Free Will in Device-Independent Cryptography

James Pope

St Catherine's College

University of Oxford

A thesis submitted for the degree of

Doctor of Philosophy

Trinity 2013

To my parents, for their unwavering love and support all of these years...

Acknowledgements

This thesis would not have been possible without contributions from many people, whether through direct collaboration or simply moral support.

I would like to thank my supervisor Artur Ekert, both for offering this opportunity to me in the first place, and for his support ever since. Whilst acclimatising to the field of quantum information theory and occasionally focussing on the small details, I could rely on Artur for reminders of the bigger picture, and fascinating insights, whether scientific or anecdotal, that helped give me direction for the rest of my doctoral candidature. I am also extremely grateful for the benefits that his position at the Centre for Quantum Technologies, Singapore, offered me, including several visits there that proved invaluable in furthering my study, as well as helpful financial contributions to enable attendance at summer schools and conferences in Canada, Switzerland and Singapore.

I would also like to thank Alastair Kay for his crucial input and valuable collaboration, giving me week-to-week (and sometimes hour-to-hour) guidance that helped to focus my research in the right direction. His insights, from quantum theory to programming to finding Western cuisine in Singapore, have always been extremely helpful and this DPhil could not have been completed without him.

There are many other people to thank for their invaluable input. These include Chiara Marletto, Michael Hall, Valerio Scarani, Dax Koh and Setiawan for collaboration on our randomness expansion paper, as well as Jonathan Oppenheim, Noah Linden, Robert Spekkens and Roger Colbeck for helpful insights, whether in person or through noteworthy lectures/talks. I would particularly like to thank Vlatko Vedral and his entire research group in the Clarendon Laboratory at Oxford, for providing several years of office space in a warm and highly supportive environment. I would also like to thank Roger and Vlatko for taking the time to examine this thesis.

The work reported in this thesis would not have been possible without the financial support of an EPSRC postgraduate studentship, for which I am very grateful.

On a personal front, there are so many people to thank it would (oddly enough) become a thankless task to list them all here. I am of course ever grateful to my loving family, who have supported me throughout not just the DPhil, but my entire

life. To my parents, my brothers Andrew and John, my Gran and particularly my aunt Lydia for her recollections of a different-yet-similar doctoral experience, I thank you all. I am also grateful to all of my friends for so many treasured memories and joyful times over the years, be they in Oxford, Liverpool, London or further afield. Special thanks go out to those I've shared housing with during my DPhil, Dan (3 years), Andy (2), Jorge (2), Luke (2) and Phil (1). Their valued friendship, easygoing personalities and shared academic experiences proved to be an enjoyable complement at home to time spent in the various departments, libraries and colleges of Oxford.

Finally, I am indebted to my girlfriend Lizzy for her constant love and support. Our relationship began at around the same time as the doctorate, but the length of the former will surely outlast the latter by a large margin. She has given me such joy and comfort, and I absolutely could not have completed this doctorate without her as my best friend and confidante. Thank you!

Statement of Originality

I hereby declare that, except where acknowledged here and at other appropriate places in the thesis, the work presented in this thesis is original and my own work, and has not been submitted in whole or part for a degree in any university.

The content of Chapter 3 is based largely on [1], which resulted from a joint research project between all named authors. Theorem 3 and Corollary 5 were proved primarily by Michael J. W. Hall (who did many of the initial calculations), Dax Enshan Koh and Setiawan. The remainder of the chapter is based on research conducted by Alastair Kay, Chiara Marletto, Artur Ekert and myself. The initial draft of [1] was written by Dax Enshan Koh and myself.

The content of Chapter 4 is based largely on research conducted by myself and Alastair Kay. I have done all the research in this chapter guided by initial ideas from Alastair Kay and weekly discussion about the project.

The content of Chapter 5 is based largely on [2], which resulted from a joint research project between myself and Alastair Kay. I have done all the research in this chapter guided by initial ideas from Alastair Kay and weekly discussion about the project. I wrote the initial draft of [2].

Abstract

Device-independent cryptography provides security in various tasks whilst removing an assumption that cryptographers previously thought of as crucial – complete trust in the machinations of their experimental apparatus. The theory of Bell inequalities as a proof of indeterminism within nature allows for secure device-independent schemes requiring neither trust in the cryptographers' devices nor reliance on the completeness of quantum mechanics. However, the extreme paranoia attributable to the relaxed assumptions within device independence requires an explicit consideration of the previously assumed ability of the experimenters to freely make random choices. This thesis addresses the so-called 'free will loophole', presenting Bell tests and associated cryptographic protocols robust against adversarial manipulation of the random number generators with which measurements in a Bell test are selected.

We present several quantitative measures for this experimental free will, otherwise known as measurement dependence. We discuss how an eavesdropper maliciously preprogramming the experimenters' untrusted devices can falsely simulate the violation of a Bell inequality. We also bound the amount of Bell violation achievable within a certain degree of measurement dependence. This analysis extends to device-independent randomness expansion, bounding the guessing probability and estimating the amount of privacy amplification required to distil private randomness. The protocol is secure against either arbitrary no-signalling or quantum adversaries. We also consider device-independent key distribution, studying adversarial models that exploit the free will loophole.

Finally, we examine a model correlated between the random number generators and Bell devices across multiple runs of a Bell test. This enables an explicit exposition of the optimal cheating strategy and how the correlations manifest themselves within this strategy. We prove that there remain Bell violations for a sufficiently high, yet non-maximal degree of

measurement dependence which cannot be simulated by a classical attack, regardless of how many runs of the experiment those choices are correlated over.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Preface

Ever since humans learned to communicate, they have wished to be able to do so privately. The quest for secrecy between our perennial heroes Alice and Bob, away from the prying eyes of nefarious Eve, has been a back-and-forth struggle for millennia, a cryptographic arms race with increasingly sophisticated protocols for encryption on one side and equally cunning eavesdropping attacks on the other. Alice uses a substitution cipher to write private correspondence and Eve uses frequency analysis to infer what substitutions took place. Bob attempts to outwit her with an Enigma rotor machine and Eve counters with a bombe.

The advent of modern computing continued this spirit of one-upmanship with new mathematically-charged encryption schemes, now used throughout commerce and industry. The desire for secure cryptography within the infrastructure of today's "online, everywhere" world is clear, and theoretically achievable with schemes that would require an adversary with massive (and currently unrealisable) computational power to falter. Of course, these protocols are only as good as their implementation, and it is common to hear of even moderately-skilled hackers exploiting faults with programming code to access supposedly secure databases. Regardless, these encryption methods can only guarantee security with assumptions of an Eve with limited resources and not in the absolute.

More recent decades have seen the rising acceptance of quantum theory as a description of the universe, leading to new cryptographic protocols with some rather grand statements which would seemingly give Alice and Bob their ultimate victory. These new schemes (included within the umbrella term of *quantum cryptography* amongst other tasks) are fundamentally different from what came before, as their security relies on physical properties in Nature, rather than mathematical obfuscation.

In short, if the assumed quantum theory is correct, the encryption is unbreakable. Privacy is guaranteed by the outcome correlations obtained from measurements on spatially-separated states in what is known as a *Bell test*.

Bell tests were first conceived to provide an experimental falsification of the local causality of Nature, thus giving credence to the validity of quantum theory. These tests can not only be adapted to prove the absence of an eavesdropper in a cryptographic scenario, but the security guarantees are more powerful than had ever been imaginable before; in the burgeoning field of *device-independent cryptography*, secure cryptographic schemes exist that need not be reliant on either the quantum theory that inspired them or complete knowledge of the devices used to implement them. Despite this remarkable advancement, Alice and Bob cannot yet claim complete security. This is because of the presence of loopholes in a Bell test that Eve can potentially exploit, including the one of primary interest in this thesis, known as the *free-will loophole*.

One of the major assumptions in the implementation of a Bell test is that the experimenters have complete free will in selecting which measurements to perform on each run of the experiment. In practice, Alice and Bob will use random number generators (RNGs) for efficient selection and can check afterwards that their measurement choices conformed to an expected distribution, typically uniform in a standard Bell test but perhaps skewed for performing a cryptographic task. However, in a device-independent situation where Eve has supplied the RNGs, she can preprogram the devices to operate according to subroutines which collectively give the impression of complete free will whilst simulating correlations which pass a Bell test and therefore give Alice and Bob false assurances of security.

The free will loophole has been given similarly rigorous treatment only in recent years. One reason for this is the heightened paranoia associated with device-independent scenarios. Whereas with trusted-device cryptography the cryptographers' RNGs were often assumed to be secure (perhaps naively), such assumptions are harder to take for granted when accounting for device-independence. This thesis examines the free-will loophole in several different contexts, showing both how Eve can exploit the loophole to her advantage and how Alice and Bob may bound their uncertainty for a given quantitative measure of free will (or more appropriately *measurement dependence*), thus safeguarding their protocols against Eve's strategies.

The cryptographic arms race is ongoing, but has now taken an exciting new leap forwards with the shift away from classical mathematical complexity and towards fundamental physical principles to make security guarantees.

1.2 Synopsis

Introduction. The remainder of this chapter lays the groundwork for discussion of the free-will loophole. We describe Bell inequalities and their violation as a proof of nonlocality, with particular emphasis given to the simplest such Bell test known as the CHSH test. We then introduce the cryptographic tasks which will be explored in the context of reduced free will in later chapters, and explain how these tasks can be implemented in a device-independent manner, achieving security even with untrusted devices. This is followed by a discussion of loopholes in Bell tests, which are particularly of concern in the more paranoid setting of device-independent cryptography, with brief discussion of the experimental progress made towards closing these loopholes.

Quantifying Measurement Dependence. Chapter 2 describes the free will loophole and introduces several quantitative measures of free will (or measurement dependence) to be used throughout the rest of the thesis, most notably M_H, M_K and P, with a discussion of each measure's advantages and disadvantages. To illuminate the discussion, a simple example of exploiting the free will loophole is provided, that of a single run of the CHSH test.

Randomness Expansion With Limited Measurement Dependence. In a randomness expansion protocol, a pre-established stock of perfect randomness is used to select the measurements in a Bell test. The quality of the outcome correlations is then used to quantitatively bound the degree to which Eve is excluded. This bound estimates the randomness of the outcomes, which can be added to the initial random seed. Chapter 3 presents a randomness expansion protocol limited to a fixed amount of measurement dependence, assuming only single-shot attacks, i.e. independent and identically distributed for each run of the experiment. If Alice and Bob know the degree to which their RNGs have been manipulated, they can still bound Eve's knowledge of the outcomes to perform appropriate privacy amplification techniques. In short, this chapter makes a randomness expansion protocol robust against the free-will loophole, for an adversary with either no-signalling or quantum capabilities.

Key Distribution With Limited Measurement Dependence. It has been long known that all that is needed for perfect encryption of a binary string is a private and completely random binary string of the same length (or *key*), and efficient key distribution between two parties was the first notable commercial application to arise

from quantum theory. Not only are QKD schemes already seeing practical implementation in industry, but they have also been extended to the device-independent scenario. Chapter 4 investigates the free-will loophole for device-independent key distribution.

Limited Measurement Dependence in Multiple Runs of a Bell Test. The previous chapters assumed Eve could only perform an attack independently on each run of the experiment, otherwise known as a *single-shot strategy*. However, Eve may also correlate a variable-free-will strategy over many runs of the experiment. Chapter 5 analyses these optimal correlated strategies, both over a finite number of runs and in the infinite limit, showing that Eve gains a significant advantage as compared to a single-shot strategy. Methods are introduced to deal with all three of our free-will measures for the CHSH inequality, as well as a generalisation to some other Bell inequalities. The main result is that for a small (yet imperfect) degree of measurement dependence, there are Bell violations which Eve cannot simulate with a classical correlated attack.

1.3 Preliminaries

Here we briefly present some basic concepts within quantum information theory. This information can be found within a wealth of textbooks, including Nielsen and Chuang's quantum information 'bible' [3]. The more informed reader is invited to skip this section entirely.

We assume familiarity with the Dirac notation that describes quantum states as rays of a Hilbert space. Within this framework, the linear-algebraic operations of taking inner products of states, adjoints of vectors and matrices, and tensor products of vector spaces are presumed to be understood. Knowledge of the qubit, as the smallest-dimensional quantum system to be investigated, as well as its Bloch sphere representation, is also assumed.

A mixed state is an ensemble of pure quantum states, which can be written in the density operator notation as $\rho = \sum_i p_i \left| \psi_i \right\rangle \left\langle \psi_i \right|$, where (p_i) is a probability distribution and the $\left| \psi_i \right\rangle$ are pure states. The density matrix associated with the operator ρ is Hermitian and positive semidefinite with unit trace. ρ describes a pure state if and only if $\mathrm{Tr}\,(\rho^2) = 1$.

A system can evolve according to unitary operations or measurements. An operation U is unitary if $UU^\dagger = U^\dagger U = \mathbb{1}$ and preserves inner products. Applying a unitary operation to the state ρ will transform the state into $U\rho U^\dagger$. A measurement

in a closed system can be described by a set of operators $\{M_k\}$, where $\sum_k M_k^\dagger M_k = \mathbb{1}$. The probability of measuring the kth outcome is given by $p(k) = \mathrm{Tr}\,(M_k^\dagger M_k \rho)$, and the state collapses to $\rho_k = \frac{M_k \rho M_k^\dagger}{\mathrm{Tr}\,(M_k^\dagger M_k \rho)}$.

The Pauli operators are well-known self-adjoint operators with ± 1 eigenvalues. Their density matrices (using the computational basis) are given by

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{1.1}$$

We assume the reader is familiar with some of the most recognisable concepts in quantum theory, such as state collapse following a measurement visualised by the Schrodinger's cat thought experiment [4][1], the inherent imprecision in measuring complementary properties described by Heisenberg's uncertainty principle [6], and particularly the 'spooky action at a distance' exhibited by quantum entanglement [7]. Mathematically, a bipartite state ρ in the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$ is entangled if it cannot be written in the separable form

$$\rho = \sum_\lambda p_\lambda \rho_A^\lambda \otimes \rho_B^\lambda, \tag{1.2}$$

i.e. a mixture of product states where $\rho_A^\lambda \in \mathcal{H}_A, \rho_B^\lambda \in \mathcal{H}_B$ and $p_\lambda \in [0,1]$ with $\sum_\lambda p_\lambda = 1$.

We also assume some familiarity with classical information theory [8, 9], especially the notions of Shannon entropy and von Neumann entropy.

1.4 Nonlocality and Bell Inequalities

Quantum information theory as we know it today is an increasingly popular and influential area of research, yet the field has only taken shape over the last few decades. There are two major reasons for the surge of interest. Firstly, acceptance of quantum theory as a valid description of the universe has led to several commercially significant applications that show great potential, much of which has already been fulfilled, which simply cannot be recreated with the classical theory. Quantum key distribution protocols [10, 11] were developed for which security guarantees could be made unconditional by fundamental natural processes, without the provisos on the computational power of adversaries that classical cryptography had previously relied upon. On the other hand, said adversarial power was being strengthened with quantum algorithms, for instance factoring large numbers in polynomial time [12].

[1] translated into English in [5]

However, just as significantly, the growth of quantum information theory is due to the emerging cultural acceptance of the quantum theory behind it, many decades after its conception. Indeed, Albert Einstein was one of quantum mechanics' most prolific detractors and in 1935 he co–authored a paper with Podolsky and Rosen [7] attacking the theory. They argued – with excellent justification – that quantum mechanics cannot be a complete theory (i.e. accurate physical description of the universe) because the theory permits indeterministic events that have no underlying precedent. It wasn't until 1964 that an impressive counter was given by John S. Bell [13] which turned the original EPR paper on its head. Bell agreed with Einstein *et al*'s arguments but countered that it was our assumptions of Nature, not the quantum theory, that were mistaken, and provided an experimentally viable test to settle the matter.

A *Bell inequality* is an inequality derived from the assumptions of local-hidden-variable theory, specifically that all observed events can be explained by a general local hidden-variable model, yet may not be satisfied by quantum mechanical predictions[2]. Furthermore, these inequalities can be experimentally tested, allowing for the refutation of the universe's compatibility with local-hidden-variable theory, apropos of experimental loopholes to be discussed.

This section provides a mathematical formalism to the concepts of nonlocality and Bell inequalities, a review of which is available in [15]. To motivate the discussion, we first present the CHSH inequality, perhaps the simplest and certainly the most well-studied form of a Bell inequality named after its authors Clauser, Horne, Shimony and Holt [16], in an approachable manner that highlights the device-independent implications of the experiment (a similar presentation can be found in [17]). This leads to a rigorous framework for investigating nonlocality and its relation to quantum phenomena such as entanglement, as well as examples of other Bell inequalities which have proved to be useful within the field[3].

1.4.1 The CHSH Inequality

1.4.1.1 CHSH As Experiment

Suppose two experimenters, Alice and Bob, each hold a device with two buttons, labelled 0 and 1 (and subsequently labelled for an outside observer as A_0 and A_1

[2]As simple mathematical statements about probability distributions, these inequalities actually pre-date John Bell's work by a large margin (see [14]), but are now attributed to Bell by the scientific community for his contribution concerning their physical implications.

[3]A more comprehensive categorisation of Bell inequalities can be found in, for instance, [18].

for Alice and B_0 and B_1 for Bob)[4]. Pressing a button on Alice's device will deliver one of two outcomes on the same device, which are labelled as values of $+1$ and -1, similarly for Bob. In a single run of the experiment, Alice and Bob each *randomly* and *independently*[5] select their input choices $j, k \in \{0, 1\}$, press the corresponding buttons and observe their device's output, recorded as a and b respectively.

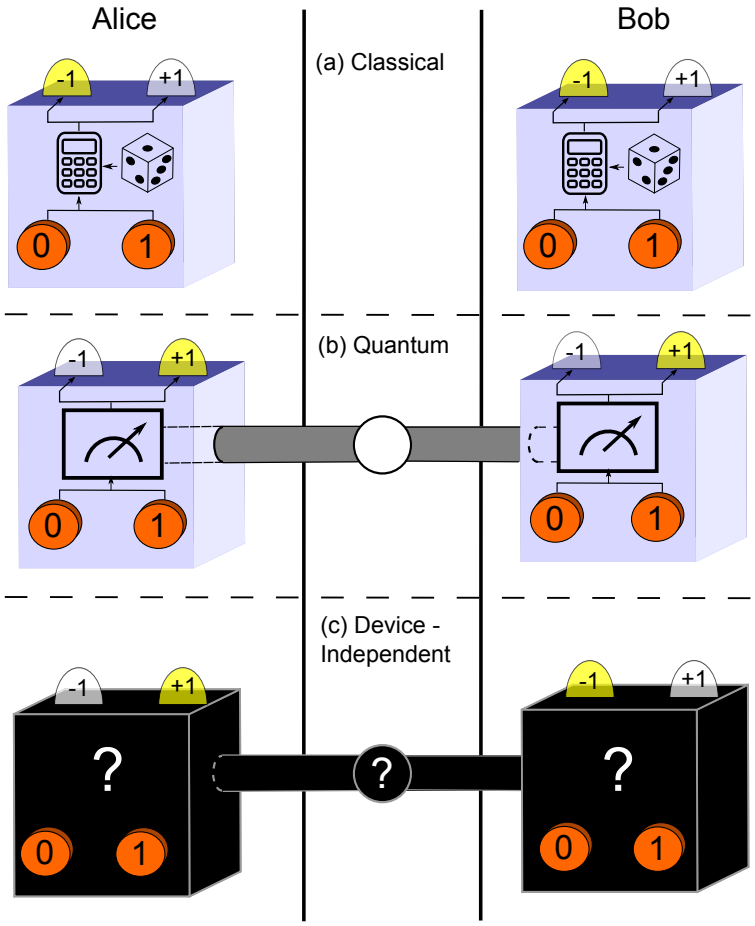

Figure 1.1: A single run of the CHSH experiment, performed by Alice and Bob in separate labs to prevent classical communication, using either (a) local classical computation with local or pre-shared randomness (b) quantum measurement apparatus sharing a source of entangled states, or (c) untrusted black-box devices.

These devices are spatially separated and the inputs are selected and outcomes

[4]As is often the case when concepts are of interdisciplinary interest, there are many discrepancies in notation to be found in the literature. Computer scientists famously tend to count from zero, and for overall cohesion this thesis will take the same approach for measurement labellings unless otherwise stated.

[5]These two seemingly innocuous words are of course worthy of further characterisation, with the bulk of this thesis dedicated to experimenters' free will in selecting inputs, but for this section we shall take them at face value.

recorded sufficiently quickly to forbid any possible subluminal communication between the devices on a given run of the experiment. After a large number of runs, Alice and Bob reveal their input/output data to each other and use this to estimate the probability distribution $p(ab|jk)$ of receiving the outputs $a, b \in \{-1, +1\}$ conditioned upon pressing the buttons j and k. We will also use the notation a_j to denote an output resulting from an input choice j, and similarly for b_k. Here, the conditioning on the input choices is apparent enough with the probability distribution $p(ab|jk)$ being considered. This distribution is used to calculate the expectation $\langle S \rangle$ of the CHSH value S defined as

$$S = a_0 b_0 + a_0 b_1 + a_1 b_0 - a_1 b_1, \tag{1.3}$$

where the correlation expectations

$$\langle a_j b_k \rangle = \sum_{a,b \in \{-1,+1\}} ab \cdot p(ab|jk) \tag{1.4}$$

must clearly lie in the range $[-1, +1]$. $\langle S \rangle$ therefore has some numerical bound. Crucially, the above description of the experiment, with reference simply to 'buttons' and 'outcomes', does not indicate the machinations of the device that leads to a particular outcome given the press of a particular button, suggesting that such knowledge is not essential to perform the experiment. This is the basis for device-independent implementations detailed later on, see also Figure 1.1(c). Of course, the original authors had certain theories and physical devices in mind which interestingly lead to different numerical bounds on $\langle S \rangle$ as follows.

In *classical theory*, the universe is deterministic and fully predictable. A discussion of what exactly this means follows in the next section, but it suffices to view the experiment's outcomes as having been determined either by some computation or measurement of a physical system contained entirely within each device, or through some pre-existing strategy agreed by Alice and Bob before the experiment (and perhaps using some pre-existing shared randomness), which fixes the outcomes. The outcomes can be treated as classical random variables $a_j, b_k \in \{\pm 1\}$. The CHSH value is determined by a new classical random variable defined by $S = a_0(b_0 + b_1) + a_1(b_0 - b_1)$, it is clear that $S = 2a_0$ if $b_0 = b_1$, $S = 2a_1$ if $b_0 = 1, b_1 = -1$ and $S = -2a_1$ if $b_0 = -1, b_1 = 1$. Therefore, averaged over a large number of runs, we see that $|\langle S \rangle| \leqslant 2$. A single run of the experiment is depicted in Figure 1.1(a).

Quantum theory predicts stronger correlations than classical theory. Assume that on a single run, the devices each receive a qubit from a bipartite state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$,

and then perform a projective measurement ($A_j \in \mathcal{H}_A$ for Alice, $B_k \in \mathcal{H}_B$ for Bob) in a basis determined by the chosen input, yielding a dichotomic outcome mapped to ± 1. This is depicted in Figure 1.1(b). The CHSH value above is then the expectation $\langle \mathcal{S} \rangle_{|\,\psi\rangle} = \langle \psi \,|\, \mathcal{S} \,|\, \psi \rangle$ of the operator

$$\mathcal{S} = A_0 \otimes B_0 + A_0 \otimes B_1 + A_1 \otimes B_0 - A_1 \otimes B_1. \tag{1.5}$$

The tensor product notation will be suppressed throughout this thesis when it is clear that local measurements are being performed on disjoint subsystems. Quantum theory predicts that the repeated measurements of the maximally entangled state $|\,\Psi\rangle = \frac{1}{\sqrt{2}}(|\,00\rangle + |\,11\rangle)$ with the following basis choices

$$A_0 = \frac{1}{\sqrt{2}}(X + Z), \qquad A_1 = \frac{1}{\sqrt{2}}(X - Z), \qquad B_0 = X, \qquad B_1 = Z \tag{1.6}$$

achieves an expectation of $\langle \mathcal{S} \rangle_{|\,\Psi\rangle} = 2\sqrt{2}$. The scheme is not unique, since applying an arbitrary unitary transformation to the state and measurements will achieve the same result. However, it has been shown [19] that the value $2\sqrt{2}$ is maximal[6].

Finally, a *no-signalling theory* yields even stronger correlations than quantum or classical theory by placing a single significant physical restriction on the experiment; Superluminal signalling is forbidden, in the sense that a measurement on Alice's side will not affect the outcome of a measurement on Bob's side, provided the two events are sufficiently spacelike separated. In the no-signalling theory, it is possible to have completely unpredictable outcomes which are nonetheless fully correlated, achieving greater violations possible than those predicted by quantum theory. A maximal violation of $\langle S \rangle = 4$ is achievable by, for instance, a *P-R box* [20], where the *correlations* are always $a_0 b_0 = a_0 b_1 = a_1 b_0 = 1$ and $a_1 b_1 = -1$.

