$$\tilde{B}_j U|\psi\rangle \overset{2\delta}{\approx} \left(U_{\tilde{\mathcal{A}}} A_j U_{\tilde{\mathcal{A}}}^\dagger\right) U|\psi\rangle. \tag{H.6}$$

We now use the properties just exhibited to examine the state $\tilde{A}_1 \dots \tilde{A}_m|\phi\rangle$. Repeated use of Eq. (6.54) and the fact that operators defined on $\tilde{\mathcal{A}}$ commute with those defined on $\tilde{\mathcal{B}}$ gives

$$\tilde{A}_1 \dots \tilde{A}_m|\phi\rangle = \tilde{B}_m \dots \tilde{B}_1|\phi\rangle. \tag{H.7}$$

Using Eq. (6.53a) one time, and again that $\|\tilde{B}_j\| \leq 1$, we can then write

$$\tilde{A}_1 \dots \tilde{A}_m|\phi\rangle \overset{\delta}{\approx} \left(\tilde{B}_m \dots \tilde{B}_1\right) U|\psi\rangle. \tag{H.8}$$

Repeated use of Eq. (H.6), noting that $\|U_{\tilde{\mathcal{A}}} A_j U_{\tilde{\mathcal{A}}}^\dagger\| \leq \|A_j\| \leq 1$ for all j since $U_{\tilde{\mathcal{A}}}$ is unitary, gives via the triangle inequality

$$\left(\tilde{B}_m \dots \tilde{B}_1\right) U|\psi\rangle \overset{2m\delta}{\approx} \left(U_{\tilde{\mathcal{A}}} A_1 U_{\tilde{\mathcal{A}}}^\dagger\right) \dots \left(U_{\tilde{\mathcal{A}}} A_m U_{\tilde{\mathcal{A}}}^\dagger\right) U|\psi\rangle. \tag{H.9}$$

Therefore,

$$\tilde{A}_1 \dots \tilde{A}_m|\phi\rangle \overset{(2m+1)\delta}{\approx} \left(U_{\tilde{\mathcal{A}}} A_1 U_{\tilde{\mathcal{A}}}^\dagger\right) \dots \left(U_{\tilde{\mathcal{A}}} A_m U_{\tilde{\mathcal{A}}}^\dagger\right) U|\psi\rangle. \tag{H.10}$$

Again using the fact that $V_{\mathcal{A}}^\dagger V_{\mathcal{A}} = I_{\mathcal{A}}$, we have

$$\begin{aligned} \left(V_{\mathcal{A}} A_1 V_{\mathcal{A}}^\dagger\right) \dots \left(V_{\mathcal{A}} A_m V_{\mathcal{A}}^\dagger\right) V &= V_{\mathcal{A}}(A_1 \dots A_m) V_{\mathcal{A}}^\dagger V \\ &= V_{\mathcal{A}}(A_1 \dots A_m) V_{\mathcal{A}}^\dagger V_{\mathcal{A}} \otimes V_{\mathcal{B}} \\ &= V_{\mathcal{A}}(A_1 \dots A_m) \otimes V_{\mathcal{B}} \\ &= V(A_1 \dots A_m), \end{aligned} \tag{H.11}$$

and similarly

$$\left(U_{\tilde{\mathcal{A}}} A_1 U_{\tilde{\mathcal{A}}}^\dagger\right) \dots \left(U_{\tilde{\mathcal{A}}} A_m U_{\tilde{\mathcal{A}}}^\dagger\right) U = U(A_1 \dots A_m). \tag{H.12}$$

Thus, Eq. (H.10) becomes

$$\tilde{A}_1 \dots \tilde{A}_m|\phi\rangle \overset{(2m+1)\delta}{\approx} U(A_1 \dots A_m)|\psi\rangle. \tag{H.13}$$

Due to the construction of U and the extended versions of the operators A_j and the state $|\psi\rangle$, we have $U(A_1 \dots A_m)|\psi\rangle = V(A_1 \dots A_m)|\psi\rangle$. Therefore,

$$\tilde{A}_1 \dots \tilde{A}_m|\phi\rangle \overset{(2m+1)\delta}{\approx} V(A_1 \dots A_m)|\psi\rangle \tag{H.14}$$

as required. □

Appendix I

State preparation

Proof of Theorem 6.11. Denote the state

$$|\psi'\rangle = \bigotimes_{j=1}^{n} |\Phi^+\rangle_{\mathcal{A}'_j\mathcal{B}'_j} \otimes |\xi\rangle \tag{I.1}$$

and projective measurement operators

$$\begin{aligned}\hat{N}_{\boldsymbol{a}|\chi} &= \bigotimes_{j=1}^{n} \left|\sigma_{\chi_j}^{a_j}\right\rangle\!\left\langle\sigma_{\chi_j}^{a_j}\right|_{\mathcal{B}'_j} \otimes |0\rangle\!\langle 0|_{\mathcal{B}''} + \bigotimes_{j=1}^{n} \left|\sigma_{\chi_j}^{a_j}\right\rangle\!\left\langle\sigma_{\chi_j}^{a_j}\right|^{*}_{\mathcal{B}'_j} \otimes |1\rangle\!\langle 1|_{\mathcal{B}''} \\ &= \bigotimes_{j=1}^{n} \left|\sigma_{\chi_j}^{a_j}\right\rangle\!\left\langle\sigma_{\chi_j}^{a_j}\right|_{\mathcal{B}'_j} \otimes |0\rangle\!\langle 0|_{\mathcal{B}''} + \bigotimes_{j=1}^{n} \left|\sigma_{\chi_j}^{a_j(-1)^{[\chi_j=\mathrm{z}]}}\right\rangle\!\left\langle\sigma_{\chi_j}^{a_j(-1)^{[\chi_j=\mathrm{z}]}}\right|_{\mathcal{B}'_j} \otimes |1\rangle\!\langle 1|_{\mathcal{B}''}.\end{aligned} \tag{I.2}$$

