Quantum Information Processing with Adversarial Devices

by

Matthew McKague

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Doctor of Philosophy
in
Combinatorics & Optimization

Waterloo, Ontario, Canada, 2010

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

We consider several applications in black-box quantum computation in which untrusted physical quantum devices are connected together to produce an experiment. By examining the outcome statistics of such an experiment, and comparing them against the desired experiment, we may hope to certify that the physical experiment is implementing the desired experiment. This is useful in order to verify that a calculation has been performed correctly, that measurement outcomes are secure, or that the devices are producing the desired state.

First, we introduce constructions for a family of simulations, which duplicate the outcome statistics of an experiment but are not exactly the same as the desired experiment. This places limitations on how strict we may be with the requirements we place on the physical devices. We identify many simulations, and consider their implications for quantum foundations as well as security related applications.

The most general application of black-box quantum computing is self-testing circuits, in which a generic physical circuit may be tested against a given circuit. Earlier results were restricted to circuits described on a real Hilbert space. We give new proofs for earlier results and begin work extending them to circuits on a complex Hilbert space with a test that verifies complex measurements.

For security applications of black-box quantum computing, we consider device independent quantum key distribution (DIQKD). We may consider DIQKD as an extension of QKD (quantum key distribution) in which the model of the physical measurement devices is replaced with an adversarial model. This introduces many technical problems, such as unbounded dimension, but promises increased security since the many complexities hidden by traditional models are implicitly considered. We extend earlier work by proving security with fewer assumptions.

Finally, we consider the case of black-box state characterization. Here the emphasis is placed on providing robust results with operationally meaningful measures. The goal is to certify that a black box device is producing high quality maximally entangled pairs of qubits using only untrusted measurements and a single statistic, the CHSH value, defined using correlations of outcomes from the two parts of the system. We present several measures of quality and prove bounds for them.

Acknowledgements

Dedication

To my beautiful wife, for her never-failing support during my studies.

Contents

List of Figures

Chapter 1

Introduction

Contents

1.1 States and statistics

The main thrust behind the development of quantum formalism, and its main usefulness, arises from its ability to predict the outcomes of experiments. Indeed, the kinds of predictions that quantum formalism makes has revolutionized physics. In this thesis, however, we take a much different approach. Instead of using quantum states and operations to determine the outcomes of an experiment, we will use the outcomes of an experiment (or rather the distribution of outcomes) to determine the quantum state and operations.

Why would we want to do this? As quantum formalism moves from the role of a theoretical tool in describing the functioning of the universe to an integral part of technological developments it becomes more important that physical devices are operating as we believe them to be. This is no more apparent than in the case of quantum key distribution in which we posit the

existence of an adversary who actively subverts the functioning of physical devices and modifies quantum states. In experiments intended for academic applications we may rely on academic integrity and repeatability to establish that results are correct, but in the world of security we must be sure that each time we use a device it actually behaves as we believe it to behave, without the benefit of time, repetition, and expert opinion. Indeed, we may have little to go on besides the assurances of the device manufacturer.

Into this context we introduce the concepts of self-testing, device independent quantum key distribution and black box state characterization. The aim of all of these techniques is to replace assumptions about a physical devices with a test. The test will rely solely on the classical data available about the devices: how are the devices connected to each other? What are the measurement setting? What are the outcomes? When we look at the probability distributions for these data we may be able to certify that the devices are behaving properly, or raise a red flag if the functioning of the devices stray from the ideal.

1.2   Terminology

1.2.1   Black box model

Devices

In this thesis we have a particular model in mind for black box computing. In particular, each black box device is a physical device with some combination of quantum and classical inputs and outputs. Devices do not communicate unless we allow them to by physically connecting them together. Each device is labeled with its intended function, but this may bear no resemblance to what the device actually does.

We will concern ourselves with three main types of black box devices

- *Sources*: The only sources we will use are bipartite state sources with two quantum outputs. They are labeled with the state they produce (always $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ in this thesis.)

- *Gates*: Gates will have an equal number of quantum inputs and outputs. Gates will be labeled with a matrix corresponding to the unitary they are supposed to apply.

- *Measurement devices*: We will be concerned with single system measurements in a small number of bases. They have one quantum input and one classical output (one bit in all the cases we consider). We may consider the different measurement bases to be implemented in different physical devices, or there may be a classical input which specifies the basis in which to measure. Measurement devices are labeled with the basis (or bases) in which they measure. We will model measurements as Hermitian observables. We may easily translate the more general POVM formalism into such a description using Naimark's theorem [Nai40]. Since the dimension of the Hilbert space is not fixed this poses no problems.

Device interaction

We need the devices to be able to interact in order to form circuits, but not in an unlimited fashion. If unlimited communication were allowed, then the various devices could operate as a single device with a classical conspiracy. An ideal interaction, from the verifier's point of view, would allow only one-way communication. This would greatly simplify models. Two way communication could lead to a situation equivalent unlimited communication depending on which devices were connected simultaneously. For example, if all devices were simultaneously connected and the graph of their connections were connected then any two devices could communicate through intermediate devices.

One way to enforce one-way communication would be to use a number of identity gate devices and pairwise communication. If we wish for device D_1 to send a state to D_2 we first interact D_1 with an identity device I and the interact I with D_2. This guarantees that no communication occurs from D_2 back to D_1.

State preparation

With black box devices we have no control over what state the device has at its disposal. We might interact a device with a source, but the device may disregard the source and use a state that it already had in memory. In this way, gate and measurement devices may share an arbitrary amount of entanglement. However, this does not give the adversary any more power since we can replace a state in memory with one prepared in the source. For

this reason, we will generally speak of the state as being prepared by the source device without loss of generality.

1.2.2 Reference experiments and simulations

Experiments

The usual way of arranging quantum gates is into a quantum circuit, which consists of a state preparation followed by several unitary gates and finally a measurement. For our purposes this will not be sufficient. In particular we will need to measure in several different bases chosen classically by an agent outside the circuit. We will refer to this type of quantum apparatus as an *experiment*. An important distinction to be made is between the experiment we wish to implement, and the experiment that is actually implemented by the quantum devices. The first we call the *reference experiment*, and the second the *physical experiment*.

Each experiment will have several classical inputs which determine measurements to be made, which we call the *measurement settings*. The *statistics generated by an experiment* is the probability distribution of the measurement outcomes, conditioned on the measurement setting. Another important aspect of an experiment is the *topology*. This is the division of the experiment into distinct elements, each implemented by a single device, and the connections between these elements. A typical topology consists of a bipartite state preparation device connected to two measurement devices. Importantly, we assume that no signalling occurs between devices that are not explicitly connected in the topology, and if there is some physical channel then this cannot be used to communicate backwards.

Assumption 1.1. *No communication occurs between quantum devices that are not explicitly connected. Further, quantum communication from the output of one device to the input of another device is one-way.*

Simulations

The verifier has two pieces of information about an experiment. First, the topology is known, since the verifier is responsible for it. Second, the verifier may estimate the statistics generated by the experiment, provided the experiment behaves the same each time it is used.

Assumption 1.2. *The quantum devices behave the same each time they are used.*[1]

The verifier has a particular reference experiment in mind and wishes to implement it. The verifier then builds a physical experiment with the same topology as the reference experiment using quantum devices and estimates the statistics it generates. Then the verifier may check if the statistics match those generated by the reference experiment.

Definition 1.1. *If a physical experiment generates the same statistics as a reference experiment with the same topology, then the physical experiment* simulates *the reference experiment.*

We will wish to compare the physical and reference systems in various ways. Our goal will always be to show that they are the same in some way or another (or determine they are not and abort.) The raw data that we obtain from any interaction with the physical system will be in the form of classical outcomes from measurements. These classical outcomes are obtained from probability distributions that are determined by the physical system.

Another important concept that we will sometimes refer to is that of a conspiracy. A conspiracy is any behaviour of the black box devices that attempts to defeat a test without actually implementing the reference circuit. One example is for a circuit to classically calculate statistics for a circuit, rather than implementing the circuit. This classical conspiracy immediately implies that we must use non-locality in our testing, since any circuit that is implemented locally has a classical conspiracy.

1.3   Summary of new results

Simulations

In chapter 2 we consider simulations of circuits, which are other circuits which produce the same outcome statistics as a reference circuit. The first main result of this section will be to develop a means of transforming a reference circuit into a simulation circuit which is described using only real numbers. Although such a simulation was known in limited contexts, the simulation we develop works for multi-partite systems general operations such

---

[1]We will consider less restrictive behaviour in Chapter 4.

as completely positive maps, POVMs (positive operator valued measure), and Hamiltonians. The second main result is to describe a family of simulations that generalizes the real simulation.

The real simulation developed is interesting from the perspective of quantum foundations. In particular, the simulation proves that there are no experiments which distinguish between quantum physics over real Hilbert spaces and quantum physics over complex Hilbert spaces (which we will from now on refer to as real quantum physics, and complex quantum physics, respectively.) From the point of view of quantum foundations this eliminates the need to specify which of these two fields to use. In this spirit we also consider other number systems that might be used, specifically quaternions. We show that if we use the quaternions it is possible to implement a non-local box, which allows for stronger non-local effects than can be achieved within complex quantum physics. In principle this allows for an experiment which can distinguish quaternionic quantum physics from complex quantum physics (although not the reverse, since complex quantum physics is contained within quaternionic quantum physics.)

Finally, in chapter 2 we consider the security of cryptographic protocols the are implemented using simulations from the continuum described above. We show that for a limited class of protocols (where all operations of the honest parties are measurements) security is not compromised as compared to the reference protocol.

Self-testing

Self-testing is the workhorse of black box computing. It allows us to test generic quantum circuits, and can be adapted to use with cryptographic protocols such as QKD. In this area our major contribution is new proofs for the major results (state and measurement testing, and gate testing.) The new proofs are simpler and much easier to understand. In the case of gate testing, we provide new proofs for two technical lemmas whose original proofs relied on incorrect assumptions.

Besides new proofs, we also introduce a new test for states and measurements. The previously known test used only measurements with real entries, whereas our new test introduces extra measurements which have complex entries. This paves the way for gate testing of arbitrary gates, where the previous test was only applicable to gates with real entries.

Device independent quantum key distribution

Device independent quantum key distribution represents a new approach to QKD security proofs by using an adversarial device model for the participants' quantum devices. The goal is to provide higher security by removing untestable assumptions and replacing them with physical tests. Previous work in this area identified the main problems, introduced a usable protocol and produced a limited security proof (analogous to security against collective attacks in the usual QKD model.) Our contribution is to push the security boundary further by proving security against a larger class of attacks. These attacks allow arbitrary states and relax the assumptions on the devices. We also introduce new proof techniques to DIQKD, adapting security proofs used for traditional QKD using the quantum de Finetti theorem.

Black box state characterization

We finally consider black box state characterization. The goal is very much similar to that of state and measurement testing we discuss in chapter 3: to test a state preparation device using only untrusted measurements. However, the focus is placed on finding a robust result, measuring the quality of the state with an operationally meaningful definition (in this case, using fidelity.) Our contributions are to find suitable definitions for measures of quality (we introduce several) and to prove bounds using these definitions. We also discuss the relationship between the various definitions.

Chapter 2

Simulations

Contents

2.1   Introduction

Suppose that a physical experiment simulates a reference experiment. What can we conclude? As we shall see, the answer to this question will be quite sensitive to the topology and specific construction of the reference experiment and will vary from nothing to quite strong statements about the structure of the physical experiment. Before we consider this question, however, we look at the complementary question: what can we never hope to conclude?

We will have to be quite specific about the topologies that we consider. For example, take a topology with only one part (i.e. a single-partite state) with a simple reference experiment that implements a search by iterating through a list. This experiment can be simulated by a Grover search, or a procedure that sorts the list and performs a binary search. The structures of these experiments are quite different. We will not be interested in these types of specific simulations. Instead, we wish to find general procedures for producing a simulation of a given circuit.

Contributions

In this chapter we make many original contributions. First, we extend the well known real circuit simulation (described below) to allow POVMs, mixed states, CP maps, and continuous time evolution, completing the suite of general tools used in quantum formalism. Next we show that the real simulation may be applied in the case of multipartite evolution through the use of entangled states.

The real simulation is then generalized to a large family of simulations. The simulations share a common construction for operators and differ in their states. Roughly, the simulations are formed as a mixture of the reference experiment and its complex conjugate.

Later, in chapter 3, we will discuss how we can ensure that a physical experiment is one of the generalized simulations. We may wish to use the physical experiment in a cryptographic protocol, in which case the security properties of the experiment become important. We show that, for a restricted set of protocols, the security properties if implemented by a generalized simulation are identical to if implemented by the reference experiment.

9

Finally, we consider some issues in quantum foundations. Specifically, we discuss how the real simulation implies that the quantum formalism produces identical predictions whether the real numbers or complex numbers are used as the underlying number system. As well, we briefly consider the possibility of using the quaternions instead of the real or complex numbers and show that there exists an experiment for which the quantum formalism over the quaternions allows for different predictions than are possible with the usual quantum formalism.

Some of the original material in this chapter was presented in [MM07] and published in [MMG09]. Further material is available in [McK09b] and is to appear in [MMar].

2.2 Literature review

The concept of a simulation is widespread in the field of quantum computing, although the notion is usually more general, requiring only that the statistics of the measurements are the same as, or approximately the same as, the reference system. As an example, Aharonov et al. [AvDK$^+$04] showed that adiabatic quantum computing is equivalent to the circuit model by describing how to construct an adiabatic simulation for any given quantum circuit. Another family of examples is the various constructions for universal sets of quantum gates (see Nielsen and Chuang [NC00]) where a new circuit containing only gates from a restricted set is constructed from a given circuit. In some of these constructions the outcome statistics are only approximately the same as in the given circuit, although the error can be made arbitrarily small. In all these constructions the form of the system is changed, and only the outcome statistics are the same. However, despite the difference in the system the final state is approximately the same as in the reference system (with an ancilla, in the case of adiabatic computing).

The simple real circuit simulation, described below in section 2.4.1, generalizes work by Rudolph and Grover [RG02]. Their simulation construction, like those for universal gate sets, has a restricted set of gates described using only real numbers, but the final state is in general not the same as in the reference circuit. The construction is well known outside of Rudolph and Grover's work. It also appears, for example, in work by Stueckelberg [Stu60].

The simulation constructions considered so far have not aimed at preserving any of the topology of the reference system. This makes them unsuitable

in situations where the division into multiple physical systems is important, as in the case of Bell inequalities. However, Pál and Vértesi [PV08] considered exactly this situation. In particular, they considered the scenario of two physical systems with local measurements. Their result, derived independently of the results presented here, provided a simulation construction that duplicated the outcome statistics with measurement observables and states described using only real numbers. Importantly, the measurements in the simulation are local, so that the division into two physical systems is respected in the simulation.

2.3   Unitarily equivalent simulations

We first explore various simple modifications on the reference system that do not modify the outcome statistics. We call the results of such modifications *unitarily equivalent simulations*. The idea we wish to convey with this terminology is that the experiment has been modified in a way that is analogous to a change of basis, or changing the description of the Hilbert space.

One obvious and simple modification of a circuit is to make a change of basis. We must be careful in order to respect the division of the circuit into multiple systems. For this reason we consider only local changes of basis. We apply the change of basis (i.e. a unitary) to the initial state and conjugate all unitaries and measurement observables in the circuit by the change of basis operation. The outcome statistics are unchanged and the circuit is not the same.

A local change of basis may also be made between operations. The idea here is that a wire between two unitaries represents a quantum channel that carries the state from one physical device to another. This quantum channel may be anything so long as it faithfully preserves the state. In particular, the channel may apply some arbitrary change of basis at the beginning, and then reverse the change of basis at the end. We may incorporate this change of basis into the two unitaries, as shown in figure 2.2. As an extension of this principle, if multiple wires leave one gate and enter another, we may apply a change of basis to all the wires simultaneously.

An experiment may be described on a particular Hilbert space, but the entire space may not be necessary to describe the state (i.e. if the support of the state is not the entire Hilbert space.) In this case the operation of the gates outside the support of the state may be changed without modifying

$$|\psi\rangle \quad \overline{\quad}\boxed{A}\overline{\quad}\boxed{B}\overline{\quad}\boxed{M}\ \big)$$

$$=$$

$$U|\psi\rangle \quad \overline{\quad}\boxed{UAU^\dagger}\overline{\quad}\boxed{UBU^\dagger}\overline{\quad}\boxed{UMU^\dagger}\ \big)$$
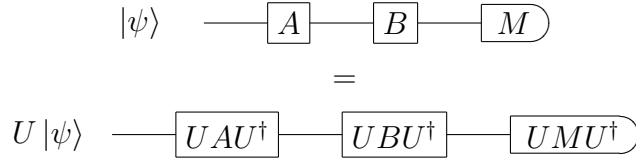
Figure 2.1: Local change of basis on a wire

$$\overline{\quad}\boxed{A}\overline{\quad\quad\quad\quad}\boxed{B}\overline{\quad}$$

$$=$$

$$\overline{\quad}\boxed{A}\overline{\quad}\boxed{U}\overline{\quad\quad}\boxed{U^\dagger}\overline{\quad}\boxed{B}\overline{\quad}$$

$$=$$

$$\overline{\quad}\boxed{UA}\overline{\quad}\boxed{BU^\dagger}\overline{\quad}$$
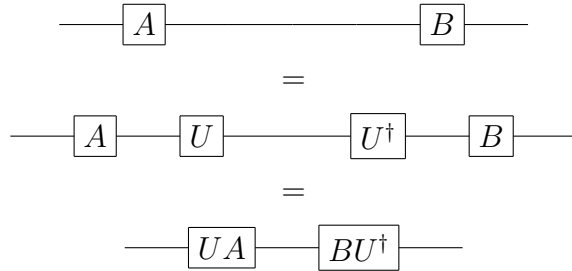
Figure 2.2: Local change of basis between gates

the functioning of the experiment. In addition, the Hilbert space may be changed, either embedded in a larger Hilbert space or reduced to only a subspace without modifying the functionality of the experiment. The idea here is that our model of the system need not consider dimensions that the state does not visit, or our model may be changed arbitrarily on those dimensions without changing how the experiment operates.

Finally, we consider ancillas. The presence of ancillas does not change the outcome statistics provided that the unitaries operate independently on the ancillas and the measurements do not operate on the ancillas. The state of the ancilla does not matter, so we may consider ancillas added to each system in the experiment, prepared in any state.

Of course, any combination of the modifications would not change the outcomes, and so would produce a simulation. After many such modifications the simulation may not look very simple, but the underlying operation of the experiment is essentially untouched. Rather, the way that we are describing it has changed since the choice of basis, division into systems and ancillas, etc. are all a product of our description of the experiment rather than inherent in the experiment itself.

One final modification of a experiment is to take the complex conjugate of every state and operation in the circuit. Obviously this does not change

the outcome statistics, and the experiment will not be the same unless every element in the circuit has only real entries (in the same basis in which we apply the complex conjugation.) However, there is no unitary operation that implements complex conjugation, so we will not consider it as unitarily equivalent. We will consider it more fully later in section 2.5.

2.4   Real simulation

2.4.1   Simple real circuit simulation

We first show a way of arriving at a real simulation of a given reference circuit.[1] This is based on the observation that the complex numbers are a two dimensional real vector space. We can thus, at least formally, represent an arbitrary quantum state as a real vector as follows

$$\sum_x \left(a_x^R + i a_x^I \right) |x\rangle \mapsto \sum_x \left(a_x^R |0\rangle + a_x^I |1\rangle \right) |x\rangle .$$

(a_x^R and a_x^I are real numbers representing the real and imaginary part of the complex number a_x.) Here we have simply replaced the two dimensional vector space spanned by 1 and i by a qubit. The new state has the correct norm as a consequence of the formula

$$|a_x|^2 = \left(a_x^R \right)^2 + \left(a_x^I \right)^2 .$$

Summing over x on the left side gives us the norm of the reference state, while summing over x on the right side gives us the norm of the simulation state. This also shows that we can measure the $|x\rangle$ register on the simulation state in the computational basis and obtain outcome x with the same probability as in the reference state.

So far we have shown how to simulate states and measurements in the computational basis. Now we show how to simulate unitaries. This is more complicated since we need to simulate, not only the norm of complex numbers, but the multiplication of complex numbers. Intuitively we can make a unitary work by making sure that the multiplication involved with each of the entries in the unitary matrix works.

---

[1] This simulation has been present in the folklore for some time.

Suppose that we have two complex numbers a, and b that we want to multiply together. We represent a by the vector $\begin{pmatrix} a^R \\ a^I \end{pmatrix}$. We want to multiply this vector by a suitable matrix derived from b so that the result is the vector

$$\begin{pmatrix} (ab)^R \\ (ab)^I \end{pmatrix}.$$

To get the real part we need $a^R b^R - a^I b^I$, so the first row of the matrix should be $(b^R, -b^I)$. For the imaginary part we want $a^R b^I + a^I b^R$, so the second row should be (b^I, b^R). Thus the matrix we want is

$$\begin{pmatrix} b^R & -b^I \\ b^I & b^R \end{pmatrix}.$$

To transform a matrix of complex numbers, we will replace each complex number by a 2×2 submatrix corresponding to the complex number as above. It is easily shown that this transformation takes unitary matrices to unitary matrices and, as intuition suggests, the resulting unitary maps the simulation state to correctly track the evolution of the reference state.

2.4.2 Complex numbers as matrices

The intuition in the previous section can be made much more rigorous by using a simple field isomorphism.

Lemma 2.1. *Define $R : \mathbb{C} \to M_2(\mathbb{R})$ by*

$$R(a) = a^R I + a^I XZ$$

where

$$XZ = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

is the product of the Pauli matrices X and Z. Then R is an isomorphism between $\mathbb{C}$ and its image under R.

The map R naturally extends to matrices and vectors, mapping $n \times n$ matrices to $2n \times 2n$ matrices, and n vectors to $2n \times 2$ matrices. To be more

rigorous, R maps $n \times n$ matrices over the complex numbers to $n \times n$ matrices over 2×2 matrices, which is naturally mapped to $2n \times 2n$ matrices.

$$R\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = \begin{pmatrix} \begin{pmatrix} a^R & -a^I \\ a^I & a^R \end{pmatrix} & \begin{pmatrix} b^R & -b^I \\ b^I & b^R \end{pmatrix} \\ \begin{pmatrix} c^R & -c^I \\ c^I & c^R \end{pmatrix} & \begin{pmatrix} d^R & -d^I \\ d^I & d^R \end{pmatrix} \end{pmatrix} \mapsto \begin{pmatrix} a^R & -a^I & b^R & -b^R \\ a^I & a^R & b^I & b^R \\ c^R & -c^I & d^R & -d^R \\ c^I & c^R & d^I & d^R \end{pmatrix}$$

It will frequently be useful to have the matrices output from R to be defined over a tensor product space. Specifically, if we are dealing with the Hilbert space $\mathcal{H}$ then we consider the output of R to be $\mathcal{H}_2 \otimes \mathcal{H}$. Using Dirac notation we can then describe R by

$$R\left(\sum_{x,y} u_{xy} |x\rangle\langle y|\right) = \sum_{x,y} \left(u_{xy}^R I + u_{xy}^I XZ\right) \otimes |x\rangle\langle y|.$$

We now give some properties of R, which are easily verified.

Lemma 2.2. *Let operators M and N (which may have 1 column) be given. Then*

1. *$R(M^\dagger) = R(M)^T = R(M)^\dagger$*

2. *$R(A + B) = R(A) + R(B)$*

3. *$R(AB) = R(A)R(B)$*

4. *If M is normal and has (non necessarily distinct) eigenvalues λ_k then $R(M)$ has eigenvalues λ_k and λ_k^*.*

5. *If M is positive semi-definite, then $R(M)$ is positive semi-definite*

6. *If M is unitary, then $R(M)$ is unitary*

7. *If M is Hermitian then $R(M)$ is Hermitian and $\mathrm{Tr}(R(M)) = 2\,\mathrm{Tr}(M)$*

Proof. Items 1 to 3 are easily verified. We prove item 6 first. If M is unitary then $MM^\dagger = I$. Applying item 3 we find

$$R(M)R(M)^\dagger = R(I) = I \otimes I \tag{2.1}$$

so $R(M)$ is also unitary.

We now prove item 4. The remaining items follow immediately. Diagonalize M as $UMU^\dagger = D$. Then

$$R(U)R(M)R(U)^\dagger = R(D) \tag{2.2}$$

Since $R(U)$ is unitary the eigenvalues of $R(M)$ are the same as the eigenvalues of $R(D)$. $R(D)$ is 2×2-block diagonal, with the kth block equal to $R(\lambda_k)$. We may calculate the eigenvalues of $R(\lambda_k)$ directly, using the characteristic equation

$$(\lambda_k^R - \lambda)^2 + (\lambda_k^I)^2 = 0 \tag{2.3}$$

which has roots $\lambda = \lambda_k, \lambda_k^*$. Hence these are the eigenvalue of $R(M)$. $\qquad \square$

2.4.3 Real simulation states and measurements

The map R lets us, at least formally, describe everything quantum using matrices instead of complex numbers. We now show that we can modify R slightly so that it maps quantum states to quantum states, quantum evolution (both discrete and continuous) to valid quantum evolution on the simulation states, and quantum measurements to valid measurements that output the correct statistics from the simulation states.

Density Matrices

Let ρ be a density matrix. Then $\rho' = R(\rho)$ is positive. We now come across a small problem, since the trace of ρ' is 2 instead of 1. We can easily deal with this by multiplying ρ' by 1/2. Below we will show that this is necessary in order to obtain the proper outcome statistics for measurements.

POVMs

Let $\{P_k\}$ be a collection of positive matrices with $\sum_k P_k = I_{\mathcal{H}}$. Then the matrices $\{P_k' = R(P_k)\}$ are all positive and

$$\sum_k P_k' = \sum_k R(P_k) = R(I_{\mathcal{H}}) = I_{\mathcal{H}_2} \otimes I_{\mathcal{H}}.$$

Thus $\{P_k'\}$ is a valid POVM.

Measurement statistics

We will verify the measurement statistics for POVMs, since any measurement can be expressed as such. Let ρ be a density matrix and $\{P_k\}$ be a POVM. As previously discussed, our simulation state will be given by the density matrix $\rho' = R(\rho)/2$ and the simulation POVM will be given by $\{P_k' = R(P_k)\}$. In the reference system the probability of outcome k is given by

$$\mathrm{Tr}(\rho P_k) = p_k$$

Applying R, we obtain

$$p_k = \mathrm{Tr}(\rho P_k) = \frac{1}{2}\mathrm{Tr}(R(\rho)P_k') = \mathrm{Tr}(\rho' P_k')\,.$$

Pure states

We began our discussion of real simulations by giving a transformation that takes pure states to pure simulation states. However, our transformation R does not have this property, since R takes vectors to matrices with two columns. Nevertheless we can define a pure simulation state for each pure reference state.

Let $|\psi\rangle$ be a pure reference state. We then have $\langle\psi|\psi\rangle = 1$. Transforming by R we obtain

$$R(|\psi\rangle)^T R(|\psi\rangle) = I_{\mathcal{H}_2}$$

Thus the two columns of $R(|\psi\rangle)$, which we will denote u and v, are orthogonal and norm 1 and each represents a valid pure state. In fact, these two vectors span the 1 eigenspace of $R(|\psi\rangle\langle\psi|)$. Now consider a reference POVM element P_k. The probability of outcome k is $\langle\psi| P_k |\psi\rangle = p_k$. Transforming by R we obtain

$$\mathrm{Tr}_{\mathcal{H}}\big(R(|\psi\rangle)^T R(P_k)R(|\psi\rangle)\big) = p_k I_{\mathcal{H}_2}$$

This tells us that

$$u^\dagger R(P_k)u = p_k, v^\dagger R(P_k)v = p_k$$

so the two pure states u and v give the same probability for outcome k as the reference experiment. Now if we want our simulation to use a pure state instead of the rank 2 density matrix, we can choose either u, v, or in fact any normalized linear combination of the two and still obtain the correct outcome statistics.

This curious splitting of a pure state into two pure simulation states has a nice interpretation. We return briefly to our original pure simulation state derived from the reference state given by

$$\sum_x (a_x^R + i a_x^I) \ket{x} \rightarrow \sum_x (a_x^R \ket{0} + a_x^I \ket{1}) \ket{x}.$$

We now multiply our reference state by the global phase i and apply the transformation, giving the state

$$\sum_x \left(i a_x^R - i a_x^I \right) \ket{x} \rightarrow \sum_x \left(a_x^R \ket{1} - a_x^I \ket{0} \right) \ket{x}.$$

A quick calculation shows that this state is orthogonal to the previous state. In fact, we can multiply by any global phase and obtain a linear combination of these two states which are exactly the two columns of $R(\ket{\psi})$. This means that we can consider the ambiguity in this 2-dimensional subspace to be equivalent to the ambiguity in assigning a global phase.

2.4.4 State evolution

We have already shown that $R(\cdot)$ maps unitary matrices to unitary matrices. We thus turn our attention to completely positive maps and continuous time evolution.

Completely positive maps

Let $\Phi(\rho) = \sum_k M_k \rho M_k^\dagger$ be a completely positive trace preserving map. Then

$$\sum_k M_k^\dagger M_k = I.$$

Let $\Phi'(\rho) = \sum_k R(M_k) \rho R(M_k)^\dagger$. Then Φ' is completely positive, by its form. It is also trace preserving, since

$$\sum_k R(M_k)^\dagger R(M_k) = R\left(\sum_k M_k^\dagger M_k \right) = R(I_\mathcal{H}) = I_{\mathcal{H}_2} \otimes I_\mathcal{H}$$

where $I_{\mathcal{H}_2}$ is the identity operating on the qubit added by R.

18

Hamiltonians

For Hamiltonians, as with density matrices, we must make a small departure. Recall that a quantum state evolves according to

$$|\psi(t)\rangle = e^{-iHt} |\psi(t_0)\rangle.$$

In order to maintain proper normalization, e^{-iHt} must be unitary. We ensure this by requiring that H be Hermitian. Thus $-iH$ has imaginary eigenvalues and e^{-iHt} will have eigenvalues which have absolute value 1.

We now apply $R(-iH) = R(-i)R(H)$ to obtain

$$|\psi'(t)\rangle = e^{-R(i)R(H)t} |\psi'(t_0)\rangle.$$

Here we have replaced $R(t) = tI$ with t. When considering everything over the field $R(\mathbb{C})$ the value $R(-i) = XZ$ is a scalar. Here we can replace this with the matrix $-XZ \otimes I_{\mathcal{H}}$ to obtain

$$|\psi'(t)\rangle = e^{-XZ \otimes I_{\mathcal{H}} R(H)t} |\psi'(t_0)\rangle.$$

By the properties of R we see that $-XZ \otimes I_{\mathcal{H}} R(H)$ will have imaginary eigenvalues and thus $e^{-XZ \otimes I_{\mathcal{H}} R(H)t}$ will be unitary. We can also use the Taylor expansion and see that each term has only real entries. Thus $e^{-XZ \otimes I_{\mathcal{H}} R(H)t}$ will have only real entries for each t.

Choi-Jamiolkowski representation

Interestingly, despite the success so far, R does not correctly transform the Choi-Jamiolkowski representation $J(\cdot)$ of a superoperator, which we discuss in section 3.5.2. The salient feature is that $J(\cdot)$ is rank 1 if the superoperator is unitary. Since $R(J(U))$ for some unitary U will have double the rank of $J(U)$, $R(J(U))$ does not represent a unitary operation despite the fact that $R(U)$ is unitary. Thus $R(J(U)) \neq J(R(U))$. This is analogous to the fact that pure density matrices are mapped by R to rank 2 matrices.