The CHSH inequality provides an experimentally viable method of admonishing any previously upheld belief that the universe behaves classically. A violation of the CHSH inequality (i.e. any value of $\langle S \rangle$ above 2) was, by 1982, observed in a number of experiments [21, 22, 23, 24] that garnered significant interest for their acceptance of a quantum universe, particularly [24] which first implemented an experiment free of the locality loophole discussed in Section 1.7.1. The predictions of quantum theory were observed by realising the qubits as photons with polarisations measured in a specific plane, although the experiment has further been conducted with other physical systems (see Section 1.7). The correlations discovered notably support the quantum theory without showing evidence of a more general no-signalling theory, and significant steps have been made to prove quantum theory's completeness [25].

[6] A simplified version of the proof can be seen in the extension discussed in Section 3.3.

1.4.1.2 CHSH As Game

The CHSH experiment described above relays useful information about what types of correlations are physically possible. The capabilities of Alice and Bob, as well as the capabilities of a potential adversary, are incredibly important for cryptographic purposes, and it is worth rephrasing the experiment in the context of a game to emphasise what Alice and Bob hope to achieve when performing a Bell test.

In a single round of a CHSH game, a referee chooses a pair $(j,k) \in \{0,1\}^2$ of questions at random for each round of the game. The referee delivers j to Alice and k to Bob, who are unaware of each other's query. Alice and Bob each send back answers $a, b \in \{-1,1\}$ to the referee, and are considered to have won if $ab = (-1)^{jk}$, which corresponds to Alice and Bob delivering correlated bits for $(j,k) \neq (1,1)$ and anticorrelated bits when $(j,k) = (1,1)$ is queried[7]. The game is repeated for arbitrarily many rounds and Alice and Bob want to win as many rounds as they can. Their winning probability is defined to be:

$$p_{\text{win}} = \frac{1}{4} \sum_{(j,k)\in\{0,1\}^2} P(ab = (-1)^{jk}|jk). \tag{1.7}$$

The correlations that win the game for every round are precisely those that maximally violate the CHSH inequality to the no-signalling limit. This game is equivalent to a test of the CHSH inequality where a and b are the outcomes of Alice and Bob performing measurements A_j and B_k respectively, as long as the referee is delivering the query pairs (j,k) with uniform probability, representing the free will that Alice and Bob have in selecting their inputs in a CHSH test. Since the expectation of the outcome correlations for each measurement pair is either $+1$ or -1, we have that $\langle S \rangle = 4(p_{\text{win}} \cdot (+1) + (1 - p_{\text{win}}) \cdot (-1))$, hence

$$p_{\text{win}} = \frac{1}{2}\left(1 + \frac{\langle S \rangle}{4}\right). \tag{1.8}$$

The winning probabilities for players with classical, quantum and no-signalling capabilities are $\frac{3}{4}, \left(\frac{1}{2} + \frac{1}{\sqrt{2}}\right)$ and 1 respectively.

1.4.2 Physical Theories

Having given a motivating example of a Bell inequality, it is prudent to introduce more mathematical precision. We will consider the correlations produced in a more

[7]The corresponding winning condition when using the other popular labelling $(a,b) \in \{0,1\}^2$ is $a \oplus b = j \cdot k$, but these predicates are equivalent.

general scenario. We focus on bipartite correlations, i.e. only two experimenters involved in the test, though general multipartite nonlocality may also be considered. We consider Alice and Bob each holding a device with m inputs and d outputs[8]. Each round consists of the experimenters choosing measurements $j, k \in \{0, \ldots, m-1\}$ and recording outcomes $a, b \in \{0, \ldots, d-1\}$. Statistics collected from repeated runs of the experiment are used to estimate the m^2d^2 joint probabilities $p(ab|jk)$ of obtaining outcomes a, b upon inputs j, k. One can see that the CHSH experiment uses such a probability distribution with $d = m = 2$ and relabelling the outcomes to ± 1 values.

A *classical* theory supposes that any correlations can be explained precisely by a set of variables $\lambda \in \Lambda$ with probability distribution $\rho(\lambda)$, existing prior to the experiment. Knowledge of λ allows a specification of the probability distribution $p(a, b|j, k, \lambda)$ of obtaining certain outcomes given certain inputs as well as the distribution $\rho(\lambda|j, k)$ characterising the influence of λ on the choice of inputs (or vice versa).

This classical theory is often referred to as *local-hidden-variable theory* (or *LHV theory*), and the hidden variables λ as local, since the distribution $p(ab|jk)$, when conditioned on complete knowledge of λ, factorises into local parts. This is often represented in the literature by the *locality* condition

$$p(ab|jk) = \int_\Lambda d\lambda \rho(\lambda) p(a|j, \lambda) p(b|k, \lambda). \tag{1.9}$$

However, care should be taken when considering this condition since it is in fact a combination of several smaller conditions that are explained separately below, and discussed in detail in [26].

$$\begin{aligned}
p(ab|jk) &= \int_\Lambda d\lambda \rho(\lambda|j, k) p(a, b|j, k, \lambda) && \text{Bayes' Theorem} && (1.10)\\
&= \int_\Lambda d\lambda \rho(\lambda) p(a, b|j, k, \lambda) && \text{Measurement Independence} && (1.11)\\
&= \int_\Lambda d\lambda \rho(\lambda) p(a|j, k, \lambda) p(b|j, k, \lambda) && \text{Outcome Independence} && (1.12)\\
&= \int_\Lambda d\lambda \rho(\lambda) p(a|j, \lambda) p(b|k, \lambda) && \text{No-Signalling} && (1.13)
\end{aligned}$$

The first equality is derived by Bayes' Theorem, which holds independently from the physical theories discussed here. Much of the early literature assumed (either

[8]The label d is given because, in the quantum scenario, it also refers to the dimension of the Hilbert space in which a measurement is performed, which is of course equivalent to the number of possible measurement outcomes for a rank-1 projective measurement.

implicitly or explicitly) that the experimenters have access to trusted RNGs for selecting inputs, such that there is no correlation between λ and the input choices. This condition, $\rho(\lambda|j,k) = \rho(\lambda)$, is known as measurement independence and will be assumed here but will be relaxed from Chapter 2 onwards.

Outcome independence is the assumption that joint measurement outcomes are uncorrelated given λ. The distribution $p(a,b|j,k,\lambda) = p(a|j,k,\lambda)p(b|j,k,\lambda)$ is *factorisable*, and observable correlations can arise only as a consequence of ignoring λ. This condition is relaxed in many of the adversarial models presented in later chapters[9]. In trusted laboratories where the experimenters used devices manufactured independently of each other, and therefore uncorrelated with each other, the assumption of outcome independence makes sense, as does the need to relax this condition in a more paranoid scenario where Eve has supplied all devices.

The final equivalence (1.13) is made by the assumption of *no-signalling* in the physical theory. Bob cannot instantaneously signal any information to Alice through his choice of input and vice versa, or do so at any speed faster than the speed of light (motivated by the theory of special relativity). This condition can be expressed mathematically as

$$\sum_{b=0}^{d-1} p(ab|jk) = \sum_{b=0}^{d-1} p(ab|jk') \qquad \forall a,j,k,k', \tag{1.14}$$

$$\sum_{a=0}^{d-1} p(ab|jk) = \sum_{a=0}^{d-1} p(ab|j'k) \qquad \forall a,k,j,j', \tag{1.15}$$

from which $p(a|j,k) = p(a|j)$ and $p(b|j,k) = p(b|k)$ are trivial equivalences. Any physical theory with this assumption is called a *no-signalling* theory, and it is beyond the scope of this thesis (and indeed beyond conventional thinking) to seriously consider a universe not constrained by this restriction. Whilst all classical models are no-signalling, the converse is not true.

The variables λ are often interpreted in the game theory context as *shared randomness*, where Alice and Bob use pre-existing shared random bits (as well as the referee's queries) to inform their outputs. The *hidden* part of 'local-hidden-variable theory' indicates that the variables are unknown and perhaps even unknowable to the experimenters, but their presumed existence will still limit the realisable probabilities $p(ab|jk)$. This is useful for the foundational attempts to characterise classical theory, though since λ can often be considered as a pre-programmed strategy known to an

[9]The restriction to factorisable distributions is discussed in Chapter 3

adversary intent on tricking the experimenters, LHV theory has gone by many different names over the years, such as *locally causal*, *local realistic* or even just *local* (see [27] for further discussion). We will refer to our adversarial models in later chapters as either classical or no-signalling rather than LHV, since the assumptions of both measurement independence and outcome independence usually associated with LHV theory shall both be relaxed.

One characteristic not addressed in the equations (1.10) - (1.13) is *determinism*. With the notation above, a theory is deterministic if all outcomes can be predicted with certainty given knowledge of the underlying variables λ, represented by

$$p(a, b|j, k, \lambda) \in \{0, 1\} \qquad \forall a, b, j, k, \lambda. \tag{1.16}$$

Trivially, such global determinism implies local determinism at the level of marginal distributions,

$$p(a, j, k, \lambda), p(b|j, k, \lambda) \in \{0, 1\} \qquad \forall a, b, j, k, \lambda. \tag{1.17}$$

Determinism can also be relaxed within a classical model [26]. Indeed, whilst the classical adversarial model discussed in Chapter 2 is deterministic, Chapter 3 discusses the advantages of using an indeterministic model for cryptographic purposes. The words classical and deterministic are often treated as synonymous, since the correlations produced by an indeterministic model can be equivalently produced by a deterministic model through the inclusion of extra underlying variables. For this reason, a classical indeterministic model is known as *stochastic*, to avoid confusion with the true indeterminism achieved by quantum theory.

As implied by the CHSH example, quantum theory imposes a restriction on $p(ab|jk)$ somewhere between the LHV and no-signalling theories. Using a bipartite quantum state ρ_{AB} in Hilbert spaces $\mathcal{H}_A \otimes \mathcal{H}_B$ of arbitrary dimension, all probabilities adhering to quantum theory are of the form

$$p(ab|jk) = \mathrm{Tr}(\rho_{AB} A_j \otimes B_k) \tag{1.18}$$

where A_j are measurement operators on H_A representing Alice's measurements given input j which deliver output a, similarly for B_k on Bob's side. Any quantum correlations satisfy the no-signalling conditions[10] (1.14) and (1.15) though there are

[10]The fact that there are correlations between entangled particles, regardless of spatial separation, suggests at first glance the possibility of instantaneous signalling. However the observed correlations in an experiment are dependent on the choice of measurements made; Alice cannot locally infer from her own measurement outcome anything about Bob's outcome without knowing what measurement he performed, and this information has to be sent by Bob to Alice at subluminal speeds.

no-signalling correlations which cannot be derived from quantum theory [28, 29] such as the above-mentioned P-R box [20].

The correlations permitted by LHV theory are included within the set of quantum correlations since they can be retrieved as the results of local commuting measurements performed on product states. However, the inclusion is strict, since there are quantum correlations which cannot be replicated by LHV theory, called *nonlocal correlations*. Making a distinction between local and nonlocal correlations is precisely the motivation for deriving Bell inequalities[11].

1.4.3 Bell Inequalities

1.4.3.1 General Framework

The classification of bipartite correlations in an m-setting, d-outcome scenario can be determined by considering a point $\boldsymbol{p} = \{p(ab|jk)\} \in \mathbb{R}^{d^2m^2}$, which satisfies the conditions of a probability distribution, namely positivity $p(ab|jk) \geqslant 0$ and normalisation $\sum_{a,b=0}^{d-1} p(ab|jk) = 1$. The conditions for local (1.9), no-signalling (1.14)-(1.15) and quantum (1.18) correlations can be used to define the sets $\mathcal{L}, \mathcal{NS}$ and $\mathcal{Q}$, which are subsets of $\mathbb{R}^{d^2m^2}$ exhibiting the strict inclusions $\mathcal{L} \subset \mathcal{Q} \subset \mathcal{NS}$. These sets are closed, bounded and convex, and furthermore $\mathcal{L}$ and $\mathcal{NS}$ are polytopes since they can be described by the intersection of a finite set of half-spaces[12]. The hyperplane separation theorem [30] can be used to find the hyperplane lying between a set $\mathcal{K} \in \{\mathcal{L}, \mathcal{Q}, \mathcal{NS}\}$ and any point $\boldsymbol{p'} \notin \mathcal{K}$. This hyperplane can be characterised by a set of coefficients $\boldsymbol{s} = \{s(abjk)\} \in \mathbb{R}^{d^2m^2}$, known for these purposes as a Bell expression, and a value $S_K \in \mathbb{R}$ such that

$$\boldsymbol{s} \cdot \boldsymbol{p} = \sum_{abjk} s(abjk)p(ab|jk) \leqslant S_K \tag{1.19}$$

for any $\boldsymbol{p} \in \mathcal{K}$, but $\boldsymbol{s} \cdot \boldsymbol{p'} > S_K$. When $\mathcal{K} = \mathcal{L}$, these inequalities are precisely the Bell inequalities used to test for nonlocality, with the corresponding values S_L, S_Q and S_{NS} being the largest achievable values for $\boldsymbol{s}$ using local, quantum and no-signalling correlations respectively[13]. If $S_Q > S_L$, then it is said that quantum mechanics violates the Bell inequality $\boldsymbol{s} \cdot \boldsymbol{p} \leqslant S_L$. Figure 1.2 provides a representation of $\mathcal{L}, \mathcal{Q}, \mathcal{NS}$ and a Bell inequality as hyperplane.

[11] A Bell test is also known as a *nonlocality test* for this reason.

[12] This follows from their construction from a set of linear conditions, and in contrast $\mathcal{Q}$ is not a polytope, though is still convex.

[13] Similarly, we can derive inequalities for $\mathcal{K} = \mathcal{Q}$ or $\mathcal{K} = \mathcal{NS}$, with the former often referred to as *Tsirelson* inequalities.

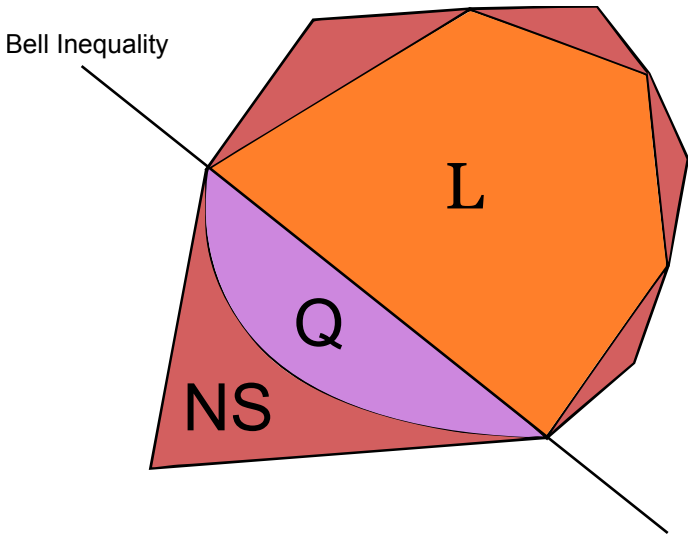

Figure 1.2: A depiction of the sets of local (L), quantum (Q) and no-signalling (NS) correlations.

What properties are required of quantum correlations of the type (1.18) to violate a Bell inequality? Unsurprisingly, since John Bell's motivation for considering such inequalities was to address the EPR paper's concerns about "spooky action at a distance", the state ρ_{AB} must be entangled to violate a Bell inequality. Indeed, supposing otherwise, the state is of the separable form (1.2), from which we can recover the locality condition (1.9) with

$$\begin{aligned} p(ab|jk) &= \mathrm{Tr}\left[\sum_{\lambda} p_\lambda(\rho_A^\lambda \otimes \rho_B^\lambda) A_j \otimes B_k\right] \\ &= \sum_{\lambda} p_\lambda \mathrm{Tr}\left(\rho_A^\lambda A_j\right) \mathrm{Tr}\left(\rho_B^\lambda B_k\right) \\ &= \sum_{\lambda} p_\lambda p(a|j,\lambda) p(b|k,\lambda). \end{aligned}$$

Furthermore, Alice's measurement operators must be non-commuting, as must Bob's [31].

A Bell expression $\boldsymbol{s}$ can be represented in the quantum framework by an operator

$$\mathcal{S} = \sum_{abjk} s(abjk) A_j \otimes B_k, \tag{1.20}$$

where $\{A_j\}$ and $\{B_k\}$ are Alice's and Bob's measurement operators. The quantum bound S_Q for a Bell expression is given by the spectral norm of $\mathcal{S}$, maximised over all possible measurements, i.e. $S_Q = \max_{\mathcal{S}} ||\mathcal{S}||$. As discussed in Section 1.4.1.1,

the well-known CHSH expression is associated with the operator given by (1.5), with a quantum bound of $2\sqrt{2}$ achievable by (1.6) and equivalent schemes under local unitaries.

The maximum evaluation of $\boldsymbol{s}$ achievable by no-signalling correlations is given by $S_{NS} = \max_{\boldsymbol{p}\in\mathcal{NS}} \boldsymbol{s}\cdot\boldsymbol{p}$. The much less restrictive conditions on such correlations means that S_{NS} is algebraically easier to compute than S_L or S_Q, and can be found with linear programming (see, for instance, Section 3 of [32])[14]. For the CHSH expression, $S_{NS} = 4$, obtained by the P-R box joint distribution $p(ab|jk) = \frac{1}{2}$ if $a \oplus b = jk$ and $p(ab|jk) = 0$ otherwise[15]

It is worth noting that, much as Section 1.4.1.2 expressed the CHSH inequality in the context of game theory, a general framework to derive game theory equivalents of all Bell inequalities has been formulated [35], and the topic of nonlocal games is popular in computer science.

Whilst there are a wealth of Bell inequalities to be found for a polytope $\mathcal{L}$, the minimal number required to define $\mathcal{L}$ entirely are given by the *facet Bell inequalities*, so called because they represent faces of the polytope $\mathcal{L}$. Specifically, for the Bell inequality $\boldsymbol{s}\cdot\boldsymbol{p} \leqslant S_L$, $F = \{\boldsymbol{p} \in \mathcal{L} | \boldsymbol{s}\cdot\boldsymbol{p} = S_L\}$ is a face of $\mathcal{L}$ and represents a facet Bell inequality. Trivially, the positivity conditions $p(ab|jk) \geqslant 0$ are facet Bell inequalities; We are interested in finding all others, because any other Bell inequality can be written as a non-negative combination of facet Bell inequalities. Furthermore, the exclusion of a point $\boldsymbol{p} \notin \mathcal{L}$ means that $\boldsymbol{p}$ does not satisfy one (or more) of the facet Bell inequalities. Conversely, any probability distribution satisfying the locality condition will satisfy all Bell inequalities, since they are defined by their separation from the polytope $\mathcal{L}$. Note that the no-signalling conditions are trivially also Bell inequalities since they are satisfied by all local correlations, but since by definition no quantum (or indeed no-signalling) correlations violate them, they are not useful to consider within the umbrella of Bell-based cryptography.

1.4.3.2 Notable Examples

As a 2-party, 2-setting, 2-outcome Bell inequality, the CHSH inequality is rather unique in that the only other non-trivial[16] facet Bell inequalities for this scenario can

[14]There is a further bound to be calculated for a Bell expression, known as the algebraic limit, which in some cases is even higher than the no-signalling limit, for instance with the *tilted CHSH inequality* [33]. However, this is not the case for any inequalities presented in this thesis. See also [34] for discussion.

[15]This distribution is named after Popescu and Rohrlich [20], though the idea had been discussed much earlier [28],[29].

[16]i.e. excluding the usual positivity constraints

be obtained from CHSH by relabelling some combination of the local experimenters ('A'↔'B'), the local measurement settings (e.g. '$j = 0$'↔'$j = 1$') or the measurement outcomes (e.g. '$b = +1$'↔'$b = -1$'), and we say that all such Bell inequalities are equivalent. The number of inequivalent facet Bell inequalities in a scenario with n parties, m local measurement settings per user, and d outcomes per measurement, scales vastly with any increases in n, m or d[17]. One can also consider asymmetric scenarios with a different number of measurements $m_A, m_B, \ldots$, or outcomes $d_A, d_B, \ldots$, for each experimenter, labelled with the quadruple (m_A, m_B, d_A, d_B) [37].

For $m_A = m_B = 3$ and $d_A = d_B = 2$, there is only one facet Bell inequality, up to equivalence, that is inequivalent to CHSH, known as the I_{3322} inequality.

$$\begin{aligned} I_{3322} = \quad & p(ab|00) + p(ab|01) + p(ab|02) + p(ab|10) + p(ab|11) - p(ab|12) \\ & + p(ab|20) - p(ab|21) - p(a|x=0) - 2p(b|y=0) - p(b|y=1) \end{aligned} \tag{1.21}$$

This expression has a local bound $S_L = 0$, whereas an optimal value of $S_Q = \frac{1}{4}$ can be achieved, again with measurements on a singlet state [37]. This inequality can be generalised for arbitrary $m_A = m_B = m$, and is given in Section 5.2.2, along with a derivation of the optimal local strategies achieving $S_L = 0$. The robustness of these inequalities against reduced measurement independence will be considered later, particularly for $m = 3$ in Section 5.2.3.

One particularly useful class of Bell inequalities is known as *chained* since they are derived from iterating over a simpler inequality such as CHSH [38]. Presented in a similar form to [39], the chained CHSH inequalities have m measurement settings on each side, using the convenient notation $j \in \{0, 2, \ldots, 2m-2\}$ for Alice and $k \in \{1, 3, \ldots, 2m-1\}$ for Bob, each with the usual dichotomic outcomes $a, b \in \{\pm 1\}$, and are defined as

$$I_m^c := p(a = b|00) + \sum_{|j-k|=1} p(a \neq b|jk). \tag{1.22}$$

For $m = 2$, this expression is equivalent to CHSH. Local variables impose that $I_m^c \geqslant 1$, whereas quantum correlations can achieve $I_m^c = 2m \sin^2(\pi/4m)$, which tends to 0 as $m \to \infty$. Chained Bell inequalities were the basis for the first device-independent quantum key distribution scheme [40] (see Section 1.6), and have recently been instrumental in proving the completeness of quantum theory's predictions under the assumption of free will [25], and also as a tool in the process of randomness amplification [41], to be discussed in Section 5.4.

[17] For instance, combinatoric methods can be used to derive an incomplete list of at least 20 million facet Bell inequalities, even when restricted to $n \leqslant 9$ [36].

Although the primary method of testing for nonlocality, that of a Bell inequality, requires outcome statistics over many runs, it is actually possible to show directly the incompatibility of quantum predictions with local models with a single logical contradiction, in what is known as an *all-or-nothing* scenario. The most popular example of this is the Greenberger-Horne-Zeilinger (GHZ) paradox [42], which involves three experimenters[18] Alice, Bob and Charlie, with respective inputs $j, k, l \in \{0, 1\}$ and dichotomic outputs $a, b, c \in \{\pm 1\}$. They share a tripartite quantum state known as the GHZ state, $|\,GHZ\rangle = \frac{1}{\sqrt{2}}(|\,000\rangle + |\,111\rangle)$, and associate with each input the measurement operators $A_0 = B_0 = C_0 = X, A_1 = B_1 = C_1 = Y$ which are performed to obtain the outcomes, e.g. $a_0 = \langle A_0 \rangle_{|\,GHZ\rangle}$. One notes that the correlations produced will satisfy

$$a_0 b_0 c_0 = +1, \qquad a_0 b_1 c_1 = -1, \qquad a_1 b_0 c_1 = -1, \qquad a_1 b_1 c_0 = -1, \tag{1.23}$$

for *every* instance of the experiment. On the contrary, an LHV model can merely assign a value[19] of $+1$ or -1 to each outcome a_j, b_k, c_l. One can verify that any such local assignments can satisfy at most three of the conditions in (1.23), but not all four. Indeed, by multiplying the left-hand-side of all four equations together, one obtains $a_0^2 a_1^2 b_0^2 b_1^2 c_0^2 c_1^2$, which as a product of $+1$ terms must itself be $+1$. This contradicts the -1 value given by multiplying the right-hand-side terms in the quantum scheme.

The crucial difference between the GHZ paradox and previously discussed Bell inequalities is that the same quantum correlations are produced on every run of the experiment, as opposed to confirming a probability distribution revealed over many runs, although the situation can nevertheless be rephrased as a Bell inequality, known as the tripartite Mermin inequality [43][20]. Despite the extra technological difficulty in implementing a tripartite nonlocality experiment (see Section 1.8), GHZ-based cryptographic protocols have been proposed [44]. The all-or-nothing quality of the tripartite Mermin inequality is also susceptible to variable-free-will analysis. This is outlined in Appendix B, assuming the remainder of this thesis as a prior.

[18] In fact, this scenario extends to general N-partite experiments rather easily, but $N = 3$ is the simplest case to consider.

[19] The model must be deterministic to reproduce any one of the correlation conditions in (1.23).

[20] The quantum scheme described will always win the associated nonlocal game, i.e. $p_{\text{win}} = 1$, showing that there are some games for which the full no-signalling theory provides no advantage over quantum theory.

1.5 Cryptographic Primitives

The essence of cryptography is ensuring that information is kept secure, be it stored locally by one party or shared between two or more parties, from the variety of eavesdropping attacks available to an adversary. Whilst the early history of cryptography is devoted to encryption schemes of ever increasing complexity, the field took a major turn with the incorporation of randomness, not complexity, as the fundamental guarantee of security. This section explores the two inextricably linked notions of *randomness* and *security* through the discussion of the cryptographic primitives relevant to this thesis.