For any $\chi \in \{1, \ldots, 5\}$, the Bell state $|\Phi^+\rangle$ can be written in the form

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}\Big(\left|\sigma_\chi^+\right\rangle^\star \otimes \left|\sigma_\chi^+\right\rangle + \left|\sigma_\chi^-\right\rangle^\star \otimes \left|\sigma_\chi^-\right\rangle\Big), \tag{I.3}$$

where the superscript $\star$ (as opposed to the usual $*$) denotes complex conjugation performed in the computational basis. This is such that

$$\begin{gathered}\left|\sigma_{\mathrm{x}}^{\pm}\right\rangle^\star = \left|\sigma_{\mathrm{x}}^{\pm}\right\rangle, \quad \left|\sigma_{\mathrm{y}}^{\pm}\right\rangle^\star = \left|\sigma_{\mathrm{y}}^{\mp}\right\rangle, \quad \left|\sigma_{\mathrm{z}}^{\pm}\right\rangle^\star = \left|\sigma_{\mathrm{z}}^{\pm}\right\rangle, \\ \left|\sigma_{\mathrm{x}\pm\mathrm{y}}^{+}\right\rangle^\star = \left|\sigma_{\mathrm{x}\mp\mathrm{y}}^{+}\right\rangle, \quad \left|\sigma_{\mathrm{x}\pm\mathrm{y}}^{-}\right\rangle^\star = \left|\sigma_{\mathrm{x}\mp\mathrm{y}}^{-}\right\rangle.\end{gathered} \tag{I.4}$$

We then have

$$\begin{aligned}\frac{\hat{N}_{\boldsymbol{a}|\chi}|\psi'\rangle}{\sqrt{\langle\psi'|\,\hat{N}_{\boldsymbol{a}|\chi}\,|\psi'\rangle}} &= \bigotimes_{j=1}^{n} \left|\sigma_{\chi_j}^{a_j}\right\rangle^\star_{\mathcal{A}'_j} \otimes \bigotimes_{j=1}^{n} \left|\sigma_{\chi_j}^{a_j}\right\rangle_{\mathcal{B}'_j} \otimes |0\rangle_{\mathcal{A}''}|0\rangle_{\mathcal{B}''} \otimes |\xi_0\rangle_{\mathcal{A}\mathcal{B}} \\ &\quad + \bigotimes_{j=1}^{n} \left|\sigma_{\chi_j}^{a_j(-1)^{[\chi_j=\mathrm{z}]}}\right\rangle^\star_{\mathcal{A}'_j} \otimes \bigotimes_{j=1}^{n} \left|\sigma_{\chi_j}^{a_j(-1)^{[\chi_j=\mathrm{z}]}}\right\rangle_{\mathcal{B}'_j} \otimes |1\rangle_{\mathcal{A}''}|1\rangle_{\mathcal{B}''} \otimes |\xi_1\rangle_{\mathcal{A}\mathcal{B}}.\end{aligned} \tag{I.5}$$

Tracing out $\mathcal{A}$, $\mathcal{A}'$, and $\mathcal{A}''$ gives

$$\begin{aligned}\mathrm{tr}_{\mathcal{A}\mathcal{A}'\mathcal{A}''}\left(\frac{\hat{N}_{\boldsymbol{a}|\chi}|\psi'\rangle\langle\psi'|\hat{N}_{\boldsymbol{a}|\chi}}{\langle\psi'|\,\hat{N}_{\boldsymbol{a}|\chi}\,|\psi'\rangle}\right) &= \bigotimes_{j=1}^{n}\left|\sigma_{\chi_j}^{a_j}\right\rangle\!\left\langle\sigma_{\chi_j}^{a_j}\right|_{\mathcal{B}'_j} \otimes |0\rangle\langle 0|_{\mathcal{B}''} \otimes \mathrm{tr}_{\mathcal{A}}(|\xi_0\rangle\langle\xi_0|) \\ &\quad + \bigotimes_{j=1}^{n}\left|\sigma_{\chi_j}^{a_j(-1)^{[\chi_j=z]}}\right\rangle\!\left\langle\sigma_{\chi_j}^{a_j(-1)^{[\chi_j=z]}}\right|_{\mathcal{B}'_j} \otimes |1\rangle\langle 1|_{\mathcal{B}''} \otimes \mathrm{tr}_{\mathcal{A}}(|\xi_1\rangle\langle\xi_1|) \\ &= \left|e_{\boldsymbol{a}|\chi}\right\rangle\!\left\langle e_{\boldsymbol{a}|\chi}\right|_{\mathcal{B}'} \otimes |0\rangle\langle 0|_{\mathcal{B}''} \otimes \beta_0 + \left|e^*_{\boldsymbol{a}|\chi}\right\rangle\!\left\langle e^*_{\boldsymbol{a}|\chi}\right|_{\mathcal{B}'} \otimes |1\rangle\langle 1|_{\mathcal{B}''} \otimes \beta_1, \quad \text{(I.6)}\end{aligned}$$

where $\beta_0 = \mathrm{tr}_{\mathcal{A}}(|\xi_0\rangle\langle\xi_0|)$ and $\beta_1 = \mathrm{tr}_{\mathcal{A}}(|\xi_1\rangle\langle\xi_1|)$ and we have $\mathrm{tr}(\beta_0)+\mathrm{tr}(\beta_1) = 1$. Using properties of the partial trace, we also have

$$\mathrm{tr}_{\mathcal{A}\mathcal{A}'\mathcal{A}''}\left(\frac{V^{\chi}\Pi^{\mathcal{A}}_{\boldsymbol{a}|\chi}|\psi\rangle\langle\psi|\Pi^{\mathcal{A}}_{\boldsymbol{a}|\chi}V^{\chi\dagger}}{\langle\psi|\,\Pi^{\mathcal{A}}_{\boldsymbol{a}|\chi}\,|\psi\rangle}\right) = V_{\mathcal{B}}\rho_{\mathcal{B}}^{\boldsymbol{a}|\chi}V_{\mathcal{B}}^{\dagger}. \quad \text{(I.7)}$$