Other encoded operations

A curious result of the real simulation is that it allows us to perform encoded operations which are not possible on the reference system. For example, we can apply X to the extra qubit and effect a complex conjugation! In this way

we can apply any anti-unitary. We can also perform global phase rotations and measurements by suitably manipulating the extra qubit. So even though we cannot apply these operations to the reference system, we can simulate what the outcome would be if we could.

2.4.5 Real simulations and locality

The simulation presented in the previous section deals with single systems only. If we are dealing with a multi-part system, then R will not generally map a local operation to a local operation. This is because we added a qubit in order to store the phase information and this qubit must be stored somewhere. Any operation involving complex numbers will be mapped to an operation that acts non-trivially on this extra qubit.

We now present a solution to this problem. We suppose that the reference system has k subsystems. The real simulation will consist of k subsystems, each of which corresponds to a reference subsystem with one added qubit.

A simple idea would be to add an extra qubit to each subsystem and perform the real simulation as though each subsystem were isolated. In this situation, a local operation on a particular subsystem would be mapped using R as in the previous section to an operation on the subsystem combined with its extra qubit. This idea quickly fails since the state would be free to move about the entire 2^k dimensional space of the k extra qubits. The isomorphism with $\mathbb{C}$ no longer works because it only has 2 dimensions as a real vector space.

We can fix the naive solution above by constraining the extra qubits to be in a suitable 2-dimensional subspace. It turns out that we can do this merely by choosing a suitable initial state for the qubits. The operators will be as described in the naive solution.

Consider a phase change of i applied to one of the subsystems. We require that this phase change combined another phase change of i to a different subsystem results in an overall phase change of -1. This means that we need the state to be a $+1$ eigenvector of $-(XZ)_m(XZ)_n$ where m and n are two different subsystems. Each of these operators can be generated using operators of the form $-(XZ)_1(XZ)_m$ for different m, so there are $k-1$ independent operators. Thus there is a 2-dimensional subspace stabilized by

these operators. The space is spanned by the vectors

$$\left|\bar{0}\right\rangle = \frac{1}{\sqrt{2^k}} \sum_{h(x)\text{even}} (-1)^{\frac{h(x)}{2}} \left|x\right\rangle$$

$$\left|\bar{1}\right\rangle = \frac{1}{\sqrt{2^k}} \sum_{h(x)\text{odd}} (-1)^{\frac{h(x)-1}{2}} \left|x\right\rangle$$

where x ranges over all k bit strings.

With a bit of accounting it can be seen that if we apply XZ to any one of the k qubits, the effect is to take $\left|\bar{0}\right\rangle$ to $\left|\bar{1}\right\rangle$ and $\left|\bar{1}\right\rangle$ to $-\left|\bar{0}\right\rangle$. Thus these non-local states, together with the local XZ operations, behave exactly as a qubit with its XZ operation. We can now create local simulation operators from local reference operations by replacing $(XZ)_m$ for XZ in our definitions of R.

2.5 General simulations

The real simulation revealed that there exist non-unitarily equivalent simulations, but is this the only non-unitarily equivalent simulation? The answer to this is no. In this section we will develop a large family of simulations. As we shall see, in section 3.7, there exist experiments for which the general simulations described here (along with the unitarily equivalent simulations) are all possible simulations.

Interestingly, if we confine ourself to experiments on a real Hilbert space, then the general simulations all collapse to unitarily equivalent simulations. This allows the self-testing Theorems to be successful for such experiments, as we shall see in chapter 3.

2.5.1 States and measurements

Consider a reference state $\left|\psi\right\rangle$ measured according to a reference POVM $\{P_k\}$.[2] We may duplicate the statistics of this experiment using the complex conjugate state $\left|\psi^*\right\rangle$ and POVM $\{P_k^*\}$. In addition, we could do some combination of the two. We may add an additional qubit register which records

---

[2]We may consider mixed states as well, but it is not necessary for our discussion since we may consider the purification of a mixed state.

which of the two experiments to perform: $|0\rangle$ for the reference experiment, and $|1\rangle$ for the complex conjugate. This qubit may be in any state, and not necessarily pure. We then arrive at new state

$$\rho' = a\,|0\rangle\langle0|\otimes|\psi\rangle\langle\psi|+(1-a)\,|1\rangle\langle1|\otimes|\psi^*\rangle\langle\psi^*|+c\,|0\rangle\langle1|\otimes|\psi\rangle\langle\psi^*|+c^*\,|1\rangle\langle0|\otimes|\psi^*\rangle\langle\psi|$$
$$(2.4)$$

with $a \geq 0$ and $|c| \leq \sqrt{a(1-a)}$. The important feature is that when we project onto $|0\rangle\langle0|$ or $|1\rangle\langle1|$ we get either $|\psi\rangle$ or $|\psi^*\rangle$, respectively. For the measurement, we form the POVM

$$\{|0\rangle\langle0| \otimes P_k + |1\rangle\langle1| \otimes P_k^*\}. \qquad (2.5)$$

This POVM measurement is equivalent to measuring the added qubit, collapsing the state into either $|\psi\rangle$ or $|\psi^*\rangle$ and then measuring either $\{P_k\}$ or $\{P_k^*\}$ as appropriate; thus the statistics of the experiment are preserved.

2.5.2 Operators

We can extend the measurement operator defined in 2.5 to arbitrary operators. We define

$$C(M) = |0\rangle\langle0| \otimes M + |1\rangle\langle1| \otimes M^*. \qquad (2.6)$$

Note that $C(M)$ can be expressed differently as

$$C(M) = I \otimes Re(M) + iZ \otimes Im(M) \qquad (2.7)$$

where $Re(M)$ and $Im(M)$ are the real and imaginary parts of M (both real matrices).

We summarize some of the properties of $C(M)$ here

Lemma 2.3. *Let M and N be matrices. Then we have the following:*

1. *$C(MN) = C(M)C(N)$.*

2. *$C(M + N) = C(M) + C(N)$.*

3. *Let a be a real number, then $C(aM) = aC(M)$.*

4. *If $|\psi\rangle$ is an eigenvector of M (normal) with eigenvalue λ, then $|0\rangle\,|\psi\rangle$ and $|1\rangle\,|\psi^*\rangle$ are eigenvectors of $C(M)$ with eigenvalues λ and λ^*, respectively.*

5. $C(M)$ *is Hermitian if and only if M is.*

6. $C(M)$ *is unitary if and only if M is.*

7. $C(M)$ *is positive semi-definite if and only if M is.*

8. *When M is Hermitian, $Tr(C(M)) = 2\,Tr(M)$.*

These properties can be derived easily. In fact, $R(\cdot)$ and $C(\cdot)$ are related by a unitary transformation, as will be seen in section 2.5.4.

Discrete time evolution

The properties of $C(\cdot)$ allow us to easily determine how the simulation states in the continuum evolve. Let U and $|\psi\rangle$ be a reference unitary operation and state and let ρ' be as in equation 2.4. By the form of $C(U)$ we have

$$C(U)\rho'C(U)^\dagger = a\,|0\rangle\langle 0| \otimes U\,|\psi\rangle\langle\psi|\,U^\dagger + (1-a)\,|1\rangle\langle 1| \otimes U^*\,|\psi^*\rangle\langle\psi^*|\,U^T +$$

$$c\,|0\rangle\langle 1| \otimes U\,|\psi\rangle\langle\psi^*|\,U^T + c^*\,|1\rangle\langle 0| \otimes U^*\,|\psi^*\rangle\langle\psi|\,U^\dagger.$$

But this is the simulation state for $U\,|\psi\rangle$, and hence $C(U)$ evolves the simulation state $|\psi'\rangle$ to produce a new simulation state corresponding to $U\,|\psi\rangle$. Compositions of unitaries will also evolve the state correctly so that the measurement statistics at the end of a circuit will be identical to that of the reference circuit.

General quantum operations may be mapped similarly. It is easy to verify that in Krauss representation a completely positive map is mapped to a completely positive map if we apply $C(\cdot)$ to each of the Kraus operators. The trace preserving property is also preserved. Applying the properties of $C(\cdot)$ we see that

$$\frac{1}{2}\sum_j C(K_j)C(\rho)C(K_j)^\dagger = \frac{1}{2}C\left(\sum_j K_j\rho K_j^\dagger\right). \tag{2.8}$$

23

Continuous time evolution

We begin with a Hamiltonian H. Instead of applying $C(\cdot)$ to obtain the simulation Hamiltonian, we make a small modification, introducing a -1 on the complex conjugated part, thus

$$H' = |0\rangle\langle 0| \otimes H - |1\rangle\langle 1| \otimes H^*. \tag{2.9}$$

This reflects the fact that complex conjugating a Hamiltonian corresponds to time reversal. The evolution of the state will be according to the Schrödinger equation

$$U(t) = e^{-iH't} \tag{2.10}$$

We may take advantage of a property of the exponential function, namely $\exp(A + B) = \exp(A) + \exp(B) - I$ when $AB = 0 = BA$, which may be easily verified by examining the Taylor expansion. Since $|0\rangle\langle 0|\,|1\rangle\langle 1| = 0$ we obtain

$$e^{-iH't} = e^{-i|0\rangle\langle 0|\otimes Ht} + e^{i|1\rangle\langle 1|\otimes H^*t} - I. \tag{2.11}$$

We now use another property of the exponential function: $\exp(P \otimes A) = P \otimes \exp(A) - P \otimes I + I$ when $P^2 = P$. We obtain

$$e^{-iH't} = |0\rangle\langle 0| \otimes e^{-iHt} + |1\rangle\langle 1| \otimes e^{iH^*t}. \tag{2.12}$$

Finally, we use the Taylor expansion and the fact that $a^*b^* = (ab)^*$ to see

$$e^{iH^*t} = (e^{(iH^*t)^*})^* = \left(e^{-iHt}\right)^*. \tag{2.13}$$

Thus

$$e^{-iH't} = C(e^{-iHt}) \tag{2.14}$$

and the simulation evolution tracks that of the reference system.

Another way to think of this is similar to that used in the real simulation in section 2.4. There, rather than considering the Hamiltonian alone, the whole matrix in the exponent, $-iHt$, was considered. Applying $C(\cdot)$ to this matrix we obtain

$$|0\rangle\langle 0| \otimes (-iHt) + |1\rangle\langle 1| \otimes (-iHt)^* = i\left(|0\rangle\langle 0| \otimes H - |1\rangle\langle 1| \otimes H^*\right)t. \tag{2.15}$$

Here the fact that $a^*b^* = (ab)^*$ means $(-iH)^* = iH^*$ and the -1 factor is explained.

2.5.3 Non-local computations

The above family of simulations suffer from the same problem as the real simulation: every operator must have access to the extra qubit added in the simulation. This makes the simulations unsuitable for multi-party computations. This problem can be solved in the same manner as for the real simulation. There an extra qubit was added for each party in the computation and an entangled state was prepared across these qubits. New operators were then defined that interact with these qubits locally in order to have the same effect as the single qubit in the original real simulation.

In order to perform the simulation correctly, each party needs to know whether to apply the original operator or the complex conjugate. For classical mixtures this is no problem, since this information can be stored in a local classical bit for each party. For quantum mixtures, the extra qubit is encoded in a logical qubit which is stored across a number of qubits, each located with a different party. More specifically, each party has a qubit and the combined state is prepared in the GHZ-like state

$$\alpha \left|00\ldots0\right\rangle \left|\psi\right\rangle + \beta \left|11\ldots1\right\rangle \left|\psi'\right\rangle . \tag{2.16}$$

Each party can perform a desired unitary by applying the operator specified in equation 2.7 with the Z operator acting on their local qubit. We see that the Z operator introduces a -1 phase on the imaginary part of the operator when the local qubit is in the state 1, thus applying the complex conjugate of the operator.

2.5.4 Real simulation in the continuum

The real simulation (section 2.4) can be expressed as a simulation in the family defined above through a change of basis. Starting with the state defined for $\alpha = \beta = \frac{1}{\sqrt{2}}$ we have

$$\left|\psi'\right\rangle = \frac{1}{\sqrt{2}} \left|0\right\rangle \left|\psi\right\rangle + \frac{1}{\sqrt{2}} \left|1\right\rangle \left|\psi^*\right\rangle .$$

We next apply a Hadamard gate followed by the relative phase rotation

$$\begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix}$$

to the extra qubit. This is the same as applying the unitary

$$U = \begin{pmatrix} 1 & 1 \\ -i & i \end{pmatrix}. \tag{2.17}$$

The resulting state is

$$\frac{1}{2} |0\rangle \left(|\psi\rangle + |\psi^*\rangle \right) - \frac{i}{2} |1\rangle \left(|\psi\rangle - |\psi^*\rangle \right)$$

which can be rewritten as

$$|0\rangle \, Re(|\psi\rangle) + |1\rangle \, Im(|\psi\rangle)$$

and the real simulation is recovered.

Operators are transformed quite easily. For operator M we conjugate $C(M)$ by $U \otimes I$. From 2.7 we see that the resulting operator is

$$(U \otimes I) \, C(M) \, (U^\dagger \otimes I) = I \otimes Re(M) + XZ \otimes Im(M) \tag{2.18}$$

which is exactly the operator used in the real simulation for M.

For the multiparty real simulation the extra qubits added for each party must also be transformed correctly. We start with the state

$$\frac{1}{\sqrt{2}} |00\ldots 0\rangle |\psi\rangle + \frac{1}{\sqrt{2}} |11\ldots 1\rangle |\psi^*\rangle \, .$$

We now apply a Hadamard gate to *each* extra qubit, resulting in the state

$$\frac{1}{\sqrt{2^{k+1}}} \sum_x |x\rangle |\psi\rangle + \frac{1}{\sqrt{2^{k+1}}} \sum_x (-1)^{h(x)} |x\rangle |\psi^*\rangle \, ,$$

where $h(x)$ is the Hamming weight (number of 1s) of the bit string x and k is the number of parties. Collecting terms gives

$$\frac{1}{\sqrt{2^{k+1}}} \sum_{h(x)\,\text{even}} |x\rangle \left(|\psi\rangle + |\psi^*\rangle \right) + \sum_{h(x)\,\text{odd}} |x\rangle \left(|\psi\rangle - |\psi^*\rangle \right).$$

We now apply the relative phase rotation as above to each extra qubit, resulting in the state

$$\frac{1}{\sqrt{2^{k+1}}} \sum_{h(x)\,\text{even}} (-1)^{\frac{h(x)}{2}} |x\rangle \left(Re(|\psi\rangle) \right) + \sum_{h(x)\,\text{odd}} (-1)^{\frac{h(x)-1}{2}} |x\rangle \, Im(|\psi\rangle)$$

which is the correct state for the multi-party real simulation.

Another way to see this latter transformation is in terms of stabilizers. In [MMG09] it is noted that the entangled states used in the simulation are stabilized by $Y_s \otimes Y_t$ for distinct s, t. Also note that the states used in the simulations defined here are stabilized by $Z_s \otimes Z_t$ for distinct s, t. The qubit-wise transformation applied transforms Z into Y. Collecting terms for the real and imaginary parts completes the transformation.

2.6 Simulations in a cryptographic setting

Suppose that two or more parties are engaged in a cryptographic protocol using self-tested apparatus. Later, in section 3.7, we will develop the extended Mayers-Yao test which allows them to determine that the devices are implementing a simulation from the family of simulations described in section 2.5. Suppose further that the adversary, Eve, knows how the devices are implemented (she provides them) and controls the preparation of the state. The honest parties only perform operations as specified for the simulation. Eve, on the other hand, is free to interact with the extra qubits in the simulation in any way she likes. Does this give any advantage to Eve?

Eve can potentially perform many operations, including entangling a qubit of her own with the extra simulation qubits allowing her to perform simulation operations. She may also interact in complex ways with the extra simulation qubits along with the original register, including performing encoded anti-unitary operations. Despite this, we are able to prove that Eve can gain no advantage for some protocols.

We explore a restricted class of protocols that are especially easy to analyze. These are protocols where the only operation that an honest party will do is a Pauli measurement. This class includes the six-state quantum key distribution protocol (implemented as an entanglement based protocol) (see [BBBW84], [Bru98]). Briefly, the 6-state QKD protocol uses three measurements, X, Y, and Z instead of only X and Z as in BB84. We will demonstrate that these protocols do not leak any more information when implemented using one of the simulations.

The proof is a series of security reductions to protocols in which each reduction only increases Eve's power. We will show that the final protocol in the reduction is just as secure as the reference protocol (without the simulation applied), hence the simulation protocol is also just as secure as the

reference protocol.

For the first reduction we suppose that the participants in the protocol measure their simulation qubit in the Z eigenbasis after the protocol is completed, and transmit the result to Eve. This does not interfere with the intended protocol and only increases Eve's information. Since the Z measurement commutes with all simulation operations, the participants could just as well have performed the measurement before the protocol began. If Eve is the one who prepares the initial state for the simulation (in other cases Eve has strictly less power) then Eve could also perform this measurement herself. This measurement would collapse the state to an eigenvector of the Z measurements and Eve's strategy would be a mixture of different strategies with the states each an eigenvector of the Z measurements.

Let us examine the result of Eve choosing one of these eigenvector states. Each of the parties will receive their extra qubit prepared in a Z eigenvector. The effect of this on their operations is either to perform the protocol's original operation (in the case of a $|0\rangle$) or the complex conjugate (in the case of a $|1\rangle$.) For Pauli measurements, only the Y measurement is affected: the output bit is flipped in the case of the complex conjugate.

If every party receives the same eigenvector in their extra qubit, then the protocol reduces to either the original or the complex conjugate. In either case the security is identical to the original protocol. If the extra qubits are not in the same eigenvector then some Y measurements outcomes will be flipped and some will not. This does not affect Eve's information since she controls which outcomes are flipped and can undo the flips in her reckoning of the final classical information. Note that the bit flips may introduce errors into the protocol. If the protocol does not explicitly check for such errors (as does the 6-state protocol) a test for these errors may be required, however the lack of such a test does not leak information to Eve. Thus the reduced protocol is as secure as the reference protocol, and so is the simulated protocol.

2.7   Quantum formalism over other rings

In the previous sections we have shown that quantum physics over the complex numbers is indistinguishable from quantum physics over the real numbers. That is to say, there is no experiment that can be designed where the predictions of complex quantum physics are different from those of real

quantum physics. The natural question to ask is whether the same is true if we move to quantum physics over the quaternions or other division rings.

2.7.1   Why other rings?

Although the amplitudes for quantum states are usually taken to be complex numbers, we might imagine other objects could be used. Of course these objects must have certain properties in order to be suitable. We will argue that the only objects that can be used are the real numbers, complex numbers, or quaternions. The argument follows that of Adler [Adl95].

Suppose that the amplitudes are drawn from a set V. Adler argues that, since all measurable quantities will reduce to real numbers, we may take V as a general division algebra over the real numbers. In order to define normalized states, and to use the square rule for deriving probabilities we must have a modulus function, N, which assigns a non-negative "size" to each element. That is, $N : V \mapsto \mathbb{R}^+$. We would like N to have the properties

1. $N(r\phi) = |r|N(\phi)$

2. $N(\phi + \theta) \leq N(\phi) + N(\theta)$

3. $N(\phi) > 0$ if $\phi \neq 0$.

These properties are required for N to be a norm on V. Adler also imposes one more constraint. We begin by considering the inner product between two states, $\langle a|b\rangle \in V$. Inserting a resolution of the identity, we obtain

$$\langle a|b\rangle = \sum_c \langle a|c\rangle \langle c|b\rangle \tag{2.19}$$

where $|c\rangle$ runs over some basis (not necessarily including $|a\rangle$ or $|b\rangle$). If there is only one non-zero term in the sum then we obtain

$$\langle a|b\rangle = \langle a|c\rangle \langle c|b\rangle . \tag{2.20}$$

Adler now imposes the restriction

$$N(\langle a|b\rangle)^2 = N(\langle a|c\rangle)^2 N(\langle c|b\rangle)^2 \tag{2.21}$$

which recovers classical probability superposition. Taking the square root everywhere, we obtain the property

$$N(\phi\theta) = N(\phi)N(\theta). \tag{2.22}$$

We now apply a result due to Albert ([Alb47]): the only division algebras over the reals for which an N exists with the properties above are the real numbers, the complex numbers, and the quaternions. This means that the only number systems that can underly the quantum formalism are these three. (Unless, of course, we modify the formalism in some important way.)

We have established a short list of number systems to consider. Why should we consider anything other than the complex numbers? From a foundations perspective we would like to eliminate all possibilities that are not the usual quantum formalism. If we can argue that using something other than the complex numbers would result in a theory that is not viable for some reason, then we do not need to assume the use of the complex numbers as an axiom. A particularly attractive outcome would be an experiment which eliminates other number systems.

2.7.2   Bell inequalities and real quantum formalism

In [Gis07], Gisin notes that all known Bell inequalities can be maximally violated using states and measurements described using only real numbers. Gisin then asks whether this is true for all possible Bell inequalities, or whether there exists a Bell inequality for which a higher violation can be achieved if complex numbers are used. If the latter is the case then such an inequality, and the accompanying physical experiment, could experimentally prove that complex numbers are required. Pál and Vértesi prove in [PV08] that the former is true. The results in this section provide a different and independent proof, since their construction is different. Moreover, the present work applies much more generally. Indeed, there is no experiment whatsoever whose outcomes cannot be duplicated by another experiment described using only real numbers.

More generally, the real simulation shows that quantum formalism over the real numbers is the same as over the complex numbers in the following sense: there are no experimental outcomes predicted by complex quantum formalism that cannot be predicted by real quantum formalism. The reference experiment in the complex formalism translates into the real formalism via the real simulation, giving the same predictions. From a foundations perspective, then, the distinction is not problematic. We can use either number system. Of course there may be more practical reasons for preferring one over the other. With the real numbers, calculations may be more cumbersome, since a larger Hilbert space will in general be necessary. Also, many
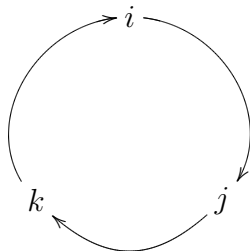
Figure 2.3: Multiplication in the quaternion group

operations are permitted by the real quantum formalism, such as an encoded complex conjugation, that do not seem to occur in nature, so the complex formalism may offer a better fit[3]. This need not be a problem, however, as the complex formalism also allows operations, such as energy non-conserving operations, that do not occur in nature as well.

2.7.3 Quaternionic quantum physics

Quaternions

The Quaternions ($\mathbb{H}$), first described by William Hamilton [Ham44], are a division ring formed by adjoining new elements, i, j, and k to the real numbers $\mathbb{R}$. Thus a quaternion looks like

$$q = a + ib + jc + kd. \tag{2.23}$$

The new elements have the properties

$$i^2 = j^2 = k^2 = ijk = -1. \tag{2.24}$$

The multiplication of the elements i, j, k is summarized in figure 2.3. When multiplying two elements along an arrow (eg. ij) the result is the third element in the cycle. When multiplying backwards along an arrow (eg. ji) a -1 factor is added. So $ij = k$ and $ji = -k$. The elements 1 and -1, of course, commute with the other elements.

Just as complex numbers have a real and imaginary part, quaternions have a scalar and vector part. The scalar part is the part which lies on the real axis. We denote it by $Re(q)$. The vector part, also called the pure

---

[3]Thanks to Bill Wootters for pointing this out.

31

imaginary part, is everything else, and in general is a vector in $\mathbb{R}^3$. We denote it by $Im(q)$. The scalar and vector parts of q, defined above, are $R(q) = a$ and $Im(q) = ib + jc + kd$.

Like in the complex numbers, we may define the *conjugate* of a quaternion, which multiplies each of the non-real parts by -1. Thus the conjugate of q is

$$q^* := a - ib - jc - kd. \tag{2.25}$$

The norm on the quaternions is analogous to that for the complex numbers, i.e.

$$||q|| = \sqrt{qq^*}. \tag{2.26}$$

The most important difference between the complex numbers and the quaternions is that the quaternions do not form a commutative algebra. This property will be the basis for the rest of our discussion.

Quaternionic quantum mechanics

Quaternionic quantum mechanics is formed, roughly speaking, by replacing every complex number in the usual quantum mechanics by a quaternion. Thus states are vectors over the quaternions, so amplitudes are now quaternions instead of complex numbers. The usual norm-squared rule applies for deriving outcome probabilities, and discrete time evolution is described by unitary matrices U over the quaternions with the usual property $UU^\dagger = I$. Now the Hermitian conjugation $(\cdot)^\dagger$ is the matrix transpose, followed by quaternionic conjugation.

Although many more aspects of quantum mechanics, such as continuous time evolution, may be considered, these few properties will suffice for our discussion. For a comprehensive treatment of quaternionic quantum mechanics, see Stephen Adler's book [Adl95].

The tensor product problem

The non-commutative nature of the quaternions introduces many new properties into quaternionic quantum mechanics. The one we are most interested in here is the nature of multi-partite systems.

Consider a bipartite system in the state $\frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)$. Define the unitary matrices R_i and R_j as

$$R_i = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \tag{2.27}$$

$$R_j = \begin{pmatrix} 1 & 0 \\ 0 & j \end{pmatrix} \tag{2.28}$$

We consider different ways that we may apply these matrices. First we apply R_i to the first subsystem, obtaining $\frac{1}{\sqrt{2}}\left(|00\rangle + i\,|11\rangle\right)$. Next we apply R_j to the second subsytem, obtaining

$$\frac{1}{\sqrt{2}}\left(|00\rangle - k\,|11\rangle\right). \tag{2.29}$$

Now consider the same operations, but applied in the reverse order. We apply R_j to the second subsystem, obtaining $\frac{1}{\sqrt{2}}\left(|00\rangle + j\,|11\rangle\right)$, followed by R_i applied to the first subsystem, obtaining

$$\frac{1}{\sqrt{2}}\left(|00\rangle + k\,|11\rangle\right). \tag{2.30}$$

Here we see the non-commutativity of $\mathbb{H}$ in action. The two states in equations 2.29 and 2.30 are orthogonal, but all we have changed is the time-ordering of two local operations on separate subsystems.

The above problem may be stated as follows: $R_i \otimes I$ and $I \otimes R_j$ do not commute. This extends to the tensor product problem: How do we define $R_i \otimes R_j$? Evidently the evolution of subsystems cannot be considered without considering the context of the system as a whole. Adler [Adl95] considers the same problem in the context of continuous evolution:

> We conclude, then, that in quaternionic quantum mechanics, a sum of $N \geq 2$ one-body Hamiltonians gives a many-body Hamiltonian that does not describe N independent particles; the particle motions are coupled through the noncommutativity of the quaternion algebra. (Adler [Adl95], p. 245)

What does this mean for locality? Is there such thing as a local transformation? Is it possible for Alice and Bob to actually perform the operations $R_i \otimes I$ and $I \otimes R_j$? The formalism does not answer this question. However, we may address this problem in another way. If Alice and Bob can locally perform these operations, then they can implement a non-local box.

2.7.4 Quaternionic non-local boxes

The non-local box, first defined by Popescu and Rohrlich in [PR94], is an imaginary device which produces non-local correlations between data in the

following way: Two distant parties, Alice and Bob, each have half of the box. They have one bit of input each, a and b, and input their bit into their half of the box. Each half of the box produces one bit of output, x and y, obeying the property

$$x \oplus y = ab. \tag{2.31}$$

The content of the famous CHSH inequality [CHSH69] is that this condition cannot be satisfied by a non-signalling classical local hidden variable theory with probability better than 0.75 when a and b are chosen uniformly at random. Quantumly, we can do better, but are bounded above by $\cos^2 \pi/8 \approx 0.85$, the Cirel'son bound [Cir80].

Now we consider the case of quaternionic quantum mechanics. Evidently it has stronger non-local behaviour than complex quantum mechanics, but how strong? Clearly we can at least achieve the Cirel'son bound since any strategy in complex quantum mechanics also exists in quaternionic quantum mechanics, but can we do better? The answer is that we simulate the non-local box perfectly.

Consider the two parties, Alice and Bob, as before. Before receiving their inputs they synchronize clocks and choose times $t_1 < t_2 < t_3 < t_4 < t_5$ such that t_1 is after they receive their inputs and t_5 is before they require the outputs (we may arrange it so that the time elapsed is too short to allow signalling by moving Alice and Bob far enough away from each other.) They also share the state $\frac{1}{\sqrt{2}}(|00\rangle + k|11\rangle)$.

Alice does the following:

1. Receive input a.

2. If $a = 0$ then apply operation R_i at time t_1.

3. If $a = 1$ then apply operation R_i at time t_3.

4. At time t_5 measure in the basis $|+\rangle / |-\rangle$ and output the result as x.

   Meanwhile, Bob does the following:

1. Receive input b.

2. If $b = 0$ then apply operation R_j at time t_4.

3. If $b = 1$ then apply operation R_j at time t_2.

4. At time t_5 measure in the basis $|+\rangle / |-\rangle$ and output the result as y.

The protocol is depicted in figure 2.4

Roughly what is happening here is that Alice applies her operation before Bob in all cases except when both of their inputs are 1. Alice and Bob then detect this event using local measurements that are correlated except when Bob goes first, in which case they are anti-correlated.

Consider the outputs that Alice and Bob generate. First note that the final state before measuring will be $|00\rangle \pm |11\rangle$. If Alice and Bob both measure in the basis $|+\rangle / |-\rangle$ their outcomes will be the same if the relative phase was $+$ and opposite if the relative phase was $-$.

Suppose that Bob's input is 0. He will wait until t_4 before applying R_j. Regardless of her input, Alice will apply R_i before Bob applies R_j. Thus the combined effect on $|\psi\rangle$ is a relative phase change of $-k$, taking the state to $|\phi_+\rangle$. Then Alice and Bob's measurements will agree and $x \oplus y = 0 = ab$.

Meanwhile, if Bob's input is 1 the situation changes. If Alice receive the input 0 then she applies R_i at time t_1, Bob applies R_j at time t_2 and the situation is the same as above. However, if Alice receives the input 1 then she applies R_i at time t_3, *after* Bob applies R_j at time t_2. In this case the effect on $|\psi\rangle$ is a relative phase change of k, taking the state to $|\phi_-\rangle$. In this case Alice and Bob's measurements will disagree and $x \oplus y = 1 = ab$.