1.5.1 Randomness Generation

The randomness of events within Nature has been a subject of philosophical debate for millennia, and one closely related to the concepts of free will and determinism. Can a human make choices freely, or have all such choices been predetermined by some higher scheme? In addition, if an event has been determined to happen, does that mean that it can be predicted with certainty? Randomness is usually seen as antonymous with predictability. Indeed, one should note the difference between genuine randomness, which can never be predicted, and *pseudorandomness*, which only seems to exhibit randomness given an absence of knowledge about its creation. An example of apparent randomness as resulting from the lack of a bigger picture was given by Thomas Aquinas [45]:

"I answer that, In this world some things seem to happen by luck or chance. Now it happens sometimes that something is lucky or chance-like as compared to inferior causes, which, if compared to some higher cause, is directly intended. For instance, if two servants are sent by their master to the same place; the meeting of the two servants in regard to themselves is by chance; but as compared to the master, who had ordered it, it is directly intended."

Whilst one can muse about the fundamental nature of randomness indefinitely, there is no question that there are many technological applications, both scientific and commercial, which require randomness. For some, psuedorandomness is enough. However, since the bits created by a pseudorandom algorithm are deterministically generated, they can easily be replicated with knowledge of the initial conditions. This replication can sometimes be desirable, for instance to identify bugs or benchmark results between codes in a Monte Carlo simulation (see Section 37 of [46]), but in other cases will not be desirable. Deterministic randomness certainly causes problems

for scenarios requiring *private* randomness such as online gambling or, of course, cryptographic protocols.

One of the fundamental aspects of quantum theory is its inconsistency with determinism. It is possible to observe truly random events through, for instance, the measurement of an atom's spin in a Stern-Gerlach experiment [47] or the polarisation of a photon, where the measurement outcome is random. However, one should note the difference between predictable and unpredictable randomness. For example, if one measures Pauli operator X repeatedly on qubits in the state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, then each measurement result is predicted to have a 0 outcome with probability $|\alpha|^2$ and a 1 with probability $|\beta|^2$. Although the outcomes themselves are random, the statistics accumulated over many runs can trivially be recreated classically. Assuming non-signalling, the correlations produced in a quantum implementation of a Bell test (from similarly random measurement outcomes), on the other hand, cannot be predicted, since any attempt will adhere to the local bound of the Bell inequality. It is thus through the successful violation of a Bell inequality that private randomness can be certified.

There are two closely related protocols for generating private randomness through Bell tests, which are differentiated by the nature of their inputs. A *randomness expansion* protocol [48, 49] takes a pre-existing finite stock (or *seed*) of perfect randomness to make measurement selections in a Bell test, and the resulting data is processed to create further random bits, the privacy of which is verified by a Bell violation. The process is described in Chapter 3 and considered within the context of limited measurement independence[21]. *Randomness amplification* [41] takes a similar approach, but assumes the availability of an infinite amount of imperfect randomness, often defined by the source's correlations with other unknown variables. Whilst no explicit randomness amplification protocol is given in this thesis, this task correlates closely with the results of Chapter 5 and is discussed in Section 5.4.

1.5.2 Key Distribution

Historically, cryptography has been concerned with *encryption* and *decryption*. When Alice wishes to communicate a message, known as the *plaintext*, to Bob, it is converted by Alice into a seemingly incomprehensible *ciphertext* (the method of encryption, regardless of physical or logistical description, is called a *cipher*) and sent to Bob. It is assumed that the ciphertext is transmitted insecurely and may

[21]Since a variable free will strategy tampers with the RNGs used to make measurement choices, the link between the two ideas is quite clear.

be intercepted by Eve. When Bob receives the ciphertext, he deciphers it using a decryption protocol previously agreed upon with Alice, thereby obtaining the original plaintext which has withstood eavesdropping.

There are two branches of cryptography which differ in the nature of the cipher being used. In *public–key cryptography*, Alice holds both an encryption and decryption key. The encryption key is usually formulated from the decryption key by an algorithm incorporating *one–way functions* which are easy to compute but difficult to invert. A popular example is the multiplication of two large prime numbers, since determining the prime numbers from the product (i.e. *factoring*) is known to be very difficult[22]. The RSA cipher [50], devised in the 1970s and still in commercial use by personal computers to this day, relies on such factoring. This branch of cryptography is known as public–key because the encryption key is made known to all parties, including adversaries. Both Bob and Eve can encrypt a message using this key but only Alice holds the decryption key[23]. Whilst this method of encryption is *computationally secure*, advances both experimental and theoretical suggest that at some point RSA will no longer be sufficient. Indeed, study of quantum theory has led to Shor's algorithm [12], a procedure which can theoretically be implemented by quantum computers to factor numbers in polynomial time, thereby endangering RSA and other public–key ciphers.

On the other hand, *private–key cryptography* employs a key that is shared privately by Alice and Bob and is used for both encryption and decryption[24]. Alice converts her message into a string of binary numbers using a standard character–encoding scheme such as ASCII. The shared key is also a binary string of the same length as the message. Alice XORs the message and key bitwise (i.e. addition modulo 2) and sends to Bob, who decrypts the message via the same operation. Shannon's seminal paper from 1948 [51] proved that so long as the key that Alice and Bob generate is perfectly random and used once only, the encryption is perfectly secure, regardless of Eve's power and resources. Such a key is known as a *one–time pad* for historical reasons. The problem of encrypting a message has thus been reduced to a more specific problem of *key distribution* between Alice and Bob. However, since classical information can simply be copied by Eve if intercepted, one must rely

[22]In terms of computational complexity, we say that multiplication can be performed by a classical algorithm in a time that is only polynomial in its input size, but current classical algorithms for factoring run in a time that is super–polynomial in its input size.

[23]The discrepancy in the keys held by Alice and Bob means that this cipher is also known as an *asymmetric–key cryptosytem*

[24]Since the shared key is identical for both Alice and Bob, this is also known as *symmetric–key cryptography.*

on either the inefficient, expensive and trust-dependent use of a personal courier to securely distribute a classically generated key, or a *quantum key distribution* (QKD) protocol to efficiently distribute keys whose security guarantees, much like with the above randomness generation protocols, rely upon nonlocal correlations.

Whilst randomness generation and key distribution may seem like essentially the same task, the latter is more difficult because of the assumed experimental setup. Randomness expansion uses the outcomes generated by two (or more) devices, but the process is conducted by a single party exclusively within the same laboratory, provided sufficient spatial separation is given to prevent causal connection. It is assumed that, even in the device-independent scenario where she may have previously had access to these devices, Eve cannot otherwise infiltrate the lab whilst the experiment is conducted. In contrast, the devices used for key distribution are operated by multiple parties within different laboratories, and Eve is assumed to be all-seeing and all-knowing in the space between. Alice and Bob (and if applicable Charlie and ...) must therefore reconcile an identical key using the results of their experiments and classical communication that Eve can intercept. This scenario is detailed in Chapter 4, again considering the free will loophole.

1.5.3 Security and Privacy Amplification

One practical method for quantifying randomness is to ask how easily an eavesdropper can make successful predictions. Supposing that Alice and Bob hold measurement devices making, as usual, measurements x and y and recording outputs a and b[25]. If the devices are behaving classically, we can view inputs and outputs as being predicted by random variables A,B,X,Y. Assuming that Eve has somehow gleaned information from the process, this information can be encapsulated by a system E, partially correlated with Alice's device, on which she can perform measurements labelled z. When z is performed, Eve's best guess at Alice's outcome is of course the one maximising $p(a|ez)$. We can thus define the *guessing probability* as the average probability to correctly guess Alice's outcome, maximised over all measurements available to Eve

$$G(A|E) := \max_z \sum_e p(e|z) \max_a p(a|e,z). \tag{1.24}$$

The guessing probability is often given in terms of the *min-entropy* [52], defined to be $H_{\min}(A|E) = -\log_2 G(A|E)$. If, as is often the case in a cryptographic setting,

[25] these labels are given in generality to the entire system, say a string of bits $\boldsymbol{x} = (x_1, \ldots, x_N)$ over several measurements $\boldsymbol{a} = (a_1, \ldots, a_N)$, but can be reduced to single-run entries when making certain causality assumptions detailed later.

the outcome space of A is an n-length bit string, $A \in \{0,1\}^n$, we see that $0 < H_{\min}(A|E) < n$, with the upper bound obtained in the ideal (for Alice) case where Eve can do no better than guessing Alice's string with uniform probability 2^{-n}.

The min-entropy has an operational interpretation, since it represents the amount of uniform randomness that Alice can extracted from the system, whether Eve holds classical [53] or quantum [54] side-information. Specifically, in what's known as the *leftover hash lemma* [53], a sequence of n bits with min-entropy $H_{\min}(A|E)$ can be reduced to a sequence of $m = H_{\min}(A|E) \leqslant n$ uniformly random bits by applying some hash function $f_r : A \to \{0,1\}^m$, so long as the function f_r is chosen uniformly from a family of two-universal hash functions. This process is known as *randomness extraction*, or in the cryptographic context as *privacy amplification*.

Clearly a seed of initial randomness is required (for selecting the hash function) to perform randomness extraction. Therefore, in a randomness expansion or key distribution protocol where the aim is to produce private randomness through a series of Bell tests, one should always consider not only the randomness required to choose the measurement inputs, but also the randomness that will be needed to classically process the resulting data.

The concept of min-entropy can be extended into the quantum scenario [52] where Alice and Eve hold a bipartite state ρ_{AE} as

$$H_{\min}(A|E) := -\inf_{\sigma_E} D_\infty(\rho_{AE}||\mathbb{1}_A \otimes \sigma_E), \tag{1.25}$$

where $\{\sigma_E\}$ is the range of all normalised density operators on system E, using

$$D_\infty(\tau||\tau') := \inf\{\lambda \in \mathbb{R} : \tau \leqslant 2^\lambda \tau'\}. \tag{1.26}$$

Privacy amplification can similarly be achieved in the quantum case [54], however no such general claim has been made for a more powerful adversary with arbitrary no-signaling side-information [55].

Crucially, the degree of violation of a Bell inequality provides bounds on the min-entropy, and thus the extent to which privacy amplification is required. It is proved in Appendix A that if Alice and Bob test the CHSH inequality using two-qubit systems achieving a violation S, and if Eve can only attack the system independently on each run of the experiment, then the guessing probability is bounded above by

$$G(A|E) \leqslant \frac{1}{2}\left(1 + \sqrt{2 - \frac{S^2}{4}}\right). \tag{1.27}$$

1.6 Device-Independent Cryptography

The preceding sections have detailed various tasks and experiments in the context of the best strategies available to Alice and Bob, whether in the classical or quantum frameworks, or according to a hypothetical stronger no-signalling theory. The advantages to exploiting quantum phenomena for cryptographic purposes are clear, so the assumption that the equipment used to perform such experiments is trusted, as well as the theory to which Nature abides is known, would seem at first glance to be obvious. Within the last decade or so, it has been shown that in fact neither assumption is necessary.

As mentioned in Section 1.4.1.1 and depicted in Figure 1.1(c), many nonlocality-based cryptographic protocols can be adapted to guarantee security that need not be reliant on either the apparatus used to implement them or on the completeness of the quantum theory that inspired them. This scenario is known as *device-independent cryptography*, and the devices used by Alice and Bob can be viewed as unknown black box devices that may have even been manufactured and maliciously pre-programmed by Eve. All that is required of the devices is the ability to register inputs, say j, k as before, and produce outcomes a, b in some fashion. If the probability distribution $p(ab|jk)$ estimated by the collected data sufficiently violates a Bell inequality, a secure protocol can be achieved, with the degree of Bell violation used to estimate precisely how securely the task has been conducted.

One should clarify that the presence of selectable inputs and readable outputs are only required to allow for a possible device-independent protocol; to work optimally, the devices should still perform the best quantum strategy available, but this setup can be certified through $p(ab|jk)$, rather than assumed with some degree of trust. Indeed, the prerequisite for Bell-based experiments that the measurement devices are spatially separated to prevent communication is still a requirement in the device-independent scenario.

All of the crucial ingredients for a device-independent quantum key distribution (or DIQKD) protocol were already present in Ekert's original entanglement-based protocol [11]. However, the realisation that several assumptions could be dropped was not made until much later. In 2005, Barrett, Hardy and Kent described a secure QKD protocol that only required the underlying physical theory to be constrained by no-signalling [40]. Whilst this protocol was based on the chained Bell inequality, a CHSH-based protocol was then developed that dropped the requirement of trust in the devices, first by suggestion [56] and then explicitly [57], although certain assumptions

on the types of attack available to Eve were still required (see the beginning of Chapter 5).

The device-independent approach can also be applied to other existing quantum cryptographic tasks. Device-independent randomness generation (DIRNG) has been proposed based on both the GHZ paradox [44] and the CHSH inequality [48], with significant practical implementations already developed [58]. Other cryptographic tasks such as bit commitment and coin flipping have also been given the device-independent treatment [59].

The umbrella of device-independent protocols can also be extended to novel ideas that certify the 'quantumness' of various situations. For instance, *self-testing* takes the quality of correlations produced in an experiment to reveal information about the states that must have been used. It was already known that a maximal CHSH violation of $2\sqrt{2}$ can only be genuinely achieved by performing measurements on a singlet state (up to local unitaries) [19]. This knowledge was adapted to make the same assumption even without knowledge of the devices' underlying machinery [60]. Furthermore, device-independent testing has been developed for a number of features, such as demonstrating genuine multipartite entanglement [61], lower bounding the dimension of Hilbert space used within the devices [62], and certifying the teleportation of a qubit [63], amongst others. In fact, the theory is reaching such development that an entirely device-independent outlook on the quantum formalism is not out of the question [64].

1.7 Loopholes

The violation of Bell inequalities has been experimentally observed many times over the last three decades, to the point that the incompatibility of the LHV theory with Nature seems to most like a foregone conclusion. However, any practical investigation of the underlying theory is subject to various experimental imperfections that must be taken into consideration before a grand statement can be made. This leads into the study of *loopholes*, potential flaws in the apparatus that can be exploited to simulate nonlocality in a decidedly local fashion.

The rapid advancement of technology is verging ever closer to the realisation of a definitively loophole-free Bell test, as will be discussed in Section 1.8, and may even be a matter of years, not decades, away. This achievement is not sought after merely to satisfy the curiosities of theorists concerned purely with the foundations of quantum physics. Indeed, whilst the exploitation of loopholes undertaken by Nature itself to

mask its own classicality seems highly dubious, it is not at all out of the question that an eavesdropper attacking a device-independent cryptographic protocol would wish to program the untrusted devices in such a way as to fake true nonlocality, and therefore give the false impression of security. The closure of loopholes is therefore a requirement to perfectly ensure security in device-independent protocols.

The following sections detail three of the most well-known loopholes, those of *detection*, *locality* and *memory*, and provide examples of how the detection and locality loopholes can be exploited to simulate nonlocality. Of course, Chapter 2 onwards is dedicated to another more recently considered loophole known as the *free will loophole*.

1.7.1 Locality Loophole

Consider the case where the measurements performed by Alice and Bob in a single run of a bipartite Bell test are not distantly separated. In the game formulation, this corresponds to Alice and Bob being *causally connected*, which is to say that they can communicate with one another in the time between receiving their questions and having to return the answers. Equivalently, in the device-independent scenario, we can visualize this as a single black box, where Eve can immediately know both inputs for a run of the experiment and subsequently choose both outputs within the required timeframe. Upon an input pair (A_j, B_k) for $j, k = 0, 1$, Eve can randomly select Alice's output as $a \in \{\pm 1\}$ and then calculate the value $b = a \cdot (-1)^{jk}$, which clearly maximizes (1.7). Since using b for Bob's output on every run will provide the maximal CHSH value of 4 (and similarly $-b$ yields -4), Eve can dilute this value and avoid suspicion from the users of the device by displaying b with probability p and otherwise $-b$ (for instance, over many runs a CHSH value of $2\sqrt{2}$ will be achieved if $p = \frac{1}{2} + \frac{1}{\sqrt{2}}$).

1.7.2 Detection Loophole

In practical implementations of a Bell test measuring photon polarisation, not all photons will be detected. This is usually represented by a *detector efficiency* η, which is the probability that a photon will be detected on any given run. In the early days of Bell tests, it was common to make the *fair sampling assumption* [65], that the detected photons were representative of all of the produced photons, so that Nature was not behaving differently with photons according to their detection. In an adversarial scenario, this assumption would be unwise.

We should therefore be concerned that Eve might fake an inefficiency in the detectors to mask her classical tampering. Consider a source emitting photons within fixed time intervals, so that Alice and Bob know when their devices should recieve a photon[26]. If detection fails, they decide to register a +1 outcome in place of the missed measurement result [67]. With probability η^2 the CHSH test runs as normal and (assuming the optimal state and measurements) $2\sqrt{2}$ is observed. However, with probability $2\eta(1-\eta)$, one of the two detectors fails and the resulting outcomes are entirely uncorrelated; for this subset of runs, the CHSH test yields 0. Finally, a proportion $(1-\eta)^2$ of runs will have failed detections in both devices, for which both users register +1 and a CHSH value of 2 is observed for these runs.

It follows that a CHSH violation (i.e. any value above 2) can only be achieved if $\eta > \frac{2}{\sqrt{2}+1} \approx 83\%$, and a maximal violation of $2\sqrt{2}$ can only be achieved when the detectors are perfectly efficient. Assuming the detector efficiency is above this threshold, we proceed as normal and, when we find the CHSH violation, assume Eve followed her optimal eavesdropping strategy as specified in the previous section. From this, we determine how much classical post-processing is necessary in order to completely exclude Eve. There are several studies of note in the literature which consider the detection loophole more extensively, from CHSH tests using non-maximally entangled states [68] or asymmetric detection efficiencies [69] and the case where the local measurements have different efficiencies [70], to considering other Bell inequalities with n users [71], m measurement settings [72] or dimension size d [73].

1.7.3 Multiple Runs and Memory Loopholes

The probability distribution $p(ab|jk)$ that Alice and Bob are concerned with in a Bell test (aside from the all-or-nothing approach such as GHZ tests (1.23)) is estimated over multiple runs of an experiment. This leads to two closely-related questions; how important is the accuracy of the observed statistics based on a finite number of trials in relation to the underlying correlations when making claims of observed nonlocality? Also, what advantage is available to Eve in attacking the system over multiple runs rather than on each run independently? Such problems are referred to as the *memory loophole* [74].

[26]This is known within the literature as heralded photon emission [66], and can be implemented by producing a *pair* of photons each time. Whilst the detection of one photon effectively destroys it and prevents further measurement, the detection heralds the successful creation time of the other photon which may then be measured.

The security of a device-independent cryptographic protocol is usually described in terms of the kinds of attacks that it is immune from [75]. Two classes of attacks worthy of differentiation are the *independent, identically distributed* (*i. i. d.*) attack and the *correlated* attack (sometimes known as *collective* and *general* attacks respectively.). An i. i. d. attack by Eve attacks independently for each run whereas a correlated attack can probe the entire system. Whilst the security of quantum and device-independent key distribution against i. i. d. attacks has been proven [57], security against the latter is much more difficult to attain. Attempts to achieve general security often amount to placing a restriction on Alice and Bob's devices being spacelike separated for each given run, essentially reducing Eve's options to performing only collective attacks, whether in the quantum [76] or device-independent [77, 55] framework.

Exploitation of the memory loophole can be described by the devices having been preprogrammed maliciously by Eve, such that the outcomes recorded on the nth run are dependent not only on the hidden variables λ but also on the previous measurement choices and outcomes in either one or both wings of the experiment, depending on the strength of the model. Such tampering could induce a statistical fluctuation resulting in the inauthentic observation of a Bell violation [74][27]. The devices are even more vulnerable in a cryptographic protocol involving public classical communication, since it is possible for the devices to independently store their previous inputs and outputs and reveal encoded information within the outputs of later runs [78].

It has been shown that, in the case of a non-cryptographic Bell test where Alice and Bob have complete free will in selecting their measurements, memory-based attacks do not possess any significant advantage [74] and Eve's optimal attack is the same single-shot attack repeated over each run of the experiment. However, when considering also the free will loophole, where Alice and Bob have only a limited amount of choice in measurement selection, this is not the case, and Eve has a significant advantage in correlating her attack over many runs of the experiment. This result is the main focus of Chapter 5.

1.8 Experimental Progress

Here we provide a brief summary of experimental progress in approaching a loophole-free Bell test. A comprehensive review can be found in [79].

[27] All memory-based attacks are included in the class of correlated attacks, but this inclusion is strict.

The locality loophole was first declared closed in one of the earliest Bell experiments [24], however the setup used an acousto-optical interaction which does not provide truly random input selections. In 1998, an experiment using electro-optic modulators and two independent quantum random number generators is generally considered as having satisfactorily closed the locality loophole [80].

Naturally the best way to make Bell tests robust against the detection loophole is to increase the detection efficiency within the measurement devices. Until very recently, this was considered to be extremely difficult with photonic systems. Of course, the Bell inequality can be applied to other physical systems, and the CHSH inequality in particular is relevant to any setup involving two spatially separated systems with dichotomic measurements. If one still considers photonic systems, there have been demonstrations of nonlocality using properties of photons other than polarisation, for instance phase and momentum [81], orbital angular momentum [82], or time-bin encoding [83].

Atomic systems may also be considered, though use of more complex systems will of course be more susceptible to the locality loophole than photons. The first such test to close the detection loophole in 2001 used Be+ ions in a magnetic trap 3μm apart [84], and the distances between devices have been steadily improved, with a recent experiment using rubidium-87 atoms that were 20m apart [85]. It is suggested that a distance of 300m is required to simultaneously close the locality loophole using the fastest procedure to measure the atomic state of atoms [86]. However, this may not be necessary as photonic detection rates have dramatically improved in recent years. A Bell violation with photons separated by more than 10km was reported in 1998 [87]. Much more recently, an experiment claiming the detection loophole had been closed with photons was detailed [58], and furthermore adapted to perform device-independent randomness expansion. Additionally, [88] proposes a scheme using available technology closing both loopholes at once, using an atom-photon setup and combining homodyne detection with photodetection. Finally, multipartite nonlocality tests, though much more difficult to perform, have been conducted with three photons using GHZ states [89] and W states [90].

Chapter 2

Quantifying Measurement Dependence

The introductory chapter of this thesis gave the preliminaries for several topics in quantum information theory and cryptography. Throughout, the necessity of experimenters to possess free will in selecting their measurements was stated, but not fully explored. This approach is reminiscent of much of the literature associated with nonlocality and its cryptographic applications, where the assumption of free will is frequently mentioned yet infrequently considered. However, in the wake of discovering the true power of Bell inequalities for ensuring privacy even in device-independent scenarios, the rather rigid statement 'experimenters have free will' must be given much more careful scrutiny to ensure that the device-independent theory is robust and ready for implementation.

The rest of this thesis is dedicated to such scrutiny. After qualitative discussion of the concept of free will, this chapter will suggest quantitative measures used to bound the power of an adversary, then incorporate the measures in the simple scenario of one-shot testing of the CHSH inequality. The implications of these results for the applications of device-independent randomness expansion and key distribution will be considered in Chapters 3 and 4 respectively. Finally, Chapter 5 will ask how advantageous the consideration of a strategy correlated over many runs of the experiment can be for an eavesdropper.

2.1 Discussion

'Does the universe permit free will?' Clearly, a rather pointed question such as this cannot be satisfactorily answered over the course of a few pages; after all, a significant amount of academia, ranging across the arts and sciences from theoretical physics to

contemporary neuroscience to criminal law, has been dedicated to this discussion over many centuries. Indeed, within the context of this thesis, any attempt to answer such a question is futile, since the foundational proof of free will involves performing a Bell test which itself requires free will to be successful, leading to a frustratingly circular argument.

A more specific, and implicitly trust-based, question to be raised is, 'Is it possible to make free choices?'. This comes closer to the context of the nonlocality tests presented in Chapter 1, where the experimenters are required to freely choose between particular measurements in order to harness the correlations of the outcomes. Decision-making in the human brain is hardly a rapid process [91], which denies the ideal scenario of instantaneous choices; electronic devices are more efficient in this regard, but their existence outside of our own consciousness implicitly raises questions of trust, particularly for cryptographic tasks.

John Bell's landmark paper [13], which kickstarted the late 20th century's investigations of nonlocality, first presumed that free will is a prior for such tests, then examined the correlations achievable by quantum mechanics as a result. More recently, however, the converse has been elevated to an equally important discussion [92, 93]; given that nonclassical correlations have been produced, and assuming that the world obeys local realism, how much free will must the experimenters have exhibited? This context of selecting measurements has led to a common usage in the literature of the terms 'experimental free will' and 'measurement independence'. These terms emphasise that the free will considered in nonlocality tests is characterised by non-sentient devices such as random number generators (RNGs) rather than human decision-making, which is far too inefficient and unreliable to withstand scrutiny [91].