Using the linearity of the partial trace to combine Eqs. (I.6) and (I.7), and since the trace class norm is decreasing under the partial trace, we have

$$\begin{aligned}&\left\|V_{\mathcal{B}}\rho_{\mathcal{B}}^{\boldsymbol{a}|\chi}V_{\mathcal{B}}^{\dagger} - \left(\left|e_{\boldsymbol{a}|\chi}\right\rangle\!\left\langle e_{\boldsymbol{a}|\chi}\right| \otimes |0\rangle\langle 0| \otimes \beta_0 + \left|e^*_{\boldsymbol{a}|\chi}\right\rangle\!\left\langle e^*_{\boldsymbol{a}|\chi}\right| \otimes |1\rangle\langle 1| \otimes \beta_1\right)\right\|_1 \\ &\qquad \leq \left\|\frac{V^{\chi}\Pi^{\mathcal{A}}_{\boldsymbol{a}|\chi}|\psi\rangle\langle\psi|\Pi^{\mathcal{A}}_{\boldsymbol{a}|\chi}V^{\chi\dagger}}{\langle\psi|\,\Pi^{\mathcal{A}}_{\boldsymbol{a}|\chi}\,|\psi\rangle} - \frac{\hat{N}_{\boldsymbol{a}}|\psi'\rangle\langle\psi'|\hat{N}_{\boldsymbol{a}}}{\langle\psi'|\,\hat{N}_{\boldsymbol{a}}\,|\psi'\rangle}\right\|_1. \quad \text{(I.8)}\end{aligned}$$

Let us introduce a bijection $u\colon \{+,-\}^n \to \{0,1\}^n$ which converts between representations of binary strings by taking every entry $+$ to 0 and every entry $-$ to 1. Let $\boldsymbol{s} \in \{0,1\}^n$ be any string. Equations (6.70a) and (6.72a) together imply that

$$A^{\boldsymbol{s}}_{\chi} = \sum_{\boldsymbol{a}\in\{+,-\}^n}(-1)^{u(\boldsymbol{a})\cdot\boldsymbol{s}}\Pi^{\mathcal{A}}_{\boldsymbol{a}|\chi}. \quad \text{(I.9)}$$

Defining $\hat{B}^{\boldsymbol{s}}_{\chi}$ by

$$\begin{aligned}\hat{B}^{\boldsymbol{s}}_{\chi} &= \sum_{\boldsymbol{a}\in\{+,-\}^n}(-1)^{u(\boldsymbol{a})\cdot\boldsymbol{s}}\hat{N}_{\boldsymbol{a}|\chi} \\ &= \bigotimes_{j=1}^{n}\left(\sigma_{\chi_j}^{\mathcal{B}'_j}\right)^{s_j} \otimes |0\rangle\langle 0|_{\mathcal{B}''} + \bigotimes_{j=1}^{n}\left(\sigma_{\chi_j}^{\mathcal{B}'_j *}\right)^{s_j} \otimes |1\rangle\langle 1|_{\mathcal{B}''},\end{aligned} \quad \text{(I.10)}$$

the result of Corollary 6.17 in this notation is that

$$\left\|V^{\chi}A^{\boldsymbol{s}}_{\chi}|\psi\rangle - \hat{B}^{\boldsymbol{s}}_{\chi}|\psi'\rangle\right\| \leq \gamma(\varepsilon, n). \quad \text{(I.11)}$$

Due to Eqs. (I.9) to (I.11), we can now apply Theorem 6.4 for each $\chi \in S$. This gives, with probability at least $1 - 4\gamma(\varepsilon,n)^{2/3}$ over all $\boldsymbol{a} \in \{+,-\}^n$ given χ, that one half

multiplied by the right-hand side of Eq. (I.8) is bounded above as

$$\frac{1}{2}\left\| \frac{V^{\chi}\Pi^{\mathcal{A}}_{\boldsymbol{a}|\chi}|\psi\rangle\langle\psi|\Pi^{\mathcal{A}}_{\boldsymbol{a}|\chi}V^{\chi\dagger}}{\langle\psi|\,\Pi^{\mathcal{A}}_{\boldsymbol{a}|\chi}\,|\psi\rangle} - \frac{\hat{N}_{\boldsymbol{a}|\chi}|\psi'\rangle\langle\psi'|\hat{N}_{\boldsymbol{a}|\chi}}{\langle\psi'|\,\hat{N}_{\boldsymbol{a}|\chi}\,|\psi'\rangle} \right\|_1 \leq \gamma(\varepsilon,n)^{2/3}. \tag{I.12}$$

Therefore, with probability at least $1-4\tau(\varepsilon,n)$ over all $\boldsymbol{a}\in\{+,-\}^n$ given $\boldsymbol{\chi}$, we have

$$\frac{1}{2}\Big\| V_{\mathcal{B}}\rho^{\boldsymbol{a}|\chi}_{\mathcal{B}}V^{\dagger}_{\mathcal{B}} - \Big(\big|e_{\boldsymbol{a}|\chi}\big\rangle\big\langle e_{\boldsymbol{a}|\chi}\big| \otimes |0\rangle\langle 0| \otimes \beta_0 + \big|e^{*}_{\boldsymbol{a}|\chi}\big\rangle\big\langle e^{*}_{\boldsymbol{a}|\chi}\big| \otimes |1\rangle\langle 1| \otimes \beta_1 \Big)\Big\|_1 \leq \tau(\varepsilon,n), \tag{I.13}$$

where we define $\tau(\varepsilon,n)=\gamma(\varepsilon,n)^{2/3}$. □

Bibliography

[1] **S. A. Adamson** and P. Wallden, "Quantum magic rectangles: characterization and application to certified randomness expansion", Phys. Rev. Research **2**, 043317 (2020).