Communication complexity and information causality

We now briefly consider *communication complexity*. Suppose two parties, Alice and Bob, receive two inputs, a and b. They wish to compute the value of some function $f(a, b)$. How much communication is necessary between Alice and Bob? (for simplicity, we suppose that Alice receives the final answer.) Here we are interested in boolean functions, whose output is a single classical bit. It has been shown by van Dam [vD05] that the communication complexity of all Boolean functions is trivial if non-local boxes are available. This means that Bob needs to send only one bit of information to Alice, and Alice does not have to send anything to Bob. However, there exist Boolean functions, such as the inner product between two strings, for which the communication complexity in either a classical or quantum setting is maximal (i.e. the optimal strategy is for Bob to transmit his entire input to Alice) [BBL+06]. Coupled with the current result we find that within quaternionic quantum mechanics the communication complexity of all boolean functions is trivial.
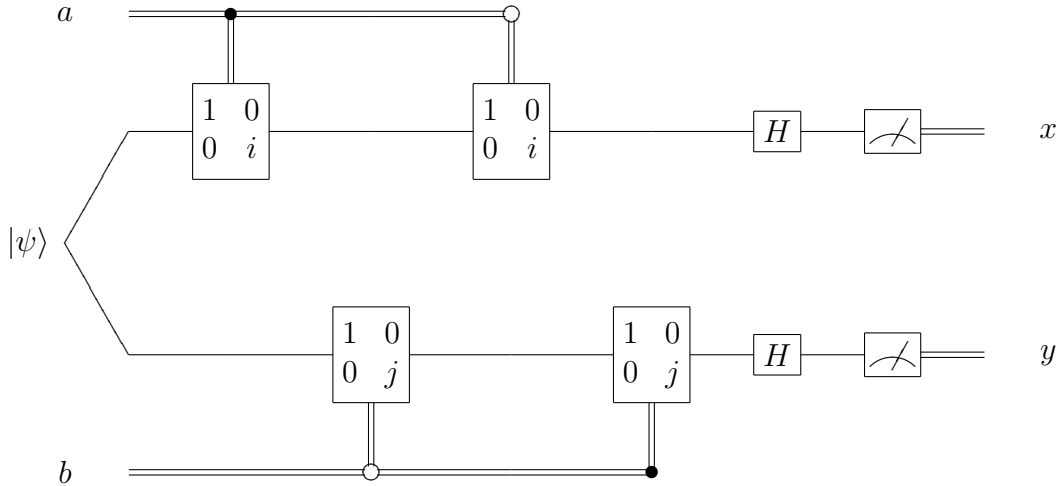
Figure 2.4: Quaternionic non-local box

Later Brassard et al. [BBL$^+$06] turn van Dam's result around, saying that if there is a non-trivial bound on the communication complexity of boolean functions, then non-local boxes do not exist. They also made this result robust by introducing a notion of probabilistic communication complexity and showing that if a non-local box can be approximated with probability better than $\approx .906$ then every boolean function has trivial probabilistic communication complexity. Linden et al [LPSW07] finally showed that for a particular boolean function (AND of two 2-bit strings) if a non-local box can be approximated with probability better than $\cos^2 \pi/8$ (the quantum upper bound) then no communication is required and the function can be approximated better than the classical (and quantum) bound of 0.75. Turning this result around, if the communication complexity of AND of 2-bit strings is non-trivial, then the non-local box cannot be approximated any better than what is achievable by quantum mechanics. In particular, if there is a non-trivial bound on communication complexity then quaternionic quantum mechanics is not a viable theory.

Following this work, Pawlowski et al. [PPK$^+$09] developed the notion of *information causality* which can be seen as a generalization of no-signalling. Both classical and quantum theories obey information causality. Pawlowski et al. were able to show that any physical theory which obeys information

causality also obeys the Cirel'son bound [Cir80]. Thus this is another way of excluding quaternionic quantum mechanics as a viable physical theory.

Chapter 3

Self-testing

Contents

3.1   Introduction

Self-testing is a solution to the follow problem: perform a quantum calculation using only untrusted quantum devices and be sure that the result is correct. For many tasks, such as factoring, this may be trivial since the result can be checked quickly using only classical computation. However, it is not known whether all problems efficiently solvable by a quantum computer can be checked in this fashion (i.e. it is not known whether $BQP \subseteq NP$). Thus there are potentially problems for which a classical check is inefficient. In this chapter we present and extend the main self-testing concepts and constructions, as developed in [MY04] and [MMMO06].

3.2   Literature review

Self-testing was introduced by Mayers and Yao in [MY98]. The initial application was to quantum key distribution. In prepare and measure QKD protocols, it is important that the photon source used does not contain side channels that leak information on the basis choices, although this may be difficult to establish for particular physical implementations. Mayers and Yao proposed to solve this problem by using a self-checking photon source. The idea is that the manufacturer who provides the photon source would also provide several measurement devices. The devices would measure the signal from the photon source and generate some statistics. Checking the classical statistics, the participants in the QKD protocol could then verify that the photon source is operating correctly before continuing the protocol.

    An important consideration in this work is that the photon source is implemented as a source of EPR pairs. One qubit from the EPR pair is measured, and the other is sent out as a signal. The self-check consists of establishing that the initial state is indeed an EPR pair, in which case the

signal does not contain any information about the basis choice since this is only made on the other photon in the pair. This reliance on EPR pairs is a feature that is present throughout the remaining self-testing literature. Another important feature is that the dimension of the Hilbert space of the source is not known beforehand, allowing the result to be applicable in situations where almost nothing is known about the physical implementation of the devices.

Mayers and Yao improved their result in [MY04]. In particular, they broadened the scope of their self-test to a generic setting of a source of EPR pairs and two sets of measurements (one for each half of the state.) Again the result shows that the source produces EPR pairs, but in addition the measurements are also characterized. This is remarkable since they begin without any trusted apparatus, and end up with both a characterized source and measurement devices.

In a parallel development, van Dam et al. [vMMS00] investigated self-testing in the context of quantum circuits. In particular, they developed a series of tests in which a verifier interacts classically with a quantum apparatus by preparing states and measuring in the computational basis and establishes that a gate is operating correctly. (The gate comes with an attached specification.) This work extends self-testing in to the realm of general computing, but relies on some important assumptions. In particular, the Hilbert space of the state is assumed to be known and the devices are used several times with the assumption that it operates identically each time. Also, the computational state preparation and measurement is trusted, and finally the self-tests are only applicable to a particular set of gates (which is sufficient for universal computation.)

The two lines of research were merged in [MMMO06] by Magniez et al.. There, the reliance on a particular Hilbert space and trusted computational bases preparation and measurement is removed. This is done by preparing states in a variety of bases; EPR pairs are prepared and one half is measured in three different bases. This initial step is self-tested using the Mayers-Yao result. As well, the Mayers-Yao result is invoked to characterize the measurement devices. Once these two steps are accomplished, the gate is the only remaining untrusted element, and it may be tested using the now trusted state preparation and measurement. Besides introducing the circuit test, Magniez et al. improved the Mayers-Yao result by making it robust, allowing their circuit test to be robust as well.

3.3 Definitions and main Theorems

3.3.1 Self-testing concepts

The context for self-testing includes a *verifier* and several black-box quantum devices. Ideally, no assumptions are made about the devices that cannot be verified in some way. For example, we wish not to make any assumptions about the Hilbert space that states live in and gates operate on.

The verifier interacts with the quantum devices in three ways. First, the verifier arranges the quantum devices into a circuit by connecting quantum inputs and outputs of various devices. Second, the verifier provides classical inputs (*measurement settings*) to the devices. Finally, the verifier obtains classical outputs from the devices (*outcomes*). Importantly, we assume that no signalling occurs between devices that are not explicitly connected in the topology, and if there is some physical channel then this cannot be used to communicate backwards.

Assumption 3.1. *No communication occurs between quantum devices that are not explicitly connected. Further, quantum communication from the output of one device to the input of another device is one-way.*

There are two pieces of information about an experiment available to the verifier. First, the topology is known, since the verifier is responsible for it. Second, the verifier may estimate the statistics generated by the experiment, provided the experiment behaves the same each time it is used.

Assumption 3.2. *The quantum devices behave the same each time they are used.*

The statistics will allow the verifier to determine if the physical experiment simulates the reference experiment. In the case that it does not, we offer no conclusions. If it does, however, then we can make some non-trivial conclusions about the structure of the physical experiment, which will be the subject of this chapter.

3.3.2 Equivalence

For general reference experiments, if the verifier is able to calculate the statistics generated in order to compare with a physical experiment, then there is little value in performing the physical experiment; the verifier may do the

calculation themselves. The strength of self-testing is in choosing experiments for which the statistics are easy to calculate - many such experiments are performed, each one adding more gates - and combining the conclusions gained from each experiment to conclude that the final experiment simulates the desired reference experiment.

In order to combine results about individual experiments and make the final conclusion, we need a notion stronger than simulation. Consider the case of factoring. A physical experiment that outputs the factors of a large number may perform the calculation in any number of ways, from Shor's algorithm to brute force search. All of these methods simulate each other, but clearly they are different in important ways. For this reason we introduce the concept of *equivalence*. We intend to capture the idea that, to the greatest extent we can possibly conclude, the physical experiment is *the same as* the reference experiment.

When defining a notion of equivalence in this setting we must first consider how me might change the reference experiment in a way that preserves the statistics of the outcomes. Any such change is invisible from the perspective of the verifier and hence we cannot rule them out. Here is a list of such changes

1. Local changes of basis

2. Adding ancillae to physical systems, prepared in any joint state

3. Changing the action of the observables outside the support of the state

4. Locally embedding the state and operators in a larger (or smaller) Hilbert space

In order to accommodate these various changes we define equivalence as follows:

Definition 3.1. *A reference experiment is described by a n-partite state $|\psi\rangle$ on Hilbert space $\mathcal{X} = \mathcal{X}_1 \otimes \ldots \mathcal{X}_n$ and local measurement observables (acting on a single part) M_m for various m. Further, consider a physical experiment described by a n-partite state $|\psi'\rangle$ on Hilbert space $\mathcal{Y} = \mathcal{Y}_1 \otimes \cdots \otimes \mathcal{Y}_n$ and local measurement observables M'_m for various m. We say that the physical experiment is* equivalent *to the reference experiment (and the physical*

state and measurement observables are equivalent to the reference state and measurement observables) if there exists a local isometry

$$\Phi = \Phi_1 \otimes \ldots \Phi_n, \quad \Phi_j : \mathcal{Y}_j \mapsto \mathcal{Y}_j \otimes \mathcal{X}_j \tag{3.1}$$

such that

$$\Phi(|\psi'\rangle) = |junk\rangle_{\mathcal{Y}} \otimes |\psi\rangle_{\mathcal{X}} \tag{3.2}$$
$$\Phi(M'_m |\psi'\rangle) = |junk\rangle_{\mathcal{Y}} \otimes M_m |\psi\rangle_{\mathcal{X}}. \tag{3.3}$$

When we are performing gate testing, we will be concerned with several experiments, and several equivalences at once. The particular isometries and junk state $|junk\rangle_{\mathcal{Y}}$ used will be important. In this case we will specify them.

The isometry Φ may be constructed by attaching ancillae in some product state $|00\ldots0\rangle_{\mathcal{X}}$ and applying local unitaries to the subsystems. Note that if we make any finite number of changes from the list above then we may construct a suitable local isometry and show that the experiment is equivalent to the reference experiment. Also, any experiment that is equivalent to the reference experiment may be constructed by applying changes from the list above: one simply attaches ancillae in the state $|junk\rangle$ and performs a suitable change of basis. Equivalence is thus exactly the notion we need to take these changes into account.

3.3.3 Results and contributions

The central idea behind self-testing is that, for certain carefully chosen experiments, simulation implies equivalence. Furthermore, experiments may be grouped together to strengthen the conclusions. This allows us to construct self-tests for

- EPR pairs along with a particular set of measurements

- Real unitaries on single qubits and CTRL-Z gates

- Arbitrary circuits composed of the above gates

These results are already present in [MY04] and [MMMO06], however we make several contributions:

- Streamlined definitions and notation

- New (and often simplified) proofs for all results

- Corrected proofs for certain technical lemmas

- Explanation of the restriction to real unitaries

We also extend the definition of equivalence, taking into account the results of chapter 2, and extend the Mayers and Yao test for EPR pairs to include complex measurements. This lays the foundation for self-testing of complex gates.

The extended Mayers and Yao test is to be published in [MMar].

3.4 State and measurement testing

The backbone of self-testing is in testing states and measurements. Since we cannot test these individually without relying on some trusted apparatus, we test them simultaneously. The test that we use here was developed by Mayers and Yao [MY04].

Theorem 3.1 (Mayers and Yao [MY04])**.** *Suppose a physical experiment has the same topology and generates the same statistics as the reference experiment described in section 3.4.1. Then the physical experiment is equivalent to the reference experiment.*

3.4.1 State and measurement self-test reference experiment

A general schematic for the Mayers-Yao reference experiment is shown in figure 3.1. A bipartite state $|\psi\rangle$ is distributed to a pair of measurement devices. The two measurement devices take classical inputs a and b, which each take one of three values. The devices then output classical bits, x and y.

The reference state is an EPR pair $|\phi_+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and the reference measurement observables are $X, Z, \frac{X+Z}{\sqrt{2}}$ for each side of the EPR pair. For brevity we label $\frac{X+Z}{\sqrt{2}} = D$. For physical devices we will have to derive this relationship, so there the separate label D is required.
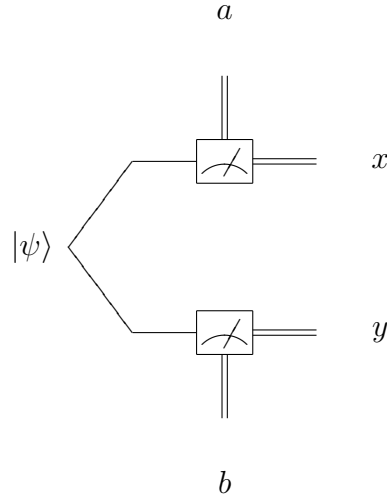
Figure 3.1: Mayers-Yao self-test circuit

3.4.2 Proof of Theorem 3.1

Proof Overview

The main advantages of the following new proof for the Mayers-Yao self-test is that it is shorter, clearer, and more naturally extends to the more general test given in this paper.

The proof has two distinct parts. The first part establishes some equations on the state and observables based on the observed statistics. These are straightforward and are a direct result of the statistics observed. Next we use these equations to show that the X and Z observables on each side anti-commute on the support of the state. The second part uses the anti-commuting observables to construct local isometries that take the state and observables to the reference state and observables.

Statistics

In the reference experiment the marginals for each observable are all 0. That is,

$$\langle \phi_+ | \, M \otimes I \, | \phi_+ \rangle = 0$$

for $M \in \{X, Z, D\}$. (Swapping the systems in this and the following equations gives the same result since $| \phi_+ \rangle$ is symmetric.) Measuring the same

45

observable on both sides always give identical outcomes. Thus

$$\langle\phi_+|\, M \otimes M \,|\phi_+\rangle = 1.$$

Additionally, X and Z measurements are uncorrelated.

$$\langle\phi_+|\, X \otimes Z \,|\phi_+\rangle = 0.$$

The interesting part comes when we measure X or Z on one side and D on the other.

$$\langle\phi_+|\, X \otimes D \,|\phi_+\rangle = \langle\phi_+|\, Z \otimes D \,|\phi_+\rangle = \frac{1}{\sqrt{2}}$$

State equalities

Using the equations on the measurement outcomes from above and the fact that $|\psi\rangle$ is normalized gives us the following equations.

$$
\begin{align}
|\psi\rangle &= X_A \otimes X_B \,|\psi\rangle \tag{3.4}\\
&= Z_A \otimes Z_B \,|\psi\rangle \tag{3.5}\\
&= D_A \otimes D_B \,|\psi\rangle \tag{3.6}\\
X_A \otimes I \,|\psi\rangle &= I \otimes X_B \,|\psi\rangle \tag{3.7}\\
Z_A \otimes I \,|\psi\rangle &= I \otimes Z_B \,|\psi\rangle \tag{3.8}\\
D_A \otimes I \,|\psi\rangle &= I \otimes D_B \,|\psi\rangle \tag{3.9}\\
X_A Z_A \otimes I \,|\psi\rangle &= I \otimes Z_B X_B \,|\psi\rangle \tag{3.10}\\
Z_A X_A \otimes I \,|\psi\rangle &= I \otimes X_B Z_B \,|\psi\rangle \tag{3.11}\\
X_A Z_A \otimes I \,|\psi\rangle &= X_A \otimes Z_B \,|\psi\rangle \tag{3.12}\\
Z_A X_A \otimes I \,|\psi\rangle &= Z_A \otimes X_B \,|\psi\rangle \tag{3.13}
\end{align}
$$

We can also establish some orthogonality relationships between various vectors. In particular the vectors $|\psi\rangle , X_A \otimes I \,|\psi\rangle , Z_A \otimes I \,|\psi\rangle , X_A Z_A \otimes I \,|\psi\rangle$ are pairwise orthogonal.

Our goal for the remainder of the proof is to show that any state for which these equations hold must be equivalent to $|\phi_+\rangle$.

Anti-commuting observables

We now move to more salient matters. First, we note that $D_A \otimes I \ket{\psi}$ must be in the space spanned by $X_A \otimes I \ket{\psi}$ and $Z_A \otimes I \ket{\psi}$ because it has overlap $\frac{1}{\sqrt{2}}$ with each of these orthogonal vectors, and it has norm 1. Thus

$$D_A \otimes I \ket{\psi} = \frac{X_A + Z_A}{\sqrt{2}} \otimes I \ket{\psi}$$

and analogously for $I \otimes D_B \ket{\psi}$. This allows us to make the following deductions.

$$
\begin{aligned}
\ket{\psi} &= D_A \otimes D_B \ket{\psi} \\
&= \frac{1}{2}(X_A + Z_A) \otimes (X_B + Z_B) \ket{\psi} \\
&= \ket{\psi} + (X_A \otimes Z_B + Z_A \otimes X_B) \ket{\psi}
\end{aligned}
$$

Applying equations 3.7 and 3.8 we obtain

$$(X_A Z_A + Z_A X_A) \otimes I \ket{\psi} = 0. \tag{3.14}$$

By Lemma 3.1, below, it follows that X_A and Z_A anti-commute on the support of $\ket{\psi}$ on A. Similarly, the observables X_B and Z_B anti-commute on support of $\ket{\psi}$ on B.

Lemma 3.1. *Let X_A and Z_A be operators and $\ket{\psi}_{AB}$ a bipartite state such that*

$$X_A Z_A \otimes I_B \ket{\psi}_{AB} = -Z_A X_A \otimes I_B \ket{\psi}_{AB}. \tag{3.15}$$

then $X_A Z_A \ket{\phi} = -Z_A X_A \ket{\phi}$ for any $\ket{\phi}$ in the support of $\ket{\psi}_{AB}$ on A.

Proof. Let

$$\ket{\psi} = \sum_j \lambda_j \ket{j}_A \ket{j}_B \tag{3.16}$$

be the singular value decomposition of $\ket{\psi}$. We then have

$$X_A Z_A \otimes I_B \sum_j \lambda_j \ket{j}_A \ket{j}_B = -Z_A X_A \otimes I_B \sum_j \lambda_j \ket{j}_A \ket{j}_B. \tag{3.17}$$

We now take the inner product with $\ket{k}_A \ket{k}_B$ for some k, to obtain

$$\lambda_k \bra{k}_A X_A Z_A \ket{k}_A = -\lambda_k \bra{k}_A X_A Z_A \ket{k}_A. \tag{3.18}$$
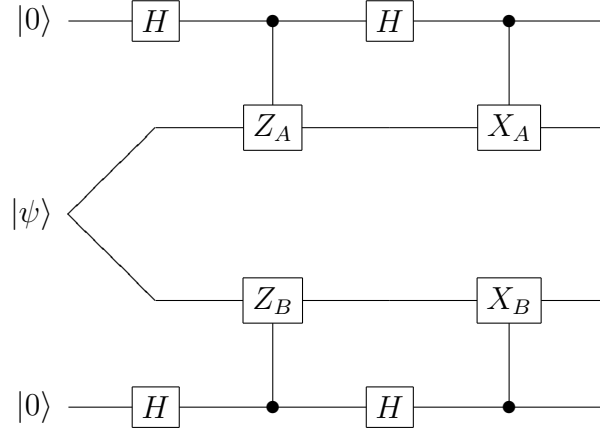
Figure 3.2: Circuit for Φ showing equivalence of physical circuit to reference circuit in Mayers-Yao test

When we restrict to the subspace to the subspace spanned by the $|k\rangle_A$ for which $\lambda_k \neq 0$ (i.e. on the support of $|\psi\rangle$ on A) we find that $X_A Z_A = -Z_A X_A$.
□

Construction of the local isometry

Now we can easily build the local unitaries required to extract the EPR pair. We use the circuit shown in figure 3.2. There the outer $|0\rangle$ states are added while the two inner wires carry the two halves of the bipartite state $|\psi\rangle$. This circuit essentially builds a SWAP gate out of two CNOT gates (the usual third gate is not necessary since we initialize with $|0\rangle$.) The SWAP gate extracts the entanglement out of $|\psi\rangle$ and swaps in a product state.

The circuit gives two isometries, one for each wire in EPR test circuit, which we denote Φ_A and Φ_B.

Isometry applied to state

After applying this circuit the resulting state is

$$
\begin{aligned}
\Phi_A \otimes \Phi_B(|\psi\rangle) &= \frac{1}{4}(I + Z_A) \otimes (I + Z_B)|\psi\rangle|00\rangle \\
&+ \frac{1}{4}(I + Z_A) \otimes X_B(I - Z_B)|\psi\rangle|01\rangle \\
&+ \frac{1}{4}X_A(I - Z_A) \otimes (I + Z_B)|\psi\rangle|10\rangle \\
&+ \frac{1}{4}X_A(I - Z_A) \otimes X_B(I - Z_B)|\psi\rangle|11\rangle .
\end{aligned}
$$

Applying some equations and the anti-commuting result from the previous section we find that this is equal to

$$
\Phi_A \otimes \Phi_B(|\psi\rangle) = \frac{1}{4}(I + Z_A) \otimes (I + Z_B)|\psi\rangle(|00\rangle + |11\rangle) +
$$

$$
(I + Z_A)(I - Z_A) \otimes X_B|\psi\rangle|01\rangle + X_A \otimes (I + Z_B)(I - Z_B)|\psi\rangle|10\rangle
$$

$$
= \frac{1}{\sqrt{2}}(I \otimes I + I \otimes Z_B)|\psi\rangle|\phi_+\rangle . \tag{3.19}
$$

This may look curious since $I + Z_A$ and $I + Z_B$ are not unitary. In fact it is easy to show that the final state still has the correct norm. To give some intuition, note that in the reference case we want to extract $|\phi_+\rangle$ and swap in $|00\rangle = \frac{1}{2\sqrt{2}}(I + Z) \otimes (I + Z)|\phi_+\rangle$.

Isometry and measurement operators

We start with X_A (the result for X_B follows analogously). Applying X_A to $|\psi\rangle$ before applying the circuit is the same as applying it at the end, with a -1 phase introduced by anti-commuting past the controlled Z_A operation (recall from section 3.4.2 that X_A and Z_A anti-commute on the relevant subspace).

The resulting state is

$$\Phi_A \otimes \Phi_B(X_A \otimes I_B \ket{\psi}) = \frac{1}{4} X_A(I - Z_A) \otimes (I + Z_B) \ket{\psi} \ket{00}$$
$$+ \quad \frac{1}{4} X_A(I - Z_A) \otimes X_B(I - Z_B) \ket{\psi} \ket{01}$$
$$+ \quad \frac{1}{4}(I + Z_A) \otimes (I + Z_B) \ket{\psi} \ket{10}$$
$$+ \quad \frac{1}{4}(I + Z_A) \otimes X_B(I - Z_B) \ket{\psi} \ket{11}.$$

Following the same logic as used in the state equivalence, we find that the final state is

$$\Phi_A \otimes \Phi_B(X_A \otimes I \ket{\psi}) = \frac{1}{\sqrt{2}}(I \otimes I + I \otimes Z_B) \ket{\psi} (X \otimes I) \ket{\phi_+}.$$

For the Z_A operation, we see that the effect is a -1 phase kicked back through the final controlled X_A operation. This phase appears on the terms with $\ket{1}$ in the qubit, exactly as if a Z operation had been applied to the qubit. The equivalence for the D operators results from the fact that $D = \frac{X+Z}{\sqrt{2}}$ on the relevant subspace, and linearity.

This concludes the proof of Theorem 3.1 .

3.5 Gate self-test

3.5.1 Main result

Unlike state and measurement testing, gate testing will require three different experiments. The first two are state and measurement tests, and the last verifies the operation of the gate. We wish to test a gate $T \in U(\mathcal{X})$ with the restriction that T have all real matrix entries. For our purposes we will consider $\mathcal{X} = \mathcal{H}_2$ with T any real unitary, and $\mathcal{X} = \mathcal{H}_2^2$ with $T = \text{CTRL-}Z$. Note that this set of gates is sufficient to simulate universal quantum computation using the real simulation given in section 2.4. The reference state $\ket{\phi}$ will either be an EPR pair, $\ket{\phi_+}$, or a pair of EPR pairs. Measurements M_a and N_b will be the tensor products of the real operators $\{I, X, Z, \frac{X+Z}{\sqrt{2}}\}$.

The experiments are as follows: First we test the state $\ket{\phi}$ and the measurements, as in figure 3.3 (experiment 1). This establishes that the state
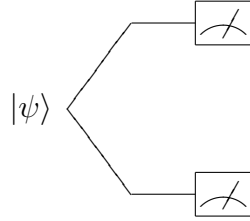
Figure 3.3: EPR test
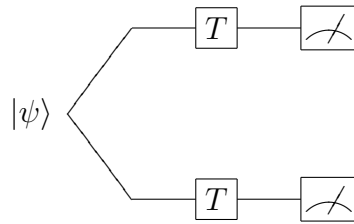
Figure 3.4: EPR test after gates applied

is correct, and that the measurements applied directly to the state are also correct. Next we apply $T \otimes T$ to $|\phi\rangle$ and then measure, as in figure 3.4, which tests whether the measurements are still operating correctly *after* the gate is applied (experiment 2). (Note that for T real and our chosen state, $T \otimes T |\phi\rangle = |\phi\rangle$.) Finally, we apply $T \otimes I$ to $|\phi\rangle$ and measure, as in figure 3.5 (experiment 3).

We can think of the final test in the following way: Measuring the B side of the maximally entangled state is equivalent to preparing a state on the A side. Critically, there is no information about the basis A side. We then apply the gate to this prepared state and measure afterwards in a variety of bases to establish that the gate is working. Also, since there is no way to distinguish the second and third tests from the A side alone, either the measurement is working correctly or will be detected as faulty.

Recall Assumption 3.2, that the devices always operate the same. Also, we assume that there is one way communication along the quantum channels and no side channels. Thus the devices cannot determine which experiment is being performed. The B side measurements devices cannot distinguish between experiments 1 and 3, and so the B side measurements on experiment 3 are implicitly tested by experiment 1. Likewise, the A side measurement devices cannot distinguish between experiments 2 and 3, and so are implicitly
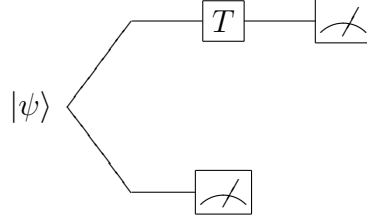
Figure 3.5: Testing a gate

verified by experiment 2 to be working correctly in experiment 3.

One potential concern is the fact that a physical device may hold the state in memory rather than receiving it from the source device. In fact this is not a concern. If this were the case, then we simply take $|\psi\rangle$ to be the state held in memory across all devices. There remains the possibility that the maximally entangled pairs found in experiment 1 and 2 are not the same pairs. However, they must in fact be the same pair since the statistics generated by experiment 3 are only possible for a maximally entangled state, with one measurement the same as in experiment 1 and the other the same as in experiment 2. The net result is that we do not have to concern ourselves with this possibility since the Theorem takes care of this case as well.

Theorem 3.2. *Suppose that a collection of physical devices are arranged into three physical experiments:*

- *(experiment 1) $|\psi\rangle$ with measurements $M'_a \otimes N'_b$*

- *(experiment 2) $G' \otimes H' |\psi\rangle$ with measurements $M''_a \otimes N''_b$*

- *(experiment 3) $G' \otimes I_{\mathcal{Y}} |\psi\rangle$ with measurements $M''_a \otimes N'_b$.*

Further suppose that each physical experiment simulates the corresponding reference experiment described above. Then there exist unitaries U_A, U_B, V_A, V_B and state $|junk\rangle_{\mathcal{Y}}$ such that

- *physical experiment 1 is equivalent to reference experiment 1 with unitaries $U_A \otimes U_B$*

- *physical experiment 2 is equivalent to reference experiment 2 with unitaries $V_A \otimes V_B$*

- *physical experiment 3 is equivalent to reference experiment 3 with unitaries $V_A \otimes U_B$*

with junk state $|junk\rangle_{\mathcal{Y}}$ in each case. Moreover,

$$V_A G' \otimes I_{\mathcal{X}} U_A^\dagger = I_{\mathcal{Y}} \otimes T \qquad (3.20)$$

on the support of $|junk\rangle_{\mathcal{Y}^2}$ on $\mathcal{Y}_A$.

The theorem compares the reference gate T with the physical gate G, and establishes, roughly, that if G simulates T then it is equivalent to T.

3.5.2 Technical background for proof

Choi-Jamiolkowski representation

We first define the Choi-Jamiolkowski representation of a linear map on operators [Jam72] [Cho75] and discuss its properties. We define it as follows

Definition 3.2. *Let $\Phi : L(X) \to L(Y)$ be a linear operator. Then the* Choi-Jamiolkowski representation *of Φ is given by the operator*

$$J(\Phi) = \sum_{x,y} \Phi(|x\rangle\langle y|) \otimes |x\rangle\langle y|$$

operating on the space $L(Y) \otimes L(X)$

An equivalent definition is

$$J(\Phi) = \Phi \otimes I_{L(X)} \left(\sum_{x,x'} |xx\rangle\langle x'x'| \right).$$

Thus $J(\Phi)$ can be found by applying Φ to one half of a maximally entangled state on $X \otimes X$, finding the density matrix, and multiplying by a suitable scaling factor (the dimension of X).

We will use the following properties of $J(\Phi)$.

Theorem 3.3. *Let $\Phi : L(X) \to L(Y)$ and $J(\Phi)$ be given. Then*

- *Φ is completely positive if and only if $J(\Phi)$ is positive semi-definite.*

- *Φ is trace preserving if and only if $Tr_Y J(\Phi) = I_X$.*

- Φ *is unitary if and only if $J(\Phi)$ is rank 1 and the above two conditions hold.*

For more details and rigorous proofs, see Watrous' lecture notes [Wat08a]. We do not give a formal proof here, but instead offer some intuition. If we interpret $J(\Phi)$ as the output from the completely positive map $\Phi \otimes I$, then it should be PSD whenever the input is. For the second property, we start with a maximally entangled state, so tracing out one side should leave us with the completely mixed state. For the last property, we are inputing a pure state, so the output should be pure if the map is unitary. The converses of these statements are, of course, more difficult and we leave out the proofs.

Technical Lemmas

The following Lemma is a restriction of Lemma 5 appearing in [MMMO06], arXiv version. The proof given by Magniez et al. contains an error, since real density matrices in general are *not* in the span of the tensor products of $\{I, X, Z\}$. As a concrete example, $|\phi_+\rangle\langle\phi_+|$ contains $Y \otimes Y$, a real matrix, in its decomposition into Paulis. Here we give correct proofs for the case of two qubits, the case of four qubits with $T = \text{CTRL-}Z$, and the case of a tensor product of such gates on any number of qubits. The proof for the second case could be adapted to work with other two qubit Clifford gates as well.

Lemma 3.2. *Let $\sigma = |\psi\rangle\langle\psi|$ be a two qubit state with $|\psi\rangle = T \otimes I \, |\Phi+\rangle$ and T a unitary having real coefficients. Further, suppose that*

$$Tr(\rho M \otimes N) = Tr(\sigma M \otimes N) \tag{3.21}$$

for $M, N \in \{I, X, Z\}$. Then $\rho = \sigma$.

Proof. We first fix some notation. Let U and V be 2-qubit Pauli operators. Let $U \cdot V$ be defined by

$$U \cdot V = \begin{cases} 1 & U \text{ and } V \text{ commute} \\ -1 & U \text{ and } V \text{ anti-commute.} \end{cases} \tag{3.22}$$

Also, for density operator ρ (and analogously for σ and other density operators) define ρ_U by

$$\rho_U = \text{Tr}(\rho U) \tag{3.23}$$

and analogously for other density operators. Note that $|\rho_U| \leq 1$.