There are various types of correlations that can be considered. One starting point would be the correlations produced by projective measurements on a singlet state. Barrett and Gisin [93] showed that at most one bit of measurement independence is required to produce a local model which reproduces these nonlocal correlations, using their information-theoretic measure defined by (2.9) below; through a more complete analysis, Hall [26] reduced this to roughly 1/15 of a bit. The bulk of this thesis considers the correlations which violate a Bell inequality, particularly CHSH, because of the direct applications of nonlocality tests to cryptographic tasks.

Practically speaking, the tasks for which these Bell tests are used require high data rates. The experimenters rely on RNGs to select their measurements for them. It would be prudent to assess the reliability of these RNGs using some quantitative measure of measurement independence. Of course, given that these devices are as

subject to paranoia as the rest of the apparatus, it raises another question of how the experimenters could evaluate this measure for themselves. Nevertheless, we will first consider the power an adversary has for a fixed value of measurement independence in these devices.

Before the measures are introduced, a note should be given on the terminology. Whilst experimental free will is characterised by how independent a random number generator's outputs are from its underlying local variables, the term 'measurement independence' found within the literature is often counterintuitive in the context of the proposed measures, since complete independence is characterised by minimal values of the measure (typically 0), whilst a maximal value suggests that the measurement selections chosen are entirely determined by underlying data. In this thesis, the more appropriate term 'measurement dependence' will be used consistently when referring to the quantitative measures, with 'measurement independence' typically conserved to mean complete experimental free will.

2.2 Measures of Measurement Dependence

Consider the definition of locality within the context of a Bell test presented in Chapter 1. Recall that when Alice and Bob select from measurements A_j and B_k with which to measure outcomes $a, b = \pm 1$, correlations that violate a Bell inequality cannot be explained by a local hidden variable model defined by a set of underlying variables λ with distribution $p(\lambda)$[1] which locally specify the outcomes conditioned on knowledge of λ. More formally, any probability distribution $p(a, b|A_j, B_k)$ is considered local if and only if it satisfies the condition

$$p(a, b|A_j, B_k) = \int d\lambda p(\lambda) p(a|A_j, \lambda) p(b|B_k, \lambda) \tag{2.1}$$

for some λ model.

Adapting this framework to incorporate limited measurement dependence, let λ specify not only the measurement outcomes but also the measurement selections, that is the distribution $p(A_j, B_k|\lambda)$ for selecting the measurement pair (A_j, B_k) given knowledge of λ. Whilst this distribution is more intuitive for describing the following scenario, we will also be concerned with the distribution $p(\lambda|A_j B_k)$, with the two

[1]The underlying variables can be drawn either from a discrete set of parameters or over a continuous range. We will be considering discrete sets in this thesis, though the measures presented here could certainly be extended to cover a continuous range.

being related by Bayes' theorem. This model satisfies the condition

$$p(a,b|A_j,B_k) = \int d\lambda p(\lambda|A_j,B_k)p(a,b|A_j,B_k,\lambda). \tag{2.2}$$

For this model to exhibit complete experimental free will, the underlying variables and measurement settings chosen must be independent of each other, namely $p(\lambda|A_j,B_k) = p(\lambda)$ and $p(A_jB_k|\lambda) = p(A_jB_k)$. This condition suggests an appropriate measure of measurement dependence introduced by Hall [92] as

$$M_H := \frac{1}{2}\max_{j,k,j',k'} \int d\lambda |p(\lambda|A_j,B_k) - p(\lambda|A_{j'},B_{k'})| \tag{2.3}$$

to which we have added the factor of $1/2$ for convenience[2]. With this factor, the measure lies in the range $[0,1]$, where $M_H = 0$ corresponds to complete free will. $M_H = 1$ occurs when there exist two distinct pairs of settings $(A_j,B_k),(A_{j'},B_{k'})$ such that for each λ, either $p(\lambda|A_j,B_k) = 0$ or $p(\lambda|A_{j'},B_{k'}) = 0$, i.e. these settings are chosen deterministically by λ indicating no measurement independence.

Calculating this measure for a discrete set of underlying variables can be easily visualised by expressing the distribution $p(\lambda|A_jB_k)$ as a table of probability densities, such as in Table 2.2 where the rows indicate λ and the columns indicate the pairs of measurement settings. M_H is then calculated as the maximum 'column difference', this being the moduli of the differences between the entries in a pair of columns, summed over all of the rows. An extension of this measure is the q-norm variant (for $q > 0$)

$$M_q := \max_{j,k,j',k'} \left(\frac{1}{2}\int d\lambda |p(\lambda|A_j,B_k) - p(\lambda|A_{j'},B_{k'})|^q\right)^{\frac{1}{q}}. \tag{2.4}$$

For the remainder of the paper we will use the notation $M_H = M_1$ interchangeably and often use the measure $M_S := M_2^2$ since this measure will be useful for the methods presented. Although M_q takes a different range of values for each q, it is clear that any increase in measurement dependence according to one of the measures necessitates an increase according to *all* of the measures. Similarly, all measures take the value 0 when there is complete free will, and take a maximal value when there is none whatsoever. Corollary 2 will further prove the equivalence of these norms for the purposes of maximising the CHSH inequality, thus justifying the choice of measure preferable for the task at hand. We can also apply Hölder's inequality so that $M_S \leqslant M_pM_q$ whenever $1/p + 1/q = 1$.

[2]Note that this measure can be used for any Bell test with m_A settings on Alice's device and m_B settings on Bob's device. The maximum is taken over all possible pairs of measurement settings.

Another appropriate measure [2] considers the maximum distance between the measurement distribution with knowledge of λ and the measurement distribution without knowledge of λ. For a 2-party protocol where Alice (Bob) chooses from m_A (m_B) settings, and assuming a discrete set of λ, this is given by

$$M_K := \frac{m_A m_B}{2(m_A m_B - 1)} \max_{\lambda} \sum_{j,k} |p(A_j, B_k|\lambda) - p(A_j, B_k)| \tag{2.5}$$

where $j \in \{0, \cdots, m_A - 1\}$, $k \in \{0, \cdots, m_B - 1\}$. This measure emphasises the advantage Eve has, by preprogramming the devices according to a λ routine, over the experimenters who only observe the distribution $p(A_j, B_k)$. Again $M_K = 0$ represents complete free will for the experimenters, since such a routine creates no discernible difference in the measurement distributions. A complete lack of free will is evident with a deterministic strategy, i.e. there is some λ, j, k for which $p(A_j, B_k|\lambda) = 1$. The normalising factor in the definition above is the reciprocal of what the deterministic strategy achieves, so that this measure also lies in $[0, 1]$. For a general measurement distribution $p(A_j, B_k)$, the normalising factor is $(2(1-\min_{j,k} p(A_j B_k)))^{-1}$ regardless of whether the distribution is uniform or skewed towards particular choices. The uniform distribution $p(A_j B_k) = 1/m_A m_B$ yields the normalising factor shown in (2.5).

A final measure will be used for the randomness generation results in Chapter 3. This measure is defined formally as

$$P := \max_{j,k,\lambda} p(A_j, B_k|\lambda) \tag{2.6}$$

and quantifies the maximum deviation of $p(A_j, B_k|\lambda)$ from the uniform distribution. For a 2-party protocol with m_A and m_B measurement settings, P takes values in the interval $[\frac{1}{m_A m_B}, 1]$. The minimum value indicates that the distribution over all pairs of measurement settings is uniform, regardless of knowledge of the underlying variables, implying maximal free will; the maximum indicates an entirely deterministic measurement selection specified by Eve. This measure has prominent ties with the min-entropy discussed in Section 1.5.3. The min-entropy of a source of randomness selecting measurements with measurement dependence P is given by $H_{\min} = -\log_2 P$, which runs from zero for deterministic sources to $\log_2 m_A m_B$ for completely random sources.

We observe a connection between M_K and P as follows, assuming the uniform distribution $p(A_j, B_k) = 1/m_A m_B$. Define the q-norm variant of M_K as

$$M_{K,q} := \frac{m_A m_B}{N_q(m_A m_B - 1)} \max_{\lambda} \left(\sum_{j,k} |p(A_j, B_k|\lambda) - p(A_j, B_k)|^q \right)^{\frac{1}{q}}, \tag{2.7}$$

where $N_q := (1 + (m_A m_B - 1)^{1-q})^{1/q}$ is a scaling factor[3] that tends to 1 as $q \to \infty$. Taking this limit, M_K approaches

$$M_{K,\infty} := \lim_{q\to\infty} M_{K,q} = \frac{m_A m_B}{m_A m_B - 1} \max_{\lambda,j,k} |p(A_j, B_k|\lambda) - p(A_j, B_k)|. \tag{2.8}$$

Assuming that the maximum is attained when $p(A_j, B_k|\lambda) > p(A_j, B_k)$, this expression reduces to $M_{K,\infty} = (m_A m_B P - 1)/(m_A m_B - 1)$, which coincides with the limits $M_{K,\infty} = 0, P = 1/m_A m_B$ for complete free will and $M_{K,\infty} = 1, P = 1$ for a deterministic selection.

Another measure of measurement independence can be discussed by introducing the concept of a Santha-Vazirani source of randomness [94]. Since the concept of a Santha-Vazirani source has been intrinsically linked with the idea of randomness amplification [41] of a source using multiple runs of a Bell test, we defer the definition of such a source to Section 5.4, where it can be more appropriately discussed.

A few other measures have been suggested in the literature that will not be examined closely in this thesis, such as the mutual information between the measurement choices and the underlying variable [93]

$$I(A, B : \lambda) = H(A, B) + H(\lambda) - H(A, B, \lambda), \tag{2.9}$$

where $H(A, B)$ denotes the Shannon entropy of the distribution $p(A_j, B_k)$ and so on, or the distance

$$M_a := \max_{j,k} \int d\lambda |p(\lambda|A_j, B_k) - \tilde{p}(\lambda)| \tag{2.10}$$

where $\tilde{p}(\lambda) = \int djdkp(A_j, B_k)p(\lambda|A_j B_k)$ is the average underlying distribution. The measures M_H and P have the advantage of not being dependent on the distributions $p(A_j, B_k)$, $p(A_j)$ and $p(B_k)$, which makes them more relevant to cryptographic applications where these distributions are not necessarily uniform[4], whilst M_K has a good operational interpretation and is more easily calculable as well as suited to more general Bell inequalities with non-uniform distributions for $p(\lambda)$.

2.3 Optimal CHSH Violation for a Single Shot

Perhaps the first serious discussion of exploiting the free will loophole appeared in [95], under the name of the 'stochastic decoupling' loophole. Whilst Feldmann derived a classical model without complete free will that violated CHSH, no attempt

[3] $N_1 = 2$ so our 1-norm definition (2.5) is recovered.

[4] For instance, the key distribution protocol in Chapter 4 employs a distribution with heavy bias towards the key generation settings over the CHSH testing settings for efficiency.

was made to suggest a quantitative measure for free will, nor discuss optimality. It wasn't until recent years that the topic again received significant interest, in light of related discussions of the effects of signalling [96] and determinism [97] on a classical model's ability to simulate quantum correlations.

The models in this section specify the 'measurement' outcomes deterministically, i.e. $p(a|A_j,\lambda) = -1$ or $+1$, similarly for $p(b|B_k,\lambda)$, such that all outcomes are given by deterministic functions of the underlying variable, $a_j(\lambda), b_k(\lambda) \in \{\pm 1\}$. Whilst indeterministic models will be of cryptographic use for evaluating the guessing probability in Chapter 3, it is helpful to consider only the relaxation of measurement independence here. Quantitative measures for (and bounds on Bell inequalities under relaxation of) indeterminism, as well as signaling, are described in [98], and further combined with relaxed measurement independence in [26].

Recall the CHSH expectation value from (1.3), defined as

$$S = \langle a_0 b_0\rangle + \langle a_0 b_1\rangle + \langle a_1 b_0\rangle - \langle a_1 b_1\rangle = \sum_{j,k\in\{0,1\}} (-1)^{jk}\langle a_j b_k\rangle. \tag{2.11}$$

With a local hidden variable model λ specifying both outputs $a_j(\lambda), b_k(\lambda)$ and input selection distribution $p(\lambda|A_j,B_k)$, one can further condition the CHSH value based on these choices. A specific choice of (j,k,λ) will lose the associated CHSH game when $a_j(\lambda)b_k(\lambda) \neq (-1)^{jk}$, i.e. when the assigned outcomes are different if $(j,k) \neq (1,1)$ and the same if $(j,k) = (1,1)$. Noting that

$$\langle a_j b_k\rangle = \sum_\lambda p(\lambda|A_j,B_k) a_j(\lambda) b_k(\lambda) \tag{2.12}$$

and defining

$$S_\lambda^{j,k} = (-1)^{jk} a_j(\lambda) b_k(\lambda), \tag{2.13}$$

we can thus rewrite (2.11) as either of

$$S = \sum_\lambda p(\lambda|A_j,B_k) S_\lambda^{j,k}, \tag{2.14}$$

$$S = \sum_{j,k} p(A_j,B_k|\lambda) S_\lambda^{j,k}. \tag{2.15}$$

The former expression is useful for evaluating S when considering M_H, since we are interested in the probabilities $p(\lambda|A_j,B_k)$, whilst the latter is convenient when considering M_K or P, as a function of $p(A_j,B_k|\lambda)$.

It turns out that a model of underlying variables, given by Tables I and II of [92] and slightly altered below, permits a CHSH value of $S = \min\{2+6M_H, 4\}$,

and therefore nonlocal correlations can be exhibited for any relaxation of free will ($M_H > 0$). Moreover, these models are optimal in the sense that no larger value of S is achievable for a given M_H. A proof for this appeared in Appendix B of [26], which simultaneously investigated relations with measures of no-signalling and indeterminism. We provide here an alternative proof that does not require those considerations. Note that the quantity P' in the following theorem refers simply to a parameter under Eve's control, and not specifically to the measurement independence measure introduced above. Of course, the two do coincide (in the sense that the model below has measurement independence $P = P'$) which motivates the choice of notation.

Theorem 1. *For a fixed measurement dependence M_H, the model with outcomes and probability densities specified by Tables 2.1 and 2.2 (using the shorthand notation $\rho_{jk}(\lambda) := p(\lambda|A_jB_k)$, and with parameters $P' \in [1/4, 1/3]$, $Q \in [0, 1/3]$) maximises the CHSH value as $S = \min\{2 + 6M_H, 4\}$.*

	$a_0(\lambda)$	$a_1(\lambda)$	$b_0(\lambda)$	$b_1(\lambda)$	$\langle a_0b_0\rangle_\lambda$	$\langle a_0b_1\rangle_\lambda$	$\langle a_1b_0\rangle_\lambda$	$-\langle a_1b_1\rangle_\lambda$
λ_0	1	1	1	1	1	1	1	-1
λ_1	1	-1	1	1	1	1	-1	1
λ_2	1	1	1	-1	1	-1	1	1
λ_3	1	-1	-1	1	-1	1	1	1

Table 2.1: Optimal outcome specifications and correlations maximising CHSH.

(a) $M_H \leqslant 1/3$

	$\rho_{00}(\lambda)$	$\rho_{01}(\lambda)$	$\rho_{10}(\lambda)$	$\rho_{11}(\lambda)$
λ_0	P'	P'	P'	$1-3P'$
λ_1	P'	P'	$1-3P'$	P'
λ_2	P'	$1-3P'$	P'	P'
λ_3	$1-3P'$	P'	P'	P'

(b) $M_H \geqslant 1/3$

	$\rho_{00}(\lambda)$	$\rho_{01}(\lambda)$	$\rho_{10}(\lambda)$	$\rho_{11}(\lambda)$
λ_0	Q	$\frac{1-Q}{2}$	$\frac{1-Q}{2}$	0
λ_1	$\frac{1-Q}{2}$	Q	0	$\frac{1-Q}{2}$
λ_2	$\frac{1-Q}{2}$	0	Q	$\frac{1-Q}{2}$
λ_3	0	$\frac{1-Q}{2}$	$\frac{1-Q}{2}$	Q

(c) Generic Model

	$\rho_{00}(\lambda)$	$\rho_{01}(\lambda)$	$\rho_{10}(\lambda)$	$\rho_{11}(\lambda)$
λ_0	p_{00}	p_{01}	p_{02}	p_{03}
λ_1	p_{10}	p_{11}	p_{12}	p_{13}
λ_2	p_{20}	p_{21}	p_{22}	p_{23}
λ_3	p_{30}	p_{31}	p_{32}	p_{33}

Table 2.2: (a) A model maximising CHSH violation S for fixed $M_H \leqslant 1/3$. (b) A model achieving the maximal CHSH value $S = 4$ for fixed $M_H \geqslant 1/3$. (c) Generic probability assignments used to prove optimality.

Proof. Firstly, we argue that only four underlying variables are needed to completely characterise the possible correlations for pairs of settings. If we write down the sixteen combinations for outcome values – $(1,1,1,1)$, $(1,1,1,-1)$ etc. – we can see that these combinations can be separated into equivalent pairs according to the four correlations $\langle A_j B_k \rangle$, $(j,k) \in \{0,1\}^2$, that they produce. Of these eight pairs, four produce exactly the negative of the correlations of the other four. Of course, S can range between -4 and 4, but to simplify matters we shall look at only the combinations that produce positive values of S, thus the four outcome sets as described by λ_n in the table (together with the conjugates $\overline{\lambda}_n$ which specify the negative of these sets, as explained in Definition 1 below) provide a complete characterisation for calculating S and M_H. The model in [92] is specified by five underlying variables, but observe that the same correlations are produced for λ_1 and λ_5, so these variables can be amalgamated.

For each underlying variable λ_n and each pair of measurement settings, the generic probability densities $p_{nj} := p(\lambda_n | A_{\lfloor j/2 \rfloor}, B_{j \bmod 2})$ are shown in Table 2.2(c). Clearly for a given measurement pair indicated by column j, we have $\sum_n p_{nj} = 1$ and so each column sums to 1 and the whole table sums to 4. We can thus reformulate S and M in terms of the generic probabilities as

$$S = 4 - 2 \sum_{j=0}^{3} p_{(3-j)j}, \tag{2.16}$$

$$M_H = \frac{1}{2} \max_{j,j'} \sum_n |p_{nj} - p_{nj'}|. \tag{2.17}$$

If we define $C_{jj'} := \sum_n |p_{nj} - p_{nj'}|$, that is the sum of the moduli of the differences between the entries in columns j and j', observe that by definition of M_H, $C_{jj'} \leqslant 2M_H$ for all j, j'. Furthermore, since all entries in the sum for $C_{jj'}$ are nonnegative, $m_{jj'} := |p_{(3-j)j} - p_{(3-j)j'}| + |p_{(3-j')j} - p_{(3-j')j'}| \leqslant C_{jj'} \leqslant 2M_H$ for any j, j'. We are interested in terms of this form due to the structure of S in (2.16). Particularly, any optimal model maximising S must have $p_{(3-j)j}$ as the smallest element in column j, thus

$$2M_H \geqslant m_{jj'} = p_{(3-j)j} - p_{(3-j)j'} + p_{(3-j')j} - p_{(3-j')j'}. \tag{2.18}$$

Summing (2.18) over all pairs of columns $j \neq j'$ yields

$$\begin{aligned} 24M_H \geqslant \sum_{j\neq j'} m_{jj'} &= \sum_{j\neq j'} \left(p_{(3-j)j} - p_{(3-j)j'} + p_{(3-j')j} - p_{(3-j')j'}\right) \\ &= 2\sum_{j\neq j'} p_{(3-j)j'} - 6\sum_{j} p_{(3-j)j} \\ &= 2\left(4 - \sum_{j} p_{(3-j)j}\right) - 6\sum_{j} p_{(3-j)j} \\ &= 8 - 8\left(\frac{4-S}{2}\right), \end{aligned} \tag{2.19}$$

where the last two lines follow from column normalisation and (2.16) successively. Thus for some fixed degree of measurement dependence M_H, we have $S \leqslant 2 + 6M_H$. This bound is tight for $M_H \leqslant 1/3$ and achieved by the optimal model proposed in Table 2.2(a), where the antidiagonal elements are the smallest elements of their respective columns as required, and the bound saturation follows from evaluating $S = 24P' - 4$ and $M_H = 4P' - 1$. Finally, note that for any fixed $M_H \geqslant 1/3$, a model with measurement dependence M_H achieving the maximum $S = 4$ is easily achievable by Table 2.2(b), where $M_H = Q$ over the range $Q \in [1/3, 1]$. Note that Tables 2.2(a) and 2.2(b) coincide when $P' = Q = 1/3$. □

Before continuing, a formal definition of a conjugate variable is required.

Definition 1. *The* conjugate *of an underlying variable λ is defined to be the underlying variable $\overline{\lambda}$ such that $a_j(\overline{\lambda}) = -a_j(\lambda)$ and $b_k(\overline{\lambda}) = -b_k(\lambda)$ for all j, k. Note that correlations are identical under either variable, i. e. $\langle a_j b_k\rangle_{\overline{\lambda}} = \langle a_j b_k\rangle_{\lambda}$ for all j, k. A model is* conjugate-inclusive *if it contains an equiprobable mixture of variables λ with their conjugates $\overline{\lambda}$, that is for each λ, $\rho(\lambda) = \rho(\overline{\lambda})$, and furthermore an identical measurement selection distribution, $p(\lambda|A_j, B_k) = p(\overline{\lambda}|A_j, B_k)$ for all j, k, λ. Unless stated otherwise, all models in this thesis are implicitly assumed to be conjugate-inclusive, where the fixture $\rho(\lambda) = p$ is a shorthand for $\rho(\lambda) = \rho(\overline{\lambda}) = p/2$.*

The reason for desiring models which are conjugate-inclusive is quite apparent. Neglecting to consider conjugates would raise suspicion by Alice and Bob of classically fixed outcomes, for instance in Table 2.1 Alice would always get outcome +1 when measuring with input 0. By including conjugates with equal probability, Eve's model will deliver local outcomes with expectation zero, as expected from a quantum implementation, whilst keeping the correlations unchanged for the purposes of evaluating a Bell expression (at least, those expressions such as CHSH which include only correlation terms in their definition).

The analytic optimality proof given above is sufficient for a single run of the experiment, but it will not suffice for a case where Eve correlates her strategy over many runs. Before investigating this problem in Chapter 5, we need some additional tools, namely methods to provide a numerical alternative to the previous analytic solution, for which we must prove the equivalence of the measures M_q (2.4), where $q \geqslant 1$, for the purposes of maximising the CHSH inequality.

Corollary 2. *The model described in Tables 2.1 and 2.2(a) maximises S for any fixed* $M_q <= M_{\max}$*, where* $q \geqslant 1$*.*

Proof. This model satisfies the relation $S = 2 + 6M_q$ for any q, so only the bound requires derivation. Observe that with the generic probability distribution,

$$\begin{aligned} M_q &= \left(\frac{1}{2}\max_{j,j'}\sum_n |p_{nj} - p_{nj'}|^q\right)^{\frac{1}{q}}, \\ 2M_q^q &\geqslant |p_{(3-j)j} - p_{(3-j)j'}|^q + |p_{(3-j')j} - p_{(3-j')j'}|^q \qquad \forall j, j' \\ &\geqslant \min_{a+b=m_{jj'}} a^q + b^q \end{aligned} \tag{2.20}$$

using $m_{jj'}$ as defined in the above theorem. Simple calculus (for instance, set $a = m_{jj'}\cos^2\theta, b = m_{jj'}\sin^2\theta$) shows the minimum attained at $a = b = m_{jj'}/2$, simplifying (2.20) as $M_q \geqslant m_{jj'}/2$. Again summing over all columns $j \neq j'$, $24M_q \geqslant \sum_{j\neq j'} m_{jj'}$, which via (2.19) gives the desired bound $S \leqslant 2 + 6M_q$. □

Finally, the optimal strategy for a fixed measurement dependence using the M_K and P measures is desirable. Whilst these measures consider $p(A_j, B_k|\lambda)$ rather than $p(\lambda|A_j, B_k)$, the optimal model is essentially the same.

Corollary 3. *For a fixed measurement dependence* M_K *or* P*, the model with outcomes specified by Table 2.1 and probability densities specified by Table 2.3, (using the shorthand notation* $\rho_{jk}(\lambda) := p(A_j, B_k|\lambda)$*, and with parameters* $Q \in [1/4, 1/3]$ *and* $R \in [1/3, 1]$*) maximises the CHSH value as* $S = \min\{2 + 6M_K, 4\}$ *or* $S = \min\{24P - 4, 4\}$*.*

Proof. Optimality proofs of these models for the M_K measure is easier than for the M_H proof above, and trivial for the P measure; Both are omitted here, and nevertheless are proved in the more general case of multiple-run attacks presented in Chapter 5 (where $N = 1$ recovers the single-shot strategies). The stated CHSH values are confirmed with the evaluations $S = 24Q - 4$, $M_K = 4Q - 1$ and $P = Q$ in Table 2.3(a), and $S = 4$, $M_K = 1/3$ for $R \in [1/3, 1/2]$ and $M_K = 2/3(2R - 1/2) \in [1/3, 1]$ for $R \in [1/2, 1]$, and $P = R$ in Table 2.3(b). □

(a) $M_K \leqslant 1/3, P \leqslant 1/3$

	$\rho_{00}(\lambda)$	$\rho_{01}(\lambda)$	$\rho_{10}(\lambda)$	$\rho_{11}(\lambda)$
λ_0	Q	Q	Q	$1-3Q$
λ_1	Q	Q	$1-3Q$	Q
λ_2	Q	$1-3Q$	Q	Q
λ_3	$1-3Q$	Q	Q	Q

(b) $M_K \geqslant 1/3, P \geqslant 1/3$

	$\rho_{00}(\lambda)$	$\rho_{01}(\lambda)$	$\rho_{10}(\lambda)$	$\rho_{11}(\lambda)$
λ_0	R	$\frac{1-R}{2}$	$\frac{1-R}{2}$	0
λ_1	$\frac{1-R}{2}$	R	0	$\frac{1-R}{2}$
λ_2	$\frac{1-R}{2}$	0	R	$\frac{1-R}{2}$
λ_3	0	$\frac{1-R}{2}$	$\frac{1-R}{2}$	R

Table 2.3: A model maximising CHSH violation S for fixed P or M_K.