[2] **S. A. Adamson** and P. Wallden, "Practical parallel self-testing of Bell states via magic rectangles", Phys. Rev. A **105**, 032456 (2022).

[3] **S. A. Adamson**, *Parallel remote state preparation for fully device-independent verifiable blind quantum computation*, Dec. 2022, arXiv:2212.05442 [quant-ph].

[4] D. Mayers and A. Yao, "Quantum cryptography with imperfect apparatus", in Proceedings 39th annual symposium on foundations of computer science (cat. no. 98CB36280) (Nov. 1998), pp. 503–509.

[5] R. Colbeck and A. Kent, "Private randomness expansion with untrusted devices", J. Phys. A Math. Theor. **44**, 095305 (2011).

[6] U. Vazirani and T. Vidick, "Fully device-independent quantum key distribution", Phys. Rev. Lett. **113**, 140501 (2014).

[7] A. Gheorghiu, E. Kashefi, and P. Wallden, "Robustness and device independence of verifiable blind quantum computing", New J. Phys. **17**, 083040 (2015).

[8] S. Kundu, J. Sikora, and E. Y.-Z. Tan, "A device-independent protocol for XOR oblivious transfer", in 15th conference on the theory of quantum computation, communication and cryptography (TQC 2020), Vol. 158, edited by S. T. Flammia, Leibniz International Proceedings in Informatics (LIPIcs) (2020), 12:1–12:15, arXiv:2006.06671 [quant-ph].

[9] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, "Proposed experiment to test local hidden-variable theories", Phys. Rev. Lett. **23**, 880–884 (1969).

[10] S. J. Freedman and J. F. Clauser, "Experimental test of local hidden-variable theories", Phys. Rev. Lett. **28**, 938–941 (1972).

[11] A. Aspect, J. Dalibard, and G. Roger, "Experimental test of Bell's inequalities using time-varying analyzers", Phys. Rev. Lett. **49**, 1804–1807 (1982).

[12] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. 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**, 682–686 (2015).

[13] M. Giustina, M. A. M. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner, J. Kofler, J.-Å. Larsson, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, J. Beyer, T. Gerrits, A. E. Lita, L. K. Shalm, S. W. Nam, T. Scheidl, R. Ursin, B. Wittmann, and A. Zeilinger, "Significant-loophole-free test of Bell's theorem with entangled photons", Phys. Rev. Lett. **115**, 250401 (2015).

[14] L. K. Shalm, E. Meyer-Scott, B. G. Christensen, P. Bierhorst, M. A. Wayne, M. J. Stevens, T. Gerrits, S. Glancy, D. R. Hamel, M. S. Allman, K. J. Coakley, S. D. Dyer, C. Hodge, A. E. Lita, V. B. Verma, C. Lambrocco, E. Tortorici, A. L. Migdall, Y. Zhang, D. R. Kumor, W. H. Farr, F. Marsili, M. D. Shaw, J. A. Stern, C. Abellán, W. Amaya, V. Pruneri, T. Jennewein, M. W. Mitchell, P. G. Kwiat, J. C. Bienfang, R. P. Mirin, E. Knill, and S. W. Nam, "Strong loophole-free test of local realism", Phys. Rev. Lett. **115**, 250402 (2015).

[15] Royal Swedish Academy of Sciences, "The Nobel prize in physics 2022", Nobel Prize (2022), `https://www.nobelprize.org/prizes/physics/2022/press-release/` (visited on 03/22/2023).

[16] R. Cleve, P. Hoyer, B. Toner, and J. Watrous, "Consequences and limits of nonlocal strategies", in Proceedings. 19th IEEE annual conference on computational complexity, 2004. (June 2004), pp. 236–249.

[17] B. S. Tsirelson, "Quantum generalizations of Bell's inequality", Lett. Math. Phys. **4**, 93–100 (1980).

[18] N. D. Mermin, "Simple unified form for the major no-hidden-variables theorems", Phys. Rev. Lett. **65**, 3373–3376 (1990).

[19] A. Peres, "Incompatible results of quantum measurements", Phys. Lett. **151**, 107–108 (1990).

[20] G. Brassard, A. Broadbent, and A. Tapp, "Quantum pseudo-telepathy", Found. Phys. **35**, 1877–1907 (2005).

[21] S. Kochen and E. P. Specker, "The problem of hidden variables in quantum mechanics", in *The logico-algebraic approach to quantum mechanics*, Vol. 1, edited by C. A. Hooker (Springer, Dordrecht, 1975), pp. 293–328.

[22] D. Gottesman, "Theory of fault-tolerant quantum computation", Phys. Rev. A **57**, 127–137 (1998).

[23] D. Mayers and A. Yao, "Self testing quantum apparatus", Quantum Inf. Comput. **4**, 273–286 (2004).

[24] I. Šupić and J. Bowles, "Self-testing of quantum systems: a review", Quantum **4**, 337 (2020).

[25] X. Wu, Y. Cai, T. H. Yang, H. N. Le, J.-D. Bancal, and V. Scarani, "Robust self-testing of the three-qubit W state", Phys. Rev. A **90**, 042339 (2014).