We will make use of the following observations about σ, which can be easily verified from the fact that T is unitary and real. For M and N Pauli operators we find

- $$\sum_{M,N \in I,X,Y,Z} \sigma^2_{M \otimes N} = 4$$

- $\sigma_{Y \otimes M} = \sigma_{M \otimes Y} = 0$ when $M \neq Y$

- $|\sigma_{Y \otimes Y}| = 1$

- $\sigma_{M \otimes I} = \sigma_{I \otimes M} = 0$ for all $M \neq I$.

Since σ and ρ are positive semi-definite, we have

$$\mathrm{Tr}\left(\rho U \sigma U^\dagger\right) \geq 0$$

for any unitary U. We may write this, using the notation above, as

$$\sum_{P \in \{I,X,Y,Z\}^{\otimes 2}} \rho_P \sigma_P (U \cdot P) \geq 0.$$

With the choice $U = Y \otimes I$ we find

$$1 - \sum_{M,N \in \{X,Z\}} \rho_{M \otimes N} \sigma_{M \otimes N} + \rho_{Y \otimes Y} \sigma_{Y \otimes Y} = -1 + \rho_{Y \otimes Y} \sigma_{Y \otimes Y} \geq 0.$$

This is obtained by removing 0 terms and noting that $\sum_{M,N \in \{X,Z\}} \sigma^2_{M \otimes N} = 2$. The implication is that $\sigma_{Y \otimes Y} = \rho_{Y \otimes Y}$ and hence $\sigma_{M \otimes N} = \rho_{M \otimes N}$ whenever $\sigma_{M \otimes N}$ is not 0.

Let S be the set of Pauli operators $M \otimes N$ for which $\sigma_{M \otimes N} \neq 0$. Then, since $\sigma_{M \otimes N} = \rho_{M \otimes N}$ for all $M \otimes N \in S$ we have

$$\mathrm{Tr}\left(\rho^2\right) = 1 + \frac{1}{4} \sum_{M \otimes N \notin S} \rho^2_{M \otimes N} \leq 1$$

since ρ has trace 1. This immediately implies that $\rho_{M \otimes N} = 0$ for $M \otimes N \notin S$ and hence $\rho_{M \otimes N} = \sigma_{M \otimes N}$ for all $M \otimes N$. Recall that the 2-fold tensor products of the Pauli operators form a basis for the space of 2-qubit states. Thus $\rho = \sigma$. $\qquad \square$

Lemma 3.3. *Let* $\sigma = |\psi\rangle\langle\psi|$ *be a four qubit state with*

$$|\psi\rangle = CTRL\text{-}Z \otimes I_B \left(\frac{1}{2} \sum_{x \in \{0,1\}^2} |x\rangle_A |x\rangle_B \right) \tag{3.24}$$

Further, suppose that

$$Tr(\rho M \otimes N) = Tr(\sigma M \otimes N) \tag{3.25}$$

for $M, N \in \{I, X, Z\}$. *Then* $\rho = \sigma$.

Proof. The proof follows the same plan as for the two qubit version. To begin, we examine the effect of CTRL-Z on the two qubit Paulis. Define $C(P)$ to be CTRL-$Z(P)$CTRL-Z for two qubit Pauli P. This is summarized in the following table:

$$
\begin{array}{c|cccc}
C(\cdot) & I & X & Y & Z \\
\hline
I & II & ZX & ZY & IZ \\
X & XZ & YY & YX & XI \\
Y & YZ & XY & XX & YI \\
Z & ZI & IX & IY & ZZ \\
\end{array}
\tag{3.26}
$$

(It may benefit the reader to note that the table is symmetric and $C(\cdot)$ is its own inverse, since CTRL-Z has these properties.) The state $\frac{1}{2}\sum_{x\in\{0,1\}^2}|x\rangle_A|x\rangle_B$, written as a density operator, is

$$\frac{1}{16} \sum_{M,N\in\{I,X,Y,Z\}} (-1)^{\delta_{M,Y}+\delta_{N,Y}} (M \otimes N)_A \otimes (M \otimes N)_B. \tag{3.27}$$

Note the coefficient, which is -1 when exactly one of M and N is Y. We find that σ is given by

$$\sigma = \frac{1}{16} \sum_{M,N\in\{I,X,Y,Z\}} (-1)^{\delta_{M,Y}+\delta_{N,Y}} C(M \otimes N)_A \otimes (M \otimes N)_B \tag{3.28}$$

and hence

$$\left| \sigma_{(M'\otimes N')_A \otimes (M\otimes N)_B} \right| = \delta_{M'\otimes N', C(M\otimes N)}. \tag{3.29}$$

As for the two qubit case, we have

$$\text{Tr}\left(\rho U \sigma U^\dagger\right) \geq 0$$

for any unitary U. Dropping the zero terms and subbing in, we may write

$$\sum_{M \otimes N} (-1)^{\delta_{M,Y} + \delta_{N,Y}} \rho_{C(M \otimes N)_A \otimes (M \otimes N)_B} \geq 0.$$

Define

$$R(M \otimes N) = (-1)^{\delta_{M,Y} + \delta_{N,Y}} \rho_{C(M \otimes N)_A \otimes (M \otimes N)_B} \tag{3.30}$$

in which case we find

$$\sum_{M,N} R(M \otimes N)(U \cdot C(M \otimes N) \otimes (M \otimes N)) \geq 0. \tag{3.31}$$

We will prove that $R(M \otimes N) = 1$, in which case we have $\rho_{(M \otimes N)_A \otimes C(M \otimes N)_B} = \sigma_{C(M \otimes N)_A \otimes (M \otimes N)_B}$. Note that this is given by the conditions of the Lemma in the cases where $C(M \otimes N) \otimes (M \otimes N)$ is a tensor product of $\{I, X, Z\}$. This occurs for $M \otimes N \in \{I \otimes I, I \otimes X, X \otimes I, Z \otimes I, I \otimes Z, Z \otimes Z, X \otimes Z, Z \otimes X\}$.

We find the inequalities with $U = (Y \otimes I)_A$, $U = (I \otimes Y)_A$, $U = (Y \otimes I)_B$, and $U = (I \otimes Y)_B$ and sum them, dividing by 4. We obtain

$$R(I \otimes Y) + R(Y \otimes I) + R(Y \otimes Z) + R(Z \otimes Y) \geq 4. \tag{3.32}$$

Since all four values R values appearing cannot exceed 1, we find that they are all equal to 1. Next we find the inequality for $U = (Z \otimes Z)_A$. For the four remaining unknown R values we obtain

$$R(X \otimes X) + R(Y \otimes Y) + R(X \otimes Y) + R(Y \otimes X) \geq 4 \tag{3.33}$$

and again all four R values must be 1.

We now have $\sigma_{C(M \otimes N)_A \otimes (M \otimes N)_B} = \rho_{C(M \otimes N)_A \otimes (M \otimes N)_B}$. There are 16 such terms. By examining the trace of the squares of σ and ρ, and following the same reasoning as in the two qubit case, we conclude that the remaining terms must all be 0. Thus $\sigma = \rho$.

$\square$

Lemma 3.4. *Let $\sigma = |\psi\rangle\langle\psi|$ be a $2n$ qubit state with $|\psi\rangle = T_A \otimes I_B |\Phi+\rangle^{\otimes n}$ and T a tensor product of gates that are either single qubit real unitaries or CTRL-Z. Further, suppose that*

$$Tr(\rho M \otimes N) = Tr(\sigma M \otimes N) \tag{3.34}$$

where $M, N \in \{I, X, Z\}^{\otimes n}$ are one of the following

- *For a single qubit gate in the tensor product, M and N measure that qubit and its pair*

- *For a two qubit gate in the tensor product, M and N measure those qubits and their pairs.*

Note that M or N may be the identity (measuring marginals). Then $\rho = \sigma$.

Note that the EPR pairs are each divided into A and B sides and T is applied to the n A side qubits.

Proof. Divide up ρ and σ into pairs or fours of qubits, depending on whether the gate is a single qubit gate or a CTRL-Z. For each piece trace out the remaining qubits and apply the appropriate two or four qubit version of the Lemma. Then, since the reduced qubit on each piece is pure, ρ and σ are both the tensor product of the reduced qubits. □

Future work. *Extend the previous Lemma to two-qubit Clifford gates, and ultimately all real gates.*

Like the previous Lemma, a similar Lemma to the following appears in [MMMO06] (arXiv version) as Lemma 6. Also like the previous Lemma, the proof given by Magniez et al. relies on the claim that the real density matrices are in the span of the tensor products of $\{I, X, Z\}$. We give a correct proof that uses the Choi-Jamiolkowski representation. The technique used will be applied several times in the remainder of this chapter.

Lemma 3.5. *Suppose that a physical experiment with bipartite state $|\psi\rangle \in \mathcal{Y}^2$ and with measurements $M'_a \otimes N'_b$ ($M_0 = N_0 = I_{\mathcal{Y}}$) is equivalent to the reference experiment with a maximally entangled state $|\phi\rangle \in \mathcal{X}^2$ and measurements $M_a \otimes N_b$ ($M_0 = N_0 = I_{\mathcal{X}}$). Then there exist unitaries $U_A, U_B \in U(\mathcal{Y} \otimes \mathcal{X})$ such that*

$$U_A \otimes U_B \left(M'_a \otimes N'_b \right) |\psi\rangle_{\mathcal{Y}} |00\rangle_{\mathcal{X}} = |junk\rangle_{\mathcal{Y}^2} M_a \otimes N_b |\phi\rangle_{\mathcal{X}} \tag{3.35}$$

and

$$U_A \left(M'_a \otimes I_{\mathcal{X}} \right) U_A^\dagger = I_{\mathcal{Y}} \otimes M_a \tag{3.36}$$

when confined to the support of $|junk\rangle_{\mathcal{Y}^2}$ on $\mathcal{Y}_A$, and analogously for N'_b.

Proof. Equation 3.35 follows directly from the definition of equivalence and a straightforward extension of the local isometry. From this fact we make the following observations:

$$|\psi\rangle|00\rangle = (M_a' \otimes I_{\mathcal{X}^2})^\dagger U_A^\dagger \otimes U_B^\dagger |junk\rangle_{\mathcal{Y}^2} M_a \otimes I_{\mathcal{X}_B} |\phi\rangle_{\mathcal{X}}. \qquad (3.37)$$

Applying equation 3.35 with M_0 and N_0, we find

$$|junk\rangle_{\mathcal{Y}^2}|\phi\rangle_{\mathcal{X}} = U_A \otimes U_B(M_a' \otimes I_{\mathcal{Y}_B} \otimes I_{\mathcal{X}^2})^\dagger U_A^\dagger \otimes U_B^\dagger |junk\rangle_{\mathcal{Y}^2} T_a \otimes I_{\mathcal{X}_B}|\phi\rangle_{\mathcal{X}} \qquad (3.38)$$

and hence

$$U_A\left(M_a' \otimes I_{\mathcal{X}}\right)U_A^\dagger |junk\rangle_{\mathcal{Y}^2}|\phi\rangle_{\mathcal{X}} = |junk\rangle_{\mathcal{Y}^2} M_a \otimes I_{\mathcal{X}}|\phi\rangle_{\mathcal{X}}. \qquad (3.39)$$

We now introduce a technique which will be quite useful. Let Φ be the quantum operation on $\mathcal{X}$ defined by adding ancilla in the state $|junk\rangle_{\mathcal{Y}^2}$, applying $U_A\left(M_a' \otimes I_{\mathcal{X}}\right)U_A^\dagger$ and finally tracing out the $\mathcal{Y}^2$ register. Note that the above equation has (after tracing out the $\mathcal{Y}^2$ register) left side equal to $J(\Phi)/\dim(\mathcal{X})$ and the right side (after tracing out the $\mathcal{Y}^2$ register) is $J(M_a)/\dim(\mathcal{X})$ (abusing notation a little). From this we may conclude that Φ equates to simply applying T_a and is hence unitary. The operator $U_A\left(M_a' \otimes I_{\mathcal{X}}\right)U_A^\dagger$ must then have the form $W_{\mathcal{Y}} \otimes M_a$ (when restricted to the support of $|junk\rangle_{\mathcal{Y}^2}$) and since the $\mathcal{Y}$ register remains in the same state, we conclude that W is the identity.

We apply the same reasoning and obtain the analogous result for N_b. $\square$

3.5.3 Proof of main Theorem

We begin by applying Lemma 3.5 twice, to obtain

$$U_A \otimes U_B M_a' \otimes N_b'|\psi\rangle|00\rangle = |junk\rangle_{\mathcal{Y}^2} M_a \otimes N_b|\phi\rangle \qquad (3.40)$$

$$U_A(M_a' \otimes I_{\mathcal{Y}})U_A^\dagger = I_{\mathcal{Y}} \otimes M_a, \ U_B(N_b' \otimes I_{\mathcal{Y}})U_B^\dagger = I_{\mathcal{Y}} \otimes N_b \qquad (3.41)$$

when confined to the support of $|junk\rangle_{\mathcal{Y}^2}$ on the appropriate side, and

$$V_A \otimes V_B M_a'' \otimes N_b'' G' \otimes H'|\psi\rangle|00\rangle = |junk_2\rangle_{\mathcal{Y}^2} M_a \otimes N_b|\phi\rangle \qquad (3.42)$$

$$V_A(M_a'' \otimes I_{\mathcal{Y}})V_A^\dagger = I_{\mathcal{Y}} \otimes M_a, \ V_B(N_b'' \otimes I_{\mathcal{Y}})V_B^\dagger = I_{\mathcal{Y}} \otimes N_b \qquad (3.43)$$

when confined to the support of $|junk_2\rangle_{\mathcal{Y}^2}$ on the appropriate side. By virtue of these equations, we find that there must be local unitaries operating on $\mathcal{Y}_A$ and $\mathcal{Y}_B$ that take $|junk_2\rangle_{\mathcal{Y}^2}$ to $|junk\rangle_{\mathcal{Y}^2}$. We may absorb these operations into $V_A \otimes V_B$ and take $|junk_2\rangle_{\mathcal{Y}^2} = |junk\rangle_{\mathcal{Y}^2}$. Note that this does not disturb equation 3.43 since the redefinition of $V_A \otimes V_B$ amounts to conjugating the $\mathcal{Y}^2$ register on the right sides. Thus we find

$$V_A \otimes V_B M_a'' \otimes N_b'' G' \otimes H' |\psi\rangle |00\rangle = |junk\rangle_{\mathcal{Y}^2} M_a \otimes N_b |\phi\rangle. \qquad (3.44)$$

Now we consider the case when G' is applied and H' is not applied. We wish to see what this means if we convert to the reference experiment, so we consider the following state:

$$|\theta\rangle = (V_A \otimes U_B)(G' \otimes I_{\mathcal{Y}} \otimes I_{\mathcal{X}^2}) |\psi\rangle |00\rangle. \qquad (3.45)$$

Applying our equations from above we find that this is equal to

$$(V_A \otimes U_B)(G' \otimes I_{\mathcal{Y}} \otimes I_{\mathcal{X}^2})\left(U_A^\dagger \otimes U_B^\dagger\right) |junk\rangle_{\mathcal{Y}^2} |\phi\rangle \qquad (3.46)$$

$$= \left(V_A(G' \otimes I_X)U_A^\dagger\right) \otimes I_B |junk\rangle_{\mathcal{Y}^2} |\phi\rangle. \qquad (3.47)$$

Define the quantum operation Φ on $\mathcal{X}$ by attaching an ancilla in the state $|junk\rangle_{\mathcal{Y}^2}$, applying $\left(V_A(G' \otimes I_X)U_A^\dagger\right)$ and tracing out the $\mathcal{Y}^2$ register. Then $J(\Phi) = \dim(\mathcal{X})\text{Tr}_{\mathcal{Y}^2}(|\theta\rangle\langle\theta|)$.

We wish to characterize $J(\Phi)$. To this end we note that $\frac{1}{\dim(\mathcal{X})}\text{Tr}(M_a \otimes N_b J(\Phi)) = \langle\theta| I_{\mathcal{Y}^2} \otimes M_a \otimes N_b |\theta\rangle$. Note that

$$V_B(H' \otimes I_{\mathcal{X}_B})U_B^\dagger |\theta\rangle = V_A \otimes V_B G' \otimes H' \otimes I_{\mathcal{X}^2} |\psi\rangle |00\rangle = |junk\rangle_{\mathcal{Y}^2} |\phi\rangle_{\mathcal{X}} \quad (3.48)$$

and since this differs from $|\theta\rangle$ only on the B side, the support of $|\theta\rangle$ on $\mathcal{Y}_B$ is the same as the support of $|junk\rangle_{\mathcal{Y}^2}$ on $\mathcal{Y}_B$. We obtain

$$\frac{1}{\dim(\mathcal{X})}\text{Tr}(M_a \otimes N_b J(\Phi)) = \langle\psi| \left((G')^\dagger \otimes I_{\mathcal{Y}}\right)(M_a'' \otimes N_b')(G' \otimes I_{\mathcal{Y}}) |\psi\rangle. \qquad (3.49)$$

Since $G' \otimes I_{\mathcal{Y}} |\psi\rangle$ with measurements $M_a'' \otimes N_b'$ simulates $T \otimes I |\phi\rangle$ with measurements $M_a \otimes N_b$ we have

$$\text{Tr}(J(\Phi)M_a \otimes N_b) = \text{Tr}(J(T)M_a \otimes N_b).$$

60

Lemma 3.2 then implies $J(\Phi) = J(T)$. From this we conclude that

$$V_a \left(G' \otimes I_\mathcal{X} \right) U_a^\dagger = W \otimes T \tag{3.50}$$

for some $W \in U(\mathcal{Y})$. Since $W \otimes T$ preserves $|junk\rangle_{\mathcal{Y}^2}$ we must have $W = I_\mathcal{Y}$ on the support of $|junk\rangle_{\mathcal{Y}^2}$ on $\mathcal{Y}_A$.

3.5.4   A conspiracy against self-testing complex gates

The restriction to real gates in the reference experiments may seem a bit curious, but has an easy explanation. If the gate had complex entries, then there would be no way of distinguishing the reference experiment from an otherwise identical experiment that had the complex conjugate applied. That is to say, the complex conjugate of an experiment simulates it. However, the definition of equivalence requires the existence of a unitary operation that takes the physical experiment to the reference experiment, but complex conjugation is anti-unitary. Thus there can be no extension of the gate testing Theorem to complex gates with the current definition of equivalence. Real gates are acceptable because complex conjugation does not affect them.

Complex conjugation does not pose very great a problem, since applying the complex conjugate can be seen as a change in convention. Nothing changes in the structure of the experiment. However, the simulations described in chapter 2 introduce many new physical experiments that simulate the reference experiment, and none of them are equivalent to the reference experiment. Further, these simulations are defined on different Hilbert spaces from the reference experiment and hence something more complex than a change in convention is happening. In the case of real gates, however, the simulations all reduce to the reference experiment, allowing the gate testing Theorem to go through.

Later, in section 3.7, we introduce a new definition of equivalence that takes the simulations into account. We then extend the Mayers and Yao result to include complex measurements. This paves the way for a gate testing Theorem allowing complex gates.
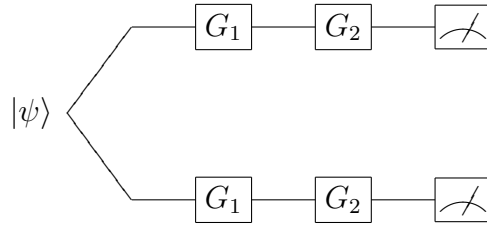
Figure 3.6: EPR test after two gates applied

3.6 Circuit testing

3.6.1 Overview

We now turn our attention to testing an entire circuit. We begin with a given circuit composed of single qubit real gates and CTRL-Z gates. We may divide this up into a sequence of unitaries operating on all qubits. Each of these unitaries is a tensor product of single qubit and CTRL-Z gates and thus is efficiently testable, as discussed in section 3.5. Each of these gates is tested against the reference gate determined by the given circuit. As explained below, this allows us to conclude that the entire physical circuit is equivalent to the reference circuit when both are considered as one large unitary. Finally, we perform the circuit by measuring on one side in the computational basis and performing the physical circuit on the other side, as shown in figure 3.8.

3.6.2 Composabiltiy

In order to test a sequence of gates we perform gate tests after each gate is added. This is illustrated in figures 3.6 and 3.7. After each gate is tested, the gate is applied to the other half of the state, taking the state back to (a state equivalent to) the maximally entangled state $|\phi\rangle$. This allows us to test the next gate in the sequence as though it were applied by itself. The following Lemma, applied inductively, allows us to conclude that the sequence of gates, applied together, is equivalent to the sequence of reference gates.

Lemma 3.6. *Suppose we have two sets of experiments satisfying the conditions of Theorem 3.2, the first testing G_1' against unitaries T_1 and the second testing G_2' against T_2 such that experiment 1 of the first set coincides with*
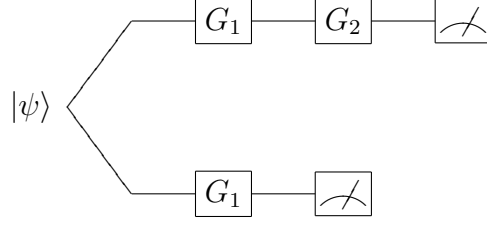
Figure 3.7: Testing a second gate
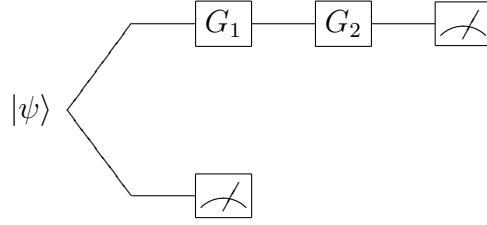
Figure 3.8: Performing a self-testing circuit

experiment 2 of the second set. The conclusions of the Theorem hold with $G_2'G_1'$ tested against T_2T_1.

Proof. From Lemma 3.5 and Theorem 3.2 we find unitaries $U_A, U_B, V_A, V_B, W_A, W_B$ such that

$$U_A(M_a' \otimes I_{\mathcal{Y}})U_A^\dagger = I_{\mathcal{Y}} \otimes M_a, \;\; U_B(N_b' \otimes I_{\mathcal{Y}})U_B^\dagger = I_{\mathcal{Y}} \otimes N_b \tag{3.51}$$

$$V_A(M_a'' \otimes I_{\mathcal{Y}})V_A^\dagger = I_{\mathcal{Y}} \otimes M_a, \;\; V_B(N_b'' \otimes I_{\mathcal{Y}})V_B^\dagger = I_{\mathcal{Y}} \otimes N_b \tag{3.52}$$

$$V_A(M_a''' \otimes I_{\mathcal{Y}})V_A^\dagger = I_{\mathcal{Y}} \otimes M_a, \;\; V_B(N_b''' \otimes I_{\mathcal{Y}})V_B^\dagger = I_{\mathcal{Y}} \otimes N_b \tag{3.53}$$

$$V_a \left(G_1' \otimes I_{\mathcal{X}} \right) U_a^\dagger = I \otimes T_1 \tag{3.54}$$

$$W_a \left(G_2' \otimes I_{\mathcal{X}} \right) V_a^\dagger = I \otimes T_2 \tag{3.55}$$

all for the support of $|junk\rangle_{\mathcal{Y}2}$ on $\mathcal{Y}_A$. Note that although we have used the gate testing Theorem twice, we can use the same junk state since experiment 2 from the first use is the same as experiment 1 from the second usage of the Theorem. We also find

$$U_A \otimes U_B M_a' \otimes N_b' |\psi\rangle |00\rangle = |junk\rangle_{\mathcal{Y}} M_a \otimes N_b |\phi\rangle \tag{3.56}$$

63

Applying these results we see that

$$(W_A \otimes U_B)\,(M_a''' \otimes N_b')\,(G_2'G_1' \otimes I_{\mathcal{Y}})\,|\psi\rangle\,|00\rangle = |junk\rangle_{\mathcal{Y}2}\,(M_A \otimes N_B)\,T_2 T_1 \otimes I_{\mathcal{X}}\,|\phi\rangle \tag{3.57}$$

and

$$W_a\,(G_2'G_1' \otimes I_{\mathcal{X}})\,U_A^\dagger = I \otimes T_2 T_1. \tag{3.58}$$

Thus the conclusions of Theorem 3.2 hold for the gate $G_2'G_1'$. $\qquad\square$

3.6.3 Testing on a particular input

Since we usually do not want to perform a circuit on a random input, we need some control over what the input will be. The solution proposed in [MMMO06] is to measure one side of the EPR pairs in the computational basis and then use the results to place X gates as necessary on the other half of each pair to correct the result to the desired input. The X gates placed this way are then incorporated into the definition of the circuit to be tested. Note that for this solution to work the calculation must come first. With Assumption 3.2 in place this is not a problem, but if we hope to adopt less restrictive assumptions then this method could easily be defeated since the devices could easily subvert the calculation and perform correctly on the subsequent tests.

Another solution to this problem assumes that the EPR pairs may be manipulated individually. Suppose we have n EPR pairs. Measure half of each EPR in the computational basis. If the result was the desired result, then keep the other half. If not, then discard the other half and prepare a new EPR pair. Repeat until n EPR pairs have been prepared. Since the EPR pairs are all prepared individually there is no problem with exponential blowup as n increases. A variation on this solution is to prepare $N > n$ EPR pairs and use only those pairs for which the measurement gives the correct result. If N is made sufficiently large then success is expected with high probability.

Blind state preparation

Although conceived with the notion of circuit testing in mind, self-testing could find application in QKD or other security related areas. In this context the state preparation method used has some advantages. For example, by measuring half of an EPR pair to prepare a state on the other half there can

be no side channel information about the basis used. One may wish to choose a particular state, however, so corrections might need to be made. If one is not careful, the correction may reveal the basis. For example if the bases are chosen from the eigenbase of X and Z, then a Z or X correction, respectively, may be necessary and the correction depends on the basis. There are several possibilities for defusing the situation. The first is to use Y as a correction, but this is not currently self-testable. A second possibility would be to always apply one of Z or X. If the X eigenbasis were chosen and a correction is needed, then Z is applied, otherwise X is applied which does not affect the state. Other possibilities exist, but the main idea is always to choose an operation that may be a correction for one basis, or not affect the other basis.

3.7   Extending the Mayers and Yao self-test

The original Mayers and Yao EPR test provided only a small set of measurements. Conspicuously missing is anything with complex coefficients. An important consequence of this is that the circuit test is not able to test gates with complex coefficients; only gates with real coefficients can be tested.

In fact the Mayers and Yao test cannot be directly extended to include any measurements with complex coefficients. This is a result of the notion of equivalence that they use. Suppose that we wish to include the Y measurement in the set of reference measurements. The devices could just as easily implement $-Y$, the complex conjugate. So long as all complex measurements were complex conjugated it would be impossible to tell. Although this does not present an immediate problem - such a transformation is internally consistent and produces the correct outcome statistics - we cannot transform such a circuit back into the reference circuit using unitary transformations. Anti-unitary transformations are required.

If this were the whole story we could simply require that the physical circuit be transformable into either the reference circuit or its complex conjugate. However, the real simulation, and now the family of simulations, defined in section 2.5, are also indistinguishable from the reference circuit and not unitarily transformable into the reference circuit.

We have one encouraging fact: all of the known simulations are equivalent to a simulation from the family of simulations (or a classical mixture of them). We now prove that we can extend the Mayers-Yao experiments

such that these are the only simulations. Hence we may extend our notion of equivalence to include these simulations and obtain a new self-testing Theorem.

Theorem 3.4. *Suppose a physical experiment duplicates the statistics generated by the reference experiment described in section 3.7.1. Then the physical experiment is equivalent to one of the simulations of the reference experiment described in section 2.5.*

With the extended state and measurement testing in place there exists the possibility of testing complex gates as well.

Future work. *Extend gate testing to complex gates using extended definition of equivalence.*

3.7.1 Extended Mayers-Yao self-test reference experiment

The extended Mayers-Yao test will consist of three regular Mayers-Yao tests, performed together. Alice and Bob will perform the Mayers-Yao test with measurement settings (labelled with subscript A when used by Alice, and subscript B when used by Bob):

1. X, Z, and D

2. X, Y, and E

3. Y, Z, and F

In the reference experiment the measurement settings X, Y and Z are realized by the Pauli operators, with $Y_B = -Y$ and otherwise $X_A = X_B = X$, $Y_A = Y$, $Z_A = Z_B = Z$. The other settings are realized by $D_A = \frac{X+Z}{\sqrt{2}}$, $E_A = \frac{X+Y}{\sqrt{2}}$, $F_A = \frac{Y+Z}{\sqrt{2}}$ on Alice's side and $D_B = \frac{X+Z}{\sqrt{2}}$, $E_B = \frac{X-Y}{\sqrt{2}}$, $F_B = \frac{Z-Y}{\sqrt{2}}$ on Bob's side. Bob's Y_B measurements all carry the -1 phase since measuring the state $|\phi_+\rangle$ with the operator $Y \otimes Y$ produces -1 instead of 1 as in the Mayers-Yao reference experiment. The reference state is again $|\phi_+\rangle$.

3.7.2 Proof of Theorem 3.4

We start by assuming that the states are all pure as in the Mayers-Yao test. Again we may incorporate the purification of a mixed state into either Alice or Bob's state by adding an ancilla.

First we apply the Mayers-Yao result with the measurements X, Z and D. We find that we may apply a suitable local isometry Φ to take the X_A, Z_A, X_B and Z_B measurements to $X_{Q_A} \otimes I_{R_A}$, $Z_{Q_B} \otimes I_{R_A}$, $X_{Q_B} \otimes I_{R_B}$ and $Z_{Q_B} \otimes I_{R_B}$ where R_A and R_B are the junk registers. Meanwhile the state has the form $|\phi_+\rangle_{Q_A Q_B} \otimes |junk\rangle_{R_A R_B}$, where Q_A and Q_B are the qubit registers that the measurements act on.

We now consider the remaining measurements. The reference circuits for these measurements can be transformed using local unitaries into the usual Mayers-Yao reference circuit. Thus we may apply the result. However, we stop short of using the full result. In section 3.4.2 we note that the measurement observables X_A and Z_A anti-commute on the support of the state, as do X_B and Z_B. When we apply this result to the remaining measurements in the extended test, we find that X_A and Y_A anti-commute on the support of the state, as do X_B and Y_B, Z_A and Y_A and Z_B and Y_B. For the remaining discussion we will limit ourselves to the support of the state.

Consider the A side measurements first. We may express Y_A as

$$Y_A = \sum_{P,k} y_{P,k} P_{Q_A} \otimes E_{k,R_A}$$

where the Ps are Pauli operators and the E_ks are other operators (i.e. pick a basis for Hermitian matrices consisting of Pauli matrices tensor product with something else). Since Y_A anti-commutes with $X_{Q_A} \otimes I_{R_A}$ all the terms with $P = X$ must be 0. Indeed, since $-Y_A = (X_{Q_A} \otimes I_{R_A})Y_A(X_{Q_A} \otimes I_{R_A})$ we have

$$-\sum_{P,k} y_{P,k} P_{Q_A} \otimes E_{k,R_A} = \sum_{P \in \{I,X\},k} y_{P,k} P_{Q_A} \otimes E_{k,R_A} - \sum_{P \in \{Y,Z\},k} y_{P,k} P_{Q_A} \otimes E_{k,R_A}$$

where on the right hand side we have separated out the terms that commute with $X_{Q_A} \otimes I_{R_A}$ and those that anti-commute. We see that we must have $y_{X,k} = -y_{X,k} = 0$ and $y_{I,k} = -y_{I,k} = 0$ for all k.

Applying similar reasoning and the test with Y and Z we find that $y_{Z,k} = 0$ for all k. Thus $Y_A = Y_{Q_A} \otimes M_{R_A}$ for some Hermitian and unitary M_{R_A}.