The threshold value $M_{\max}$ is defined as the minimum measurement dependence required to attain the Bell inequality's no-signalling bound S_{NS}, where the measure used will be clear from the context. Clearly for the CHSH inequality $M_{\max} = 1/3$ using any of the measures M_H, M_K and P. In the following chapters $M_{\max}$ will be derived for other inequalities but little consideration is given beyond this threshold. Whilst Table 2.2(b) explicitly provides a model achieving maximal S for any $M_H > M_{\max}$, this is in fact quite obvious; Since the maximal S can be achieved from a model with $M_H = M_{\max}$ (by definition) and a model with $M_H = 1$ (such as $Q = 1$ in Table 2.2(b)), then a probabilistic mixture of these two models can obtain any intermediate value of M_H whilst maintaining $S = 4$, similarly for M_K or P. Furthermore, the crucial question for the following cryptographic scenarios is how little measurement independence do Alice and Bob need to ensure robustness against adversarial attack, and so only values of measurement dependence below $M_{\max}$ are of interest.

In fact, since no stronger-than-quantum physical theories are currently considered compatible with Nature, Alice and Bob will typically expect a more modest Bell violation constrained by the quantum theory, since anything higher by a statistically significant margin will send alarm bells ringing. For the CHSH test discussed here, Eve's model should only exhibit a measurement dependence value below $M_H = M_K = (\sqrt{2}-1)/3 \approx 0.138$ or $P < (2+\sqrt{2})/12 \approx 0.285$, to avoid violations above the quantum bound $2\sqrt{2}$.

Instead of fixing a limitation on measurement dependence, one could ask what fraction of runs of a CHSH experiment must sacrifice *absolute* free will in order to simulate singlet state correlations [1]. Table 2.4 provides an underlying model which with probability f uses complete free will ($P = 1/4$), and with probability $1-f$ exhibits full measurement independence ($P = 1/3$) with a deterministic exclusion[5]. Using (2.15), we see that $S = 4-2f$. Therefore, to simulate singlet state correlations of $S = 2\sqrt{2}$, free will must be given up in a fraction of runs $1-f = \sqrt{2}-1 \approx 41\%$.

The bounds and models derived in this chapter are summarised in Table 5.5.

[5]Conjugate inclusion as explained in Definition 1 is again implicitly assumed.

	$p(\lambda)$	$a_0(\lambda)$	$a_1(\lambda)$	$b_0(\lambda)$	$b_1(\lambda)$	$\rho_{00}(\lambda)$	$\rho_{01}(\lambda)$	$\rho_{10}(\lambda)$	$\rho_{11}(\lambda)$
λ_0	$(1-f)/4$	1	1	1	1	1/3	1/3	1/3	0
λ_1	$(1-f)/4$	1	-1	1	1	1/3	1/3	0	1/3
λ_2	$(1-f)/4$	1	1	1	-1	1/3	0	1/3	1/3
λ_3	$(1-f)/4$	1	-1	-1	1	0	1/3	1/3	1/3
λ_4	$f/4$	1	1	1	1	1/4	1/4	1/4	1/4
λ_5	$f/4$	1	-1	1	1	1/4	1/4	1/4	1/4
λ_6	$f/4$	1	1	1	-1	1/4	1/4	1/4	1/4
λ_7	$f/4$	1	-1	-1	1	1/4	1/4	1/4	1/4

Table 2.4: A model for which individual runs have a probability $1-f$ of full measurement dependence $(\lambda_0, \ldots, \lambda_3)$ and probability f of full measurement independence $(\lambda_4, \ldots, \lambda_7)$, where $\rho_{jk}(\lambda) = p(A_j, B_k|\lambda)$.

Chapter 3

Randomness Expansion With Limited Measurement Dependence

A randomness expansion protocol takes a pre-existing stock of perfect randomness as input and produces further randomness as output. The initial randomness is used to make measurement selections in a series of Bell tests, as well as for the ensuing privacy amplification (see Section 1.5.3). The outcomes to these tests are then used to produce the further randomness. Furthermore the privacy of this randomness, or alternatively the degree of an eavesdropper's power, is certified by the degree of Bell violation obtained from the outcome correlations, which in turn informs how much privacy amplification must be performed to ensure sufficiently private randomness.

Randomness expansion with untrusted devices was first proposed in Roger Colbeck's thesis [44] (later condensed into a paper [49]), testing for GHZ correlations (1.23). The concept was expanded to incorporate arbitrary Bell inequalities and implemented experimentally [48] and shown to be both robust against noise and secure from eavesdroppers with only classical side information [99, 100]. The experimental procedure has recently been improved by over 4 orders of magnitude [58]. However, one of the assumptions of these protocols is that Alice and Bob can select their measurements uniformly and independently, or equivalently that they hold trusted RNGs. The following chapter removes this assumption and considers the potential for private randomness expansion under limited measurement dependence, using the P measure (2.6) introduced in the previous chapter. In the following we will distinguish between no-signalling (Section 3.2) and an adversary being further (and more believably) restricted to using only quantum states and measurements (Section 3.3), in both cases assuming only single-shot attacks and testing for the CHSH inequality.

3.1 The Model

In this randomness expansion protocol, Alice and Bob use RNGs, as discussed in the previous chapter, to make their measurement selections A_j and B_k, where $j, k \in \{0, 1\}$, and record their respective measurement outcomes $a_j, b_k \in \{0, 1\}$ (with subscripts suppressed when the choice of input is clear). Eve manipulates both input and output probabilities using an underlying variable scheme λ to determine the conditional probability densities $p(\lambda|A_j, B_k)$ and $p(a, b|A_j, B_k, \lambda)$, which are related via Bayes' Theorem,

$$p(a, b|A_j, B_k) = \int d\lambda p(a, b|A_j, B_k, \lambda)p(\lambda|A_j, B_k). \tag{3.1}$$

The probability distribution of the outputs $p(a, b|A_j, B_k)$ is determined by Alice and Bob over many runs of the experiment, as well as the measurement selection distribution $p(A_j, B_k)$ which Eve must make sure is the uniform $(\frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4})$ distribution, as expected from a CHSH test, to avoid suspicions.

The marginal probabilities for the outcomes are

$$\begin{aligned} p^{(A)}(a|A_j, \lambda) &= p^{(A)}(a|A_j, B_k, \lambda) = \sum_b p(a, b|A_j, B_k, \lambda), \\ p^{(B)}(b|B_k, \lambda) &= p^{(B)}(b|A_j, B_k, \lambda) = \sum_a p(a, b|A_j, B_k, \lambda), \end{aligned} \tag{3.2}$$

where the first equality in each line is consistent with either choice of B_k (or A_j) by the constraints of no-signalling (see Section 1.4.2). Note that the outcomes are indeterministically generated, in contrast to the deterministic examples given in Chapter 2. This indeterminism plays a vital role in estimating the *guessing probability* or *predictability*, introduced in Section 1.5.3 as the probability with which Eve correctly guesses a generated bit. By introducing indeterminism into her model, Eve can achieve larger CHSH violations at the expense of knowledge of the outcomes [98].

The guessing probability is upper bounded by the largest of the marginal probabilities (3.2), whether on the side of Alice or Bob, since Eve will do best to guess the most likely candidate. For a given λ, this is given by

$$G(\lambda) = \max_{a,b,j,k} [p^{(A)}(a|A_j, \lambda), p^{(B)}(b|B_k, \lambda)] \tag{3.3}$$

and without knowledge of λ, such as for Alice or Bob, the guessing probability is weighted over all λ as

$$G = \int d\lambda p(\lambda)G(\lambda). \tag{3.4}$$

This quantity is the average of Eve's maximum guessing probabilities conditioned on λ. Of course, if Eve has access to λ (as we assume she does), her guessing probability may vary and Alice and Bob can only work to bound the guessing probability in the average case. The model is completely deterministic when $G = 1$. Since $G(\lambda) \geqslant 1/2$, it must be that $G(\lambda) = 1/2$ for all λ when $G = 1/2$, so that the model is completely indeterministic for Eve as well as for Alice and Bob by definition.

An estimate of G will be dependent on the degree of manipulation Eve employs, which can be measured using any one of the free will measures (M_H, M_K, P) discussed in the previous chapter, although it is simplest to consider P. We present bounds on G subject to a fixed P and an observed CHSH violation of S, assuming eavesdroppers with both no-signalling and quantum capabilities. The implications of these predictability bounds for the privacy amplification step of a randomness expansion protocol is discussed in Section 3.4.

3.2 No-signalling Bounds and Strategies

The CHSH game played can be characterised by the correlation function[1]

$$S = \Big| \sum_{a,b,j,k \in \{0,1\}} (-1)^{a+b+jk} p(a,b|A_j,B_k) \Big| \tag{3.5}$$

and is bounded above, according to Eve's models guessing probability G and free will measure P, by the following theorem.

Theorem 4. *The maximum possible CHSH expectation value $S_{NS}^{\max}(G,P)$, for a guessing probability G and free will parameter P, for any no-signalling model with $p(A_j,B_k) = \frac{1}{4}$ (i.e. all inputs are equally likely), is*

$$S_{NS}^{\max}(G,P) = \begin{cases} 4 - 8(2G-1)(1-3P) & P \leqslant \frac{1}{3}, \\ 4 & P \geqslant \frac{1}{3}. \end{cases} \tag{3.6}$$

Optimality was proved in Appendix A of [1], the proof itself being an extension of Hall's proof for the non-cryptographic scenario in Appendix B of [26]. An optimal model obtaining the maximum possible CHSH value for fixed G and P was also given in [1], and is replicated in Table 3.1 below for convenience.

There are several borderline cases of the above theorem which make intuitive sense. $G = \frac{1}{2}$ corresponds to a fully indeterministic model which gives Eve no helpful

[1]This expression is different from (2.14) and (2.15) since we no longer assume deterministic outcome choices, but the correlation function can similarly be derived from (2.11).

information, and with which Alice and Bob may share any no-signalling distribution, enabling $S \leqslant 4$. In the case of $P = \frac{1}{4}, G = 1$, Eve does not manipulate the RNGs' measurement selection distribution and deterministically sets the outcomes, therefore Alice and Bob have complete free will and their CHSH score adheres to the LHV bound of $S \leqslant 2$. Finally, when $P = 1, G = 1$, Eve deterministically programs both the measurement choices and the measurement outcomes to yield any CHSH violation S up to 4.

λ	A_jB_k	$p(A_j, B_k\|\lambda)$	$\rho_{jk\lambda}(00)$	$\rho_{jk\lambda}(01)$	$\rho_{jk\lambda}(10)$	$\rho_{jk\lambda}(11)$
λ_0	A_0B_0	P	G	0	0	$1-G$
	A_0B_1	P	G	0	0	$1-G$
	A_1B_0	P	G	0	0	$1-G$
	A_1B_1	$1-3P$	$2G-1$	$1-G$	$1-G$	0
λ_1	A_0B_0	P	G	0	0	$1-G$
	A_0B_1	P	G	0	0	$1-G$
	A_1B_0	$1-3P$	$1-G$	0	$2G-1$	$1-G$
	A_1B_1	P	0	$1-G$	G	0
λ_2	A_0B_0	P	G	0	0	$1-G$
	A_0B_1	$1-3P$	$1-G$	$2G-1$	0	$1-G$
	A_1B_0	P	G	0	0	$1-G$
	A_1B_1	P	0	G	$1-G$	0
λ_3	A_0B_0	$1-3P$	$1-G$	$2G-1$	0	$1-G$
	A_0B_1	P	G	0	0	$1-G$
	A_1B_0	P	$1-G$	0	0	G
	A_1B_1	P	0	$1-G$	G	0

Table 3.1: Optimal indeterministic model with guessing probability G, for $\frac{1}{4} \leqslant P \leqslant \frac{1}{3}$, specifying for each underlying λ and measurement pair (A_j, B_k) the probability $p(A_jB_k|\lambda)$ of measurement selection and the probabilities $\rho_{jk\lambda}(ab) := p(a, b|A_j, B_k, \lambda)$ of obtaining the outcomes a and b.

For the purposes of randomness expansion, Alice and Bob wish to tightly bound G subject to a fixed CHSH value S and measurement independence P. Whilst it has not been possible with the algebra involved to do this directly, Theorem 4 allows Alice and Bob to do this in a roundabout way. For instance, if Alice and Bob measure a CHSH correlation $S^* \leqslant S_{NS}^{\max}(1, P) = 24P - 4$, they know that a deterministic model could have feasibly been preprogrammed by Eve and should abort the protocol. Conversely, if $S^* > S_{NS}^{\max}(1, P)$, Alice and Bob know that $G < 1$ and can determine an upper bound. When $P < \frac{1}{3}$ this bound is given by

$$G(S^*, P) \leqslant \min\left\{\frac{1}{2}\left(1 + \frac{4 - S^*}{4 - S_{NS}^{\max}(1, P)}\right), 1\right\}, \qquad P < \frac{1}{3}. \tag{3.7}$$

A plot of $G(S^*, P)$ for various observed violations S^* is given in Figure 3.1.

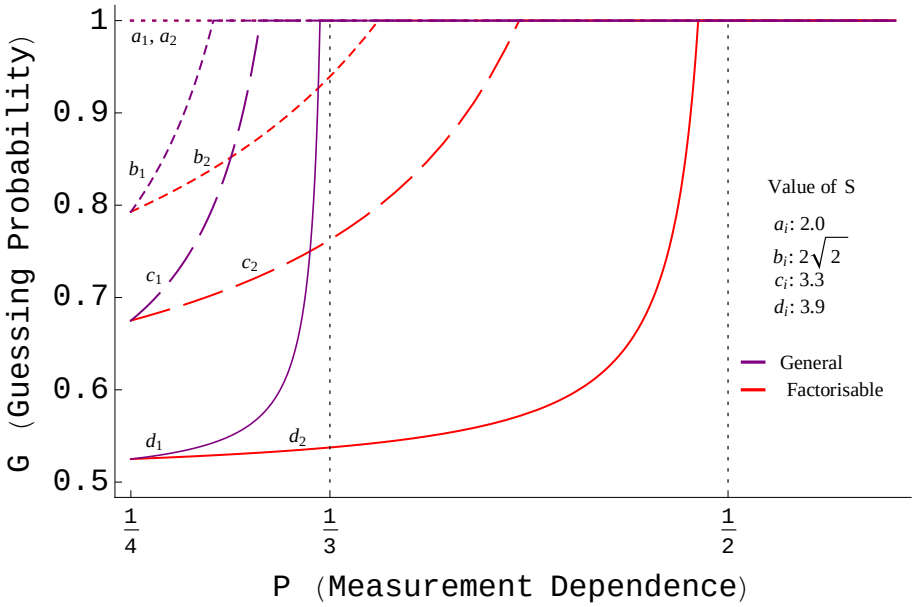

Figure 3.1: Optimal guessing probability $G(S, P)$ for no-signalling models at different CHSH expectation values, including $S = 2$ (local deterministic) and $S = 2\sqrt{2}$ (Tsirelson bound). In the cases of general and factorizable distributions, the optimal guessing probabilities approach the vertical dotted lines as S goes to 4.

Although Theorem 4 applies to any no-signalling distribution Eve wishes to employ, it is also wise to consider placing the restriction that the distribution be factorisable, i.e. $p(A_j, B_k|\lambda) = p^{(A)}(A_j|\lambda)p^{(B)}(B_k|\lambda)$. Whilst a non-factorisable distribution can be made factorisable through the addition of extra hidden variables, the measurement dependence P would be affected. For a fixed P, quantum technology is needed to generate such distributions, for example with RNGs sharing the state $|\phi_\lambda\rangle = \sum_{j,k} \sqrt{p(A_j, B_k|\lambda)}\,|j\rangle \otimes |k\rangle$. The factorisability condition allows for a weaker class of variable-free-will models in the absence of such technology.

Corollary 5. *The maximum possible CHSH expectation value $S^{\max}_{fac}(G, P)$, for a guessing probability G and free will parameter P, for any no-signalling model with $p(A_j, B_k) = \frac{1}{4}$ and factorisable distribution $p(A_j, B_k|\lambda)$, is*

$$S^{\max}_{fac}(G, P) = \begin{cases} 4 - 4(2G - 1)(1 - 2P) & P \leqslant \frac{1}{2} \\ 4 & P \geqslant \frac{1}{2}, \end{cases} \tag{3.8}$$

Proof of optimality and provision of an optimal model is also found in Appendix A of [1]. The restriction to factorisable distributions clearly lessens Eve's capabilities,

reducing the corresponding upper bound on G for a fixed P and observed S^*. Figure 3.1 compares this bound for the optimal general and factorisable distributions. Note that in the case of complete free will ($P = 1/4$), the bound on G reduces to $G \leqslant \frac{3}{2} - \frac{S}{4}$, as derived in [48].

3.3 Quantum Bounds and Strategies

The previously derived bounds apply under the weak assumption of no-signalling, which means that Eve might be able to supply Alice and Bob with any no-signalling distribution, such as a P-R box [19, 29, 20], giving the maximal violation of the CHSH inequality. However, assuming the validity of quantum mechanics, Eve can achieve only much lower limits; in the case of $P = \frac{1}{4}$, she can do no better than $S = 2\sqrt{2 - (2G-1)^2}$ ([48], alternatively proved in Appendix A.) In the case of $P > \frac{1}{4}$, Alice and Bob perform a CHSH test and calculate their expectation value averaged over all runs of the experiment, as before.

Theorem 6. *Suppose Alice and Bob play a measurement-biased version of the CHSH game with the correlation function*

$$S = 4 \left| \sum_{a,b,j,k} (-1)^{a+b+jk} p_{jk} p(a,b|A_j, B_k) \right|, \tag{3.9}$$

where $p_{jk} = p(A_j, B_k)$ and the measurement selection distribution $\overline{p} = (p_{jk})$ may be non-uniform. The maximum CHSH score achievable with quantum technologies is given by

$$S_Q^{\max}(\overline{p}) = \begin{cases} 4\sqrt{p_{00}p_{01} + p_{10}p_{11}} \sqrt{\frac{p_{00}^2 + p_{01}^2}{p_{00}p_{01}} + \frac{p_{10}^2 + p_{11}^2}{p_{10}p_{11}}} & \sum_{j,k} (p_{jk})^{-1} \geqslant \frac{2}{p_{\min}}, \\ 8 - 4p_{\min} & \sum_{j,k} (p_{jk})^{-1} < \frac{2}{p_{\min}}. \end{cases} \tag{3.10}$$

Proof. We derive the generalized Tsirelson bound for this class of games and find a scheme of quantum measurements that satisfy this bound. Consider

$$S_Q(\overline{p}) = 4 \Big| \sum_{j,k \in \{0,1\}} (-1)^{jk} \langle \psi \,|\, p_{jk} A_j B_k \,|\, \psi \rangle \Big| \tag{3.11}$$

We first derive necessity of the Tsirelson bound, which makes no assumptions on the quantum state used (although we show later that a two-qubit state is sufficient). In the black-box scenario, Alice and Bob interpret the outputs of their measurements as ± 1 values, imposing that the A_j and B_k have these as their eigenvalues, i.e. are Pauli-like. This maximisation was achieved in a restricted scenario in [101], which

gave the maximum value of S when the measurement distribution exhibits only local bias. We extend their methods to the more general case that can be implemented by Eve.

First, we formulate a Tsirelson–type bound on the expectation of outcome correlations, using the matrix norm $||M||$ defined as the eigenvalue of M with maximum modulus, which has the property $||M|| \leqslant \sqrt{||M^2||}$.

$$\begin{aligned} \frac{S_Q(\overline{p})}{4} &\leqslant ||A_0 \otimes (p_{00}B_0 + p_{01}B_1)|| + ||A_1 \otimes (p_{10}B_0 - p_{11}B_1)|| && (3.12) \\ &\leqslant ||\mathbb{1} \otimes (p_{00}B_0 + p_{01}B_1)|| + ||\mathbb{1} \otimes (p_{10}B_0 - p_{11}B_1)|| \\ &\leqslant \sqrt{p_{00}^2 + p_{01}^2 + p_{00}p_{01}\alpha} + \sqrt{p_{10}^2 + p_{11}^2 - p_{10}p_{11}\alpha}, && (3.13) \end{aligned}$$

where

$$\alpha = \langle \psi \,|\, I \otimes (B_0B_1 + B_1B_0) \,|\, \psi \rangle \,. \tag{3.14}$$

By setting $\frac{\partial}{\partial\alpha} S_Q(\overline{p}) = 0$, the value of α obtaining maximum $S_Q(\overline{p})$ is

$$\alpha = \frac{p_{00}^2 p_{01}^2 (p_{10}^2 + p_{11}^2) - p_{10}^2 p_{11}^2 (p_{00}^2 + p_{01}^2)}{p_{00}p_{01}p_{10}p_{11}(p_{00}p_{01} + p_{10}p_{11})}. \tag{3.15}$$

Substituting (3.15) into (3.13), we obtain

$$S_Q^{\max}(\overline{p}) = 4\sqrt{p_{00}p_{01} + p_{10}p_{11}} \sqrt{\frac{p_{00}^2 + p_{01}^2}{p_{00}p_{01}} + \frac{p_{10}^2 + p_{11}^2}{p_{10}p_{11}}}. \tag{3.16}$$

The physical limit to (3.14) is $|\alpha| \leqslant 2$, which in terms of the p_{jk} in (3.15) can be written as

$$\frac{1}{p_{00}} + \frac{1}{p_{01}} + \frac{1}{p_{10}} + \frac{1}{p_{11}} - \frac{2}{p_{\min}} \geqslant 0. \tag{3.17}$$

For the physically impossible case of $\alpha \geqslant 2$, the best approach is to use $\alpha = 2$, for which the quantum bound (3.16) coincides with the optimal deterministic strategy $S_D^{\max}(\overline{p}) = 4 - 8p_{\min}$, which is achieved for example, if $p_{\min} = p_{11}$, by pre-programming the devices to always output $+1$ regardless of the input.

We now show that for all $\overline{p}$ with $-2 < \alpha < 2$ there exists a quantum strategy that achieves the quantum bound given in (3.16), which exceeds the deterministic bound $S_D^{\max}(\overline{p})$. This strategy is achievable using a two-qubit state $|\,\psi\rangle = \frac{1}{\sqrt{2}}(|\,00\rangle + |\,11\rangle)$, by using freedom over local unitaries to specify that $B_0 = X$ and $B_1 = X\cos\beta + Z\sin\beta$. The condition (3.14) instantly imposes that $2\cos\beta = \alpha$. One can readily verify that the correct expectation value can be realised by using the initial state and

measurement settings

$$\begin{aligned} |\psi\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \\ A_0 &= \frac{(p_{00} + p_{01}\cos\beta)X + p_{01}\sin\beta Z}{\sqrt{(p_{00} + p_{01}\cos\beta)^2 + (p_{01}\sin\beta)^2}}, \\ A_1 &= \frac{(p_{10} - p_{11}\cos\beta)X - p_{11}\sin\beta Z}{\sqrt{(p_{10} - p_{11}\cos\beta)^2 + (p_{11}\sin\beta)^2}}, \\ B_0 &= X, \\ B_1 &= X\cos\beta + Z\sin\beta. \end{aligned} \tag{3.18}$$

A_0 and A_1 are the normalized versions of the operators $p_{00}B_0+p_{01}B_1$ and $p_{10}B_0-p_{11}B_1$ respectively. This choice was made in order for the equality to hold in (3.13). □

The proof of this theorem will also be helpful to proving a similar result in the key distribution scenario in Chapter 4, and we can immediately apply it here to the current randomness expansion context through the following two corollaries, the first of which will also be used when analysing multiple-run quantum attacks in Section 5.3.2.

Corollary 7. *Using a preprogrammed model with measurement dependence P, an observed uniform measurement selection $p(A_j, B_k) = \frac{1}{4}$, and supplemented by quantum technologies, the maximum achievable CHSH score is given by*

$$S_Q^{\max}(P) = \begin{cases} \frac{4(1-2P)^{3/2}}{\sqrt{1-3P}} & P \leqslant \frac{3}{10}, \\ 24P - 4 & P > \frac{3}{10}. \end{cases} \tag{3.19}$$

Proof. We first make an observation about symmetry in the probabilities. First note that in (3.12) the terms were grouped according to Alice's operators. Since Alice's and Bob's operators have entirely the same characteristics, we can group the terms according to Bob's operators. Doing so results in exactly the same bound on the quantum violation (for which we can specify a similar-looking measurement scheme which satisfies this bound) but with the probabilities p_{01} and p_{10} interchanged throughout. Furthermore, by observation the bound (3.10) is symmetric under the exchange of p_{00} with p_{01} and under the exchange of p_{10} with p_{11}. Taking these two observations together, both the bound (3.10) and the conditions defining its regime change must be symmetric under any permutation of the probabilities and thus does not require any ordering of the probabilities.