[26] M. Coudron and A. Natarajan, *The parallel-repeated magic square game is rigid*, Sept. 2016, arXiv:1609.06306 [quant-ph].

[27] A. Coladangelo, "Parallel self-testing of (tilted) EPR pairs via copies of (tilted) CHSH and the magic square game", Quantum Inf. Comput. **17**, 831–865 (2017).

[28] A. Natarajan and T. Vidick, "A quantum linearity test for robustly verifying entanglement", in Proceedings of the 49th annual ACM SIGACT symposium on theory of computing, STOC 2017 (June 2017), pp. 1003–1015.

[29] M. McKague, "Interactive proofs for BQP via self-tested graph states", Theory Comput. **12**, 1–42 (2016).

[30] M. Hajdušek, C. A. Pérez-Delgado, and J. F. Fitzsimons, *Device-independent verifiable blind quantum computation*, Dec. 2015, arXiv:1502.02563 [quant-ph].

[31] A. Gheorghiu, P. Wallden, and E. Kashefi, "Rigidity of quantum steering and one-sided device-independent verifiable quantum computation", New J. Phys. **19**, 023043 (2017).

[32] D. Castelvecchi, "IBM's quantum cloud computer goes commercial", Nature **543**, 10.1038/nature.2017.21585 (2017).

[33] D. Alsina and J. I. Latorre, "Experimental test of Mermin inequalities on a five-qubit quantum computer", Phys. Rev. A **94**, 012314 (2016).

[34] S. J. Devitt, "Performing quantum computing experiments in the cloud", Phys. Rev. A **94**, 032329 (2016).

[35] IBM Research, *IBM Quantum*, `https://quantum-computing.ibm.com/` (visited on 12/08/2022).

[36] Amazon Web Services, *Amazon Braket*, `https://aws.amazon.com/braket/` (visited on 12/08/2022).

[37] Microsoft, *Azure Quantum*, `https://azure.microsoft.com/products/quantum/` (visited on 12/08/2022).

[38] J. F. Fitzsimons, M. Hajdušek, and T. Morimae, "*Post hoc* verification of quantum computation", Phys. Rev. Lett. **120**, 040501 (2018).

[39] M. Hayashi and M. Hajdušek, "Self-guaranteed measurement-based quantum computation", Phys. Rev. A **97**, 052308 (2018).

[40] J. F. Fitzsimons and E. Kashefi, "Unconditionally verifiable blind quantum computation", Phys. Rev. A **96**, 012303 (2017).

[41] R. Raussendorf and H. J. Briegel, "A one-way quantum computer", Phys. Rev. Lett. **86**, 5188–5191 (2001).

[42] V. Danos, E. Kashefi, and P. Panangaden, "The measurement calculus", J. ACM **54**, 8–es (2007).

[43] A. Broadbent and E. Kashefi, "Parallelizing quantum circuits", Theor. Comput. Sci. **410**, 2489–2510 (2009).

[44] E. Kashefi and P. Wallden, "Optimised resource construction for verifiable quantum computation", J. Phys. A Math. Theor. **50**, 145306 (2017).

[45] Q. Xu, X. Tan, and R. Huang, "Improved resource state for verifiable blind quantum computation", Entropy **22**, 996 (2020).

[46] D. Aharonov, M. Ben-Or, E. Eban, and U. Mahadev, *Interactive proofs for quantum computations*, Apr. 2017, arXiv:`1704.04487 [quant-ph]`.

[47] T. Morimae, "Verification for measurement-only blind quantum computing", Phys. Rev. A **89**, 060302 (2014).

[48] M. Hayashi and T. Morimae, "Verifiable measurement-only blind quantum computing with stabilizer testing", Phys. Rev. Lett. **115**, 220502 (2015).

[49] A. Broadbent, "How to verify a quantum computation", Theory Comput. **14**, 1–37 (2018).

[50] K. Fujii and M. Hayashi, "Verifiable fault tolerance in measurement-based quantum computation", Phys. Rev. A **96**, 030301 (2017).

[51] T. Morimae, Y. Takeuchi, and M. Hayashi, "Verification of hypergraph states", Phys. Rev. A **96**, 062321 (2017).

[52] J. F. Fitzsimons, "Private quantum computation: an introduction to blind quantum computing and related protocols", npj Quantum Information **3**, 1–11 (2017).

[53] A. Coladangelo, A. B. Grilo, S. Jeffery, and T. Vidick, "Verifier-on-a-leash: new schemes for verifiable delegated quantum computation, with quasilinear resources", in Advances in cryptology – EUROCRYPT 2019, edited by Y. Ishai and V. Rijmen (Apr. 2019), pp. 247–277.

[54] C. A. Miller and Y. Shi, "Universal security for randomness expansion from the spot-checking protocol", SIAM J. Comput. **46**, 1304–1335 (2017), arXiv:1411.6608 [quant-ph].

[55] A. E. Rastegin, "Relations for certain symmetric norms and anti-norms before and after partial trace", J. Stat. Phys. **148**, 1040–1053 (2012).

[56] P. K. Aravind, "Quantum mysteries revisited again", Am. J. Phys. **72**, 1303–1307 (2004).

[57] L. Masanes, A. Acín, and N. Gisin, "General properties of nonsignaling theories", Phys. Rev. A **73**, 012112 (2006).

[58] A. Fine, "Hidden variables, joint probability, and the Bell inequalities", Phys. Rev. Lett. **48**, 291–295 (1982).

[59] M. Navascués, S. Pironio, and A. Acín, "Bounding the set of quantum correlations", Phys. Rev. Lett. **98**, 010401 (2007).

[60] M. Navascués, S. Pironio, and A. Acín, "A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations", New J. Phys. **10**, 073013 (2008).