We consider the two eigenspaces of M_{R_A}. If they are not the same dimension (or if there is only one eigenvalue), we may construct an isomorphism that adds extra dimensions to R_A and extend M_{R_A} onto the new dimensions so that both eigenspaces have the same dimension. Next we construct an isomorphism that maps the space to a tensor product between a qubit and a space with half the dimension of R_A. We construct it so that the $+1$ eigenspace gets mapped to the subspace spanned by states of the form $|0\rangle |\chi\rangle$ and the -1 eigenspace gets mapped to the subspace spanned by $|1\rangle |\chi\rangle$. Then M_{R_A} gets mapped to $Z \otimes I$. Let P_A be the qubit register, and R'_A the remaining register. We obtain

$$Y_A \mapsto Y_{Q_A} \otimes Z_{P_A} \otimes I_{R'_B} \tag{3.59}$$

under the isomorphism described above. Importantly this isomorphism does not disturb X_A or Z_A since it only operates on the junk register. Thus we may modify Φ obtained from Theorem 3.1 to additionally perform the isomorphism just described.

The above process can be repeated for Bob's side, with analogous conclusions. In order to be consistent with the reference experiment, we may construct our isomorphism so that $Y_B \mapsto -Y_{Q_B} \otimes Z_{P_B} \otimes I_{R'_B}$.

Now we turn our attention to the state. From the Mayers-Yao test on X and Z we know that the state on $Q_A \otimes Q_B$ (after applying Φ) is $|\phi_+\rangle$. We next consider the state on the remaining registers, which we denote $|\theta\rangle$. We may express this in the singular value decomposition, split between P_{AB} and R'_{AB}:

$$|\theta\rangle = \sum_j \lambda_j |j\rangle_{P_{AB}} |j\rangle_{R'_{AB}} \tag{3.60}$$

with $\lambda_j > 0$. Since the Y measurement setting gives correlated results (recall we introduced a -1 factor on the B side measurement observable) and the form of Y_A and Y_B, the states $|j\rangle_{P_{AB}}$ must all be $+1$ eigenvectors of $Z_{P_A} \otimes Z_{P_B}$. If this were not the case then a -1 phase would be introduced and the measurement results would be incorrect at least some of the time. Thus the only possible states for $|j\rangle_{P_{AB}}$ are superpositions of $|00\rangle$ and $|11\rangle$. We do some relabelling and arrive at

$$|\psi\rangle = |\phi_+\rangle_{Q_{AB}} \otimes \left(\alpha |00\rangle_{P_{AB}} |\theta_{00}\rangle_{R'_{AB}} + \beta |11\rangle_{P_{AB}} |\theta_{11}\rangle_{R'_{AB}} \right) \tag{3.61}$$

with $|\theta_{00}\rangle$ and $|\theta_{11}\rangle$ not necessarily orthogonal. Note that tracing out the R'_{AB} ancillae results in a state of the form in equation 2.4. Thus we have

demonstrated that the physical experiment is equivalent to the reference experiment, and completed the proof of Theorem 3.4.

3.8 Robustness and assumptions for implementations

The results in this chapter are concerned with probability distributions which exactly match. However, if there is any hope for a physical implementation then this requirement must be relaxed and the Theorems made robust. Robustness was established for the Mayers and Yao test, as well as the gate test in [MMMO06]. These robustness results show that error in the statistics translates to a polynomial sized error in the equivalence. This is measured in terms of the 2-norm on states and the operator norm on gates. These are not the preferred measures of error since they do not have a straightforward operational interpretation.

Future work. *Determine robustness of the tests using operationally meaningful measures such as the trace norm on states and diamond norm on operations.*

Another consideration is that the robustness results relied on technical Lemmas with incorrect proofs. Also, the robustness of the extended Mayers and Yao test has yet to be determined.

Future work. *Determine robustness of Lemmas 3.2, 3.3, 3.4, 3.5 and Theorem 3.4.*

Another important consideration for potential physical implementations is the assumptions necessary to gather statistics. Here the physical experiment defines a probability distribution on outcomes, but in order to estimate this probability distribution many trials must be made. For this to make sense, we must make some repeatability assumptions:

Assumption 3.3. *The physical devices have no memory and always operate identically and the state for each trial is unentangled with other trials.*

This allows us to take many samples from a single physical experiment and estimate the probability distribution. In some situations this assumption may not be reasonable. One potential means of relaxing this assumption

would be to use techniques from QKD proofs, such as the quantum de Finetti Theorem, to allow arbitrary states.

Future work. *Relax assumptions on state and devices.*

3.9   Authenticated quantum computing

A recent development with goals very similar to self-testing is blind quantum computing, introduced by Broadbent et al. in [BFK08]. We are specifically interested in authenticated quantum computing, which is an extension of blind quantum computing. Authenticated quantum computing involves a semi-quantum verifier (able to only prepare qubits in a finite number of states) and a quantum prover. Using measurement based quantum computing [RB01] and fault-tolerant quantum computing techniques the verifier sends the prover several qubits prepared in random states known only to the verifier and then interacts classically with the prover. The goal is for the verifier to have the prover perform a quantum circuit and be able to certify, through classical interaction only, that the correct circuit has been performed. An important side effect of the process is that the prover does not know what the circuit is, even at the end of the protocol (hence *blind* computing.)

The goal is similar to that of self-testing, but the verifier requires some quantum capacity. In an extension of their result, the authors claim that the verifier can interact with *two* isolated provers (who are entangled) and eliminate the requirement for state preparation by the verifier. The idea is to begin with the two provers sharing a number of EPR pairs. The verifier first interacts with one prover, using the authenticated blind quantum computing protocol (without first sending qubits) to implement a circuit that simply measures half of each EPR pair in a randomly chosen bases, emulating the verifier's state preparation. Next, the verifier interacts with the second prover, again using the authenticated blind quantum computing protocol, performing the desired circuit with the other half of each EPR pair. A similar result was shown by Aharonov et al. in [ABOE08].

The claim is that the verifier cannot distinguish between errors occurring in each prover, and so we can assume that all errors happen in the second prover. Then the authenticated blind quantum computing protocol used with the second prover will catch all errors. Hence a pair of cheating provers will be caught (with high probability).

From the perspective of black-box quantum computing we may identify two important problems with this argument. The first is that the argument is not sound. The simulations in Chapter 2 indicated that it is possible for the two provers to perform a conspiracy that produces the correct outcome statistics, but does not implement the reference circuit. In particular, the measurement based quantum computing model used in the protocol requires operations that are complex. Thus the general simulations are not unitarily equivalent to the reference circuit. We may view the conspiracy as "errors", in which case the claim that all errors will be caught during the interaction with the second prover does not hold: there are conspiracies in which *both* provers perform "errors" that cannot be caught at all.

One counterargument to the above criticism is that all the general simulations would still provide the correct classical outcome, regardless, and hence the protocol is still sound. To be clear, we do not claim that the protocol is not sound, only that the proof is not sufficient. As well, this simply highlights the second problem, which is a lack of a rigorous claim. The final claim is that any language in the complexity class BQP has an interactive proof with a BPP verifier and two non-interacting BQP provers. However, this is not immediate since the authenticated blind quantum computing protocol is not about recognizing languages in BQP, but performing quantum circuits. The implied mediating claim is that the two prover protocol, for any desired reference circuit, certifies that the reference circuit was performed, hence any language in BQP may be recognized by the protocol.

Here it is unclear how to precisely say that the reference circuit was performed. The obvious interpretation, that the initial state was correct and each gate and measurement in the circuit was performed, is clearly not sufficient, since the general simulations (and even the unitarily equivalent simulations, if we are to be precise) defeat this claim. From the perspective of self-testing we may offer a more suitable claim: that the physical experiment was unitarily equivalent to either the reference experiment or one of the general simulations of it. As our counterargument above shows, this is the most that can be established. Fortunately, it is sufficient to imply the desired final claim: that all languages in BQP have classical interactive proofs with two non-interacting BQP provers. Unfortunately, there is currently no proof of such a claim.

Future work. *Show that the authenticated blind quantum computing protocol, with two entangled provers, certifies that a general simulation of the*

desired reference circuit was implemented by the provers.

Chapter 4

Device independent quantum key distribution

Contents

4.1   Introduction

Traditional quantum key distribution protocols, such as BB84 [BB84] and Ekert91 [Eke91] rely on a model of the physical devices being used in order to determine a secure key rate. In prepare and measure protocols, for example, a model of the source is used to determine to what extent Eve may differentiate between the various states sent and in all protocols a model of the measurements performed is incorporated into the parameter estimation portion of the protocols, deriving estimates of the states received.

In contrast, device independent quantum key distribution (DIQKD) aims to provide security without relying on a particular physical device model. The intent is to provide a higher level of security. Physical devices used for implementing QKD protocols are vastly more complicated than the simple physical models used in security proofs, allowing for a mismatch between theory and reality. If the security models are not conservative enough this may lead to an insecure physical implementation of a theoretically secure protocol.

In this chapter we describe the device model used in DIQKD and discuss the existing literature on the subject. In particular, we will be interested in the line of inquiry leading to the AMP06 protocol [AMP06] and subsequent reinterpretation in the DIQKD framework. We then consider the previous security models and provide some partial results extending security to a more general model.

The original material in this chapter is published in [McK09a].

4.2 Literature review

For the current work we are interested in four different lines of research. The first line of research is that of non-signalling based key distribution, from which the AMP06 protocol is drawn. The second is a pair of articles that introduce the notion of DIQKD and give a partial proof of security of the AMP06 protocol within the DIQKD framework. For our expanded proof we require some techniques from the literature on QKD security proofs, particularly those of Renner. Finally, it will be useful to review some concepts from the literature on Bell inequalities.

4.2.1 Non-signalling key distribution

The AMP06 protocol was introduced in [AMP06], which belongs to the literature on non-signalling based key distribution protocols. These protocols do not rely on quantum mechanics being correct for their security. Rather, they consider a wider context of probability distributions which are limited by being non-signalling.

Non-signalling distributions

Consider a probability distribution $P(x, y|a, b)$ which assigns a probability to outcomes x and y for each inputs a and b. The inputs a and b are analogous to measurement settings in the usual QKD framework, with x and y the measurement outcomes. We associate the variables x, a with one location, controlled by Alice, and y, b with another location, controlled by Bob.

We define a probability distribution of this form to be non-signalling according to the following definition

Definition 4.1. *A probability distribution $P(x, y|a, b)$ is* non-signalling *if for every a, b, x, y*

1. $P(x|a, b) = P(x|a)$

2. $P(y|a, b) = P(y|b)$.

The marginal distributions above are found by summing over the possible values of the variables not mentioned. For example

$$P(x|a) = \sum_{y', b'} P(x, y = y'|a, b = b'). \tag{4.1}$$

The definition of a non-signalling distribution says that the distribution of one outcome is not dependent on the measurement setting in the other location. Such distributions are consistent with general relativity and cannot be used to transmit information.

Non-signalling key distribution makes use of different principles for security than does QKD. While QKD uses measurements to perform some quantum state estimation (typically measuring deviation from a maximally entangled state), non-signalling key distribution uses correlation functions on probability distributions (measuring deviation from a non-local probability distribution).

Often, Bell inequalities are central in the discussion of non-signalling key distribution, but the security of such schemes usually depends, not on the inequality itself, but on an analysis of the correlation functions that Bell inequalities bound. The Bell inequality provides a lower bound on the strength of correlations necessary for secure key generation, since local distributions cannot generate secure key. However, the bound may not be tight, as in the CHSH based protocol considered by Masanes [Mas08] where even quantum correlations give a zero secure key rate.

Non-signalling literature

Non-signalling key distribution was anticipated by Barrett et al. [BLM$^+$05] with a study on the value of non-signalling distributions as information theoretic resources that may be converted between one another much like how different entangled quantum states may be converted to one another using LOCC operations. Later, Barrett et al. [BHK05] introduced a proof-of-concept protocol which uses many trials to estimate the expected value of a correlation function and produces a single bit of secure key. Their protocol is not robust against noise and is inefficient in the use of the channel. However, this early work opened up the area to further research.

Theoretical work in this area continued with results by Barrett et al. on monogamy of maximally entangled quantum states [BKP06]. They introduce a correlation function similar to that used in the chaining inequality [BC90] and show that if two parties in a 3-partite non-signalling distribution produces the same correlations achieved by a $d \times d$-dimensional maximally entangled quantum state (measured by the new correlation function) then the third party can have no information about the measurement outcomes of the first two parties. This opens up the potential for a higher dimen-

sional non-signalling key distribution protocol implementable by quantum apparatus.

New protocols were introduced in [AGM06] and [AMP06]. Both of these protocols are based on the correlation function in the CHSH inequality [CHSH69] (see section 4.2.4). The latter is the AMP06 protocol which we will consider in detail in this chapter, and is a refinement of the protocol in [AGM06].

All security proofs up to this point were concerned with individual or collective attacks only. Proofs of security against general attacks were developed in [MRW+06], with universal composability achieved in [Mas08]. However, the proof makes some impractical assumptions. In particular, the probability distribution is assumed to be $n + 1$-fold non-signalling, with one party controlling n parts (corresponding to n trials) and the other controlling 1 part (the n trials need not be non-signalling for the second party.)

4.2.2 DIQKD

Non-signalling protocols and security proofs perform poorly in a quantum context. As an example, we consider the two protocols analyzed by Masanes in [Mas08]. The first protocol analyzed is that presented in [AMP06], which is also the first (and so far only) DIQKD protocol. This protocol has secure key rate 0 in the non-signalling framework when implemented by quantum devices. The non-local correlations required for key generation cannot be generated by quantum devices. The second protocol relies on a larger number of measurements. For a particular Bell inequality (the Braunstein-Caves inequality [BC90]) quantum devices may (asymptotically in the number of measurements) achieve the same correlations as arbitrary non-signalling distributions. This allows a quantum implementation that achieves the full non-signalling secure key rate, but practical implementation is problematic due to the large number of measurements required.

Non-signalling based QKD is likely limited to a theoretical context because of its impracticality in a quantum setting, but its reliance on a smaller set of assumptions than traditional QKD is appealing. For this reason Acin et al. [ABG+07] [PAB+09] reinterpreted the protocol of [AMP06] in a quantum setting. The result is DIQKD. The initial work in this area consists of a proof of security in the quantum setting against a limited class of attacks. This class of attacks is analogous to the collective attack model in QKD and bears the same name. In this model the state is a tensor product

$\rho^{\otimes n}$ of n identical states. This is measured by measurement devices with a fixed (but unknown) operation. That is, the measurement operators for each measurement setting are fixed.

4.2.3 Security proofs in QKD

The results in this chapter rely on Renner's PhD thesis on the security of traditional QKD [Ren05]. Renner's work provides a robust framework for security proofs of QKD protocols against general attacks. Renner's work is notable for several reasons. First, he adopts a composable security definition, which means that the final key is secure for any application [KRBM07]. Second, he develops and uses a finite version of the quantum de Finetti Theorem [Ren07], which allows the security proofs to be applicable to general attacks in which the combined state across all measurements is arbitrary. Another important contribution is Renner's development of smooth min- and max-entropies, which play a major role in his security proofs and allow for finite, rather than asymptotic, analysis of security.

In order to use Renner's framework with a particular QKD protocol one must consider the states and measurements used in the protocol and determine two things. The first is the set of states that pass the parameter estimation phase. These are found by considering the measurements used during parameter estimation along with various security parameters. Once this set of states is found one must determine the minimum secure key rate (found by calculating conditional entropies on the state) over all states that pass the parameter estimation phase.

4.2.4 CHSH inequality

The main idea for the AMP06 protocol is foreshadowed in Ekert's work on entanglement based QKD protocols [Eke91]. Ekert's protocol, Ekert91, used the CHSH inequality [CHSH69] (or rather the correlation function that the CHSH inequality bounds) to estimate how close the measured state is to a pair of maximally entangled qubits. This estimate was then used to prove that a secure key may be extracted. However, the state estimate is determined assuming that the measurement devices exactly implement the Pauli X and Z basis measurements. The AMP06 protocol retains the use of the CHSH inequality but uses the black box device model.

The CHSH inequality is a Bell inequality utilizing two measurement settings and two measurement outcomes for two parties. The two parties, Alice and Bob, each randomly apply one of the two measurement operators to a bipartite state ρ and compare outcomes. The measurement operators are A_a and B_b, where $a, b \in \{0, 1\}$ are the measurement settings for Alice and Bob, respectively. The operators A_a and B_b are Hermitian with eigenvalues 1 and -1. The CHSH operator is a non-local measurement defined by

$$CHSH = \sum_{a,b=0,1} A_a \otimes B_b (-1)^{ab}. \tag{4.2}$$

The CHSH inequality may be expressed as

$$S = \text{Tr}(CHSH\rho) = \sum_{a,b=0,1} \text{Tr}(A_a \otimes B_b \rho)(-1)^{ab} \leq 2 \tag{4.3}$$

for local classical strategies, with an upper bound of $2\sqrt{2}$ for quantum strategies. Equivalently, we may use uniformly distributed random variables $a, b \in \{0, 1\}$ for the measurement settings and random variables $x, y \in \{0, 1\}$ for measurement outcomes, and derive the inequality

$$p = P(x \oplus y = ab) \leq 0.75 \tag{4.4}$$

for local classical strategies, with an upper bound of $\cos^2 \frac{\pi}{8} \approx 0.85$ for quantum strategies. We say that a trial is successful if $x \oplus y = ab$. In this notation the scenario may be described as a binary XOR game in which a referee supplies uniformly distributed queries a and b and receives replies x and y. Alice and Bob win the game if $x \oplus y = ab$.

The values p and S are related by

$$S = 8p - 4. \tag{4.5}$$

Both of these quantities will be useful in this paper. We will be interested in the maximum value of S or p achievable by a state ρ, maximized over all possible measurements. We denote these values by $S_{max}(\rho)$ and $p_{max}(\rho)$.

Later, we need to determine $S_{max}(\rho)$ for a pair of qubits. For this, we turn to Horodecki et al. [HHH95] who did exactly the required calculation. Later, Verstraete and Wolf [VW02] gave a different presentation of this calculation, which we will use here.

We begin by writing

$$\rho = \sum_{U,V \in \{I,X,Y,Z\}} \frac{R_{U,V}}{4} U \otimes V \qquad (4.6)$$

with

$$R_{U,V} = \mathrm{Tr}(\rho U \otimes V). \qquad (4.7)$$

We define a matrix R', with rows and columns indexed by X, Y, Z and entries $R_{U,V}$. Meanwhile, we may write the measurement operators as

$$A_a = \sum_{U \in \{X,Y,Z\}} s_{a,U} U \qquad (4.8)$$

$$B_b = \sum_{V \in \{X,Y,Z\}} t_{b,V} V. \qquad (4.9)$$

We further define a matrix M by

$$M = \begin{pmatrix} s_0 & s_1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} t_0^T \\ t_1^T \end{pmatrix}, \qquad (4.10)$$

which is constrained by having $\mathrm{Tr}(M^T M) = 4$ and $\mathrm{Rank}(M) = 2$. Then the value of the CHSH operator may be written as $\mathrm{Tr}(R'M)$. Using standard optimization techniques (least squares approximation) we find the maximum to be $2\sqrt{u^2 + v^2}$ where u and v are the largest singular values of R' (or square roots of the eigenvalues of $R'(R')^T$. In the case where R' is diagonal, u and v are the two largest (in absolute value) of the diagonal entries.

4.2.5 The AMP06 protocol

The AMP06 protocol was originally described in [AMP06] and shown to be secure against collective quantum attacks in [ABG$^+$07] and [PAB$^+$09]. Two parties, Alice and Bob, share a small amount of secret key and wish to expand this into a larger key. They have access to an uncharacterized device which emits bipartite states, connected by quantum channels to a pair of uncharacterized measurement devices. Alice's measurement device has three settings, while Bob's has two. Finally, they have access to an insecure classical channel. They use some secret key to authenticate data sent on the classical channel.

1. Before beginning, Alice randomly chooses a list of m trials to be used for parameter estimation which she sends to Bob encrypted, using some private key bits.

2. For each trial, Alice and Bob request a state from the source. If the trial is to be used for parameter estimation, Alice and Bob choose their measurement settings uniformly at random from $\{0, 1\}$. Otherwise Alice chooses setting 2 and Bob chooses setting 0.

3. After all trials are completed, Alice and Bob announce their measurement settings.

4. Alice and Bob publicly announce a permutation and reorder their trials according to this permutation.

5. Alice and Bob estimate S, the CHSH value, from the parameter estimation trials.

6. Alice and Bob perform error correction on the remaining trials, correcting Alice's outcomes to correspond with Bob's, resulting in the raw key.

7. Alice and Bob perform privacy amplification on the raw key according to the secure key rate predicted by S.

The above protocol could be efficiently implemented using quantum apparatus by a source of qubit pairs in the state $|\phi_+\rangle = \frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle$, with Alice's measurements given by the operators X, Y, and $\frac{X+Y}{\sqrt{2}}$. Bob's measurement operators are $\frac{X+Y}{\sqrt{2}}$ and $\frac{X-Y}{\sqrt{2}}$. The security comes from the fact that in order to achieve a high value of S, the state that Alice and Bob measure must be close to $|\phi_+\rangle$ and hence Bob's measurements are uncorrelated with Eve. The efficiency of the protocol comes from the fact that Alice can align her measurement with Bob's a significant amount of the time and obtain strongly correlated results, so long as she chooses the other measurements often enough to detect any deviation in the state from $|\phi_+\rangle$.

Instead of choosing which trials to use for parameter estimation in advance, Alice and Bob may choose their settings independently, saving some key. This introduces trials which are unusable (when Alice chooses 2 and Bob chooses 1) and unless Bob chooses 0 and 1 uniformly, there will be some

parameter estimation settings that occur more than others. Conceptually it is easier to suppose that the parameter estimation trials are first chosen and then the settings are chosen uniformly.

In [ABG+07] and [PAB+09] the protocol requires that Alice and Bob symmetrize their data by flipping their outcomes according to a random string which is publicly broadcast. This simplifies the analysis by introducing symmetries in the quantum state. However, the symmetrization procedure need not be done in practice since it does not change the amount of information leaked to an adversary; Eve may account for the symmetrization in her own analysis after observing the public random string. Here we omit the symmetrization.

4.3   Security models

4.3.1   Black box model

DIQKD uses a black box model of quantum devices as in self-testing. The devices are considered to be adversarial, always operating in such a way as to maximize the information leakage to Eve. Of course we must place some restrictions on the devices, otherwise they may simply transmit all their information to Eve. We require:

Assumption 4.1. *The measurement devices do not leak any information to Eve.*

The black box measurement devices have a quantum input, a classical input (measurement setting) and a classical output (measurement outcomes). Alice (or Bob for his device) has exclusive control of the classical input and output, and there are no other side channels. The quantum input is strictly input only. There can be no quantum or classical states "leaking" from the quantum input. We may model each device as a quantum channel that has two input registers, one the quantum input and the other the measurement setting, and one output register. Alice possesses both classical registers.

The device model for DIQKD is sometimes described as "Eve provides the measurement devices." However, this depiction is only applicable if we can for some reason trust Eve not to build the device in such a way that it leaks information. Instead, the model should be understood as a theoretical tool which eliminates the dependance on a particular physical model. In a

secure physical implementation there must still be a physical model which makes assumption 4.1 reasonable.

4.3.2 Collective attack model and security

As described above, the protocol could be performed using the same devices over and over. Pironio et al. ([PAB$^+$09]) originally considered security against collective attacks, which relies on the assumption that the devices operate identically each time, and have no memory of the previous trials. For the source this means that state emitted over n trials has the form $\rho^{\otimes n}$. A physical implementation using devices that are used repeatedly must meet the following assumptions

Assumption 4.2 (DIQKD Collective attacks).

- *On each trial the source emits ρ.*

- *The combined state that the source emits is $\rho^{\otimes n}$.*

- *The measurement devices have no memory.*

Pironio et al. proved security in this model with a secure key rate depending on S and the error rate between the measurement outcomes for setting 2 on Alice's side and setting 0 on Bob's side.

Theorem 4.1 (Pironio et al. [PAB$^+$09]). *The AMP06 protocol is secure against collective quantum attacks with secure key rate*

$$1 - h\left(\frac{1 + \sqrt{(S/2)^2 - 1}}{2}\right) - h(q). \qquad (4.11)$$

where S is the CHSH value and q is the bit error rate.

4.3.3 Memoryless device attack model

In this chapter we will give a partial result on security in a more relaxed model than the collective attack model. We may describe it in two different ways: in a serial or parallel fashion, which are equivalent given certain assumptions. In order to illustrate the difference and how the current model differs from the collective attack model we give two descriptions of the latter. In the collective

attack model there are several trials, and each trial is identical; the states are identical and independent, and the measurement applied for each trial (for a given measurement setting) is the same. In a physical implementation we may consider two means of achieving this scenario. The first is a serial model where a source emits identical and independent copies of a particular state, which is measured by a measurement device which operates identically (for a given setting) each time it is used. In a parallel model, by contrast, each trial is implemented by a separate physical system (prepared in identical states) which is measured by separate devices (each operating identically). Clearly for the collective attack model these two physical depictions carry no theoretical difference. Physical implementation is of course easier with a serial model, while security proofs for QKD protocols typically rely on the parallel model.

We now move to the memoryless device attack model. The goal is to achieve as general a security proof as possible. We consider first the parallel model. The most general attack model would be to allow any state and any measurement. Taken to the extreme, one may consider a single large POVM, dependent on the measurement settings for all trials, outputting the results for all trials simultaneously. A more restrictive model would have the measurement for each trial arbitrary, but operating on a separate physical system. The separation could be enforced by some type of shielding, which is already necessary to obtain Assumption 4.1.

Clearly a large number of space-like separated measurements is not practical. A practical implementation could be made with single devices used serially, with only the following assumption:

Assumption 4.3 (DIQKD Global attacks with memoryless devices)**.**

- *The measurement devices have no memory.*

Suppose we operate the memoryless measurement devices in a lockstep fashion with the measurement settings so that the next measurement setting is only given to the device once the result of the previous trial has been given. In this case, since the devices have no memory, the various trials are completely independent and the measurements on each trial commute with all other measurements. Thus this model is equivalent to the parallel model with measurements operating on separate physical systems.

Thus we arrive at the memoryless device attack model. The source may emit any type of state, which may include a complete specification on how

the measurement devices are to operate on a particular trial, and the state may be entangled between trials. There is no restriction on the dimension of the state or on the form of the measurement operators. However, the measurement devices have no memory.

4.4 Security of AMP06

The main result in this chapter is to give a partial result showing that the AMP06 protocol described in [ABG$^+$07] is secure in the memoryless device attack model. Unfortunately we are not able to give a full proof, and instead give a partial result which depends on a conjecture. To be precise, we give a proof of the following Theorem:

Theorem 4.2. *The AMP06 protocol is secure against qubit strategies with a symmetric state and memoryless measurement devices with secure key rate*

$$1 - h\left(\frac{1 + \sqrt{(S/2)^2 - 1}}{2}\right) - h(q). \tag{4.12}$$

where S is the CHSH value and q is the bit error rate.

We also outline how this can might be extended to qubit strategies with an arbitrary state and memoryless measurement devices. Unfortunately, the proof is incomplete:

Conjecture 4.1. *Permuting trials of a qubit strategy is equivalent to a qubit strategy with a symmetric state and a lower S_{max}.*

Applying techniques from [PAB$^+$09] the result can then be extended to strategies with a state of any dimension.

Theorem 4.3. *If conjecture 4.1 is true, then the AMP06 protocol is secure against quantum attacks with memoryless measurement devices.*

4.4.1 Proof overview

We will make extensive use of Renner's framework for QKD security proofs ([Ren05] chapter 6), but it will require adaptation in order to be applicable within the black-box model. In particular the parameter estimation in Renner's framework assumes that the same measurement (for a given setting) is

applied for every trial, which cannot be assumed within the black-box model. Also, the finite de Finetti Theorem is sensitive to the dimension of the Hilbert space. Since in the black-box model the Hilbert space is unknown, we cannot use the finite de Finetti Theorem directly to obtain any bounds.

In addition to solving the above problems, we must also characterize the set of states that pass the parameter estimation phase (in this case, a Bell inequality) and determine the minimum key rate for these states. For this stage we will make use of state parameterization and entropy bounds from [PAB+09].

Overview of Renner's security proof

Since our proof of Theorem 4.3 is an adaptation of Renner's security proof, we sketch the steps in that proof here:

1. Permute trials to obtain a symmetric state

2. Apply the finite de Finetti Theorem

3. Measure m trials and apply parameter estimation Lemma

4. Measure remaining trials to obtain the raw key

5. Estimate the min-entropy of the raw key

6. Apply classical post-processing to obtain final key

The final security claim consists of an estimate of the trace distance (induced by the 1-norm) between the processed measurement outcomes and a uniformly random key independent of Eve. In order to obtain this estimate we make use of two tools: the triangle inequality and the fact that trace distance is non-increasing under quantum operations. This produces a chain of inequalities finally ending with the security claim.

Outline of proof of Theorem 4.3

Our proof follows the same sketch as that of Renner's security proof, but we must make adaptations at all but the last step:

1. Reduce arbitrary strategies to qubit strategies

2. Show permuting trial outcomes is sufficient in the black box model

3. Prove new parameter estimation Lemma for black box model and CHSH value

4. Minimize min-entropy over possible measurements

5. Estimate min-entropy from CHSH value estimate

6. Apply classical post-processing to obtain final key

The physical model we use in the proof is that of many parallel trials where the state for each trial is contained in a pair of subsystems (one for Alice and one for Bob), as introduced in section 4.3.3. Some careful thought will show that all the procedures used can be either serialized or performed once all the quantum systems have been measured solely using the classical data.

The remainder of this section is divided into subsections devoted to each of the above steps.

4.4.2 Reduction to qubit strategies

Before we can use Renner's QKD proof framework we must first fix the dimension of the subsystems. This is because the finite de Finetti Theorem, described below in section 4.4.3, is sensitive to the dimension. In particular, if the dimension is unbounded then no conclusion may be drawn. Since we have no *a priori* bound on the dimension, we must make some form of reduction. Our main tool will be the following Lemma, which is originally due to Jordan [Jor75], but has been rediscovered many times. Modern proofs appear in [Mas06b] and [PAB$^+$09]. We will use the formulation appearing in [PAB$^+$09].

Lemma 4.1 (Pironio et al. [PAB$^+$09] Lemma 2)**.** *Let A^0 and A^1 be two operators on $\mathcal{H}$ with two eigenvalues. Then A^0 and A^1 can be simultaneously block diagonalized with block sizes 2×2 and 1×1.*

Corollary 4.1. *Let A^0 and A^1 be two Hermitian operators on $\mathcal{H}$ with dimension $2n$ or $2n-1$ and eigenvalues 1 and -1, then there exists an isometry*

F from $\mathcal{H}$ to $\mathcal{H}_n \otimes \mathcal{H}_2$ and Hermition operators $A^{a,z}$ on $\mathcal{H}_2$ with eigenvalues 1 and -1, such that

$$F(A^a) = \sum_z |z\rangle\langle z| \otimes A^{a,z} \tag{4.13}$$

with $A^{a,z}$ 2×2 operators with eigenvalues in $\{1, -1\}$.

This corollary says that we can think of applying one of these two observables as first applying a projection to learn z. The value of z then simultaneously determines a measurement strategy for either measurement setting. Importantly, the projection onto z can be applied before learning the measurement setting. This will allow us to consider an arbitrary strategy as a probabilistic combination of qubit strategies.