We now investigate the measurement distribution $\overline{p}$ which yields the largest violation for a given $P = \max\{p_{00}, p_{01}, p_{10}, p_{11}\}$. By the above symmetry property, we

can without loss of generality choose the largest and smallest of these probabilities to be, say, $p_{00} = p_{\max}$ and $p_{11} = p_{\min}$. The normalisation is

$$p_{00} = 1 - p_{01} - p_{10} - p_{11}.$$

To find the optimal choice of $S_Q^{\max}$, we differentiate it with respect to p_{01}. This derivative is non-negative in the range $p_{01} \in [p_{\min}, p_{\max}]$, and zero if and only if $p_{01} = p_{\max} = P$, thus this choice maximizes $S_Q^{\max}$. By symmetry, we also demand that $p_{10} = P$. Therefore the optimal measurement distribution (up to permutations) is $(P, P, P, 1-3P)$. Via Eq. (3.17), we see that such a quantum strategy gives an advantage over deterministic strategies only when $P < \frac{3}{10}$. When $\frac{3}{10} \leqslant P \leqslant \frac{1}{3}$, this distribution still yields the largest violation, but is achieved through a deterministic strategy with $S_Q^{\max} = 24P - 4$.

Of course, Alice and Bob are expecting to observe a uniform measurement selection distribution $p(A_j, B_k) = \frac{1}{4}$ so Eve's model must achieve this. Fortunately, by the symmetry property above, and inspired by the local model in Table 2.2 (a), Eve may take an equiprobable mixture of the distributions $(P, P, P, 1-3P)$, $(P, P, 1-3P, P)$, $(P, 1-3P, P, P)$ and $(1-3P, P, P, P)$, along with the corresponding optimal measurement schemes, to achieve an observed uniform measurement selection over many runs. □

Corollary 8. *The maximum possible CHSH expectation value $S_Q^{\max}(G, P)$, for a guessing probability G and free will parameter P, for any quantum model with uniform observed distribution $p(A_j, B_k) = \frac{1}{4}$ occurs at $G = \frac{1}{2}$ when $P < \frac{3}{10}$:*

$$S_Q^{\max}(\frac{1}{2}, P) = \frac{4(1-2P)^{3/2}}{\sqrt{(1-3P)}}. \tag{3.20}$$

For $P \geqslant \frac{3}{10}$, a deterministic strategy is used, and hence, $S_Q^{\max}(1, P) = S^{\max}(1, P)$.

Proof. Having specified the measurement selection distribution for each run (according to the choice of λ) in her hidden variable model, Eve just has to optimise her quantum strategy for each of the different values of λ independently, and the corresponding probabilities $p(A_j, B_k|\lambda)$. This corresponds to Alice and Bob playing the measurement-biased CHSH game with the correlation function

$$S(\lambda) = 4\Big| \sum_{a,b,j,k} (-1)^{a+b+jk} p(a, b|A_j, B_k) p(A_j, B_k|\lambda) \Big|. \tag{3.21}$$

which is optimised by the measurement strategy (3.18) and the measurement distribution $(P, P, P, 1-3P)$ up to permutations as proved above. Since $|\psi\rangle$ is a maximally

entangled state, we know that the guessing probability $G = \frac{1}{2}$. It remains to prove that this strategy is unique up to local unitaries, i.e. that there isn't another strategy with a higher G. We already know that Bob's operators are uniquely specified up to local unitaries. In order to see that Alice's operators are also uniquely specified, it suffices to realise that in order to saturate the bound (3.13), it must be that $|\psi\rangle$ must simultaneously be the maximal eigenvector of $A_0 \otimes (p_{00}B_0 + p_{01}B_1)$ and $A_1 \otimes (p_{10}B_0 - p_{11}B_1)$. We again use local unitary freedom, this time on Alice's side, to specify A_0 as in (3.18), and let $A_1 = X\cos\gamma + Z\sin\gamma$. We can now diagonalise both operators and ascertain when they have a simultaneous maximal eigenvector. Up to sign changes such as $\gamma \mapsto -\gamma$ (which are associated with a further local unitary freedom), the unique result is that of the A_1 used previously. It is then easy to check that the overall operator has only one maximal eigenvector, which is $|\psi\rangle$. Hence, we can conclude that in the quantum limit (and within the quantum regime), $G = \frac{1}{2}$. Of course, in the region $\alpha = 2$ we know that $G = 1$.

When $\frac{3}{10} \leqslant P \leqslant \frac{1}{3}$, this distribution still yields the largest violation, but is achieved through a deterministic strategy with $S_{NS}^{\max}(1, P) = 24P - 4$. □

We have not succeeded in finding a closed form for the general $S_Q^{\max}(G, P)$ trade-off in the quantum strategy, except for recovering known limits such as $P = \frac{1}{4}$ and $G = 1$, and thus cannot analytically bound G for a given P and observed S^* in a similar manner to (3.7) for the quantum regime, although this can be solved numerically. Nevertheless the maximally deterministic and maximally indeterministic regimes can be compared as in Figure 3.2.

Since Eve clearly has access to quantum technology, there is no reason to restrict the probability distribution $\overline{p}$ to be factorisable. Nevertheless, one would obtain

$$S_{Q,\text{fac}}^{\max}(\frac{1}{2}, P) = 4\sqrt{4P^2 + (1-2P)^2},$$

for any $\frac{1}{4} \leqslant P < \frac{1}{2}$.

3.4 Privacy Amplification

For the task of randomness expansion, we need to evaluate the amount of true randomness that we can produce via post-processing from the above bounds on G. As described in Section 1.5.3, the degree to which this can be achieved is characterised by the min-entropy, which is used by a classical randomness extraction procedure in order to condense the original output string to a new string which sacrifices length for absolute privacy. For a single run, the min-entropy is defined to

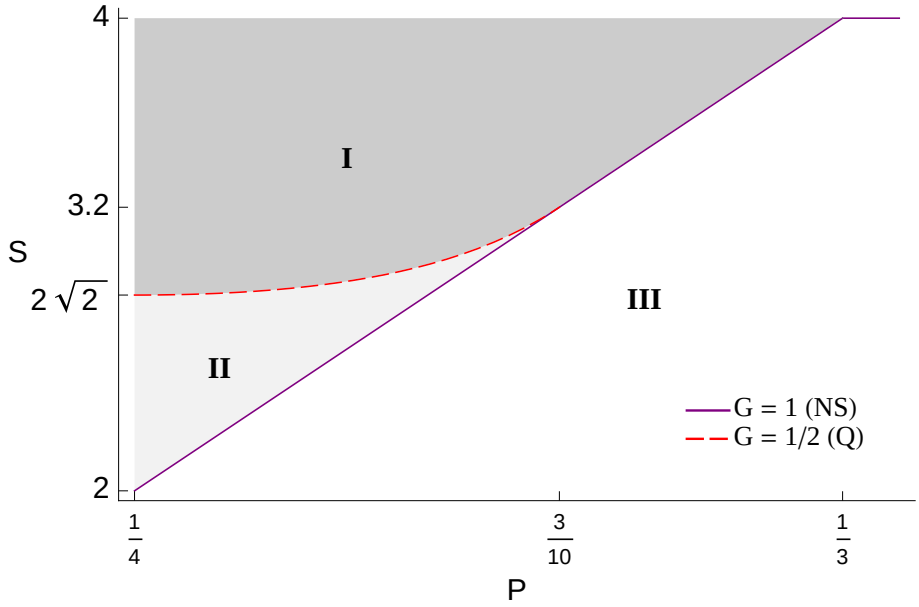

Figure 3.2: The maximal CHSH expectation value $S^{\max}(G, P)$ plotted against the free will parameter P, for the no-signalling (NS) $G = 1$ model (solid line), and the quantum (Q) $G = \frac{1}{2}$ model (dashed line). Region III (unshaded) can be explained by a deterministic $G = 1$ model. In regions I (darker gray) and II (lighter gray), the results cannot be deterministic; Eve cannot know the outputs with certainty. Regions II and III together give the set of (P, S) values that may be attained by a quantum model.

be $H_{\min}(p(ab|jk)) = -\log_2 \max_{a,b,j,k} p(ab|jk)$ [52], which is clearly bounded from below by $-\log_2 G$. For experimental estimation of a Bell violation, a Bell test must be performed on the devices many times in succession, requiring a bound for the min-entropy over a series of N runs. Assuming that Eve can only perform a collective attack without memory, i.e. that the devices behave independently and identically in each run, then $p(\boldsymbol{ab}|\boldsymbol{jk}) = \prod_{n=1}^{N} \tilde{p}(a_n b_n|j_n k_n)$ by independence and so $H_{\min}(p(\boldsymbol{ab}|\boldsymbol{jk})) \geqslant -N \log_2 G$ [48]. A more sophisticated analysis is necessary to bound the min-entropy when Eve employs correlated attacks over many runs of an experiment, as indicated by the analysis in Chapter 5.

Existing privacy amplification methods rely on the use of a perfectly random seed to, for instance, select uniformly from a family of hashing functions. In the scenario of limited measurement independence, where Alice and Bob's RNGs are already contaminated, such perfect randomness may not be possible. Assuming only memoryless collective attacks by Eve, we can outline an effective privacy amplification strategy. Suppose that Alice and Bob have succeeded in generating a string of bits

x_k, and have obtained a bound on Eve's maximum probability for guessing any one of Alice's bits, G. If Alice takes N such bits and XORs them, the resulting output bit can be guessed by Eve only if she has incorrectly guessed an even number of the outcomes of the individual measurements, which occurs with probability $(1+(2G-1)^N)/2$. As N becomes large, this tends to $1/2$. By setting an allowable threshold ϵ and choosing $N = \log(\epsilon)/\log(2G-1)$, Alice and Bob can pick their desired bound on security of the generated bit as a compromise on the number of raw key bits required to calculate it. Privacy amplification procedures where Eve employs a more sophisticated attack than the collective attack are discussed in [41]. It is an open question as to how privacy amplification methods may be made robust against such sophisticated attacks in the case of limited measurement independence.

Chapter 4

Key Distribution With Limited Measurement Dependence

The problem of obtaining perfectly secure communication between two parties, as explained in Section 1.5, can be conveniently filtered down to the simple primitive of key distribution. Alice and Bob need to generate a random binary string secure from Eve, which they can then use for both encryption and decryption. Since the key can be used only once to maintain security [51], key distribution should be as efficient as possible to allow for large amounts of data encryption.

Whilst the key should be perfectly random, key distribution differs from the randomness generation scenario of Chapter 3 in the use of an extra practical assumption, namely that the two parties are separated in different laboratories. They have access to quantum technologies but may only communicate through classical channels, accessible to eavesdroppers. Much like randomness generation, performing this task is reliant on conducting a series of Bell tests and appropriately processing the results afterwards. The first entanglement-based key distribution scheme was proposed by Ekert [11] in 1991[1], and here we discuss a variant of this protocol, based on [56], that will be adapted to consider limited measurement dependence in Section 4.4[2].

[1]This was not the first quantum key distribution scheme to be proposed. Bennett and Brassard's 'BB84' protocol [10], an example of a *prepare-and-measure* scheme, requires one party to produce a qubit in one of the four basis states of two mutually orthogonal bases, such as $\{|0\rangle, |1\rangle\}$ and $\{\frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)\}$, and the other party to measure each qubit in one of these bases. However, this protocol requires trusted devices from both parties, and the outcomes do not carry the same device-independent security guarantees as correlations produced by nonlocality tests.

[2]A related paper is [102], which considers weak randomness in quantum key distribution using the CGLMP inequality.

4.1 A Quantum Key Distribution Protocol

The QKD protocol presented here has a setup that is remarkably similar to the CHSH experiment, with the addition of an extra measurement input. We forgo possible experimental implementations, though typically one may use polarisation analysers to measure the polarisation of photons emitted from a source producing pairs of entangled photons (see Section 1.8). Whilst there are protocols based on the CHSH test with only two settings on each device, and the subsequent key being produced by classical post-processing on the outcomes [103], we do not wish to investigate the effects of limited measurement dependence in such a scenario, and consider instead a protocol that gives Bob an extra measurement setting with which to efficiently generate key bits.

In a single run of the protocol, Alice and Bob each receive a single qubit from the maximally entangled Bell state $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and select randomly and independently from their choice of inputs, $j \in \{0, 1\}$ for Alice and $k \in \{0, 1, 2\}$ for Bob. They then perform the measurements A_j and B_k respectively on their qubits, which are projective with outcomes $a_j, b_k \in \pm 1$. The measurement operators are designed to maximise the CHSH inequality and is thus equivalent to the scheme (1.6), up to permutations of players and measurement operators, with Bob's extra measurement fixed as $B_2 = A_0$:

$$A_0 = Z, \quad A_1 = X, \quad B_0 = \frac{1}{\sqrt{2}}(Z + X), \quad B_1 = \frac{1}{\sqrt{2}}(Z - X), \quad B_2 = Z. \tag{4.1}$$

After many runs of the experiment, the two parties announce the inputs they used and process the outputs according to which measurement pair was used. For $(j, k) \in \{(0, 0), (0, 1), (1, 0), (1, 1)\}$, the outputs are used in a standard CHSH evaluation to calculate the expectation $\langle\psi|\mathcal{S}|\psi\rangle$ of the operator $\mathcal{S} = A_0B_0 + A_0B_1 + A_1B_0 - A_1B_1$, which according to the above scheme will approach $2\sqrt{2}$, the maximal value achievable within quantum theory.

If instead Alice and Bob choose $(j, k) = (0, 2)$, they know they performed the same measurement on their constituent qubits of $|\psi\rangle$ and so their outcomes will be perfectly correlated, allowing distillation of an identical key on both sides[3]. Finally, the data from inputs $(j, k) = (1, 2)$ is not used for either key generation or security tests, but with the orthogonality of A_1 and B_2 in the above scheme, the measurements

[3]Some protocols, such as those instead distributing singlet states $\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$, will actually produce perfectly anticorrelated outcomes under the key generation settings, though an identical key can easily be distilled by Bob simply flipping all of his outcomes.

satisfy $\langle\psi \,|\, A_1 B_2 \,|\, \psi\rangle = 0$. This data does not bear any importance in a standard QKD protocol where the device's operations are trusted, but will provide a helpful checking mechanism against adversaries when later assuming device independence.

Any attempt by Eve to eavesdrop by intercepting and measuring the entangled qubits introduces a "physical element of reality" to the measured property, thus subsequent measurements by Alice and Bob of these qubits adhere to the local bound of the CHSH inequality and reduce the overall expectation of S. Alice and Bob may choose as close a value of $\langle S\rangle$ to $2\sqrt{2}$ as to satisfy their suspicions; If the value is not high enough, they either abort the protocol and start over, otherwise they perform privacy amplification to distil a secure key through classical methods.

Since it is desirable to have highly efficient key distribution, the measurement selections are typically not uniform and are heavily biased towards the key generation settings. In this case, whilst Alice does pick her input $j \in 0, 1$ with probability $\frac{1}{2}$, Bob picks his key setting $k = 2$ with high probability ϵ and the CHSH testing settings each with probability $(1-\epsilon)/2$, thus their joint measurement settings have the probability distribution given in the table below.

$p(A_0B_0)$	$p(A_0B_1)$	$p(A_1B_0)$	$p(A_1B_1)$	$p(A_0B_2)$	$p(A_1B_2)$
$\frac{1-\epsilon}{4}$	$\frac{1-\epsilon}{4}$	$\frac{1-\epsilon}{4}$	$\frac{1-\epsilon}{4}$	$\frac{\epsilon}{2}$	$\frac{\epsilon}{2}$

Table 4.1: Observed measurement selection probabilities in a key distribution protocol.

As described above, this key distribution protocol clearly guarantees security when Alice and Bob hold trusted devices, but it has been shown to also provide such guarantees in a device-independent scenario [57] assuming complete experimental free will. In the following, this protocol will be adapted to consider an adversarial attack where Eve also has the ability to manipulate the RNGs with which Alice and Bob select their measurements through some preprogramming λ (which as before specifies the probabilities $p(A_j, B_k|\lambda)$ and either the measurement operators in a quantum strategy or the outcomes themselves in a deterministic strategy), although as with the randomness expansion analysis we will consider only single-shot attacks.

With either the classical or quantum attack, the strategies must of course emulate the observed measurement selection distributions in Table 4.1 to avoid suspicion from Alice and Bob. Eve's information on the generated key, for a single-shot strategy, is characterised by the probability K of correctly guessing a generated key bit, known as the *key predictability*. This is essentially identical to the guessing probability G in the randomness expansion analysis, which allows Alice and Bob to bound Eve's

information about the key and perform the requisite privacy amplification. However, we shall use the K notation to emphasise the key distribution scenario where the data must be established between experimenters in isolated laboratories.

The amount of measurement dependence present in a preprogrammed model is here evaluated by the measure M_K defined in (2.5), although we will remove the K subscript to avoid confusion with the key predictability. For simplicity, we will also omit the normalising factor, in this case $(3+\epsilon)/2$, which would align the measure to run from 0 to 1. The measurement dependence is therefore evaluated by

$$M = \max_{\lambda} \sum_{j,k} |p(A_j, B_k|\lambda) - p(A_j, B_k)| \tag{4.2}$$

and the CHSH expectation S is evaluated in the usual way. We have chosen the M_K measure because of its operational interpretation, however an analysis could be performed with the P and M_H measures as well.

The optimal cheating strategies presented thus far for a CHSH test are of course very relevant, but in this chapter we will consider both classical and quantum strategies, as well as convex combinations. We will investigate a mixed strategy that employs a classical strategy with probability p_C and a quantum strategy with $1-p_C$. For a fixed measurement dependence M and key generation efficiency ϵ, the classical strategy will give a CHSH violation S_C and key predictability K_C, whilst the quantum strategy delivers a corresponding S_Q and K_Q. The motive behind combining the two strategies is to exploit both the full determinism of a classical strategy, ensuring that $K_C > K_Q$, with the indeterminism of a quantum strategy, which ensures that $S_Q > S_C$. One can therefore attempt to skew the classical strategy towards key generation and the quantum strategy towards CHSH testing. However, the conclusion of this investigation will be that such a combination of classical and quantum does not provide any significant advantage for our purposes.

It should be noted that, unlike the randomness expansion analysis, we do not claim optimality in our model. Whilst optimal strategies from the previous chapters have been incorporated into the scheme in an intuitive way, it is possible that a better strategy exists, perhaps through solving appropriate linear or semi-definite programming problems. The results here are simply a proof of principle.

4.2 Classical Adversary

In the classical attack, Eve deterministically programs the outcomes through hidden variables λ in the usual way, as represented by Table 4.2, where $p(\lambda_i) = 1/4$

	$a_0(\lambda)$	$a_1(\lambda)$	$b_0(\lambda)$	$b_1(\lambda)$	$b_2(\lambda)$
λ_0	1	1	1	1	1
λ_1	1	-1	1	1	1
λ_2	1	1	1	-1	1
λ_3	1	-1	-1	1	1

Table 4.2: Deterministic outcomes for a classical adversary in a key distribution scheme.

for $i \in \{0, 1, 2, 3\}$. The outcomes for Bob's key generation setting B_2 are such that $\langle a_0 b_2 \rangle = 1$ and $\langle a_1 b_2 \rangle = 0$, corresponding with the QKD protocol described above. We once again assume the model to be conjugate-inclusive, as explained in Definition 1, to avoid suspicion of fixed outcomes.

The measurement selection probabilities $p(A_j, B_k|\lambda)$ are given in Table 4.3. Standard probability laws determine the relation $r_C + a_C + b_C = 1$ and, since we are aiming to skew the classical model away from CHSH testing and towards key generation, $r_C \leqslant 1-\epsilon$. The CHSH testing probabilities are inspired by the previous optimal models such as Tables 2.2(a) and 3.1, and designed to give the highest CHSH score possible, $S_C = 24P_C - 4$, where $P_C \in [1/4, 1/3]$. Since the generated key bits are produced from outcomes that have been deterministically programmed by Eve, she clearly has full information on these bits and so $K_C = 1$.

	$\rho_{00\lambda}$	$\rho_{01\lambda}$	$\rho_{10\lambda}$	$\rho_{11\lambda}$	$\rho_{02\lambda}$	$\rho_{12\lambda}$
λ_0	$r_C P_C$	$r_C P_C$	$r_C P_C$	$r_C(1-3P_C)$	a_C	b_C
λ_1	$r_C P_C$	$r_C P_C$	$r_C(1-3P_C)$	$r_C P_C$	a_C	b_C
λ_2	$r_C P_C$	$r_C(1-3P_C)$	$r_C P_C$	$r_C P_C$	a_C	b_C
λ_3	$r_C(1-3P_C)$	$r_C P_C$	$r_C P_C$	$r_C P_C$	a_C	b_C

Table 4.3: Measurement selection probabilities $\rho_{jk\lambda} := p(A_j, B_k|\lambda)$ for a classical adversary in a key distribution scheme.

The measurement dependence of this model, according to the measure M in (4.2), is

$$M = 3\left|r_C P_C - \frac{1-\epsilon}{4}\right| + \left|r_C(1-3P_C) - \frac{1-\epsilon}{4}\right| + \left|a_C - \frac{\epsilon}{2}\right| + \left|b_C - \frac{\epsilon}{2}\right|. \qquad (4.3)$$

Assuming the classical strategy skews towards key generation, we have $a_C \geqslant \frac{1}{2}\epsilon$. We also set $b_C = \frac{1}{2}\epsilon$ for simplicity, which hopefully should have no effect on an optimal strategy. Since $P \geqslant 1-3P$, we also obtain $r(1-3P) \leqslant \frac{1-\epsilon}{4}$. Finally, the first modulus in (4.3) can be dealt with by noting that M is independent of P_C when $r_C P_C \leqslant \frac{1-\epsilon}{4}$,

thus to maximise S_C the optimal choice of P_C is $P_C = \frac{1-\epsilon}{4r_C}$. Therefore, we make the extra assumption that $r_C P_C \geqslant \frac{1-\epsilon}{4}$, and (4.3) reduces to

$$M = 2r_C(3P_C - 1) + \frac{1}{2}(1-\epsilon). \tag{4.4}$$

One could attempt to create a linear problem to solve for this system of constraints, but we shall instead consider a convex combination of the classical strategy with the quantum strategy below.

4.3 Quantum Adversary

Eve's quantum strategy is almost identical to the classical strategy in terms of measurement selection probabilities, which are described in Table 4.4, where $r_Q + a_Q + b_Q = 1$. The measurement dependence is evaluated as

$$M = 3\left|r_Q P_Q - \frac{1-\epsilon}{4}\right| + \left|r_Q(1-3P_Q) - \frac{1-\epsilon}{4}\right| + \left|a_Q - \frac{\epsilon}{2}\right| + \left|b_Q - \frac{\epsilon}{2}\right| \tag{4.5}$$

and can similarly be simplified by noting that $a_Q \leqslant \frac{1}{2}\epsilon$, $r_Q P_Q \geqslant \frac{1-\epsilon}{4}$ and assuming $r_Q(1-3P_Q) \leqslant \frac{1-\epsilon}{4}$ by a similar argument to the one in the classical strategy. We assume that $b_Q = \frac{\epsilon}{2}$ for simplicity, though this is already enforced by (4.10) below. (4.5) reduces to

$$M = \frac{3}{2}(4r_Q P_Q + \epsilon - 1). \tag{4.6}$$

	$\rho_{00\lambda}$	$\rho_{01\lambda}$	$\rho_{10\lambda}$	$\rho_{11\lambda}$	$\rho_{02\lambda}$	$\rho_{12\lambda}$
λ_0	$r_Q P_Q$	$r_Q P_Q$	$r_Q P_Q$	$r_Q(1-3P_Q)$	a_Q	b_Q
λ_1	$r_Q P_Q$	$r_Q P_Q$	$r_Q(1-3P_Q)$	$r_Q P_Q$	a_Q	b_Q
λ_2	$r_Q P_Q$	$r_Q(1-3P_Q)$	$r_Q P_Q$	$r_Q P_Q$	a_Q	b_Q
λ_3	$r_Q(1-3P_Q)$	$r_Q P_Q$	$r_Q P_Q$	$r_Q P_Q$	a_Q	b_Q

Table 4.4: Measurement selection probabilities $\rho_{jk\lambda} := p(A_j, B_k|\lambda)$ for a quantum adversary in a key distribution scheme.