[61] M. Navascués, Y. Guryanova, M. J. Hoban, and A. Acín, "Almost quantum correlations", Nat. Commun. **6**, 1–7 (2015).

[62] T. Fritz, A. B. Sainz, R. Augusiak, J. B. Brask, R. Chaves, A. Leverrier, and A. Acín, "Local orthogonality as a multipartite principle for quantum correlations", Nat. Commun. **4**, 1–7 (2013).

[63] G. Brassard, H. Buhrman, N. Linden, A. A. Méthot, A. Tapp, and F. Unger, "Limit on nonlocality in any world in which communication complexity is not trivial", Phys. Rev. Lett. **96**, 250401 (2006).

[64] S. Pironio, A. Acín, S. Massar, A. B. de La Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, "Random numbers certified by Bell's theorem", Nature **464**, 1021–1024 (2010).

[65] M. Coudron, T. Vidick, and H. Yuen, "Robust randomness amplifiers: upper and lower bounds", in Approximation, randomization, and combinatorial optimization. algorithms and techniques, edited by P. Raghavendra, S. Raskhodnikova, K. Jansen, and J. D. P. Rolim, APPROX 2013, RANDOM 2013 (Aug. 2013), pp. 468–483.

[66] C. A. Miller and Y. Shi, "Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices", J. ACM **63**, 33:1–33:63 (2016), arXiv:1402.0489 [quant-ph].

[67] A. De, C. Portmann, T. Vidick, and R. Renner, "Trevisan's extractor in the presence of quantum side information", SIAM J. Comput. **41**, 915–940 (2012).

[68] M. McKague and M. Mosca, "Generalized self-testing and the security of the 6-state protocol", in Theory of quantum computation, communication, and cryptography, edited by W. van Dam, V. M. Kendon, and S. Severini (2011), pp. 113–130.

[69] J. Kaniewski, "Self-testing of binary observables based on commutation", Phys. Rev. A **95**, 062323 (2017).

[70] R. Chao, B. W. Reichardt, C. Sutherland, and T. Vidick, "Test for a large amount of entanglement, using few measurements", Quantum **2**, 92 (2018).

[71] T. H. Yang and M. Navascués, "Robust self-testing of unknown quantum systems into any entangled two-qubit states", Phys. Rev. A **87**, 050102 (2013).

[72] C. Bamps and S. Pironio, "Sum-of-squares decompositions for a family of Clauser–Horne–Shimony–Holt-like inequalities and their application to self-testing", Phys. Rev. A **91**, 052111 (2015).

[73] C. S. Harvey and J. P. Chryssanthacopoulos, *BKS theorem and Bell's theorem in 16 dimensions*, Apr. 2008, https://digitalcommons.wpi.edu/mqp-all/3505/ (visited on 08/10/2020).

[74] M. Saniga and M. Planat, "Finite geometry behind the Harvey–Chryssanthacopoulos four-qubit magic rectangle", Quantum Inf. Comput. **12**, 1011–1016 (2012), arXiv:1204.6229 [quant-ph].

[75] A. Cabello, "Bell's theorem without inequalities and without probabilities for two observers", Phys. Rev. Lett. **86**, 1911–1914 (2001).

[76] A. Cabello, ""All versus nothing" inseparability for two observers", Phys. Rev. Lett. **87**, 010403 (2001).

[77] P. K. Aravind, "Bell's theorem without inequalities and only two distant observers", Found. Phys. Lett. **15**, 397–405 (2002).

[78] G. Brassard, A. Broadbent, and A. Tapp, "Multi-party pseudo-telepathy", in Algorithms and data structures (2003), pp. 1–11, arXiv:quant-ph/0306042 [quant-ph].

[79] R. Cleve and R. Mittal, "Characterization of binary constraint system games", in Automata, languages, and programming (2014), pp. 320–331, arXiv:1209.2729 [quant-ph].

[80] A. Arkhipov, "Extending and characterizing quantum magic games", MA thesis (Massachusetts Institute of Technology, Sept. 2012), arXiv:1209.3819 [quant-ph].

[81] A. Coladangelo and J. Stark, *Robust self-testing for linear constraint system games*, 2017, arXiv:1709.09267 [quant-ph].

[82] S. Pironio, "Aspects of quantum non-locality", PhD thesis (Université libre de Bruxelles, 2004).

[83] S. Popescu and D. Rohrlich, "Causality and nonlocality as axioms for quantum mechanics", in Causality and locality in modern physics (1998), pp. 383–389, arXiv:quant-ph/9709026 [quant-ph].

[84] P. Wittek, "Algorithm 950: ncpol2sdpa—sparse semidefinite programming relaxations for polynomial optimization problems of noncommuting variables", ACM Trans. Math. Softw. **41**, 21:1–21:12 (2015), arXiv:1308.6029 [cs.MS], https://gitlab.com/peterwittek/ncpol2sdpa (visited on 08/10/2020).

[85] MOSEK ApS, *MOSEK optimizer API for Python*, version 9.2.17 (Aug. 2020), https://docs.mosek.com/9.2/pythonapi/index.html.

[86] N. Johnston, *QETLAB: a MATLAB toolbox for quantum entanglement*, version 0.9, Jan. 2016, http://qetlab.com.

[87] MOSEK ApS, *MOSEK optimization toolbox for MATLAB*, version 9.2.17 (Aug. 2020), https://docs.mosek.com/9.2/toolbox/index.html.

[88] CVX Research, Inc., *CVX: MATLAB software for disciplined convex programming*, version 2.2, Jan. 2020, http://cvxr.com/cvx/.

[89] SDPA Project, *SemiDefinite Programming Algorithm, SDPA-GMP*, version 7.1.3, Mar. 2015, https://sdpa.sourceforge.net/.