Let A_j^a be the observable for Alice 's mesaurements on the jth trial with setting a, and analogously for Bob. We apply corollary 4.1 to pairs of observables A_j^0 and A_j^1 to obtain isometry F_j, from the Hilbert space of the original state to $\mathcal{Z}_j^A \otimes \mathcal{H}_2$. The result is that we can map $A_j^{a_j}$ to

$$\sum_{z_j} \Pi_{z_j}^j \otimes A_j^{a_j, z_j} \tag{4.14}$$

with the $\Pi_{z_j}^j$ commuting for different j. We do the same with observables B_j^0 and B_j^1 and map $B_j^{b_j}$ to

$$\sum_{w_j} \Pi_{w_j}^j \otimes B_j^{b_j, w_j} \tag{4.15}$$

At this point we may decompose Eve's strategy into qubit strategies, indexed by $z = (z_1, \ldots, z_n)$ and $w = (w_1 \ldots w_n)$. However, we make a further simplification. It may be the case that some A_j^{a,z_j} is either I or $-I$, and the measurement outcome is fixed. We may replace the state for Alice's jth qubit in each strategy (z, w) for this value of z_j with $|0\rangle$ or $|1\rangle$ and replace A_j^{a,z_j} with Z. This new strategy is identical in terms of Eve's information and the outcomes as the previous strategy. Applying this reduction many times we obtain a strategy in which each measurement operator is 2-outcome. This is important since our proof of security for qubit strategies will make this assumption.

As a final reduction, we note that different trials may have different sized Hilbert spaces. We may map the Hilbert space for each trial to the maximum sized Hilbert space, leaving the state intact and extending the measurement

operator onto the extra dimensions in any arbitrary fashion. This makes no change in Eve's information or the measurement outcomes.

We have mapped a strategy of Eve to a strategy with state ρ on Hilbert space $\mathcal{Z} \otimes (\mathcal{H}_2^{\otimes n})_A \otimes (\mathcal{H}_2^{\otimes n})_B$ with measurement operators of the form above. Note that we may perform a projective measurement with projectors $\Pi_{z_j}^j$ for each j to determine all the z_j and analogously for Bob's side to determine the w_js before determining the measurement setting without changing anything, since these projectors commute with the measurements $A_j^{a,}$ and B_j^b. Eve loses nothing by performing this measurement herself, so we may assume that she does so and learns (z, w). We may also suppose that we first project the state down to a block diagonal state since this operation commutes with measuring (z, w). The result is that any strategy is equivalent to one in which Eve prepares a mixture of qubit strategies. We may further suppose that Eve holds the purification for each possible qubit strategy and only increase her power.

We have reduced all possible strategies to a mixture of strategies on qubits.

4.4.3 Reduction to symmetric qubit strategies

Symmetric states and the de Finetti Theorem

A symmetric state on n subsystems is a state that is invariant under permutation of the subsystems. For our purposes the subsystems will correspond to different trials in the DIQKD protocol. One set of particularly useful symmetric states is the symmetric subspace along a state.

Definition 4.2. *The* symmetric subspace of $\mathcal{H}^{\otimes n}$ *along* $|\phi\rangle^{\otimes n-r}$ *is the subspace spanned by states*

$$\Pi(|\phi\rangle^{\otimes n-r} \otimes |\phi'\rangle) \tag{4.16}$$

for any $|\phi'\rangle$ *on* $\mathcal{H}^{\otimes r}$ *and operation* Π *which permutes the subsystems. This subspace is denoted by* $Sym(\mathcal{H}, |\phi\rangle^{\otimes n-r})$.

This subspace is important because the states in it are very close to symmetric product states, and are hence easy to work with. The finite quantum de Finetti Theorem allows us to break symmetric states into a mixture of these near-product states.

Theorem 4.4 (Renner [Ren07] Theorem 4.3.2). *Let $\rho \in \mathcal{H}^{\otimes n+k}$ be a pure, permutationally invariant state and let $0 \le r \le n$. There exists a measure ν on the normalized pure states of $\mathcal{H}$, and for each normalized pure state $|\phi\rangle$ in $\mathcal{H}$ a pure density operator ρ_ϕ on $Sym(\mathcal{H}, |\phi\rangle^{\otimes n-r})$ such that*

$$\left\| Tr_k(\rho) - \int \rho_\phi \nu(\phi) \right\|_1 \le 2 \exp\left(-\frac{k(r+1)}{2(n+k)} + \frac{1}{2} \dim(\mathcal{H}) \ln k \right) \qquad (4.17)$$

Here $\text{Tr}_k(\cdot)$ means tracing out any k subsystems.

Does permuting trials imply a symmetric state?

In the Renner's QKD security proof a symmetric state is implied by the fact that Alice and Bob randomly permute their measurement outcomes. Although this operation does not operate directly on the state, it commutes with the measurements since the measurements are identical for each trial (for a given measurement setting) and the measurement settings are chosen uniformly at random. In the black box scenario the former is not true and the measurements may differ for each trial.

For general strategies we may repair this problem by mapping a strategy to a larger Hilbert space by attaching to each trial a variable indicating its position. Then the measurement operators may all be replaced with a single measurement that reads this new variable and implements the appropriate measurement strategy. The measurements are then all identical, but the dimension has been multiplied by the number of trials. We then permute outcomes, which is equivalent to permuting the state.

Unfortunately, this does not help us. A symmetric strategy does not necessarily reduce to a mixture of symmetric qubit strategies. Since we aim to apply the quantum de Finetti Theorem at the qubit level (since the Theorem is sensitive to dimension) we must have a symmetric qubit state.

From this point we offer a possible means of providing a symmetric qubit strategy from an arbitrary qubit strategy. Unfortunately, this method will result in a decrease in the secure key rate as we detail below. The main idea is similar to the usual argument: permute the results and show that this is equivalent to a symmetric state, but the symmetric state we obtain will have a different S_{max} than the original state.

To begin with, we identify the critical security constraint: measuring the original state ρ and permuting the outcomes must be the same as measuring the symmetric state ρ'. We may satisfy this constraint as follows. When

90

permuting ρ to obtain ρ' we must identify the basis in which we are working. Since ρ is provided within a black box device, we have no natural basis to use. Instead, we will specify one. The ideal candidate is for the B side basis of each trial to be the eigenbasis of B_0. That is to say, we choose the B side basis for each trial so that $B_0 = Z$. Then we partially recover the QKD mechanism: measuring ρ according B_0 on each trial and permuting the outcomes *is* the same as measuring ρ' according to B_0.

In order to provide a full solution we must also be able to estimate S_{max} for the trials in ρ' (it is the same for each trial), but ρ' is merely a convenient fiction. However, ρ' is derived from ρ and we may hope to provide a lower bound using the average S_{max} for ρ (averaged over all trials). In order to do this we must specify the basis for the A side of each trial.

Recall from section 4.2.4 that we may express the CHSH operator as a matrix M indexed by the Pauli operators X, Y, Z. We may choose our bases so that A_0 and A_1 lie on the X, Z plane of the Bloch sphere. For the B side we have already fixed $B_0 = Z$. By choosing an appropriate phase reference we may also have B_1 on the X, Z plane. Then we may consider only the entries of M indexed X and Z since the others are all 0.

Ideally, we would choose the bases so that M is diagonal with positive entries, but since B_0 is already fixed this will not be possible in general. We still have some freedom in the choice of the A side basis, though, and we may arrange it so that M is symmetric with positive diagonal. Recall that $S = \text{Tr}(R'M)$, where R' is determined by the state. Thus the only parameters of R' that matter are the entries R'_{XX}, R'_{ZZ}, and $R'_{XZ} = R'_{ZX}$.

The goal at this point is to show that averaging S_{max} over trials puts a lower bound on S_{max} of the symmetrized state. There are only three parameters in this analysis, so the hope is that it can be accomplished. Unfortunately, we have not been able to derive the bound. Thus the result remains a conjecture.

4.4.4 Parameter estimation in symmetric qubit strategies

At this point we need to develop techniques for estimating the CHSH value of states in $Sym(\mathcal{H}, |\phi\rangle^{\otimes n-r})$. This is analogous to Theorem 4.5.2 in [Ren05]. However, in that case the measurement operations on each subsystem are all known and identical. In our case the measurements are not in our control,

and we may have no description of them. Fortunately this is not a very important issue. The CHSH value that can be achieved by a particular state is a property of the state itself. If the measurements used are not optimal, then the observed CHSH value can only be lower than if the measurements are optimal. Since we are only interested in lower bounding the CHSH value, this is sufficient. Any CHSH value that we observe will (leaving statistical fluctuations aside) be a lower bound on the maximum CHSH value achievable by the state.

Lemma 4.2 (Parameter estimation). *Let $|\psi\rangle \in Sym(\mathcal{H}_2 \otimes \mathcal{H}_2, |\phi\rangle^{\otimes n+m-r})$ and let $p = p_{max}(|\phi\rangle)$ be the maximum expected value for success on the CHSH test on $|\phi\rangle$, optimized over all measurements. Let Y be the number of successes after conducting the CHSH test on the first m subsystems of $|\psi\rangle$ according to any measurement strategy. Then for $\mu > 0$*

$$P\left(Y/m > p + \mu\right) \le \exp \frac{-2(m\mu - r(1-p))^2}{(n-r)cos^4\pi/8} + (n+m)h\left(\frac{r}{n+m}\right)\ln 2.$$
(4.18)

The proof has two main steps and parallels the proof of Renner's Theorem 4.5.2 [Ren05]. The step first is to bound the given probability for states of the form $\Pi(|\phi\rangle^{\otimes m-r} \otimes |\phi'\rangle)$ for some permutation Π. Next we use Lemma 4.1.6 of Renner which that says $|\psi\rangle$ can be expressed as a superposition of a small number of such states and use Lemma 4.5.1 of Renner which bounds how much the probability can change for such superpositions.

Proof. We now suppose our system is in the state $|\psi'\rangle = |\phi\rangle^{\otimes m-r} \otimes |\phi'\rangle$ for some $|\phi'\rangle$ on r subsystems. (We may also permute the subsystems without changing the argument.) Let X_j be the random variable corresponding to the success or failure of the CHSH test on the jth subsystem for the measurement strategy actually used (which may vary with j). Since the measurement strategy cannot do better than the optimal strategy, we have $E(X_j) < p$ for $1 \le j \le m-r$ and $E(X_j) < \cos^2 \frac{\pi}{8}$ for $j > m-r$. Applying Hoeffding's inequality ([Hoe63]) to the first $m-r$ subsystems, we obtain for $t > 1$

$$Pr\left(\sum_{j=1}^{m-r} X_j > (m-r)(p+t)\right) \le e^{\frac{-2(m-r)t^2}{\cos^4 \frac{\pi}{8}}}.$$
(4.19)

The remaining r subsystems cannot add very much if r is small. Thus

$$Pr\left(\sum_{j=1}^{m} X_j > m(p+t) + r\left(1-p-t\right)\right) \leq e^{\frac{-2(m-r)t^2}{\cos^4 \frac{\pi}{8}}}. \tag{4.20}$$

where $m(p+t) + r(1-p-t) = (m-r)(p+t) + r$ and the additional r upper bounds the value of $\sum_{j=m-r+1}^{m} X_j$.

We now turn our attention back to $|\psi\rangle$. Let z be an m-tuple with $z_j = 1$ if the jth trial is successful and $z_j = 0$ if it is a failure. We may write the measurement operator for the CHSH tests together as one large projective measurement $\{M_z\}$ with M_z the projector corresponding to the outcomes of success and failure given according to z. Then the probability of getting the success/failure outcomes according to z is $\langle\psi| M_z |\psi\rangle$. Note that M_z is positive semi-definite.

We are only interested in the number of successful outcomes, which is given by $w(z)$, the Hamming weight of z. We can restate the above result as

$$\sum_{w(z)>m(p+t)+r(1-p-t)} \langle\psi'| M_z |\psi'\rangle \leq e^{\frac{-2(m-r)t^2}{\cos^4 \frac{\pi}{8}}}. \tag{4.21}$$

Now suppose that $|\psi\rangle$ is in $Sym(\mathcal{H}, |\phi\rangle^{\otimes n+m-r})$. We can express $|\psi\rangle$ as a superposition of states of the form $|\phi\rangle^{n+m-r} \otimes |\phi'\rangle$ up to permutations of subsystems. We can apply the above argument to each of these terms in the superposition. We are only measuring m of the subsystems, so depending on the permutation anywhere between $m-r$ and m of the subsystems may be in the state $|\phi\rangle$. Note that our bound still applies since the last r subsystems are arbitrary. The following two Lemmas from [Ren05] bound how much error may be introduced by this procedure.

Lemma 4.3 (Renner [Ren05] Lemma 4.5.1). *Let $|\psi\rangle = \sum_{x\in X} |x\rangle$ and let P be a positive semi-definite operator, then*

$$\langle\psi| P |\psi\rangle \leq |X| \sum_{x\in X} \langle x| P |x\rangle. \tag{4.22}$$

Lemma 4.4 (Renner [Ren05] Lemma 4.1.6). *Let $|\psi\rangle$ be a state in $Sym(\mathcal{H}, |\phi\rangle^{\otimes n-r})$. Then there exist orthogonal vectors $|x\rangle$, which are permutations of $|\phi\rangle^{\otimes n-r} \otimes |\phi_x\rangle$ for $x \in X$ such that $|\psi\rangle$ is in the span of the $|x\rangle$ for various x, and $|X| \leq 2^{nh(r/n)}$ where $h(\cdot)$ is the binary Shannon entropy.*

Applying these results we obtain

$$\sum_{w(z) > m(p+t) + r(1-p-t)} \langle \psi | \, M_z \, | \psi \rangle \leq e^{\frac{-2(m-r)t^2}{\cos^4 \frac{\pi}{8}}} 2^{(n+m)h(\frac{r}{n+m})}. \qquad (4.23)$$

Rewriting as a probability, we get

$$P\left(Y > m(p+t) + r\left(1 - p - t\right)\right) \leq e^{\frac{-2(m-r)t^2}{\cos^4 \frac{\pi}{8}}} 2^{(n+m)h(\frac{r}{n+m})} \qquad (4.24)$$

or, equivalently

$$P\left(Y/m > p + \mu\right) \leq \exp\left(\frac{-2(m\mu - r(1-p))^2}{(m-r)cos^4\pi/8} + (n+m)h(\frac{r}{n+m})\ln 2\right). \tag{4.25}$$

$\square$

4.4.5 Estimating conditional entropies

In this section we put some bounds on conditional entropies which will later provide us with the asymptotic key rate. We begin with a 2 qubit state ρ_{ABE}, to which Eve holds the purification, with the property $S_{max}(\rho_{AB}) = S$. We then measure Bob's system with an adversarial measurement and estimate $H(X|E)$, the entropy of Bob's outcome conditioned on Eve's system.

There are several tasks. First, we show that we may take ρ to be a Bell diagonal state on Alice and Bob's qubits. Second, we estimate $S_{max}(\rho_{AB})$ from the eigenvalues of a Bell diagonal state. We then use this estimate to bound certain entropies on the eigenvalues of the state. Finally, we estimate $H(X|E)$, minimized over possible measurements. Once these tasks are complete we may bound $H(X|E)$ using a function of $S_{max}(\rho_{AB})$.

The material in this section largely follows Pironio et al.'s argument in [PAB+09]. We indicate where we deviate from their work.

Bell diagonalization

We now prove the following Lemma:

Lemma 4.5. *Let ρ_{AB} be a given two qubit state with measurements A^a and B^b and consider $H(B|E)$, where B is Bob's system after being measured by*

B^0, and E indicates Eve's system, which is a purification of ρ_{AB}. If there exists f such that

$$H(B|E) \leq f(S_{max}(\rho_{AB})) \tag{4.26}$$

for all Bell diagonal ρ_{AB}, then the bound also holds for arbitrary ρ_{AB}.

We begin by supposing that all marginals of ρ_{AB} after being measured by Alice or Bob are uniform. Pironio et al. originally considered a protocol in which Alice and Bob actively symmetrize the marginals of their measurement outcomes by flipping each outcome randomly and announcing whether or not they did so. This is fine for qubit strategies, but is slightly problematic for arbitrary strategies since a strategy on a larger Hilbert space may have symmetric marginals but decompose into qubit strategies which do not. Here we offer a different argument that arrives at the same conclusion: we may take the marginals to be symmetric without compromising security.

Consider any qubit strategy. We may fix any basis for our discourse, so we choose one so that A^0 and A^1 are in the X, Z plane of the Bloch sphere, and analogously for Bob's measurements. We may produce a new qubit strategy by applying $Y \otimes Y$ to the state. This simply flips all outcomes, so it has the same S_{max} and error rate, and gives Eve the same information. Now consider a strategy which is formed by combining the two states with equal probability, with Eve recording which one is performed. This strategy again has the same S_{max}, error rate, and gives Eve the same information. Thus we may consider this final strategy alone, and if it is secure then so must be the original strategy.

We now return to Pironio et al.'s argument with a presentation of the proof of Lemma 3 from [PAB$^+$09]. We retain the basis above, with the measurements on the X, Z plane and assume that $Y \otimes Y$ has been applied with probability $1/2$. In the Bell basis we obtain

$$\rho_{AB} = \begin{pmatrix} \lambda_{\phi_+} & r_1 e^{i\theta_1} & 0 & 0 \\ r_1 e^{-i\theta_1} & \lambda_{\psi_-} & 0 & 0 \\ 0 & 0 & \lambda_{\phi_-} & r_2 e^{i\theta_2} \\ 0 & 0 & r_2 e^{-i\theta_2} & \lambda_{\psi_+} \end{pmatrix} \tag{4.27}$$

since $|\phi_+\rangle$ and $|\psi_-\rangle$ are eigenvectors of $Y \otimes Y$ with eigenvalue 1 while the other two Bell basis vectors have eigenvalue -1.

There is still freedom in the choice of basis, and we may make a rotation about Y on both Alice and Bob's side while keeping the measurements on

the X, Z plane. The rotation angles may be chosen (see [PAB$^+$09] Lemma 3 for details) to obtain

$$\rho_{AB} = \begin{pmatrix} \lambda_{\phi_+} & ir_1 & 0 & 0 \\ -ir_1 & \lambda_{\psi_-} & 0 & 0 \\ 0 & 0 & \lambda_{\phi_-} & ir_2 \\ 0 & 0 & -ir_2 & \lambda_{\psi_+} \end{pmatrix}. \tag{4.28}$$

Finally, we apply an argument analogous to the marginal symmetrization and find that an equal mixture of the above state and its complex conjugate gives the same security. This mixture has no off-diagonal entries in the Bell basis, and thus is Bell diagonal. This allows us to consider only Bell diagonal states.

Estimating S_{max}

We prove the following:

Lemma 4.6. *Let ρ_{AB} be a given two qubit Bell diagonal state. Then*

$$S_{max}(\rho_{AB}) \geq 2\sqrt{2}\sqrt{\left(\lambda_{\phi_+} - \lambda_{\psi_-}\right)^2 + \left(\lambda_{\phi_-} - \lambda_{\psi_+}\right)^2}. \tag{4.29}$$

Proof. First, we recall the definition of R' from section 4.2.4. For Bell diagonal operators we find

$$R' = \begin{pmatrix} \lambda_{\phi_+} - \lambda_{\phi_-} + \lambda_{\psi_+} - \lambda_{\psi_-} & 0 & 0 \\ 0 & -\lambda_{\phi_+} + \lambda_{\phi_-} + \lambda_{\psi_+} - \lambda_{\psi_-} & 0 \\ 0 & 0 & \lambda_{\phi_+} + \lambda_{\phi_-} - \lambda_{\psi_+} - \lambda_{\psi_-} \end{pmatrix}. \tag{4.30}$$

Note that R' is diagonal. Using R_{XX} and R_{ZZ} as the largest in absolute value (if this is not then case, then we still get a lower bound) we find exactly the desired lower bound on S_{max}.[1] $\qquad\square$

Entropy inequalities

We prove:

---

[1]Note that in [PAB$^+$09], Lemma 7 S_{max} is found as a maximum over two values. The second of these values is obtained for measurements in the (Z, Y) plane.

Lemma 4.7 (Pironio et al. [PAB$^+$09] Lemma 6). *Let ρ_{AB} be a two qubit state. Then*

$$h(\overline{\lambda}) - h(\lambda_{\Phi_+} + \lambda_{\Phi_-}) \leq h\left(\frac{1 + \sqrt{(S_{max}(\sigma_{AB})/2)^2 - 1}}{2}\right). \qquad (4.31)$$

where h is the Shannon entropy.

The proof is long and technical, so we refer the reader to [PAB$^+$09] for details. Briefly, the proof introduces a parameterization of the λs in terms of S and two other parameters. Then the entropies on the left hand side of the bound are written in terms of this parameterization. Finally, optimization techniques are used to find the maximum, giving the required bound.

Bounding $H(B|E)$ for Bell diagonal states

Lemma 4.8. *Let ρ_{AB} be a two qubit Bell-diagonal state with eigenvalues $\overline{\lambda}$, purified on system E. Suppose the B system is measured with an observable in the X, Z plane to obtain random variable Y. Then*

$$H(Y|E) \geq 1 + h(\lambda_{\Phi_+} + \lambda_{\Phi_-}) - h(\overline{\lambda}). \qquad (4.32)$$

.

Although this Lemma does not appear in [PAB$^+$09], the proof roughly follows that of Lemma 5 from [PAB$^+$09]. We fill in several details, including the derivation of ρ_{YE} and the calculation of its eigenvalues[2]

We begin with a slight change of notation which will allow more compact formulas below. We may write the Bell states as

$$|\psi_{st}\rangle = \frac{1}{\sqrt{2}} \sum_{r=0,1} (-1)^{rt} |r\rangle |r \oplus s\rangle \qquad (4.33)$$

with $|\phi_+\rangle = |\phi_{00}\rangle$, $|\phi_-\rangle = |\phi_{01}\rangle$, $|\psi_+\rangle = |\phi_{10}\rangle$ and $|\psi_-\rangle = |\phi_{11}\rangle$.

We may write a purification of ρ_{AB} as

$$|\Psi_{ABE}\rangle = \frac{1}{\sqrt{2}} \sum_{r,s,t=0,1} \sqrt{\lambda_{st}} (-1)^{rt} |r\rangle |r \oplus s\rangle |e_{st}\rangle. \qquad (4.34)$$

---

[2]Note that in [PAB$^+$09] there is a typo in equation 31. The final σ should appear with $|e_3\rangle$ rather than $|e_4\rangle$. Also, the final eigenvalues contain a $\cos 2\phi$ rather than $\cos 4\theta$ here. This is due the fact that ϕ is an angle in the Bloch sphere and so corresponds to 2θ.

Tracing out the A system may be accomplished by measuring in the Z eigenbasis and ignoring the outcome, obtaining a mixture of the two non-normalized states:

$$\sum_{s,t} \sqrt{\frac{\lambda_{st}}{2}} \left| s \oplus x \right\rangle (-1)^{xt} \left| e_{st} \right\rangle \tag{4.35}$$

for $x = 0, 1$, corresponding to the two reduced states on obtaining outcome x.

Next we measure the B system in the basis $q_0 \left| 0 \right\rangle + q_1 \left| 1 \right\rangle$ / $q_1 \left| 0 \right\rangle - q_0 \left| 1 \right\rangle$ with $q_0^2 + q_1^2 = 1$. For outcome y the E system is left in a mixture of the two non-normalized states

$$\sum_{s,t} \sqrt{\frac{\lambda_{st}}{2}} q_{s \oplus x \oplus y} \left| s \oplus x \right\rangle (-1)^{xt \oplus ys} \left| e_{st} \right\rangle \tag{4.36}$$

for $x = 0, 1$. The state ρ_{YE} is then a direct sum of two blocks. The blocks may be written as

$$M_y = \sum_{s,t,u,v,x} \frac{1}{2} \sqrt{\lambda_{st} \lambda_{uv}} q_{(x \oplus y \oplus s)} q_{(x \oplus y \oplus u)} (-1)^{x(t \oplus v) \oplus y(s \oplus u)} \left| e_{st} \right\rangle \!\! \left\langle e_{uv} \right| \tag{4.37}$$

Finally we determine the eigenvalues of ρ_{YE}, which is the direct sum of the two mixed states above. For each block (corresponding to a particular outcome y) we may obtain the eigenvalues using the following procedure: determine the trace of the block (which in this case is $1/2$ for each block since either outcome is equally likely for ρ_{AB} Bell diagonal). Next we determine the trace of the square of the block. Since each block is a mixture of two states, there will be two eigenvalues, Λ_w for $w = 0, 1$. Then for block M we have $m = \text{Tr}(M_y) = \Lambda_0 + \Lambda_1$ and $n = \text{Tr}(M_y^2) = \Lambda_0^2 + \Lambda_1^2$. We solve for Λ_w in terms of m and n by noting that $m^2 = n + 2\Lambda_0\Lambda_1$, subbing in $\Lambda_0 = m - \Lambda_1$, and solving the resulting quadratic for Λ_0. We obtain

$$\Lambda_w = \frac{1}{2} \left(\frac{1}{2} + (-1)^w \sqrt{2n - \frac{1}{4}} \right). \tag{4.38}$$

Squaring M_y and tracing we obtain

$$\text{Tr}(M_y) = \sum_{s,t,u,v,x,z} \frac{1}{4} \lambda_{st} \lambda_{uv} q_{(x \oplus y \oplus s)} q_{(x \oplus y \oplus u)} q_{z \oplus y \oplus s} q_{z \oplus y \oplus u} (-1)^{(x \oplus z)(t \oplus v)}. \tag{4.39}$$

Fixing s, t, u, v and summing over x and z, we find that the qs sum to

$$
\begin{cases}
(q_0^2 + q_1^2)^2 = 1 & t = v, u = s \\
(q_0^2 - q_1^2)^2 & t \neq v, u = s \\
4(q_0^2 q_1^2) & t = v, u \neq s \\
0 & t \neq v, u \neq s.
\end{cases}
\tag{4.40}
$$

We may write $q_0 = \cos\theta$, $q_1 = \sin\theta$, in which case $(q_0^2 - q_1^2)^2 = \cos^2 2\theta = \frac{1+\cos 4\theta}{2}$, $q_0^2 q_1^2 = \sin^2 2\theta = \frac{1-\cos 4\theta}{2}$, and

$$
\mathrm{Tr}(M_y) = \frac{1}{4}\left(\lambda_{00}^2 + \lambda_{01}^2 + \lambda_{10}^2 + \lambda_{11}^2 + \lambda_{00}\lambda_{01} + \lambda_{00}\lambda_{10} + \lambda_{01}\lambda_{11} + \lambda_{10}\lambda_{11}\right)
\tag{4.41}
$$

$$
+ \frac{\cos 4\theta}{4}\left(\lambda_{00}\lambda_{01} - \lambda_{00}\lambda_{10} - \lambda_{01}\lambda_{11} + \lambda_{10}\lambda_{11}\right).
$$

Collecting some terms, recalling that $\sum_{st}\lambda_{st} = 1$, and factoring we obtain

$$
\frac{1}{2}\left(1 + (\lambda_{00} - \lambda_{11})^2 + (\lambda_{01} - \lambda_{10})^2 + 2\cos 4\theta(\lambda_{00} - \lambda_{11})(\lambda_{01} - \lambda_{10})\right).
\tag{4.42}
$$

Substituting in, we find

$$
\Lambda_w = \frac{1}{4}\left(1 + (-1)^w\sqrt{(\lambda_{\phi_+} - \lambda_{\psi_-})^2 + (\lambda_{\phi_-} - \lambda_{\psi_+})^2 + 2\cos 4\phi(\lambda_{\phi_+} - \lambda_{\psi_-})(\lambda_{\phi_-} - \lambda_{\psi_+})}\right).
\tag{4.43}
$$

Each eigenvalue occurs with multiplicity 2, for the two values of y. Recall that for state ρ_{YE}, $H(Y|E) = H(\rho_{YE}) - H(\rho_Y)$. We find $H(\sigma_{YE})$ to be $1 + h(\Lambda_+)$, which is minimized for $\theta = 0$ if the term with cos is positive, or $\theta = \pi/4$ when the term with cos is positive. In these cases we obtain $\Lambda_+ = \lambda_{\phi_+} + \lambda_{\phi_-}$. Meanwhile, the state ρ_E has the same eigenvalues as ρ_{AB} since ρ_E is the purification. The eigenvalues are thus given by $\overline{\lambda}$, so $H(E) = h(\overline{\lambda})$. We obtain

$$
H(Y|E) \geq 1 + h(\lambda_{\phi_+} + \lambda_{\phi_-}) - h(\overline{\lambda}).
\tag{4.44}
$$

Bounding $H(Y|E)$ in terms of S

We finally obtain the bound we seek:

Lemma 4.9. *Let ρ_{AB} be a 2-qubit state, measured on the B system in the X, Z plane to obtain a system X. Further suppose that ρ_{AB} is purified by system E. Then*

$$H(Y|E) \geq 1 - h\left(\frac{1 + \sqrt{(S/2)^2 - 1}}{2}\right) \tag{4.45}$$

4.4.6 Security for qubit strategies on symmetric states

In this section we restrict our attention to the case where the state source emits a pair of qubits and the devices each measure one of these qubits. Our proof of security is derived from the one given by Renner in [Ren05]. The main difference is in the parameter estimation. Central to the argument is the finite quantum de Finetti Theorem published in [Ren07]. Security for qubit strategies follows from the same proof as Theorem 6.5.1 in [Ren05], with different parameters. Since the proof is laid out in great detail in [Ren05] we will only sketch the proof and indicate the necessary changes.

We begin with a symmetric state $n+m+k$ pairs of qubits, which we purify (according to Lemma 4.2.2 of [Ren05]) on Eve's system to a pure symmetric state ρ. Importantly, the purification is symmetric even when considering Eve's systems. According to the finite quantum de Finetti Theorem (4.4), we may drop k subsystems and obtain

$$\left\|\mathrm{Tr}_k(\rho) - \int \rho_\phi \nu(\phi)\right\|_1 \leq \frac{2}{9}\epsilon \tag{4.46}$$

with $\rho_\phi \in Sym(H_2^{\otimes 4}, |\phi\rangle^{\otimes n+m-r})$ and r depending on n, m, k, ϵ according to table 6.2 of [Ren05]. We next apply parameter estimation by measuring m systems with measurement settings chosen uniformly at random for Alice and Bob, and determine the number of CHSH successes, y. Then $\frac{y}{m}$ is our estimate of p. If this estimate is below some threshold, $p_{thres} + \mu$ (p_{thres} is used to determine the key rate in the privacy amplification phase) we abort and map the state to 0. According to Lemma 4.2, if we choose μ to be

$$\mu = \frac{4r}{m}\sqrt{\left(-\ln\frac{2\epsilon}{9} - (n+m)h\left(\frac{r}{n+m}\right)\ln 2\right)(m-r)\cos^4\frac{\pi}{8}}, \tag{4.47}$$

then the true value of p is lower than $\frac{y}{m} - \mu$, only with probability less than

$\frac{2}{9}\epsilon$. Thus we may apply the parameter estimation to obtain

$$\left\| \rho^{PE} - \int_V \rho_\phi^{PE} \nu(\phi) \right\|_1 \leq \frac{4}{9}\epsilon \tag{4.48}$$

where we restrict the integral to the set of states $|\phi\rangle$ which have CHSH probability of success p_{thres} or higher (denoted by V). The PE superscripts indicate the application of the parameter estimation protocol.

We now have (if the protocol did not abort) a state ρ^{PE} which is nearly indistinguishable from a mixture of near-product states each with CHSH success probability better than p_{thres}. We may characterize the smooth min entropy of this family of states and apply privacy amplification, deriving a security bound for the finite case. However, the calculation is essentially the same as it appears in [Ren05] and is beyond our scope. Instead, we will appeal to the final result and calculate the asymptotic key rate.