Both the CHSH expectation S_Q and the key predictability K_Q depend on the choice of quantum state that Eve distributes to Alice and Bob and the choice of measurement operators performed. Without loss of generality, the measurement operators $A_0 = B_2 = Z$ may be set, so that the perfect correlation of key generation outcomes, i.e. $A_0 \otimes B_2 \,|\, \psi\rangle = |\, \psi\rangle$, requires the distributed state to be $|\, \psi\rangle = \cos\chi \,|\, 00\rangle + \sin\chi \,|\, 11\rangle$ for some $\chi \in [0, \pi/4]$, which in turn evaluates the predictability to be $K_Q = \cos^2\chi$. Whilst one could simplify to $\chi = \pi/4$ as in the randomness expansion protocol, this

enforces $K_Q = 1/2$, whereas we would like to investigate the entire range of K_Q. The remaining operators A_1, B_0 and B_1 are chosen so as to maximise S_Q, the method being similar to that of the proof of Theorem 6. The measurement scheme for the underlying variable λ_0, where the CHSH settings are distributed as $(P_Q, P_Q, P_Q, 1-3P_Q)$, is given by

$$\begin{aligned} |\,\psi\rangle &= \cos\chi\,|\,00\rangle + \sin\chi\,|\,11\rangle\,, \\ A_0 &= Z, \\ A_1(\lambda_0) &= \frac{\mu(\lambda_0)Z + \tau(\lambda_0)X}{\sqrt{\mu(\lambda_0)^2 + \tau(\lambda_0)^2}}, \\ B_0 &= \cos\theta Z + \sin\theta X, \\ B_1 &= \cos\phi Z + \sin\phi X, \\ B_2 &= Z, \end{aligned} \tag{4.7}$$

where $\theta \in [0, \pi]$ and $\phi \in [-\pi, \pi]$. A_1 is chosen to be the normalised operator of $P_Q B_0 + (1-3P_Q)B_1$, noting that $\langle\psi\,|\,Z\otimes Z\,|\,\psi\rangle = 1$, $\langle\psi\,|\,Z\otimes X\,|\,\psi\rangle = \langle\psi\,|\,X\otimes Z\,|\,\psi\rangle = 0$ and $\langle\psi\,|\,X\otimes X\,|\,\psi\rangle = \sin^2(2\chi) = 4K_Q(1-K_Q)$, such that $\mu(\lambda_0) = P_Q\cos\theta - (1-3P_Q)\cos\phi$ and $\tau(\lambda_0) = (P_Q\sin\theta - (1-3P_Q)\sin\phi)\cdot 2\sqrt{K_Q(1-K_Q)}$. $A_1(\lambda)$ may similarly be defined for λ_1, λ_2 and λ_3 according to the corresponding permutation of $(P_Q, P_Q, P_Q, 1-3P_Q)$. Indeed, a uniform mixture of each variable is necessary to replicate the observed measurement distribution in Table 4.1. The CHSH expectation is thus given by $S_Q = (S_{\lambda_0} + S_{\lambda_1} + S_{\lambda_2} + S_{\lambda_3})/4$, where

$$\begin{aligned} S_{\lambda_0} &= 4\max_{\theta,\phi}\left(P_Q\cos\theta + P_Q\cos\phi + \sqrt{\mu(\lambda_0)^2 + \tau(\lambda_0)^2}\right) \\ S_{\lambda_2} &= 4\max_{\theta,\phi}\left(P_Q\cos\theta + (1-3P_Q)\cos\phi + \sqrt{\mu(\lambda_2)^2 + \tau(\lambda_2)^2}\right), \end{aligned}$$

where $\mu(\lambda_2) = P_Q(\cos\theta - \cos\phi)$ and $\tau(\lambda_2) = P_Q(\sin\theta - \sin\phi)\cdot 2\sqrt{K_Q(1-K_Q)}$. Furthermore, $S_{\lambda_1}(\theta,\phi) = S_{\lambda_0}(\phi,\theta)$ and $S_{\lambda_3}(\theta,\phi) = S_{\lambda_2}(\phi,\theta)$. This means that if S_{λ_0} is optimised by $\theta = \theta^*$ and $\phi = \phi^*$, then S_{λ_1} is optimised by $\theta = \phi^*$ and $\phi = \theta^*$, which equates to $A_1(\lambda_1) = -A_1(\lambda_0)$, and one can similarly show that $A_1(\lambda_3) = -A_1(\lambda_2)$. Thus, averaged over all λ, $\langle\psi\,|\,A_1\otimes B_2\,|\,\psi\rangle = 0$, as desired for Eve to avoid suspicion.

4.4 Convex Combination

Since any convex combination of strategies with a given measurement dependence M and key efficiency ϵ will also display the same M and ϵ, it is worth considering a

strategy which picks the classical attack with probability p_C and the quantum attack with probability $1 - p_C$, such that the aim is to maximise

$$S = \frac{p_C r_C S_C + (1 - p_C) r_Q S_Q}{p_C r_C + (1 - p_C) r_Q} \tag{4.8}$$

subject to fixed M,ϵ and

$$K = \frac{p_C a_C K_C + (1 - p_C) a_Q K_Q}{p_C a_C + (1 - p_C) a_Q}, \tag{4.9}$$

where Bayes' Rule determines the following constraints:

$$p_C a_C + (1-p_C) a_Q = \frac{\epsilon}{2}, \quad p_C b_C + (1-p_C) b_Q = \frac{\epsilon}{2}, \quad p_C r_C + (1-p_C) r_Q = 1-\epsilon. \tag{4.10}$$

To simplify matters we will first consider combining the classical strategy with a Bell state strategy, i.e. the quantum strategy above with $\chi = \pi/4$, so that $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and $K_Q = 1/2$. When fixing $K = 1$, so that $a_Q = 0, r_Q = 1 - \epsilon/2$, we rearrange (4.4) and (4.6) to obtain

$$P_C = \frac{1}{3}\left(\frac{(M - \frac{1}{2}(1-\epsilon))p_C}{2(1-\epsilon-\delta)} + 1\right), \qquad P_Q = \frac{\frac{2}{3}M + 1 - \epsilon}{4(1 - \frac{\epsilon}{2})},$$

where $\delta = (1 - p_C)(1 - \frac{\epsilon}{2})$. According to Corollary 7, the quantum strategy only provides an advantage to the classical strategy in the region $1/4 \leqslant P_Q \leqslant 3/10$, and here we investigate a combination of classical and quantum strategies, whereas outside of this range it suffices to consider the classical strategy. Thus

$$S = \begin{cases} \left((1-\epsilon-\delta)S_C + \delta S_Q\right)/(1-\epsilon) & 3\epsilon/4 \leqslant M \leqslant 3(1+2\epsilon)/10 \\ S_C/(1-\epsilon) & \text{else,} \end{cases}$$

where $S_C = 24P_C - 4$ and $S_Q = (4(1-2P_Q)^{3/2})/\sqrt{1-3P_Q}$.

Since Alice and Bob expect to generate key on more attempts than evaluating the CHSH expectation, $\epsilon/2 > 1 - \epsilon$, or $\epsilon > 1/3$. However, as $\epsilon \to 1$, we have by setting $P_C = 1/3$ that $M = 0$ and $S_C = 4$, so using the classical strategy ($p_C = 1$) would deliver completely untrustworthy results. Therefore their best hope is to set ϵ as low as possible, i.e. $\epsilon = 1/3$.

For $K = 1$ within the region of quantum advantage (i. e. $3\epsilon/4 \leqslant M \leqslant 3(1+2\epsilon)/10$, implying $2\sqrt{2} \leqslant S_Q \leqslant 16/5$), one can calculate the derivative

$$\frac{\partial S}{\partial p_C} = \frac{2 + 4M - (1 - \frac{\epsilon}{2})S_Q}{1 - \epsilon}, \tag{4.11}$$

which is positive. It is therefore best to set $p_C = 1$ and use the entirely classical strategy. Thus

$$S_{K=1}(M,\epsilon) = \begin{cases} 2(1+2M-\epsilon)/(1-\epsilon) & M < (1-\epsilon)/2 \\ 4 & M \geqslant (1-\epsilon)/2. \end{cases}$$

This shows, perhaps surprisingly, that when ensuring perfect key predictably for Eve, the best possible strategy is purely classical, with no advantage gained by supplementing with a quantum strategy.

On the other hand, for $K = 1/2$ we use the singlet state in the region of quantum advantage, so that

$$S_{K=1/2}(M,\epsilon) = \begin{cases} \frac{2\sqrt{2}\left(3-\frac{2M}{1-\epsilon}\right)^{3/2}}{3\sqrt{3}\sqrt{1-\frac{2M}{1-\epsilon}}} & M < 3(1-\epsilon)/10 \\ S_{K=1}(M,\epsilon) & M \geqslant 3(1-\epsilon)/10 \end{cases}$$

Any convex combination of these two strategies will yield the same M and ϵ therefore the best option, denoted with subscript α, is to take

$$S_\alpha(K,M,\epsilon) = (2K-1)S_{K=1}(M,\epsilon) + 2(1-K)S_{K=1/2}(M,\epsilon). \tag{4.12}$$

Although this strategy performs well, for $K \neq 1$ it is better to consider the quantum strategy in Section 4.3 with a full range of χ (and subsequently a full range of $K_Q \in [1/2, 1]$), denoted by $S_Q(K,M,\epsilon)$ and plotted in Figure 4.1 for $\epsilon = 1/3$ and certain values of M. The plot confirms that $S_Q(K,0,1/3) = 2\sqrt{2-(2K-1)^2}$, which is the intuitive strategy for complete free will (see Appendix A). This strategy can further be improved since, for fixed $0 < M < 1/5$, there is a point $K_f(M)$ at which the tangent to the curve $S_Q(K,M,1/3)$ reaches the classical $K = 1$ point. One can numerically approximate sufficiently many of these points (over various M) and interpolate between them to approximate the function $f(M) := K_f(M)$. For any $K > f(M)$, $S_Q(K,M,1/3)$ lies beneath the corresponding tangent but a strategy can achieve the values at the tangent through the convex combination

$$S_\beta(K,M) = \frac{1-K}{1-f(M)} S_Q(f(M),M,1/3) + \left(1 - \frac{1-K}{1-f(M)}\right) S_Q(1,M,1/3). \tag{4.13}$$

Outside of this region (i. e. $K \leqslant f(M)$, or $M > 1/5$), one simply takes $S_\beta(K,M) = S_Q(K,M,1/3)$.

In Figure 4.1, the dashed lines display $S_Q(K,M,1/3)$, whereas the solid lines show $S_\beta(K,M)$, the two coinciding for $M = 0$ and $M \geqslant 1/5$. This strategy matches or outperforms $S_\alpha(K,M,\epsilon)$ at all points in the (K,M)-regime, and is the best strategy

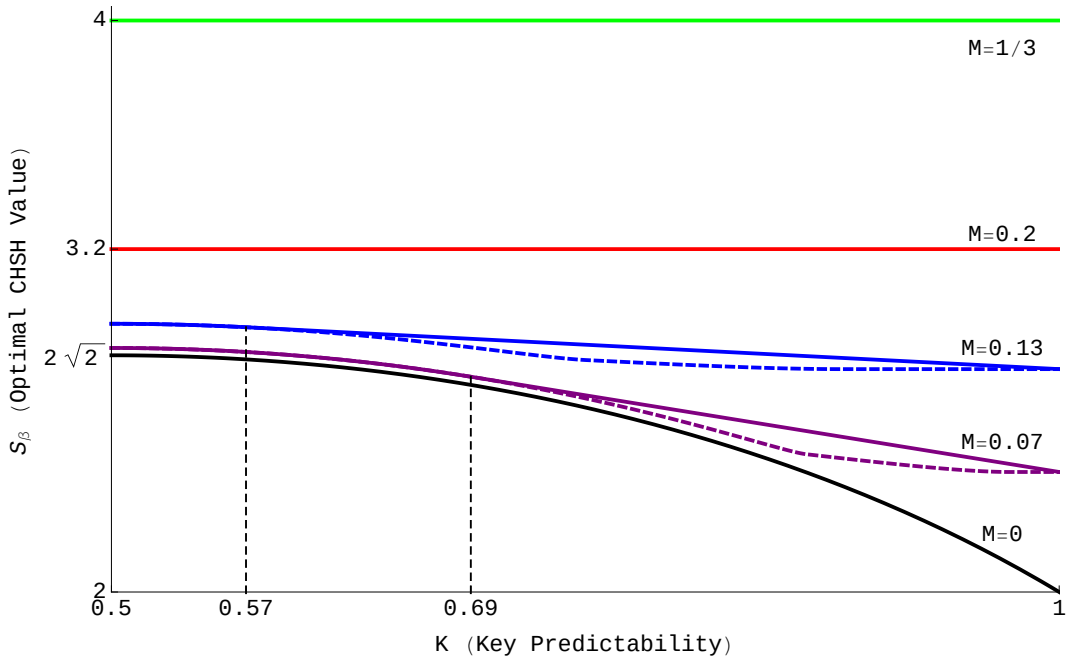

Figure 4.1: $S_Q(K, M, 1/3)$ (dashed) and $S_\beta(K, M)$ (solid) vs K for fixed values of measurement dependence M, which coincide at $M = 0$ and $M > 0.2$. The points $f(0.13) \approx 0.57$ and $f(0.07) \approx 0.69$ have been numerically approximated.

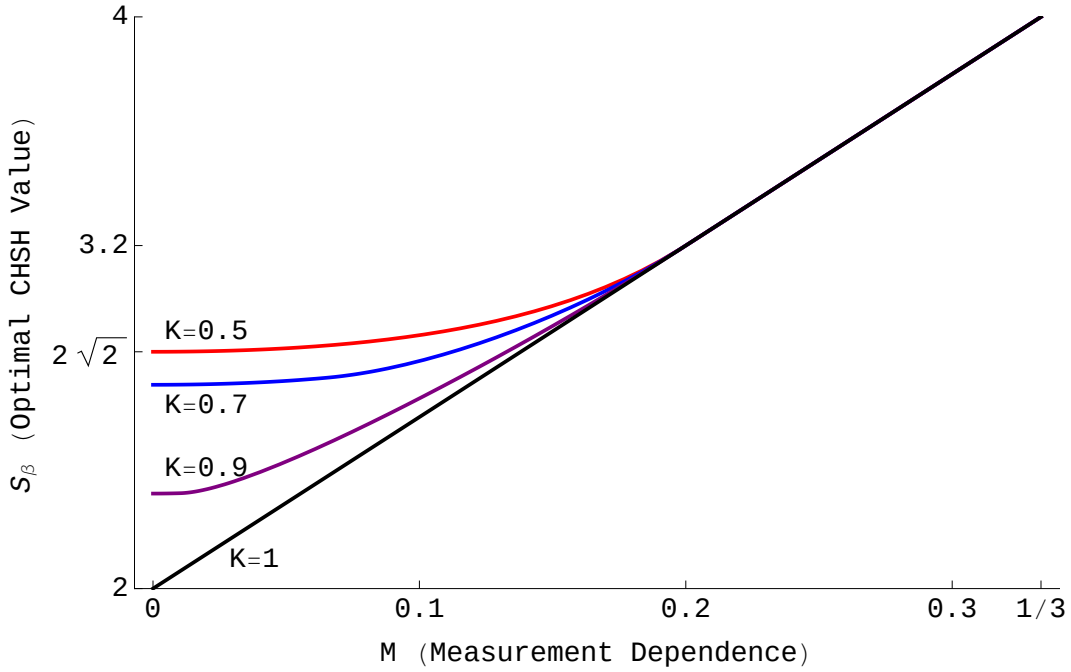

Figure 4.2: $S_\beta(K, M)$ vs M for fixed values of K.

we have found, though we do not claim optimality. A plot of $S_\beta(K, M)$ over M for fixed values of K is shown in Figure 4.2.

The analysis here shows that, despite attempts to examine whether it was possible to skew the quantum strategy away from (and the classical strategy towards) key generation, our best convex combinations of strategies only combine strategies with the same values of the probabilities for the key generation step, so this idea may not be helpful.

Chapter 5

Multiple Runs of a Bell Test

When proving the security of a cryptographic protocol, one must always provide assumptions on the capabilities of the eavesdropper from whom the cryptographers are trying to keep their information secure. After all, history provides a wealth of examples of encryption schemes being broken by technologies more sophisticated than the cryptographer first imagined. This is no less true within the new era of quantum cryptography, and whilst device-independent protocols seek to remove as many unknowns as possible, there are still some assumptions that it is worth differentiating between, one of which (introduced in Section 1.7.3) is the degree of control Eve may have over multiple runs of a Bell test.

Whilst it has been shown that attacks correlated over multiple runs cannot provide a stronger Bell violation than i. i. d. when assuming complete experimental free will [74], a variable free-will scenario necessitates re-investigation. In particular, it is worth asking whether an adversary has an advantage by correlating the hidden variable strategies presented in Chapter 2 over many runs; since these strategies are preprogrammed before the experiment begins, Alice and Bob can no longer rely on spatial separation to reduce Eve's capabilities. Assume, as before, that Eve has written a program that tells Alice's and Bob's devices what to do (using the local measurement settings as inputs), except that this time the program encodes instructions for blocks of N runs together.

Over the course of this chapter it will be shown, both through analytic methods and numerical confirmation, that such a correlated strategy is indeed more powerful than the single-shot attack. The treatment is applied to all three measures of measurement dependence, M_H (or at least the 2-norm equivalent $M_S := M_2^2$), M_K and P in Sections 5.1, 5.2 and 5.3 respectively. Benefits and disadvantages to each measure are discussed within their sections. The results of 5.2 and 5.3, as well as discussion of the closely related topic of randomness amplification, can also be found in [2].

5.1 Using M_S and Quadratic Constraints

Before considering an N-run strategy, let us first tackle the problem of numerically determining what has already been analytically proven in Section 2.3, an optimal classical model that maximises the CHSH value for a fixed measurement dependence in a single-shot attack. We will rephrase the problem in a more computationally friendly way. Specifically in this section, we formulate a *second-order cone programming* (SOCP) problem that is equivalent to our own, which can be solved by the semidefinite programming package SeDuMi in MATLAB.

5.1.1 Numerical Verification of Optimal Single-Shot Model

The single-shot case considers the set of deterministic outcomes defined by a set of underlying λ to optimise the CHSH expectation, described in Table 2.1. We examine a generic probability distribution for the measurement selections that is similar to Table 2.2(c) but programmatically easier to use. Table 5.1 defines 12 variables, introducing normalisation into the bottom row to reduce the number of constraints later on.

	$p(\lambda\|A_0B_0)$	$p(\lambda\|A_0B_1)$	$p(\lambda\|A_1B_0)$	$p(\lambda\|A_1B_1)$
λ_0	x_1	x_4	x_7	x_{10}
λ_1	x_2	x_5	x_8	x_{11}
λ_2	x_3	x_6	x_9	x_{12}
λ_3	$1-\sum_1^3 x_i$	$1-\sum_4^6 x_i$	$1-\sum_7^9 x_i$	$1-\sum_{10}^{12} x_i$

Table 5.1: A probability distribution table for use with the semidefinite programming method.

Recall in Corollary 2 that the M_q measure of measurement independence (2.4) is essentially equivalent for the purposes of maximising a CHSH evaluation using a classical model. In this section we use the measure $M_S := M_2^2$ to numerically determine our model through semidefinite programming. We initially chose this measure over the M_H measure because we did not yet know how to treat the modulus terms present in M_H. However, the problem with moduli was later overcome with a linear programming method (see Section 5.2 for the treatment to the M_K measure).

A fixture of M_S leads to six constraints, one for each distinct pair of columns. For instance, the constraint on the first and second column is

$$(x_1-x_4)^2+(x_2-x_5)^2+(x_3-x_6)^2+(1-x_1-x_2-x_3-(1-x_4-x_5-x_6))^2 \leqslant 2M_S.$$

These six constraints can be written as $||\boldsymbol{A}_n^T\boldsymbol{x}||_2 \leqslant \sqrt{2M_S}$ for $n = 1,\cdots,6$. Each matrix $\boldsymbol{A}_n$ has the block structure $\boldsymbol{A}_n^T = \begin{pmatrix} \boldsymbol{A}_n^1 & \boldsymbol{A}_n^2 & \boldsymbol{A}_n^3 & \boldsymbol{A}_n^4 \end{pmatrix}$, where each $\boldsymbol{A}_n^k$ is a

4×3 matrix specified by

$$\boldsymbol{A}_n^k = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix} \cdot (\delta_{k,j(n)} - \delta_{k,j'(n)}).$$

For the nth constraint, the functions j and j' pick out two columns of Table 5.1 for which we sum the squares of the differences in each row. A specification that considers all six distinct column pairs is $(j(n), j'(n)) = (1,2), (1,3), (1,4), (2,3), (2,4), (3,4)$ for $n = 1, \cdots, 6$ respectively.

We also have linear constraints to satisfy, namely that each variable (being a probability) is in the range $[0,1]$ and also that the variables in each column, not including the normalising element, sum to a value in $[0,1]$. These constraints can be encoded into $\boldsymbol{D}^T\boldsymbol{x} + \boldsymbol{f} \geqslant \boldsymbol{0}$, where $\boldsymbol{D} = (\mathbb{1}_{12}, -\boldsymbol{D}_{\text{cs}}^T)$ and $\boldsymbol{f}^T = (\vec{0}_{12}, \vec{1}_4)$. Here, $\boldsymbol{D}_{\text{cs}}$ encodes the 'column sums'

$$\boldsymbol{D}_{\text{cs}} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

We wish to maximize the CHSH value

$$\begin{aligned} S &= \sum_{n,j,k} p(\lambda_n | A_j B_k)(-1)^{jk} \langle A_j B_k \rangle_{\lambda_n} \\ &= 4 - 2(1 - x_1 - x_2 - x_3 + x_6 + x_8 + x_{10}) \\ &= 2 - 2\boldsymbol{b}^T\boldsymbol{x} \end{aligned}$$

where $\boldsymbol{b}^T = (-1,-1,-1,0,0,1,0,1,0,1,0,0)$. Maximising S is therefore equivalent to minimising $\boldsymbol{b}^T\boldsymbol{x}$.

In summary, our problem of maximizing S subject to the required probability constraints and subject to fixed M_S is equivalent to the SOCP problem,

$$\begin{aligned} \text{minimize} \quad & \boldsymbol{b}^T\boldsymbol{x} \\ \text{subject to} \quad & \boldsymbol{D}^T\boldsymbol{x} + \boldsymbol{f} \geqslant \boldsymbol{0} \\ & ||\boldsymbol{A}_n^T\boldsymbol{x}|| \leqslant \sqrt{2M_S} \qquad \text{for } n = 1, \cdots, 6 \end{aligned}$$

with $\boldsymbol{b}, \boldsymbol{D}, \boldsymbol{f}$ and $\boldsymbol{A}_n$ as defined above. This problem is easily solvable by SeDuMi (see for example Section III of [104]) and the optimal model up to the threshold M_S that achieves maximum S is as specified in Table 2.2(a).

5.1.2 Extension to N runs

To relay the results obtained in analysing a model for N runs, a framework for this model must first be put in place. Firstly, we enumerate a set of N measurement settings that Alice and Bob use by a string $\boldsymbol{j} = j_1 j_2 \dots j_N \in \{0,1,2,3\}^N$. For each $\boldsymbol{j}$, the measurement settings used on the nth run, indicated by a superscript n, are $A^n_{\lfloor j_n/2 \rfloor} B^n_{j_n \bmod 2}$.

The underlying variables determining the measurement outcomes can similarly be enumerated. In the previous section, we showed that the only specified outcome sets that need to be considered for the purposes of maximising S over a single run are precisely those specified by $\lambda_0, \lambda_1, \lambda_2, \lambda_3$ in Table 5.1 (and, 50% of the time, the conjugates of these sets). It easily follows that, for the purposes of maximizing S over N runs, any specification of outcomes for N runs must deliver one of these specifications for each run of the experiment. We therefore enumerate the measurement results by $\boldsymbol{i} = i_1 i_2 \dots i_N \in \{0,1,2,3\}^N$ so that the outcomes on the nth run are as specified by λ_{i_n} (or $\overline{\lambda}_{i_n}$) in Table 5.1.

We wish to find an optimal model of the $4^N \times 4^N$ probabilities $p(\boldsymbol{i}|\boldsymbol{j})$ that maximises the measurement dependence (here using the 'squares' version)

$$M_S = \sup_{\boldsymbol{j} \neq \boldsymbol{j}'} \sum_{\boldsymbol{i}} (p(\boldsymbol{i}|\boldsymbol{j}) - p(\boldsymbol{i}|\boldsymbol{j}'))^2. \tag{5.1}$$

The CHSH value averaged over N runs must be determined. For a given underlying variable $\boldsymbol{i}$ and given measurement settings $\boldsymbol{j}$, the CHSH expectation value is

$$S^{\boldsymbol{j}}_{\boldsymbol{i}} = \frac{4}{N} \sum_{n=1}^{N} (-1)^{\delta_{j_n,3}} \langle A^n_{\lfloor j_n/2 \rfloor} B^n_{j_n \bmod 2} \rangle. \tag{5.2}$$

The $(-1)^{\delta_{j_n,3}}$ term is to indicate that we subtract, rather than add, the expectations of runs where the measurement pair (A_1, B_1) is used. There is also a multiplicative factor of 4, as explained previously in the derivation of (2.11).