[90] M. Yamashita, K. Fujisawa, K. Nakata, M. Nakata, M. Fukuda, K. Kobayashi, and K. Goto, *A high-performance software package for semidefinite programs: SDPA 7*, Research Report B-463 (Department of Mathematical and Computing Science, Tokyo Institute of Technology, Sept. 2010).

[91] M. Nakata, "A numerical evaluation of highly accurate multiple-precision arithmetic version of semidefinite programming solver: SDPA-GMP, -QD and -DD.", in 2010 IEEE international symposium on computer-aided control system design (IEEE, Sept. 2010), pp. 29–34.

[92] F. Dowker, J. Henson, and P. Wallden, "A histories perspective on characterizing quantum non-locality", New J. Phys. **16**, 033033 (2014).

[93] R. Arnon-Friedman, R. Renner, and T. Vidick, "Simple and tight device-independent security proofs", SIAM J. Comput. **48**, 181–225 (2019), arXiv:1607.01797 [quant-ph].

[94] P. J. Brown, S. Ragy, and R. Colbeck, "A framework for quantum-secure device-independent randomness expansion", IEEE Trans. Inf. Theory **66**, 2964–2987 (2020), arXiv:1810.13346 [quant-ph].

[95] R. Colbeck, "Quantum and relativistic protocols for secure multi-party computation", PhD thesis (University of Cambridge, Dec. 2006), arXiv:0911.3814 [quant-ph].

[96] U. Vazirani and T. Vidick, "Certifiable quantum dice: or, true random number generation secure against quantum adversaries", in Proceedings of the forty-fourth annual acm symposium on theory of computing, STOC '12 (May 2012), pp. 61–76, arXiv:1111.6054 [quant-ph].

[97] A. Acín and L. Masanes, "Certified randomness in quantum physics", Nature **540**, 213–219 (2016).

[98] F. Dupuis, O. Fawzi, and R. Renner, "Entropy accumulation", Commun. Math. Phys. **379**, 867–913 (2020).

[99] F. Dupuis and O. Fawzi, "Entropy accumulation with improved second-order term", IEEE Trans. Inf. Theory **65**, 7596–7612 (2019), arXiv:1805.11652 [quant-ph].

[100] A. Gheorghiu, T. Kapourniotis, and E. Kashefi, "Verification of quantum computation: an overview of existing approaches", Theory Comput. Syst. **63**, 715–808 (2019).

[101] X. Wu, J.-D. Bancal, M. McKague, and V. Scarani, "Device-independent parallel self-testing of two singlets", Phys. Rev. A **93**, 062121 (2016).

[102] M. McKague, "Self-testing in parallel", New J. Phys. **18**, 045013 (2016).

[103] A. Natarajan and T. Vidick, "Low-degree testing for quantum states, and a quantum entangled games PCP for QMA", in 2018 IEEE 59th annual symposium on foundations of computer science (FOCS) (Oct. 2018), pp. 731–742.

[104] A. Natarajan and J. Wright, "NEEXP is contained in MIP*", in 2019 IEEE 60th annual symposium on foundations of computer science (FOCS) (Nov. 2019), pp. 510–518.

[105] Z. Ji, A. Natarajan, T. Vidick, J. Wright, and H. Yuen, "MIP* = RE", Commun. ACM **64**, 131–138 (2021).

[106] I. Šupić, D. Cavalcanti, and J. Bowles, "Device-independent certification of tensor products of quantum states using single-copy self-testing protocols", Quantum **5**, 418 (2021).

[107] H. Fu, "Constant-sized correlations are sufficient to self-test maximally entangled states with unbounded dimension", Quantum **6**, 614 (2022).

[108] L. Mančinska, J. Prakash, and C. Schafhauser, *Constant-sized robust self-tests for states and measurements of unbounded dimension*, Mar. 2021, arXiv:2103.01729 [quant-ph].

[109] S. Sarkar, D. Saha, J. Kaniewski, and R. Augusiak, "Self-testing quantum systems of arbitrary local dimension with minimal number of measurements", npj Quantum Information **7**, 151 (2021).

[110] T. H. Yang, T. Vértesi, J.-D. Bancal, V. Scarani, and M. Navascués, "Robust and versatile black-box certification of quantum devices", Phys. Rev. Lett. **113**, 040401 (2014).

[111] J.-D. Bancal, M. Navascués, V. Scarani, T. Vértesi, and T. H. Yang, "Physical characterization of quantum devices from nonlocal correlations", Phys. Rev. A **91**, 022115 (2015).

[112] E. Kashefi and P. Wallden, "Garbled quantum computation", Cryptography **1**, 6 (2017).

[113] E. Kashefi and A. Pappa, "Multiparty delegated quantum computing", Cryptography **1**, 12 (2017).

[114] V. Dunjko and E. Kashefi, *Blind quantum computing with two almost identical states*, Apr. 2016, arXiv:1604.01586 [quant-ph].

[115] M. McKague, "Self-testing in parallel with CHSH", Quantum **1**, 1 (2017).

[116] J. Bowles, I. Šupić, D. Cavalcanti, and A. Acín, "Self-testing of pauli observables for device-independent entanglement certification", Phys. Rev. A **98**, 042336 (2018).

[117] I. Agresti, B. Polacchi, D. Poderini, E. Polino, A. Suprano, I. Šupić, J. Bowles, G. Carvacho, D. Cavalcanti, and F. Sciarrino, "Experimental robust self-testing of the state generated by a quantum network", PRX Quantum **2**, 020346 (2021).

[118] Y. Wang, X. Wu, and V. Scarani, "All the self-testings of the singlet for two binary measurements", New J. Phys. **18**, 025021 (2016).