In [Ren05], Corollary 6.5.2 we find the asymptotic key rate after privacy amplification to be

$$\min_{\sigma_{AB}:S_{max}(\sigma_{AB})\geq S} H(Y|E) - H(Y|X) \tag{4.49}$$

with $H(Y|E)$ and $H(Y|X)$ evaluated for state σ_{AB}, and $S = 8p_{thres} - 4$, while X and Y are the classical outcomes for Alice and Bob upon measuring σ_{AB}. The system E is Eve's system, which we take to be a purification of σ_{AB}. Additionally, we must minimize over measurement strategies of Bob's devices.

By Lemma 4.9 the secret key rate is thus bounded below by

$$1 - h\left(\frac{1 + \sqrt{(S/2)^2 - 1}}{2} \right) - h(q) \tag{4.50}$$

where $H(Y|X) = h(q)$ and q is the bit error rate between Alice and Bob's raw keys (Alice error corrects). This is the same asymptotic rate achieved in [ABG$^+$07]. Note that there is no relationship between S and q, since Alice's raw key comes from an unknown measurement. Her measurement may measure ρ or some other system. In all cases it is possible for q to range from 0 to 1, regardless of the value of S.

4.5 Issues with practical implementations and discussion

Since DIQKD aims to provide higher security in practical implementations than QKD we must carefully examine the extent to which this is true. In particular we must address issues regarding the selection of measurement settings.

4.5.1 Detector efficiency

Detector efficiency loophole

A common complaint against DIQKD is the detector efficiency loophole, which was originally studied in the context of Bell inequalities. In practical optical experiments the detectors in the measurement devices do not always record a photon when it is present. This means that some trials in a Bell experiment give a "no outcome" result. In a non-adversarial setting this is not problematic, but if we suppose that the measurement devices are adversarial and we discard "no outcome" results then the adversary may *selectively* choose a "no outcome" result, allowing them to post-select for favourable conditions. In particular, the devices may post-select for a particular measurement setting, allowing the adversary *de facto* control over the measurement settings.

Consider the following strategy. Eve determines, for each trial, a measurement setting and outcome for Alice's device and an adaptive strategy for Bob's device. Alice's device waits for the measurement setting input and if it does not agree with the predetermined setting then the device gives no output, as though the photon was lost. On the trials for which an output is produced, the adaptive strategy in Bob's device allows for $S = 4$ since the measurement and outcome on Alice's side is known.

In the above strategy the detector efficiency of Alice's side is 0.5 and on Bob's side it is 1. By randomly exchange roles, so that Bob's measurement setting is post-selected, we obtain a randomized strategy with efficiency 0.75 for both Alice and Bob's detectors. Thus for detector efficiency below 0.75 there is a local hidden variable model which obtains $S = 4$.

Clearly if the observed detector efficiency is too low then DIQKD is not secure; the devices may seem to be lossy, but in fact are implementing a predetermined strategy that allows Eve to know all information. How efficient

must the detectors be to obtain a secure DIQKD implementation? Currently there has been only minimal study of the robustness of DIQKD against low detector efficiency. Pironio et al. [PAB+09] consider a scenario where "no outcome" results are assigned a random outcome. In this case the inefficiency of the detectors translates directly into effective noise. Their analysis concludes that a positive key rate is achievable for detector efficiency over 92.4% and they provide a bound for maximum key rate vs. efficiency using this strategy.

A proper analysis of DIQKD accounting for detector efficiency would likely use a modified CHSH inequality. It is possible to derive Bell type inequalities that account for detector efficiency (see [Ebe93] for one such derivation) which could be used to characterize a set of quantum states which from which secret key may be extracted. An important roadblock in this program is the fact that Lemma 4.1 is restricted to observables with two outcomes and no extension is known.

Future work. *Derive robust security bounds for DIQKD that take into account low detector efficiency.*

In practical implementations we may make the following assumption:

Assumption 4.4 (Fair sampling). *The efficiency on each trial of Alice and Bob's detectors is independent of the measurement setting.*

With this assumption in place there is no post-selection of measurement settings and the problems outlined in this section do not exist. Of course this assumption is clearly not satisfied in practical settings, as outlined below. Nevertheless, in security proofs the assumption is often made implicitly.

Comparison with QKD

Although the detector efficiency loophole is sometimes given as reason for preferring QKD over DIQKD, this argument does not hold. In fact, QKD is also susceptible to the detector efficiency loophole. This point is usually not addressed, since the devices are considered to be under Alice and Bob's control, and hence the efficiency could not vary depending on the measurement setting. As a concrete counterexample to the validity of this assumption, we consider the class of attacks based on detector efficiency mismatch.

Detector efficiency mismatch attacks were described by Makarov et al. [MAS06a] and have been implemented against commercially available QKD

systems by Zhao et al. [ZFQ$^+$08]. Generally speaking, detector efficiency mismatch attacks exploit the fact that different detectors are often used for different measurement settings, and individual detectors differ in their efficiency. The specific attacks implemented by Zhao et al. are called time shift attacks. These attacks are viable against detectors operating in gated mode, where they become sensitive for short periods of time. The efficiency of the detector thus varies over time in a way that is specific to individual detectors. The detector for one measurement setting has a relatively high efficiency at a time when the detector for another measurement setting has a low efficiency. In this case Eve may selectively adjust the arrival time of a photon to match the period where the efficiencies are mismatched, favouring one measurement setting over the other.

4.5.2   Coincidences and timings

Since the likelihood of a photon being absorbed within the air or a fibre optic cable is so high, and stray photons and dark counts generate detector clicks when no signal photon is present, it is common to record the timing of detector clicks at both Alice and Bob's labs and look later for coincidences, which are times when a detector clicks for both Alice and Bob. These coincidences are then used as the raw data for the remainder of the protocol.

Although convenient, finding coincidences may introduce side channels. For example, if there is also some detector inefficiency mismatch then precise timing data could reveal that a coincidence occurred at a time when the detector is more efficient than another, in which case Eve will learn that one measurement setting or measurement outcome was more likely than another. Another attack using timing information was described by Lamas-Linares and Kurtsiefer in [LLK07]. There the specific entangled photon source used has a timing signature that, together with precise coincidence timing data, can leak information to Eve.

The two examples given here show that there may be complex interactions between timing data and other channels which may leak information. For this reason we make the following assumption (for both DIQKD and typical QKD security models), which is likely to be untrue in many implementations:

Assumption 4.5. *There are no correlations between coincidence timing data and the raw key.*

4.5.3 The role of DIQKD

With so many assumptions necessary for security, one may wonder if there is any benefit to DIQKD. However, these assumptions are also necessary for security in QKD. Certainly there are fewer assumptions in DIQKD because of the adversarial device model used. The practical value of DIQKD is limited because of the lower key rates it achieves, but the theoretical value is high because DIQKD places an emphasis on carefully analyzing the assumptions necessary for security and introduces new tools for security analysis.

Chapter 5

Black box state characterization

Contents

5.1 Introduction

In the previous chapters we have concentrated on using black box devices for specific tasks, which has limited our investigation to particular technical properties that allow us to achieve the goals for each task. In this chapter we expand the context and consider characterizing a black box state source without reference to its final use. In particular, we will use robust measures of the quality of the state source with an operational interpretation that will allow us to estimate its behaviour in any context.

5.1.1 Reference experiment

The reference experiment that we will consider is the typical CHSH setup, with a state source emitting a bipartite state, measured by a pair of devices, each with two measurement settings. The measurements statistics are boiled down into a single number, the CHSH value, as defined in section 4.2.4. Using this value alone we wish to estimate the state emitted by the source, comparing it to an EPR pair, $|\phi_+\rangle$.

The reference experiment consists of an EPR pair, $|\phi_+\rangle$ with measurements $A_0 = X$, $A_1 = Z$, $B_0 = \frac{1}{\sqrt{2}}(X + Z)$, and $B_1 = \frac{1}{\sqrt{2}}(X - Z)$. The CHSH value for the reference experiment is $2\sqrt{2}$.

5.1.2 Measures of quality

A major obstacle in this line of research is choosing a suitable measure of quality for the state. Although our reference state is already chosen, there are many options for how we may compare it to the physical state. Complicating the picture is the fact that the physical state has an unknown dimension. Finding a measure that has a reasonable operational interpretation across all possible physical states is challenging. In this chapter we will develop several measures and compare them. We will also prove several bounds. The picture is incomplete, however, as we shall see. For certain measures proving a bound is problematic, while for less desirable bounds (from an operational perspective) the bounds are reasonably easy to find.

5.1.3 Literature review

There has been limited work in this area to date. The results in this chapter are all joint work with co-authors Bardyn, Liew, Massar and Scarani and are published in [BLM+09]. Certain aspects were anticipated by Mayers and Yao [MY04] in their work on self-testing of EPR pairs discussed in section 3.4. Various articles on the CHSH inequality are also relevant, particularly the work by Horodecki et al. [HHH95], which may be seen as a non-robust version of the results in this chapter. Their work shows that any two qubit state that maximally violates the CHSH inequality must be maximally entangled. Also, the authors developed a method of calculating the maximal CHSH value achievable for any two qubit state, which we used in the proof of Lemma 4.6 (although the notation we used was based on [VW02].)

5.1.4 Contributions

In this chapter we develop several measures of quality for an entangled pair source and prove bounds on them. The definition of these measures presents a significant technical challenge because of the black box nature of the test and the fact that we compare the physical state to a fixed reference state. These two aspects of the problem mean that the measures must be defined regardless of the dimension of the state and nevertheless have a consistent interpretation that does not depend on the dimension.

We are able to prove bounds for several of the measures of quality that we define. In particular, we have a complete characterization for qubits: a lower bound and a set of states that achieve the bound, proving that it is tight. When we extend the definition to arbitrary dimensions we have some partial results. For the most restrictive definition (F_{MY}, defined below) we have a conjectured lower bound for pure states, and examples that saturate this bound. For the least restrictive definition (F_{LOCC}) we have a lower bound, but no examples that saturate it. This bound is conjectured to be tight. Meanwhile, for the final measure (F_{LO}), which is bounded above and below by the previous two measures, we have a lower bound but conjecture that it is not tight.

The material in this chapter was published in [BLM+09] and is joint work with the co-authors.

5.2 Two qubits

Although our ultimate goal will be to have no assumptions on the dimension of the physical state, we will first investigate the case of two qubits, both because it is easier to analyze and because the bound we derive will be useful when we move to the case of higher dimensions.

5.2.1 Fidelity and trace distance

In the case where the physical state is known to be two qubits it is quite easy to measure the quality of an entangled pair. We simply choose an appropriate distance function on states. The most meaningful distance, from an operational point of view, is the trace distance given by[1]

$$||\rho - \sigma||_{Tr} = \frac{1}{2}\text{Tr}(|\rho - \sigma|) = \frac{1}{2}\text{Tr}\left(\sqrt{(\rho - \sigma)^2}\right) \qquad (5.1)$$

which measures how distinguishable two states are by any procedure. Watrous' lecture notes [Wat08b] provides a good introduction.

An easier figure to calculate is the fidelity, given by[2]

$$F(\rho, \sigma) = \text{Tr}(\sqrt{\rho}\sigma\sqrt{\rho}). \qquad (5.2)$$

Watrous' lecture notes [Wat08c] again give a good introduction. The fidelity is related to the trace distance by

$$1 - \sqrt{F(\rho, \sigma)} \leq ||\rho - \sigma||_{Tr} \leq \sqrt{1 - F(\rho, \sigma)} \qquad (5.3)$$

(the Fuchs-van de Graaf Inequalities) which is saturated on the right when ρ and σ are both pure. Since the fidelity is easier to calculate, we will use it for the remainder of this chapter.

It is often convenient to calculate the fidelity by means of a purification using the following Lemma (with a proof appearing in Watrous' lecture notes [Wat08c].)

---

[1] The trace distance is sometimes given without the factor of $\frac{1}{2}$, particularly in Watrous' lecture notes.

[2] The fidelity is also sometimes given as the square root of this value, particularly in Watrous' lecture notes.

Lemma 5.1 (Uhlmann's Theorem). *Let ρ and σ be given with $|\psi\rangle$ any purification of ρ. Then*

$$F(\rho, \sigma) = \max_{|\phi\rangle \ purification \ of \ \sigma} |\langle\psi|\phi\rangle|^2. \tag{5.4}$$

As well, if $\rho = |\psi\rangle\langle\psi|$ is pure (as frequently will be the case in our discussion) then

$$F(|\psi\rangle\langle\psi|, \sigma) = \langle\psi|\sigma|\psi\rangle. \tag{5.5}$$

5.2.2 Measuring the state

Suppose we have a bipartite state ρ on a pair of qubits. Our reference state will always be a pair of maximally entangled qubits: $|\phi_+\rangle$. Ideally we would like to bound the trace distance between these two states:

$$||\rho - |\phi_+\rangle\langle\phi_+|\,||_{Tr} \tag{5.6}$$

but we will settle for estimating the fidelity, $F(\rho, |\phi_+\rangle\langle\phi_+|)$, which will also provide a bound on the trace distance. There is some ambiguity, though, since we have no natural local bases when considering ρ, and our description of the reference state assumes that the local bases are known. To this end we define F_{MY} as

$$F_{MY}(\rho) = \max_{U,V \ \text{unitary}} F(U \otimes V \rho U^\dagger \otimes V^\dagger, |\phi_+\rangle\langle\phi_+|). \tag{5.7}$$

The maximization takes into account our lack of preference for particular local bases for ρ. The value of $F_{MY}(\rho)$ will vary between $1/4$ for a maximally mixed state and 1 for a maximally entangled state.

Another measure that we will use allows for arbitrary local operations, rather than just changes of bases. For pure states this will not offer any advantage, but for mixed states it allows a slightly higher fidelity. We define this by

Definition 5.1. *Let a two qubit state ρ be given. Then*

$$F_{LO}(\rho) = \max_{\Phi_A, \Phi_B} F(\Phi_A \otimes \Phi_B(\rho), |\phi_+\rangle\langle\phi_+|) \tag{5.8}$$

where Φ_A and Φ_B range over completely positive trace preserving maps taking qubits to qubits.

By the simple fact that unitary operations are local, we know that $F_{MY} \leq F_{LO}$. For pure states the two quantities are equal; if the state is a product state then unitaries will take it to $|00\rangle$ giving the highest possible fidelity for a product state (mixed or not). If the state is entangled than no operation can increase the entanglement; only a change of basis is required.

In the case of mixed states, however, we may find strict inequality. Any separable state may be replaced by a pure product state. In the case of the completely mixed state, for example, we find $F_{MY}(I/2) = 1/4$ while $F_{LO}(I/2) = 1/2 = F_{LO}(|00\rangle)$.

5.2.3 Model for measurement operators

We will model the measurement operators for the CHSH test as two-outcome observables. Thus, each measurement operator will be Hermition with eigenvalues ± 1. For qubits an important consideration is whether we allow all eigenvalues to be 1 or -1, that is, whether we allow I or $-I$ as a measurement operator. More generally speaking, how do we model a fixed outcome? We may model a fixed outcome by a I or $-I$ as the measurement, or by using eigenvectors of some non-trivial measurement as the state.

Generally speaking this will not pose a problem. We will be only interested in cases where $S > 2$ since if $S \leq 2$ then the experiment may be simulated with a local hidden variable model and we have no interest. For $S > 2$, a non-trivial measurement must be used.

5.2.4 Bound for qubits

We will prove the following Theorem:

Theorem 5.1. *Let a two qubit state ρ be given. Then*

$$F_{MY}(\rho) \geq \frac{1 + \sqrt{\left(\frac{S_{max}(\rho)}{2}\right)^2 - 1}}{2}. \tag{5.9}$$

Furthermore, the bound is saturated for $S \geq 2$ by the states $\cos\theta\,|00\rangle + \sin\theta\,|11\rangle$.

There are many ways of approaching this proof. For a different proof, see Bardyn et al. [BLM+09].

Proof. **Lower bound**

We begin much as in section 4.4.5 by reducing to the case of Bell diagonal states. Suppose that $S_{max}(\rho)$ is achieved for measurements A_a, and B_b. We may choose any basis we like for our discourse, so we suppose that the measurements are all in the X, Z plane. Note that if we apply $Y \otimes Y$ to ρ then all the outcomes on both sides are flipped, but S is not affected since the only thing that matters is whether the outcomes are the same or different. As in the proof for Lemma 4.5 we may thus construct a new state by applying $Y \otimes Y$ with probability $1/2$, and the local bases may be chosen so that the off-diagonal entries of the density matrix in the Bell basis are all imaginary. As well, complex conjugation does not affect S since the measurements are all in the real plane. We may thus take an equal mixture of the state and its complex conjugate to obtain a state

$$\sigma = \frac{1}{4} \left(\rho + \rho^* + Y \otimes Y (\rho + \rho^*) Y \otimes Y \right) \tag{5.10}$$

with $S_{max}(\sigma) \geq S_{max}(\rho)$.

Now consider $F_{MY}(\sigma)$

$$F_{MY}(\sigma) = \langle \phi_+ | \sigma | \phi_+ \rangle \tag{5.11}$$

$$= \langle \phi_+ | \rho | \phi_+ \rangle + \langle \phi_+ | \rho^* | \phi_+ \rangle + \langle \phi_+ | Y \otimes Y \rho Y \otimes Y | \phi_+ \rangle + \langle \phi_+ | Y \otimes Y \rho^* Y \otimes Y | \phi_+ \rangle . \tag{5.12}$$

Since $|\phi_+\rangle$ has all real entries, complex conjugation does not matter. Also, we may rewrite

$$\langle \phi_+ | Y \otimes Y \rho Y \otimes Y | \phi_+ \rangle = \text{Tr}(Y \otimes Y | \phi_+ \rangle\langle \phi_+ | Y \otimes Y \rho) . \tag{5.13}$$

The reader may verify that $Y \otimes Y | \phi_+ \rangle = - | \phi_+ \rangle$. Finally, since complex conjugation and multiplying by $Y \otimes Y$ do not change the state $|\phi_+\rangle$, we conclude that the optimal basis for ρ is also the optimal basis for the other states in the mixture as well. Combining these facts, we obtain

$$F_{MY}(\sigma) = F_{MY}(\rho). \tag{5.14}$$

Let f be defined by

$$f(S) = \frac{1 + \sqrt{\left(\frac{S}{2}\right)^2 - 1}}{2}. \tag{5.15}$$

Note that f is increasing. If we find that $F_{MY}(\sigma) \geq f(S)$ then we obtain

$$F_{MY}(\rho) = F_{MY}(\sigma) \geq f(S_{max}(\sigma)) \geq f(S_{max}(\rho)). \qquad (5.16)$$

Thus we may restrict ourselves to Bell diagonal states.

We now assume that ρ is Bell diagonal with eigenvalues $\lambda_{\phi_+}, \lambda_2, \lambda_3, \lambda_4$ with largest eigenvalue λ_{ϕ_+} (if this is not the case, then a local change of basis will make it so and keep the state Bell diagonal). The ordering of the remaining eigenvalues is not important. Following the proof of Lemma 4.6 we find

$$S_{max}(\rho) = 2\sqrt{2}\sqrt{\left(\lambda_{\phi_+} - \lambda_2\right)^2 + \left(\lambda_3 - \lambda_4\right)^2} \qquad (5.17)$$

for some ordering of the remaining eigenvalues. For a particular value of λ_{ϕ_+} the largest possible value of S_{max} occurs when $\lambda_2 = \lambda_4 = 0$ and $\lambda_3 = 1 - \lambda_{\phi_+}$, hence

$$\left(\frac{S_{max}}{2\sqrt{2}}\right)^2 \leq \lambda_{\phi_+}^2 + (1 - \lambda_{\phi_+})^2 = 2\lambda_{\phi_+}^2 + 1 - 2\lambda_{\phi_+} \qquad (5.18)$$

$$\frac{1}{2}\left[\left(\frac{S_{max}}{2}\right)^2 - 1\right] \leq 2(\lambda_{\phi_+}^2 - \lambda_{\phi_+} + \frac{1}{4}) = 2\left(\lambda_{\phi_+} - \frac{1}{2}\right)^2 \qquad (5.19)$$

$$\frac{1 + \sqrt{\left(\frac{S_{max}}{2}\right)^2 - 1}}{2} \leq \lambda_{\phi_+} = F_{MY}(\rho). \qquad (5.20)$$

Tightness of the bound

We claim that the states $|\psi\rangle = \cos\theta\,|00\rangle + \sin\theta\,|11\rangle$ saturate the bound. We first refer the reader to the proof of Lemma 4.6. The matrix R' for this state is

$$\begin{pmatrix} 2\cos\theta\sin\theta & 0 & 0 \\ 0 & -2\cos\theta\sin\theta & 0 \\ 0 & 0 & 1 \end{pmatrix}. \qquad (5.21)$$

Then $S_{max} = 2\sqrt{1 + 4\cos^2\theta\sin^2\theta}$. Meanwhile, $F_{MY}(|\psi\rangle)$ is just $|\langle\psi|\phi_+\rangle|^2 = \frac{1}{2}(\cos\theta + \sin\theta)^2$ since it is obvious that no unitary operation can improve this. (This fact is proven in Lemma 5.4 below.) We then find

$$\frac{1 + \sqrt{\left(\frac{S_{max}(\rho)}{2}\right)^2 - 1}}{2} = \frac{1 + 2\cos\theta\sin\theta}{2} = F_{MY}(|\psi\rangle) \qquad (5.22)$$

and the state saturates the bound.

$\square$

The above bound immediately extends to F_{LO} if we replace ρ with $|00\rangle$ whenever ρ has $S_{max}(\rho) < 2$. Hence we obtain the following Lemma.

Lemma 5.2. *Let a bipartite state ρ be given. Then*

$$F_{LO}(\rho) \geq \frac{1 + \sqrt{\left(\frac{\max(S_{max}(\rho),2)}{2}\right)^2 - 1}}{2}. \tag{5.23}$$

Further, this bound is tight.

Note that the bounds for F_{MY} and F_{LO} coincide for $S \geq 2$. As mentioned previously, arbitrary operations do not improve on F_{MY} for pure states, so the pure state also saturate this bound for $S \geq 2$. For $S \leq 2$, any state can be transformed to a pure product state using LO and a deterministic strategy gives $S = 2$, so the bound is saturated for these states as well.

Later we will use the qubit bound when considering bounds for higher dimensional systems. In that application we will need to apply convexity arguments and the following Lemma will be useful.

Lemma 5.3. *Define f by*

$$f(S) = \frac{1 + \sqrt{\left(\frac{S}{2}\right)^2 - 1}}{2}. \tag{5.24}$$

Then $f(x)$ is concave down on the domain $2 \leq x \leq 2\sqrt{2}$.

Proof. We instead consider $g(x) = \sqrt{x^2 - 1}$ for $1 \leq x \leq \sqrt{2}$. The second derivative of $g(x)$ is

$$-\frac{\sqrt{x^2 - 1}}{(x^2 - 1)^2}. \tag{5.25}$$

For $1 \leq x \leq \sqrt{2}$ this is always negative. Hence $g(x)$ and $f(x)$ are concave down. $\square$

5.3 Measures of quality for higher dimensions

For higher dimensional physical systems we run into an important question of definition: how do we compare a physical state on a state of arbitrary dimension with one of a fixed dimension? The only reasonable reference state

to compare the physical state with is a maximally entangled pair of qubits since these are the only states that maximally violate the CHSH inequality, and without further information about the physical state we cannot rule out the two qubit case either. We present several approaches to this problem. The most useful measure will likely depend on the intended application.

5.3.1 Mayers-Yao type fidelity

We begin using the approach begun by Mayers and Yao in [MY04] and continued by Magniez et al. in [MMMO06]. Let $|\psi\rangle_{AB}$ be a bipartite pure physical state. Mayers and Yao evaluate the physical state by asking whether or not there exists a state of the form $|\psi'\rangle_{AB} \otimes |\phi_+\rangle_{AB}$ that is equivalent to $|\psi\rangle$ under local unitary transformations. Later, Magniez et al. make the notion robust by considering the quantity

$$\min_{U,V,|\psi'\rangle} ||U_A \otimes V_B |\psi\rangle - |\psi'\rangle |\phi_+\rangle ||_1 \tag{5.26}$$

where U and V are unitary transformations. We may easily transform this to match the fidelity measure we use for qubits as follows (abusing notation a little).

Definition 5.2. *Let a pure bipartite physical state $|\psi\rangle$ be given. Then $F_{MY}(|\psi\rangle)$ is defined by*

$$F_{MY}(|\psi\rangle) = \max_{U,V,|\psi'\rangle} F(U_A \otimes V_B |\psi\rangle, |\psi'\rangle |\phi_+\rangle). \tag{5.27}$$

where U and V are unitary transformations and $|\psi'\rangle$ is any state on the appropriate space.

We may extend this definition to mixed states by replacing $|\psi'\rangle$ with a mixed state ρ'. We need to keep the transformations unitary however, otherwise we could always take $|\psi'\rangle$ to be a maximally mixed state and have the transformation completely mix the corresponding portion of the physical state.

With this definition we are able to provide a complete characterization for pure states in the following Lemma. This relies on the singular value (Schmidt) decomposition for pure bipartite states.

Lemma 5.4. *Let bipartite $|\psi\rangle$ be given with*

$$|\psi\rangle = \sum_j \lambda_j \, |a_j\rangle \, |b_j\rangle \, . \tag{5.28}$$

Then

$$F_{MY}(|\psi\rangle) = \sum_l \frac{(\lambda_{2l} + \lambda_{2l+1})^2}{2}. \tag{5.29}$$

Proof. The closest state of the form $|?\rangle \otimes |\phi_+\rangle$ has Schmidt decomposition

$$|\phi\rangle = \sum_j \mu_j \, |c_j\rangle \, |d_j\rangle \tag{5.30}$$

with $\mu_{2l} = \mu_{2l+1}$. For concreteness, we may assume that the λ_js and μ_js are both in decreasing order

We first show that we may take $|c_j\rangle = |a_j\rangle$ and $|d_j\rangle = |b_j\rangle$. Note that

$$|\langle\psi|\phi\rangle| \le \sum_{jk} \lambda_j \mu_k |\langle a_j|c_k\rangle \langle b_j|d_k\rangle|. \tag{5.31}$$

Let us define the matrix M by

$$M_{jk} = |\langle a_j|c_k\rangle \langle b_j|d_k\rangle|. \tag{5.32}$$

The values $|\langle a_j|b_k\rangle|$ for various k and fixed j form a vector of norm 1 since $|b_k\rangle$ is a basis and $|a_j\rangle$ has norm 1. The same is true for the values $|\langle b_j|d_k\rangle|$ and if we fix k and vary j instead. Thus columns (and rows) of M are formed by entrywise products of norm 1 vectors and the sum of each row and column of M is at most 1. This means that we can find a new matrix N with positive entries such that $M + N$ is doubly stochastic. Note that

$$|\langle\psi|\phi\rangle| \le \sum_{jk} \lambda_j \mu_k (M + N)_{jk}. \tag{5.33}$$

By the Birkhoff-von Neumann Theorem we may write $M + N$ as a convex combination of permutation matrices, thus

$$M + N = \sum_m p_m P_m \tag{5.34}$$

116

with $\sum_m p_m = 1$ and P_m permutation matrices. Since the combination is convex, there exists some m for which

$$|\langle\psi|\phi\rangle| \le \sum_{jk} \lambda_j \mu_k (P_m)_{jk}. \tag{5.35}$$

The permutations merely reorder the μ_js and it is easy to prove that the maximum is achieved when the λ_js and μ_js are both in decreasing order. Hence $P_m = I$ satisfies the above equation. We may achieve this by choosing the bases $|c_j\rangle = |a_j\rangle$ and $|d_j\rangle = |b_j\rangle$, so we need not consider any other bases.

We now optimize over μ_j subject to the condition $\mu_{2l} = \mu_{2l+1}$. By the Cauchy-Schwarz inequality we have

$$|\langle\psi|\phi\rangle|^2 = \left(\sum_l (\lambda_{2l} + \lambda_{2l+1})\mu_{2l}\right)^2$$

$$\le \left(\sum_l (\lambda_{2l} + \lambda_{2l+1})^2\right)\left(\sum_l \mu_{2l}^2\right) \tag{5.36}$$

with equality when μ and λ are collinear. Thus we set

$$\mu_{2l} = \mu_{2l+1} = \frac{\lambda_{2l} + \lambda_{2l+1}}{N} \tag{5.37}$$

with N a normalization constant equal to

$$N = \sqrt{2\sum_l (\lambda_{2l} + \lambda_{2l+1})^2}. \tag{5.38}$$

With these values, we obtain

$$F_{MY}(|\psi\rangle) = |\langle\psi|\phi\rangle|^2 = \sum_l \frac{(\lambda_{2l} + \lambda_{2l+1})^2}{2}. \tag{5.39}$$

$\square$

5.3.2   Local operations and LOCC

The F_{LO} we defined for qubits could be extended in a number of ways. In particular, F_{MY} defined in the previous section reduces to F_{MY} in the case

where the physical state is a pair of qubits, which is equal to F_{LO} for states with $S > 2$. Here we will extend it in another way. We begin with a physical bipartite state ρ and ask the question "What is the most entangled pair of qubits we can obtain through local operations?" This gives rise to the following definition:

Definition 5.3.

$$F_{LO}(\rho) = \max_{\Phi_A, \Phi_B} F(\Phi_A \otimes \Phi_B(\rho), |\phi_+\rangle\langle\phi_+|) \tag{5.40}$$

with Φ_A and Φ_B ranging over completely positive trace preserving maps from the spaces of the physical state a qubits.

For qubits this definition is not the same as F_{MY} since arbitrary qubit channels are allowed instead of just unitaries. In the Lemma below we establish a relationship between F_{MY} and F_{LO}.

Lemma 5.5. *Let bipartite ρ be given. Then*

$$F_{MY}(\rho) \leq F_{LO}(\rho) \tag{5.41}$$

with equality if ρ is pure.

Proof. Let ρ be given. Then

$$F_{LO}(\rho) = \max_{\Phi \in LO} F(\Phi(\rho), |\phi_+\rangle\langle\phi_+|) \tag{5.42}$$

with LO the set of local operations that take the space AB to a pair of qubits. We may restrict this set to operations which only apply local unitaries and trace out everything but a pair of qubits to obtain

$$F_{LO}(\rho) \geq \max_{U,V} F(\text{tr}_X(U \otimes V \rho U^\dagger \otimes V^\dagger), |\phi_+\rangle\langle\phi_+|) \tag{5.43}$$

where tr_X means tracing out everything but a pair of qubits. Since the fidelity cannot decrease when a system is traced out we have

$$F_{LO}(\rho) \geq \max_{U,V} F(U \otimes V \rho U^\dagger \otimes V^\dagger, \rho' \otimes |\phi_+\rangle\langle\phi_+|) \tag{5.44}$$

for all ρ', and in particular for the ρ' which maximizes the expression and gives $F_{MY}(\rho)$. Thus

$$F_{LO}(\rho) \geq F_{MY}(\rho) \tag{5.45}$$

118

Now suppose that $\rho = |\psi\rangle\langle\psi|_{AB}$. We may write an operation in LO as adding a pair of ancillas and a pair of target qubits, applying a pair of unitaries, and tracing out everything but the target qubits. Thus

$$F_{LO}(|\psi\rangle) = \max_{U,V} F(\mathrm{tr}_{ABX_aX_b}(U \otimes V |\psi\rangle_{AB} |00\rangle_{X_aX_b} |00\rangle_{Y_aY_b}), |\phi_+\rangle\langle\phi_+|_{Y_aY_b})$$

(5.46)

Applying Uhlmann's Theorem, we obtain

$$F_{LO}(|\psi\rangle) = \max_{U,V,|\phi\rangle} \left| \langle\psi|_{AB} \langle 00|_{X_aX_b} \langle 00|_{Y_aY_b} U^\dagger \otimes V^\dagger |\phi\rangle \otimes |\phi_+\rangle_{Y_aY_b} \right|^2 \quad (5.47)$$

The right hand side is equal to $F_{MY}(|\psi\rangle \otimes |00\rangle \otimes |00\rangle)$ by definition. This in turn is equal to $F_{MY}(|\psi\rangle)$ since the value of F_{MY} for a pure state is only dependent on the Schmidt decomposition, which the product state ancillas do not change. Thus

$$F_{LO}(|\psi\rangle) = F_{MY}(|\psi\rangle). \tag{5.48}$$

$\square$

For mixed states there exist cases with a strict inequality. For example $F_{MY}(\frac{I}{4}) = \frac{1}{4}$, but $F_{LO}(\frac{I}{4}) = \frac{1}{2}$ since the class LO allows us to replace the state with $|00\rangle$.

The proof of the Lemma implies a construction for the optimal local operations for extract an approximate EPR pair. First take the singular value decomposition with singular values ordered in a decreasing fashion. Then pair them up and introduce some new variables to obtain

$$|\psi\rangle = \sum_j \sqrt{p_j} \left(c_j |2j\rangle |2j\rangle + s_j |2j+1\rangle |2j+1\rangle \right) \tag{5.49}$$

where $c_j^2 + s_j^2 = 1$ and $\lambda_{2j} = p_j c_j$, $\lambda_{2j+1} = p_j s_j$, further implying that $\sum_j p_j = 1$. The decreasing ordering implies that c_j and s_j are as close together as possible, overall. We can then think of the state as a direct sum of pairs of qubits, with each pair of qubits close as possible to an EPR pair. The optimal local operations consist of projecting onto the spaces spanned by $|2j\rangle$ and $|2j+1\rangle$ for various j, and then mapping $|2j\rangle$ to $|0\rangle$ and $|2j+1\rangle$ to $|1\rangle$ to obtain a qubit.

Larger classes of operations

We may further extend the definition of F_{MY} on qubits using different classes of operations. Instead of considering local operations of the form $\Phi_A \otimes \Phi_B$ we may instead consider separable maps or local operations with classical communication (LOCC). The latter is most interesting to us because they are the largest class of reasonably implementable operations that do not increase entanglement. (Separable operations are the largest class that do not increase entanglement, but they may require quantum communication to implement.) Thus we define one more measure of fidelity:

Definition 5.4.

$$F_{LOCC}(\rho) = \max_{\Phi} F(\Phi(\rho), |\phi_+\rangle\langle\phi_+|) \tag{5.50}$$

with Φ ranging over LOCC maps that take the state ρ to a pair of qubits.

Since $LOCC$ contains LO we have

$$F_{MY}(\rho) \leq F_{LO} \leq F_{LOCC}. \tag{5.51}$$

5.4 Bounds for higher dimensions

5.4.1 Bounds for F_{MY}

Recall that for pure states we are able to analytically calculate F_{MY} in terms of the singular values (Schmidt coefficients). Conveniently, Gisin and Peres [GP92] have studied the case of determing S_{max} of a pure state in terms of the singular values. Although they were not able to find an analytic solution, they make the following conjecture

Conjecture 5.1 (Gisin, Peres [GP92])**.** *Let a bipartite state $|\psi\rangle$ be given with singular value decomposition*

$$|\psi\rangle = \sum_j p_j \left(c_j |2j\rangle |2j\rangle + s_j |2j+1\rangle |2j+1\rangle\right). \tag{5.52}$$

with $p_0 c_0 \geq p_0 s_0 \geq p_1 c_1 \geq p_1 s_1 \geq \ldots$. Then

$$S_{max}(|\psi\rangle) = \sum_j p_j \left(2\sqrt{1 + 4c_j^2 s_j^2}\right). \tag{5.53}$$

Later numerical studies by Liang and Doherty [LD06] supported the conjecture.

Gisin and Peres give an explicit construction for the measurement operators which achieve their conjectured value of S_{max}. The general idea is much the same as for the optimal local operations for pure states that achieve F_{LO}, as discussed in section 5.3.2. The state is divided up into a direct sum of pairs of qubits, and the measurements are a projection onto one of the summands followed by the optimal measurement for that pair of qubits.

We now prove that the Gisin-Peres conjecture implies a bound on F_{MY} in terms of S_{max} for pure states.

Lemma 5.6. *If conjecture 5.1 holds, then for pure bipartite state $|\psi\rangle_{AB}$ we have*

$$F_{MY}(|\psi\rangle) \geq \frac{S_{max}(|\psi\rangle) + 2\sqrt{2} - 4}{4\left(\sqrt{2} - 1\right)}. \tag{5.54}$$

Furthermore, this bound is tight.

Proof. We may write $|\psi\rangle$ in the singular value decomposition with decreasing singular values $\sqrt{p_j}c_j$, $\sqrt{p_j}s_j$. Let $|\psi_j\rangle = c_j |00\rangle_{AB} + s_j |11\rangle_{AB}$. Mapping to a different space (possibly adding one more dimension on each side if the original dimension was not even on both sides) $|\psi\rangle = \sum_j \sqrt{p_j} |\psi_j\rangle_{AB} |jj\rangle_{AB}$. Then the Gisin-Peres conjecture implies

$$S_{max}(|\psi\rangle) = \sum_j p_j S_{max}\left(|\psi_j\rangle_{AB}\right). \tag{5.55}$$

This may be seen as a result of the fact that the Gisin-Peres construction for the optimal measurement strategy is to project onto $|jj\rangle_{AB}$, obtaining the value j on both sides (with probability p_j), and implement the optimal measurement strategy for $|\psi_j\rangle$. Also, the fact that $S_{max}(c|00\rangle + s|11\rangle) = 2\sqrt{1 + 4c^2 s^2}$ completes the argument. This equation may be obtained using the techniques from the proof of Theorem 5.1. We set $S_j = S_{max}(|\psi_j\rangle)$.

Meanwhile, applying Lemma 5.4, we find that F_{MY} may also be written

$$F_{MY}(|\psi\rangle) = \sum_j p_j F_{MY}(|\psi_j\rangle), \tag{5.56}$$

and we set $F_j = F_{MY}(|\psi_j\rangle)$.

Now we are in a position to prove the bound. Using the bound for qubits we find

$$F_{MY} = \sum_j p_j F_{MY}(|\psi_j\rangle) = \sum_j p_j \frac{1 + \sqrt{\left(\frac{S_{max}(|\psi_j\rangle)}{2}\right)^2 - 1}}{2}. \tag{5.57}$$

We now know that the convex hull of the qubit bound provides our needed bound. We find the line connecting the extreme points, namely $S = 2, F_{MY} = 1/2$ for the state $|00\rangle$ and $S = 2\sqrt{2}, F_{MY} = 1$ for the state $|\phi_+\rangle$. By Lemma 5.3 this line is always below a convex combination of the qubit bound since the qubit bound is concave down. Hence

$$F_{MY}(|\psi\rangle) \geq \frac{S_{max}(|\psi\rangle) + 2\sqrt{2} - 4}{4\left(\sqrt{2} - 1\right)}. \tag{5.58}$$

Now consider the state

$$|\psi\rangle = \sqrt{p}\,|00\rangle_{AB}\,|00\rangle_{AB} + \sqrt{1-p}\,|\phi_+\rangle_{AB}\,|11\rangle_{AB} \tag{5.59}$$

for some p with $0 \leq p \leq 1$. The construction for the CHSH measurement operators given by Gisin and Peres give $S_{max}(|\psi\rangle)$ to be $2p + (1-p)2\sqrt{2}$. Meanwhile, $F_{MY} = p/2 + (1-p)$. Thus these states saturate the conjectured lower bound. $\qquad\square$

5.4.2 Bounds for F_{LOCC}

Our main motivation for introducing F_{LOCC} is that we are able to obtain a tight bound, which we are unable to obtain for F_{LO}. The bound obtained is the same is for F_{MY}, and the proof is very similar.

Lemma 5.7. *Let a bipartite state ρ be given, then*

$$F_{LOCC}(\rho) \geq \frac{S_{max}(\rho) + 2\sqrt{2} - 4}{4\left(\sqrt{2} - 1\right)} \tag{5.60}$$

Proof. We begin with optimal measurements A_a and B_b for $a, b = 0, 1$. Applying Lemma 4.1 twice, we obtain a 2×2 block diagonalization for both sides, which we may turn into a 4×4 block diagonalization on the state as a

whole. We project ρ onto the blocks, obtaining a direct sum of four dimensional bipartite states $p_{jk}\rho_{jk}$, which we interpret as pair of qubits. We choose p_{jk} so that $\text{Tr}(\rho_{jk}) = 1$. The indices j and k indicate the block on the A and B sides respectively. Note that ρ may have off-diagonal entries as well, so it may not be the case that $\sum_{jk} p_{jk}\rho_{jk} = \rho$, but because the measurements have the same block structure, S_{max} is unaffected by the projection.

We may interpret the measurement as first projecting onto block (j, k) with probability p_{jk} obtaining reduced state ρ_{jk}, followed by a two qubit measurement on ρ_{jk}. The measurement on the (j, k)th block must be optimal for ρ_{jk}, otherwise we could increase $S_{max}(\rho)$. This fact allows us to write

$$S_{max}(\rho) = \sum_{j,k} S_{max}(\rho_{jk}). \tag{5.61}$$

Meanwhile, to extract the approximate EPR pair using LOCC operations we first project onto block (j, k) obtaining the state ρ_{jk}. We transmit j and k classically, so that the block is identified on both sides, then apply a local change of bases exactly as in the qubit case, allowing us to extract an EPR pair with fidelity $F_{LO}(\rho_{jk})$. The combined fidelity is

$$F_{LOCC}(\rho) \geq \sum_{jk} F_{LO}(\rho_{jk}). \tag{5.62}$$

From here we follow the latter half of the proof of Lemma 5.6, which we reproduce here using the current notation. Using the bound for qubits we find

$$F_{LOCC} \geq \sum_{j,k} p_{jk} F_{LO}(\rho_{jk}) = \sum_{j,k} p_{jk} \frac{1 + \sqrt{\left(\frac{\max(S_{max}(\rho_{jk}),2)}{2}\right)^2 - 1}}{2}. \tag{5.63}$$

We now know that the convex hull of the qubit bound provides our needed bound. We find the line connecting the extreme points, namely $S = 2, F_{LO} = 1/2$ for the state $|00\rangle$ and $S = 2\sqrt{2}, F_{LO} = 1$ for the state $|\phi_+\rangle$. By Lemma 5.3 this line is always below a convex combination of the qubit bound since the qubit bound is concave down. Hence

$$F_{LOCC}(\rho) \geq \frac{S_{max}(\rho) + 2\sqrt{2} - 4}{4\left(\sqrt{2} - 1\right)}. \tag{5.64}$$

$\square$

At first it appears as though the bound is tight. Consider the states

$$\rho = p\,|00\rangle\langle00|_{AB} \otimes |00\rangle\langle00|_{AB} + (1-p)\,|\phi_+\rangle\langle\phi_+|_{AB} \otimes |11\rangle\langle11|_{AB} \qquad (5.65)$$

It appears that the optimal CHSH measurements would be to identify block (0,0) or (1,1) and apply the optimal CHSH measurement for either $|00\rangle$ in the case of block (0,0), or for $|\phi_+\rangle$ in the case of $(1,1)$. Similarly, the optimal LOCC operations seem to be to identify one of these blocks and map to a pair of qubits. However, we have no proof that either of these strategies is optimal. It may be the case that the CHSH measurements are optimal and the LOCC operations are not, in which case the bound would not be tight.

Conjecture 5.2. *The bound*

$$F_{LOCC}(\rho) \geq \frac{S_{max}(\rho) + 2\sqrt{2} - 4}{4\left(\sqrt{2} - 1\right)} \qquad (5.66)$$

is tight, saturated by the states

$$\rho = p\,|00\rangle\langle00|_{AB} \otimes |00\rangle\langle00|_{AB} + (1-p)\,|\phi_+\rangle\langle\phi_+|_{AB} \otimes |11\rangle\langle11|_{AB}. \qquad (5.67)$$

5.4.3 Bounds for F_{LO}

For local operations there is a significant problem in using the proof techniques developed above. In particular, the block diagonalization into 2 qubit states is indexed by two variables j and k, with j the result of a projection on the A side and k the result of a projection on the B side. Since the operations necessary to fix the local bases may depend on both j and k, classical communication is in general required to control the operations. When calculating F_{LO} this becomes important since classical communication is not allowed. Nonetheless, we are able to obtain a bound.

Lemma 5.8. *Let a bipartite state ρ be given. Then*

$$F_{LO}(\rho) \geq \frac{S_{max}(\rho) - 2}{2(\sqrt{2} - 1)}. \qquad (5.68)$$

The proof of this result is due to our coauthor on [BLM$^+$09], Serge Massar. We omit the proof, but instead provide this insight: the main idea is to use the measurements to define local bases for each two qubit block. Since

the measurements are completely local in nature, this allows for only local operations.

We conjecture that this bound is not tight. The reason is simply that the conjectured lower bound for F_{MY}, which must also be a lower bound on F_{LO} since $F_{MY} \leq F_{LO}$, is higher than the current bound on F_{LO}. Another fact of interest is that, if the conjectured bound on F_{MY} holds, and the bound on F_{LOCC} is tight, then all three measures would have the same tight lower bound since F_{MY} lower bounds them all and F_{LOCC} upper bounds them.

Chapter 6

Concluding Remarks

As we have demonstrated, the field of black box quantum computing is varied and fruitful. The general circuit testing construction of self-testing allows for wide application of the black box methodology, while a more tailored approach allows us to draw more specific conclusions for DIQKD and black box state characterization. Additionally, techniques developed here have application in other settings such as foundations and complexity.

There remain important challenges as well. For all the results presented in this thesis we need to make additional assumptions in order to collect statistics about the devices. Even for DIQKD, we must assume that the devices have no memory. Finding a mechanism for collecting statistics without assuming independent and identical trials is the most important open problem in this field.

Bibliography

[ABG+07]   Antonio Acin, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio, and Valerio Scarani. Device-independent security of quantum cryptography against collective attacks. *Physical Review Letters*, **98**(23):230501, 2007. DOI:10.1103/PhysRevLett.98.230501. EPRINT arXiv:quant-ph/0702152, URL `http://link.aps.org/abstract/PRL/v98/e230501`. 77, 80, 82, 85, 101

[ABOE08]   Dorit Aharonov, Michael Ben-Or, and Elad Eban. Interactive proofs for quantum computations, October 2008. EPRINT arXiv:0810.5375. 70

[Adl95]   Stephen Adler. *Quaternionic Quantum Mechanics and Quantum Fields*. Oxford University Press, New York, 1995. 29, 32, 33

[AGM06]   Antonio Acin, Nicolas Gisin, and Lluis Masanes. From bell's theorem to secure quantum key distribution. *Phys. Rev. Lett.*, **97**(12):120405, Sep 2006. DOI:10.1103/PhysRevLett.97.120405. EPRINT arXiv:quant-ph/0510094, URL `http://prl.aps.org/abstract/PRL/v97/i12/e120405`. 77

[Alb47]   A. A. Albert. Absolute valued real algebras. *The Annals of Mathematics*, **48**(2):495–501, 1947. URL `http://www.jstor.org/stable/1969182`. 30

[AMP06]   Antonio Acin, Serge Massar, and Stefano Pironio. Efficient quantum key distribution secure against no-signalling eavesdroppers. *New Journal of Physics*, **8**(8):126, 2006. DOI:10.1088/1367-2630/8/8/126. EPRINT arXiv:quant-ph/0605246, URL `http://stacks.iop.org/1367-2630/8/126`. 74, 75, 77, 80

[AvDK⁺04] Dorit Aharonov, Wim van Dam, Julia Kempe, Zeph Landau, Seth Lloyd, and Oded Regev. Adiabatic quantum computation is equivalent to standard quantum computation. *Foundations of Computer Science, Annual IEEE Symposium on*, **0**:42–51, 2004. DOI:http://doi.ieeecomputersociety.org/10.1109/FOCS.2004.8. EPRINT arXiv:quant-ph/0405098. 10

[BB84] C. H. Bennett and G. Brassard. Quantum cryptography: Public-key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India*, pp. 175–179, December 1984. 74

[BBBW84] C. H. Bennett, G. Brassard, S. Breidbart, and S Wiesner. Eavesdrop-detecting quantum communications channel. *IBM Technical Disclosure Bulletin*, **26**(8):4363 – 4366, January 1984. 27

[BBL⁺06] Gilles Brassard, Harry Buhrman, Noah Linden, Andre Allan Methot, Alain Tapp, and Falk Unger. Limit on non-locality in any world in which communication complexity is not trivial. *Physical Review Letters*, **96**(25):250401, 2006. DOI:10.1103/PhysRevLett.96.250401. EPRINT arXiv:quant-ph/0508042, URL http://link.aps.org/abstract/PRL/v96/e250401. 35, 36

[BC90] Samuel L. Braunstein and Carlton M. Caves. Wringing out better bell inequalities. *Annals of Physics*, **202**(1):22 – 56, 1990. DOI:10.1016/0003-4916(90)90339-P. URL http://www.sciencedirect.com/science/article/B6WB1-4DF4X9V-KC/2/eb7ed1a32d924d02e5f0ef125885386c. 76, 77

[BFK08] Anne Broadbent, Joseph Fitzsimons, and Elham Kashefi. Universal blind quantum computation, July 2008. EPRINT arXiv:0807.4154. 70

[BHK05] Jonathan Barrett, Lucien Hardy, and Adrian Kent. No signaling and quantum key distribution. *Phys. Rev. Lett.*, **95**(1):010503, Jun 2005. DOI:10.1103/PhysRevLett.95.010503.

EPRINT arXiv:quant-ph/0405101, URL `http://link.aps.org/doi/10.1103/PhysRevLett.95.010503`. 76

[BKP06] Jonathan Barrett, Adrian Kent, and Stefano Pironio. Maximally nonlocal and monogamous quantum correlations. *Phys. Rev. Lett.*, **97**(17):170409, Oct 2006. DOI:10.1103/PhysRevLett.97.170409. EPRINT arXiv:quant-ph/0605182, URL `http://prl.aps.org/abstract/PRL/v97/i17/e170409`. 76

[BLM+05] Jonathan Barrett, Noah Linden, Serge Massar, Stefano Pironio, Sandu Popescu, and David Roberts. Nonlocal correlations as an information-theoretic resource. *Phys. Rev. A*, **71**(2):022101, Feb 2005. DOI:10.1103/PhysRevA.71.022101. EPRINT arXiv:quant-ph/0404097, URL `http://pra.aps.org/abstract/PRA/v71/i2/e022101`. 76

[BLM+09] C.-E. Bardyn, T. C. H. Liew, S. Massar, M. McKague, and V. Scarani. Device-independent state estimation based on bell's inequalities. *Physical Review A (Atomic, Molecular, and Optical Physics)*, **80**(6):062327, 2009. DOI:10.1103/PhysRevA.80.062327. EPRINT arXiv:0907.2170, URL `http://link.aps.org/abstract/PRA/v80/e062327`. 108, 111, 124

[Bru98] Dagmar Bruß. Optimal eavesdropping in quantum cryptography with six states. *Phys. Rev. Lett.*, **81**(14):3018–3021, Oct 1998. DOI:10.1103/PhysRevLett.81.3018. 27

[Cho75] Man-Duen Choi. Completely positive linear maps on complex matrices. *Linear Algebra and its Applications*, **10**(3):285 – 290, 1975. DOI:DOI: 10.1016/0024-3795(75)90075-0. URL `http://www.sciencedirect.com/science/article/B6V0R-45GMWJF-W/2/19c43ca73684ddb298ecf1cf25f8b2c2`. 53

[CHSH69] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, **23**(15):880–884, Oct 1969.

DOI:10.1103/PhysRevLett.23.880. URL http://link.aps.org/doi/10.1103/PhysRevLett.23.880. 34, 77, 78

[Cir80]   B. S. Cirel'son.   Quantum generalizations of bell's inequality.   *Letters in Mathematical Physics*, **4**(2):93–100, 03 1980. DOI:10.1007/BF00417500.   URL http://www.springerlink.com/content/l57053g573430450/. 34, 37

[Ebe93]   Philippe H. Eberhard.   Background level and counter efficiencies required for a loophole-free einstein-podolsky-rosen experiment.   *Phys. Rev. A*, **47**(2):R747–R750, Feb 1993. DOI:10.1103/PhysRevA.47.R747. 103

[Eke91]   Artur K. Ekert.   Quantum cryptography based on bell's theorem.   *Phys. Rev. Lett.*, **67**(6):661–663, Aug 1991. DOI:10.1103/PhysRevLett.67.661. 74, 78

[Gis07]   Nicolas Gisin. Bell inequalities: many questions, a few answers, 2007. EPRINT arXiv:quant-ph/0702021v2. 30

[GP92]   N. Gisin and A. Peres. Maximal violation of bell's inequality for arbitrarily large spin. *Physics Letters A*, **162**(1):15–17, 1992. 120

[Ham44]   William Rowan Hamilton. On quaternions, or on a new system of imaginaries in algebra. *Philosophical Magazine*, **25**:10–13, 1844.   URL http://www.emis.ams.org/classics/Hamilton/OnQuat.pdf. 31

[HHH95]   R. Horodecki, P. Horodecki, and M. Horodecki.   Violating bell inequality by mixed states: necessary and sufficient condition.   *Physics Letters A*, **200**(5):340–344, 1995. URL   http://www.sciencedirect.com/science/article/B6TVM-3YCF1NN-14/1/7e99c8485537e8e8a9378cb2f39ad8a4. 79, 108

[Hoe63]   Wassily Hoeffding. Probability inequalities for sums of bounded random variables. *Journal of the American Statistical Association*, **58**(301):13–30, March 1963. URL http://www.jstor.org/stable/2282952. 92

[Jam72] A. Jamiolkowski. Linear transformations which preserve trace and positive semidefiniteness of operators. *Reports on Mathematical Physics*, **3**(4):275 – 278, 1972. DOI:10.1016/0034-4877(72)90011-0. URL `http://www.sciencedirect.com/science/article/B6VN0-45DJ285-S/2/7c06018aea4e1057a86ebf24bd8c40c8`. 53

[Jor75] Camille Jordan. Essai sur la géométrie à n dimensions. *Bulletin de la Société Mathématique de France*, **3**:103, 1875. URL `http://archive.numdam.org/article/BSMF_1875_3__103_2.pdf`. 87

[KRBM07] Robert König, Renato Renner, Andor Bariska, and Ueli Maurer. Small accessible quantum information does not imply security. *Phys. Rev. Lett.*, **98**(14):140502, Apr 2007. DOI:10.1103/PhysRevLett.98.140502. EPRINT arXiv:quant-ph/0512021. 78

[LD06] Yeong-Cherng Liang and Andrew C. Doherty. Better bell-inequality violation by collective measurements. *Physical Review A (Atomic, Molecular, and Optical Physics)*, **73**(5):052116, 2006. DOI:10.1103/PhysRevA.73.052116. URL `http://link.aps.org/abstract/PRA/v73/e052116`. 121

[LLK07] Antía Lamas-Linares and Christian Kurtsiefer. Breaking a quantum key distribution system through a timing side channel. *Opt. Express*, **15**(15):9388–9393, 2007. EPRINT arXiv:0704.3297, URL `http://www.opticsexpress.org/abstract.cfm?URI=oe-15-15-9388`. 104

[LPSW07] Noah Linden, Sandu Popescu, Anthony J. Short, and Andreas Winter. Quantum nonlocality and beyond: Limits from nonlocal computation. *Physical Review Letters*, **99**(18):180502, 2007. DOI:10.1103/PhysRevLett.99.180502. EPRINT arXiv:quant-ph/0610097, URL `http://link.aps.org/abstract/PRL/v99/e180502`. 36

[MAS06a] Vadim Makarov, Andrey Anisimov, and Johannes Skaar. Effects of detector efficiency mismatch on security of quan-

131

tum cryptosystems. *Phys. Rev. A*, **74**(2):022313, Aug 2006. DOI:10.1103/PhysRevA.74.022313. EPRINT arXiv:quant-ph/0511032. 103

[Mas06b]   Lluis Masanes. Asymptotic violation of bell inequalities and distillability. *Physical Review Letters*, **97**(5):050503, 2006. DOI:10.1103/PhysRevLett.97.050503. EPRINT arXiv:quant-ph/0512153, URL http://link.aps.org/abstract/PRL/v97/e050503. 87

[Mas08]   Lluis Masanes. Universally-composable privacy amplification from causality constraints, 2008. EPRINT arXiv:0807.2158v2. 76, 77

[McK09a]   Matthew McKague. Device independent quantum key distribution secure against coherent attacks with memoryless measurement devices. *New Journal of Physics*, **11**(10):103037 (11pp), October 2009. DOI:10.1088/1367-2630/11/10/103037. EPRINT arXiv:0908.0503, URL http://stacks.iop.org/1367-2630/11/103037. 74

[McK09b]   Matthew McKague. Quaternionic quantum mechanics allows non-local boxes, November 2009. EPRINT arXiv:0911.1761. 10

[MM07]   Matthew McKague and Michele Mosca. Simulating quantum circuits using real valued unitaries. *Asian Conference on Quantum Information Science (AQIS'07), Kyoto, Japan*, September 2007. 10

[MMG09]   Matthew McKague, Michele Mosca, and Nicolas Gisin. Simulating quantum systems using real hilbert spaces. *Physical Review Letters*, **102**(2):020505, 2009. DOI:10.1103/PhysRevLett.102.020505. EPRINT arXiv:0810.1923, URL http://link.aps.org/abstract/PRL/v102/e020505. 10, 27

[MMMO06]   Frédéric Magniez, Dominic Mayers, Michele Mosca, and Harold Ollivier. Self-testing of quantum circuits. In M et al. Bugliesi,

editor, *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming*, number 4052 in Lecture Notes in Computer Science, pp. 72–83, 2006. EPRINT arXiv:quant-ph/0512111v1 . 39, 40, 43, 54, 58, 64, 69, 115

[MMar]   Matthew McKague and Michele Mosca. Generalized self-testing and the security of the 6-state protocol. *5th Conference on the Theory of Quantum Computation, Communication and Cryptography*, 2010 (To appear). 10, 44

[MRW+06] Ll Masanes, R. Renner, A. Winter, J. Barrett, and M. Christandl. Security of key distribution from causality constraints, 2006. EPRINT arXiv:quant-ph/0606049v3. 77

[MY98]   Dominic Mayers and Andrew Yao. Quantum cryptography with imperfect apparatus. In *FOCS*, pp. 503–509, September 1998. EPRINT arXiv:quant-ph/9809039. 39

[MY04]   Dominic Mayers and Andrew Yao. Self testing quantum apparatus. *QIC*, **4**(4):273–286, July 2004. EPRINT arXiv:quant-ph/0307205. 39, 40, 43, 44, 108, 115

[Nai40]   Mark Naimark. Spectral functions of a symmetric operator. *Izv. Akad. Nauk SSSS, Ser. Mat.*, **4**:277–318, 1940. 3

[NC00]   Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, October 2000. 10

[PAB+09] Stefano Pironio, Antonio Acin, Nicolas Brunner, Nicolas Gisin, Serge Massar, and Valerio Scarani. Device-independent quantum key distribution secure against collective attacks. *New Journal of Physics*, **11**(4):045021 (25pp), 2009. DOI:10.1088/1367-2630/11/4/045021. EPRINT arXiv:0903.4460, URL http://stacks.iop.org/1367-2630/11/045021. 77, 80, 82, 83, 85, 86, 87, 94, 95, 96, 97, 103

[PPK+09] M. Pawlowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter, and M. Zukowski. A new physical principle: Information causality. *Nature*, **461**:1101–1104, May

2009. DOI:10.1038/nature08400. EPRINT arXiv:0905.2292, URL http://www.nature.com/nature/journal/v461/n7267/suppinfo/nature08400_S1.html. 36

[PR94]   Sandu Popescu and Daniel Rohrlich. Quantum nonlocality as an axiom. *Foundations of Physics*, **24**(3):379–385, 03 1994. URL http://dx.doi.org/10.1007/BF02058098. 33

[PV08]   Karoly F. Pál and Tamas Vértesi. Efficiency of higher-dimensional hilbert spaces for the violation of bell inequalities. *Physical Review A (Atomic, Molecular, and Optical Physics)*, **77**(4):042105, 2008. DOI:10.1103/PhysRevA.77.042105. EPRINT arXiv:0712.4320v2 [quant-ph]. 11, 30

[RB01]   Robert Raussendorf and Hans J. Briegel. A one-way quantum computer. *Phys. Rev. Lett.*, **86**(22):5188–5191, May 2001. DOI:10.1103/PhysRevLett.86.5188. EPRINT arXiv:quant-ph/0010033, URL http://prl.aps.org/abstract/PRL/v86/i22/p5188_1. 70

[Ren05]   Renato Renner. *Security of Quantum Key Distribution*. PhD thesis, Swiss Federal Institute of Technology, 2005. EPRINT arXiv:quant-ph/0512258v2. 78, 85, 91, 92, 93, 100, 101

[Ren07]   Renato Renner. Symmetry of large physical systems implies independence of subsystems. *Nature Physics*, **3**:645 – 649, July 2007. DOI:10.1038/nphys684. EPRINT arXiv:quant-ph/0703069, URL http://www.nature.com/nphys/journal/v3/n9/suppinfo/nphys684_S1.html. 78, 90, 100

[RG02]   Terry Rudolph and Lov Grover. A 2 rebit gate universal for quantum computing, 2002. EPRINT arXiv:quant-ph/0210187v1. 10

[Stu60]   E. C. G. Stueckelberg. Quantum theory in real hilbert space. *Helvetica Physica Acta*, **33**:727, 1960. 10

[vD05]   Wim van Dam. Implausible consequences of superstrong nonlocality, January 2005. EPRINT arXiv:quant-ph/0501159. 35

134

[vMMS00] Wim van Dam, Frederic Magniez, Michele Mosca, and Miklos Santha. Self-testing of universal and fault-tolerant sets of quantum gates. In *STOC '00: Proceedings of the thirty-second annual ACM symposium on Theory of computing*, pp. 688–696, New York, NY, USA, 2000. ACM. DOI:doi:10.1145/335305.335402. EPRINT arXiv:quant-ph/9904108 . 40

[VW02] Frank Verstraete and Michael M. Wolf. Entanglement versus bell violations and their behavior under local filtering operations. *Phys. Rev. Lett.*, **89**(17):170401, Oct 2002. DOI:10.1103/PhysRevLett.89.170401. 79, 108

[Wat08a] John Watrous. Characterizations of admissible operations, 2008. URL http://www.cs.uwaterloo.ca/~watrous/quant-info/lecture-notes/05.pdf. 54

[Wat08b] John Watrous. Operator decompositions and norms; operator-vector correspondence, 2008. URL http://www.cs.uwaterloo.ca/~watrous/quant-info/lecture-notes/02.pdf. 109

[Wat08c] John Watrous. Overview of quantum information; purifications and fidelity, 2008. URL http://www.cs.uwaterloo.ca/~watrous/quant-info/lecture-notes/03.pdf. 109

[ZFQ+08] Yi Zhao, Chi-Hang Fred Fung, Bing Qi, Christine Chen, and Hoi-Kwong Lo. Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems. *Phys. Rev. A*, **78**(4):042333, Oct 2008. DOI:10.1103/PhysRevA.78.042333. EPRINT arXiv:0704.3253. 104