[119] V. Dunjko, J. F. Fitzsimons, C. Portmann, and R. Renner, "Composable security of delegated quantum computation", in Advances in cryptology – ASIACRYPT 2014, edited by P. Sarkar and T. Iwata (Dec. 2014), pp. 406–425.

[120] A. Broadbent, J. Fitzsimons, and E. Kashefi, "Universal blind quantum computation", in 2009 50th annual IEEE symposium on foundations of computer science (Oct. 2009), pp. 517–526.

[121] D. Leichtle, L. Music, E. Kashefi, and H. Ollivier, "Verifying BQP computations on noisy devices with minimal overhead", PRX Quantum **2**, 040302 (2021).

[122] B. W. Reichardt, F. Unger, and U. Vazirani, *A classical leash for a quantum system: command of quantum systems via rigidity of CHSH games*, Sept. 2012, arXiv:1209.0448 [quant-ph].

[123] B. W. Reichardt, F. Unger, and U. Vazirani, "Classical command of quantum systems", Nature **496**, 456–460 (2013).

[124] U. Mahadev, "Classical verification of quantum computations", in 2018 IEEE 59th annual symposium on foundations of computer science (FOCS) (Oct. 2018), pp. 259–267.

[125] A. Gheorghiu and T. Vidick, "Computationally-secure and composable remote state preparation", in 2019 IEEE 60th annual symposium on foundations of computer science (FOCS) (Nov. 2019), pp. 1024–1033.

[126] A. Gheorghiu, T. Metger, and A. Poremba, *Quantum cryptography with classical communication: parallel remote state preparation for copy-protection, verification, and more*, Sept. 2022, arXiv:2201.13445 [quant-ph].

[127] A. Coladangelo, K. T. Goh, and V. Scarani, "All pure bipartite entangled states can be self-tested", Nature Communications **8**, 1–5 (2017).

[128] I. Šupić, J. Bowles, M.-O. Renou, A. Acín, and M. J. Hoban, "Quantum networks self-test all entangled states", Nat. Phys., 1–6 (2023).

[129] L. Mančinska, "Maximally entangled state in pseudo-telepathy games", in *Computing with new resources*, edited by C. S. Calude, R. Freivalds, and I. Kazuo (Springer International Publishing, Cham, Dec. 2014), pp. 200–207.

[130] D. Ostrev, "The structure of nearly-optimal quantum strategies for the non-local XOR games", Quantum Inf. Comput. **16**, 1191–1211 (2016).

[131] A. Coladangelo, "Generalization of the Clauser-Horne-Shimony-Holt inequality self-testing maximally entangled states of any local dimension", Phys. Rev. A **98**, 052115 (2018).

[132] A. Acín, S. Pironio, T. Vértesi, and P. Wittek, "Optimal randomness certification from one entangled bit", Phys. Rev. A **93**, 040102 (2016).

[133] M.-O. Renou, D. Trillo, M. Weilenmann, T. P. Le, A. Tavakoli, N. Gisin, A. Acín, and M. Navascués, "Quantum theory based on real numbers can be experimentally falsified", Nature **600**, 625–629 (2021).

[134] T. Metger and T. Vidick, "Self-testing of a single quantum device under computational assumptions", Quantum **5**, 544 (2021).

[135] P.-S. Lin, D. Rosset, Y. Zhang, J.-D. Bancal, and Y.-C. Liang, "Device-independent point estimation from finite data and its application to device-independent property estimation", Phys. Rev. A **97**, 032309 (2018).

[136] M. McKague, T. H. Yang, and V. Scarani, "Robust self-testing of the singlet", J. Phys. A Math. Theor. **45**, 455304 (2012).

[137] A. M. Childs, D. W. Leung, and M. A. Nielsen, "Unified derivations of measurement-based schemes for quantum computation", Phys. Rev. A **71**, 032318 (2005).

[138] R. Arnon-Friedman and H. Yuen, "Noise-tolerant testing of high entanglement of formation", in 45th international colloquium on automata, languages, and programming (ICALP 2018), Vol. 107, edited by I. Chatzigiannakis, C. Kaklamanis, D. Marx, and D. Sannella, Leibniz International Proceedings in Informatics (LIPIcs) (July 2018), 11:1–11:12.

[139] J. Kaniewski, "Analytic and nearly optimal self-testing bounds for the Clauser-Horne-Shimony-Holt and Mermin inequalities", Phys. Rev. Lett. **117**, 070402 (2016).

[140] W. T. Gowers and O. Hatami, "Inverse and stability theorems for approximate representations of finite groups", Sb. Math. **208**, 1784 (2017).

[141] P. Sekatski, J.-D. Bancal, S. Wagner, and N. Sangouard, "Certifying the building blocks of quantum computers from Bell's theorem", Phys. Rev. Lett. **121**, 180505 (2018).

[142] X. Li, Y. Wang, Y. Han, S. Qin, F. Gao, and Q. Wen, "Analytic robustness bound for self-testing of the singlet with two binary measurements", J. Opt. Soc. Am. B **36**, 457–463 (2019).

[143] R. Arnon-Friedman and J.-D. Bancal, "Device-independent certification of one-shot distillable entanglement", New J. Phys. **21**, 033010 (2019).

[144] R. D. Sorkin, "Quantum mechanics as quantum measure theory", Mod. Phys. Lett. A **9**, 3119–3127 (1994).

[145] C. Paddock, V. Russo, T. Silverthorne, and W. Slofstra, *Arkhipov's theorem, graph minors, and linear system nonlocal games*, July 2022, arXiv:2205.04645 [math.CO].

[146] T. Kapourniotis, E. Kashefi, D. Leichtle, L. Music, and H. Ollivier, *Asymmetric quantum secure multi-party computation with weak clients against dishonest majority*, Mar. 2023, arXiv:2303.08865 [quant-ph].