One noteworthy observation, which will be used to much greater effect in the following section, is that the sum in (5.2) is a sum of N terms that only take ± 1 values, reflecting how many runs of the experiment give a 'correct answer' to the CHSH test. $S^{\boldsymbol{j}}_{\boldsymbol{i}}$ thus depends only on the number of correct answers given for a specific $(\boldsymbol{i}, \boldsymbol{j})$-pair, denoted $k(\boldsymbol{i}, \boldsymbol{j}) \in \{0, 1, \dots, N\}$, yielding from (5.2) the relation

$$S^{\boldsymbol{j}}_{\boldsymbol{i}} = \frac{4}{N} \left(k(\boldsymbol{i}, \boldsymbol{j}) - (N - k(\boldsymbol{i}, \boldsymbol{j})) \right) = 8 \frac{k(\boldsymbol{i}, \boldsymbol{j})}{N} - 4. \tag{5.3}$$

Since Alice and Bob traditionally require free will to perform the CHSH test, the choice of inputs without knowledge of any underlying variables must be uniform, i.e.

$$p(\boldsymbol{j}) = \frac{1}{4^N} \qquad \forall \boldsymbol{j}.$$

The probabilities are again constrained by a normalisation condition, namely that

$$\sum_{\boldsymbol{i}} p(\boldsymbol{i}|\boldsymbol{j}) = 1 \qquad \forall \boldsymbol{j}, \tag{5.4}$$

and subsequently $\sum_{\boldsymbol{i},\boldsymbol{j}} p(\boldsymbol{i}|\boldsymbol{j}) = 4^N$. For fixed measurement settings $\boldsymbol{j}$,

$$S^{\boldsymbol{j}} = \sum_{i} p(\boldsymbol{i}|\boldsymbol{j}) S_{\boldsymbol{i}}^{\boldsymbol{j}}. \tag{5.5}$$

The equations (5.3) – (5.5) are used to formulate the CHSH value S averaged over N runs and all measurement inputs and outcomes.

$$\begin{aligned} S &= \sum_{\boldsymbol{j}} p(\boldsymbol{j}) S^{\boldsymbol{j}} \\ &= \sum_{\boldsymbol{j}} p(\boldsymbol{j}) \sum_{\boldsymbol{i}} p(\boldsymbol{i}|\boldsymbol{j}) S_{\boldsymbol{i}}^{\boldsymbol{j}} \\ &= \frac{1}{4^N} \sum_{\boldsymbol{i},\boldsymbol{j}} p(\boldsymbol{i}|\boldsymbol{j}) \left(8 \frac{k(\boldsymbol{i},\boldsymbol{j})}{N} - 4 \right) \\ &= -4 + \frac{2}{N \cdot 4^{N-1}} \sum_{\boldsymbol{i},\boldsymbol{j}} k(\boldsymbol{i},\boldsymbol{j}) p(\boldsymbol{i}|\boldsymbol{j}). \end{aligned} \tag{5.6}$$

As expected, the achievable S is in the range $[-4, 4]$, with the upper bound (or lower bound) obtained by a model that prescribes nonzero probabilities only to the $(\boldsymbol{i},\boldsymbol{j})$-pairs that answer all (or zero) queries correctly.

The semidefinite programming methods introduced in the previous section can now be applied to the N-run scenario. There are however two major disadvantages to this approach, the first of which shall be addressed here, whilst the other will severely limit the usefulness of the semidefinite programming method.

The first problem is that there is no intuitive way to compare the measures M_S for different values of N, since the supremum is taken over an increasing number of column pairs. However, we can at least compare our results for repeated uses of the optimal one-shot model in the following way. Using the notation introduced in this section, recall that for $N = 1$ (where $\boldsymbol{i} = i_1$ and $\boldsymbol{j} = j_1$), the optimal one-shot model is defined by a parameter $P \in [1/4, 1/3]$ such that $p(i_1|j_1) = P + (1 - 4P)\delta_{i_1+j_1=3}$, which corresponds to a probability P for all (i_1, j_1)-pairs that answer the CHSH game

$\boldsymbol{i}$ \ $\boldsymbol{j}$	00	01	02	03	10	11	12	13	20	21	22	23	30	31	32	33
00	2	2	2	1	2	2	2	1	2	2	2	1	1	1	1	0
01	2	2	1	2	2	2	1	2	2	2	1	2	1	1	0	1
02	2	1	2	2	2	1	2	2	2	1	2	2	1	0	1	1
03	1	2	2	2	1	2	2	2	1	2	2	2	0	1	1	1
10	2	2	2	1	2	2	2	1	1	1	1	0	2	2	2	1
11	2	2	1	2	2	2	1	2	1	1	0	1	2	2	1	2
12	2	1	2	2	2	1	2	2	1	0	1	1	2	1	2	2
13	1	2	2	2	1	2	2	2	0	1	1	1	1	2	2	2
20	2	2	2	1	1	1	1	0	2	2	2	1	2	2	2	1
21	2	2	1	2	1	1	0	1	2	2	1	2	2	2	1	2
22	2	1	2	2	1	0	1	1	2	1	2	2	2	1	2	2
23	1	2	2	2	0	1	1	1	1	2	2	2	1	2	2	2
30	1	1	1	0	2	2	2	1	2	2	2	1	2	2	2	1
31	1	1	0	1	2	2	1	2	2	2	1	2	2	2	1	2
32	1	0	1	1	2	1	2	2	2	1	2	2	2	1	2	2
33	0	1	1	1	1	2	2	2	1	2	2	2	1	2	2	2

Table 5.2: Specification of $k(\boldsymbol{i}, \boldsymbol{j})$ for $N = 2$.

correctly and $1 - 3P$ for those that answer incorrectly. It is clear that for the model which simply repeats the optimal one-shot model N times, the probabilities $p(\boldsymbol{i}|\boldsymbol{j})$ may be written solely as a function of $k(\boldsymbol{i}, \boldsymbol{j})$, so that the full set of probabilities is given by a single set $\{p_k\}$, where the shorthand k has an implicit dependence on $\boldsymbol{i}$ and $\boldsymbol{j}$[1]. The repeated optimal one-shot model is then wholly specified by

$$p_k = P^k(1 - 3P)^{N-k}. \tag{5.7}$$

The presence of only $N + 1$ distinct probabilities in the model allows us to specify the measurement dependence for an optimal one-shot model repeated over N runs in terms only of P. Table 5.2, which completely specifies $k(\boldsymbol{i}, \boldsymbol{j})$ for a 2-run model, is included here not for direct calculation, but as a verification of the arguments in the proofs below and to highlight the permutation-invariance of the columns, should such illustration be desirable.

Theorem 9. *Provided that the condition*

$$p_0 \leqslant p_1 \leqslant \cdots \leqslant p_{N-1} \leqslant p_N \tag{5.8}$$

holds, the maximum 'column difference' in a table enumerated by underlying variable $\boldsymbol{i}$ *and measurement settings* $\boldsymbol{j}$ *is determined by any* $\boldsymbol{j}, \boldsymbol{j}'$ *for which* $j_n \neq j'_n$ $\forall n$.

[1] In fact, we will argue later that this is true of *any* optimal model.

Proof. Define $M_H^{\boldsymbol{j},\boldsymbol{j}'} := \sum_{\boldsymbol{i}} |p(\boldsymbol{i}|\boldsymbol{j}) - p(\boldsymbol{i}|\boldsymbol{j}')|$ to be the 'column difference' between $\boldsymbol{j} = j_1 j_2 \cdots j_N$ and $\boldsymbol{j}' = j'_1 j'_2 \cdots j'_N$, such that $M_H = \frac{1}{2} \max_{\boldsymbol{j},\boldsymbol{j}'} M_H^{\boldsymbol{j},\boldsymbol{j}'}$, and similarly for $M_S^{\boldsymbol{j},\boldsymbol{j}'}$. Suppose that there exists some n for which $j_n = j'_n$, and pick a new column $\boldsymbol{j}''$ such that $j''_m = j'_m \ \forall m \neq n$ but $j''_n \neq j_n$. We will show that $M_H^{\boldsymbol{j},\boldsymbol{j}''} \geqslant M_H^{\boldsymbol{j},\boldsymbol{j}'}$, meaning that measurement dependence can never be decreased by changing the settings for a given run from being the same to being different.

Recall from the one-shot model that the single-run pair (i_n, j_n) gives a correct answer to the CHSH game if and only if $i_n + j_n \neq 3$. Since $\boldsymbol{j}'$ and $\boldsymbol{j}''$ differ only on the nth run, we have the following relations.

$$\begin{aligned} \text{If } i_n = 3 - j'_n \quad &, \quad k(\boldsymbol{i},\boldsymbol{j}') = k(\boldsymbol{i},\boldsymbol{j}'') - 1, \\ \text{if } i_n = 3 - j''_n \quad &, \quad k(\boldsymbol{i},\boldsymbol{j}') = k(\boldsymbol{i},\boldsymbol{j}'') + 1, \\ \text{otherwise} \quad &, \quad k(\boldsymbol{i},\boldsymbol{j}') = k(\boldsymbol{i},\boldsymbol{j}''). \end{aligned}$$

If the final condition is true for a given row $\boldsymbol{i}$, then clearly the corresponding difference between the two column entries for that row is 0. We can use this conditioning to obtain

$$\begin{aligned} M_H^{\boldsymbol{j},\boldsymbol{j}'} - M_H^{\boldsymbol{j},\boldsymbol{j}''} \quad = \quad & \sum_{\boldsymbol{i}:i_n=3-j'_n} \left(|p_{k(\boldsymbol{i},\boldsymbol{j})} - p_{k(\boldsymbol{i},\boldsymbol{j}')}| - |p_{k(\boldsymbol{i},\boldsymbol{j})} - p_{k(\boldsymbol{i},\boldsymbol{j}')+1}| \right) \\ + \quad & \sum_{\boldsymbol{i}:i_n=3-j''_n} \left(|p_{k(\boldsymbol{i},\boldsymbol{j})} - p_{k(\boldsymbol{i},\boldsymbol{j}')}| - |p_{k(\boldsymbol{i},\boldsymbol{j})} - p_{k(\boldsymbol{i},\boldsymbol{j}')-1}| \right). \end{aligned} \tag{5.9}$$

These two sums each contain 4^{N-1} terms, and a one-to-one correspondence can be made between the terms in the following way. For each $\boldsymbol{i} = i_1 i_2 \cdots i_N$ such that $i_n = 3 - j'_n$, define $\boldsymbol{i}'' := i''_1 i''_2 \cdots i''_N$ where $i''_m = i_m \ \forall m \neq n$ and $i''_n = 3 - j''_n$. We obtain the relations

$$k(\boldsymbol{i}'',\boldsymbol{j}) = k(\boldsymbol{i},\boldsymbol{j}) + 1 \qquad , \qquad k(\boldsymbol{i}'',\boldsymbol{j}') = k(\boldsymbol{i},\boldsymbol{j}') + 1,$$

and use this correspondence to combine the two sums in (5.9).

$$\begin{aligned} M_H^{\boldsymbol{j},\boldsymbol{j}'} - M_H^{\boldsymbol{j},\boldsymbol{j}''} = \sum_{\boldsymbol{i}:i_n=3-j'_n} \quad (\quad & |p_{k(\boldsymbol{i},\boldsymbol{j})} - p_{k(\boldsymbol{i},\boldsymbol{j}')}| - |p_{k(\boldsymbol{i},\boldsymbol{j})} - p_{k(\boldsymbol{i},\boldsymbol{j}')+1}| \\ + \quad & |p_{k(\boldsymbol{i},\boldsymbol{j})+1} - p_{k(\boldsymbol{i},\boldsymbol{j}')+1}| - |p_{k(\boldsymbol{i},\boldsymbol{j})+1} - p_{k(\boldsymbol{i},\boldsymbol{j}')}|). \end{aligned} \tag{5.10}$$

For brevity, use the notation $a = p_{k(\boldsymbol{i},\boldsymbol{j})}$, $b = p_{k(\boldsymbol{i},\boldsymbol{j}')}$, $c = p_{k(\boldsymbol{i},\boldsymbol{j}')+1}$ and $d = p_{k(\boldsymbol{i},\boldsymbol{j})+1}$. Each term in the summation is of the form $|a-b| - |a-c| + |d-c| - |d-b|$, where invoking the ordering condition (5.8) gives $a \leqslant d$ and $b \leqslant c$. By examining case-by-case over all possible orderings ($b \leqslant c \leqslant a \leqslant d$ etc.), we see that each summand in

(5.10) and thus the whole sum is non-positive, and therefore $M_H^{\boldsymbol{j},\boldsymbol{j}'} \leqslant M_H^{\boldsymbol{j},\boldsymbol{j}''}$. The proof for M_S works exactly the same way, where the moduli in the terms above are replaced by brackets squared. Each summand in the corresponding form of (5.10) is reduced to $2(b-c)(d-a) \leqslant 0$, therefore the same result holds for M_S. □

The ordering (5.8) of the probabilities p_k is satisfied by the repeated optimal one-shot model (5.7), but will also be clearly satisfied by any optimal model since obtaining the maximum S value requires more weight given to the pairs of measurement settings that answer a larger proportion of the N queries correctly.

Corollary 10. *Provided that the ordering* (5.8) *holds, the measurement dependence is*

$$M_H = \frac{1}{2}\sum_{s=0}^{N}\sum_{t=0}^{N-s}\frac{N!}{s!t!(N-s-t)!}2^{N-s-t}|p_{N-s}-p_{N-t}|, \tag{5.11}$$

$$M_S = \frac{1}{2}\sum_{s=0}^{N}\sum_{t=0}^{N-s}\frac{N!}{s!t!(N-s-t)!}2^{N-s-t}(p_{N-s}-p_{N-t})^2. \tag{5.12}$$

Proof. By Theorem 9, we calculate the column difference between a pair $\boldsymbol{j},\boldsymbol{j}'$ of columns for which $j_n \neq j'_n\ \forall n$. Recall from the one-shot model that the single-run pair (i_n, j_n) gives a correct answer to the CHSH game if and only if $i_n + j_n \neq 3$. For a given underlying variable $\boldsymbol{i}$, $k(\boldsymbol{i},\boldsymbol{j}) = N - \#\{n : i_n = 3 - j_n\}$ and $k(\boldsymbol{i},\boldsymbol{j}') = N - \#\{n : i_n = 3 - j'_n\}$, so partition all strings $\boldsymbol{i}$ into strings containing s instances of $i_n = 3 - j_n$ and t instances of $i_n = 3 - j'_n$. Using counting arguments, there are

$$\binom{N}{s}\binom{N-s}{t}2^{N-s-t} \tag{5.13}$$

such strings, for which the entry in column $\boldsymbol{j}$ is p_{N-s} and the entry in column $\boldsymbol{j}'$ is p_{N-t}. The measurement dependence is thus given by (5.11) and (5.12). □

Using the repeated optimal one-shot model (5.7), we recognise the presence of binomial expansions to obtain

$$M_S(P) = ((3P^2 + (1-3P)^2)^N - (2P)^N(1-2P)^N). \tag{5.14}$$

Observe that there is no similar closed form solution for $M_H(P)$ due to the use of moduli that complicate the expression. Thus, M_S can be calculated much more quickly than M_H – this is noteworthy for later sections.

We use a SeDuMi program similar to Section 5.1.1 to vary N and compare plots of maximal S against M_S, using $M_S(P)$ for $P \in [1/4, 1/3]$ as the fixed measurement

dependence constraint, such as in Figure 5.1 for $N = 1, 2$. The plot clearly shows that there is an advantage to an eavesdropper employing a correlated strategy rather than a repeated single-shot strategy, and provides motivation for extending the study to larger N.

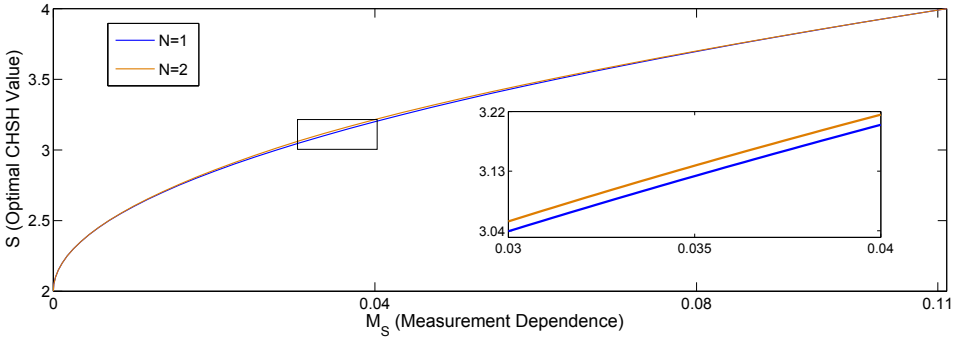

Figure 5.1: S vs M_S for $N = 1, 2$, using the semidefinite programming method.

The code used to generate this plot did not take full advantage of the p_k reduction, instead working with a set of (assuming normalisation in the bottom row of the $p(\boldsymbol{j}|\boldsymbol{i})$ table) $4^N \cdot 4^{N-1}$ variables similar to the one-run method in Section 5.1. As such, the code is very inefficient and could not generate a single solution for $N = 4$ due to insufficient memory. With ample reasoning the reduction of these probabilities to the set $\{p_k\}$ could simplify the code to consider only $N + 1$ variables, but in practice the methods presented in the next sections supersede a method using semidefinite programming due to faster running times. Nevertheless, the observation made here that the conditional probabilities have a dependence only on the number of queries answered correctly will be crucial. The following method simplifies the semidefinite problem to a solvable linear system of equations.

5.1.3 Using Lagrange Multipliers

To begin, we will reduce the probabilities $p(\boldsymbol{i}|\boldsymbol{j})$ to a set consisting solely of p_k, invoking symmetry of permutations to justify the optimal solution[2]. We use counting arguments to write the 'fixed norm' and 'fixed S' constraints in a similar way to the formulation for M_S given by (5.12) in Corollary 10, and this is the same for each column (observe from Table 5.2 that each column contains the same numbers of each

[2]This argument is given after description of the method on page 77.

$p_k)^3$. Since there are $\binom{N}{k}3^k$ instances of p_k in a column, these are simply

$$\sum_{k=0}^{N}\binom{N}{k}3^k p_k = 1, \tag{5.15}$$

$$-4+\frac{8}{N}\sum_{k=0}^{N}\binom{N}{k}3^k k p_k = S. \tag{5.16}$$

The method of Lagrange multipliers will be used to minimise (5.12) subject to the constraints (5.15) and (5.16), which will be assigned multipliers μ and $\lambda N/8$ respectively. A set of $N+1$ linear constraints can be found by differentiating with respect to each p_k. For $k = 0, 1, \ldots, N$,

$$\frac{\partial}{\partial p_k}\left(\sum_{s=0}^{N}\sum_{t=0}^{N-s}\frac{N!}{s!t!(N-s-t)!}2^{N-s-t-1}(p_{N-s}-p_{N-t})^2\right)-\mu\binom{N}{k}3^k-\lambda\binom{N}{k}3^k k = 0. \tag{5.17}$$

The first term is calculated by making the substitutions $j = N-s$ and $l = N-t$:

$$\begin{aligned}
&\frac{\partial}{\partial p_k}\left(\sum_{j=0}^{N}\sum_{l=N-j}^{N}\frac{N!}{(N-j)!(N-l)!(j+l-N)!}2^{j+l-N-1}(p_j-p_l)^2\right)\\
=\;&\frac{\partial}{\partial p_k}\left(\sum_{l=N-k}^{N}\frac{N!}{(N-k)!(N-l)!(k+l-N)!}2^{k+l-N}(p_k-p_l)^2\right)\\
=\;&2\binom{N}{k}\left(\sum_{l=N-k}^{N}\binom{k}{N-l}2^{k+l-N}(p_k-p_l)\right)\\
=\;&2\cdot 3^k\binom{N}{k}p_k-2\binom{N}{k}\sum_{l=N-k}^{N}\binom{k}{N-l}2^{k+l-N}p_l,
\end{aligned} \tag{5.18}$$

where the second line follows by collecting only the terms including p_k. The linear equations follow from (5.17) and (5.18) as

$$2\cdot 3^k p_k-2\sum_{l=N-k}^{N}\binom{k}{N-l}2^{k+l-N}p_l-\mu 3^k-\lambda 3^k k = 0 \qquad , \qquad k = 0, 1, \ldots, N. \tag{5.19}$$

There are now $N+3$ linear equations ((5.15), (5.16) and (5.19)) in the $N+3$ variables μ, λ and $(p_k)_{k=0,1,\ldots,N}$. These are immediately solvable by inverting the matrix K in the equation $K\,|\,v\rangle = |\,b\rangle$, where $|\,v\rangle$ is our vector of parameters $|\,v\rangle = \sum_{k=0}^{N} p_k\,|\,k\rangle +$

[3]This simplification can also be applied directly to the semidefinite approach, such that the problem becomes polynomial in N, though the new method here is faster.

$\mu\,|\,N+1\rangle + \lambda\,|\,N+2\rangle$, $|\,b\rangle$ is the solution vector $|\,b\rangle = |\,N+1\rangle + \frac{N}{8}(4+S)\,|\,N+2\rangle$ and K encodes the equations, explicitly

$$\begin{aligned} K \;=\; & \sum_{k=0}^{N} |\,k\rangle \left(2\cdot 3^k \,\langle k\,| - 2\sum_{l=N-k}^{N} \binom{k}{N-l} 2^{k+l-N}\,\langle l\,| - 3^k\,\langle N+1\,| - 3^k k\,\langle N+2\,| \right) \\ + \;\; & |\,N+1\rangle \left(\sum_{l=0}^{N} 3^l \binom{N}{l} \langle l\,| \right) + |\,N+2\rangle \left(\sum_{l=0}^{N} 3^l l \binom{N}{l} \langle l\,| \right). \end{aligned} \tag{5.20}$$

Note however that a vital ingredient is missing from the above specifications – each parameter p_k is a probability and must be positive. Without this restriction, our solution yields the probabilities

$$p_k = \frac{1}{3\cdot 2^{2N+1}}(6 + (S-2)(4k-3N)) \tag{5.21}$$

In the region of interest $S > 2$, the probabilities satisfy the ordering $p_0 \leqslant p_1 \leqslant \cdots \leqslant p_N$. However, non-negativity is not guaranteed. For instance, $p_0 < 0$ whenever $S > S^{(1)} := 2 + \frac{2}{N}$, therefore we can only use the model (5.21) in the range $S \leqslant S^{(1)}$, and evaluate M_S for this model with (5.12). When $S \geqslant S^{(1)}$, we may simply set $p_0 = 0$ and re-solve the problem above, minus the parameter p_0 and its associated constraint. This is achieved by deleting the first row and first column of K and again leads to a solution that nevertheless satisfies non-negativity only up to a value $S^{(2)} \in [S^{(1)}, 4]$, at which point $p_1 = 0$. Above this value, fix $p_1 = 0$, remove p_1 and its associated constraint from the linear problem, and repeat.

Once the routine has run through all constraints, the values $S^{(r)}$ for $r = 1, 2, \ldots, N$ are obtained, indicating the 'crossover' points where the probabilities $p_0, p_1, \ldots, p_{r-1}$ are set to zero. The solutions also allow for the evaluations of M_S at any value of S, however we will just be concerned with evaluating at the crossover points, writing them as $M_S^{(1)}, M_S^{(2)}, \ldots, M_S^{(N)}$. Note that $(S^{(N)}, M_S^{(N)}) = (4, \frac{1}{3^{2N}}(3^N - 2^N))$, which intuitively agrees with the notion of a maximal model answering every CHSH query correctly, i.e. $p_N = \frac{1}{3^N}$, else $p_k = 0$.

The efficiency of this routine can be enhanced, since the values $S^{(r)}$ and $S^{(r+1)}$ are separated by $O(\frac{1}{N})$ and are therefore arbitrarily close together in the limit of large N, in which case the points $(S^{(r)}, M_S^{(r)})$ can be used to define our plot of maximal S against M_S, removing the necessity to evaluate for all S. To quickly find the point $S^{(r)}$, assume the fixture $p_0 = \cdots = p_{r-1} = 0$ has been made, and evaluate the value of S for which the optimal solution has $p_r = 0$. This is done by removing the first

$r-1$ rows and r columns from the original K, as well as the final row of K which encoded the restriction on S. The new problem can thus be written as

$$K_{r-1\ldots N+1,r\ldots N+2}\left(\sum_{k=r+1}^{N} p_k\,|\,k\rangle + \mu\,|\,N+1\rangle + \lambda\,|\,N+2\rangle\right) = |\,N+1\rangle \qquad (5.22)$$

where $K_{r-1\ldots N+1,r\ldots N+2}$ denotes the submatrix formed by rows $r-1,\ldots,N+1$ and columns $r,\ldots,N+2$ of the matrix K defined in (5.20). The pair $(S^{(r)}, M_S^{(r)})$ can be evaluated from the solution vector and a plot of these points for $r=1,\ldots,N$, together with the basic point $(S^{(0)}, M_S^{(0)}) := (2,0)$, can define the curve in the limit of large N. Figure 5.2 gives the plot for varying N to illustrate the convergence (for $N\to\infty$) to the optimal curve. However, as with the semidefinite approach in Figure 5.1, the values of M_S are not directly comparable for different values of N. A helpful comparison can still be made by finding $P\in[1/4,1/3]$ such that $M_S = M_S(P)$ as given by the measurement dependence (5.14) for a repeated optimal one-shot model, then plotting $(4P-1)^2$, the corresponding measurement dependence for one run of the model.

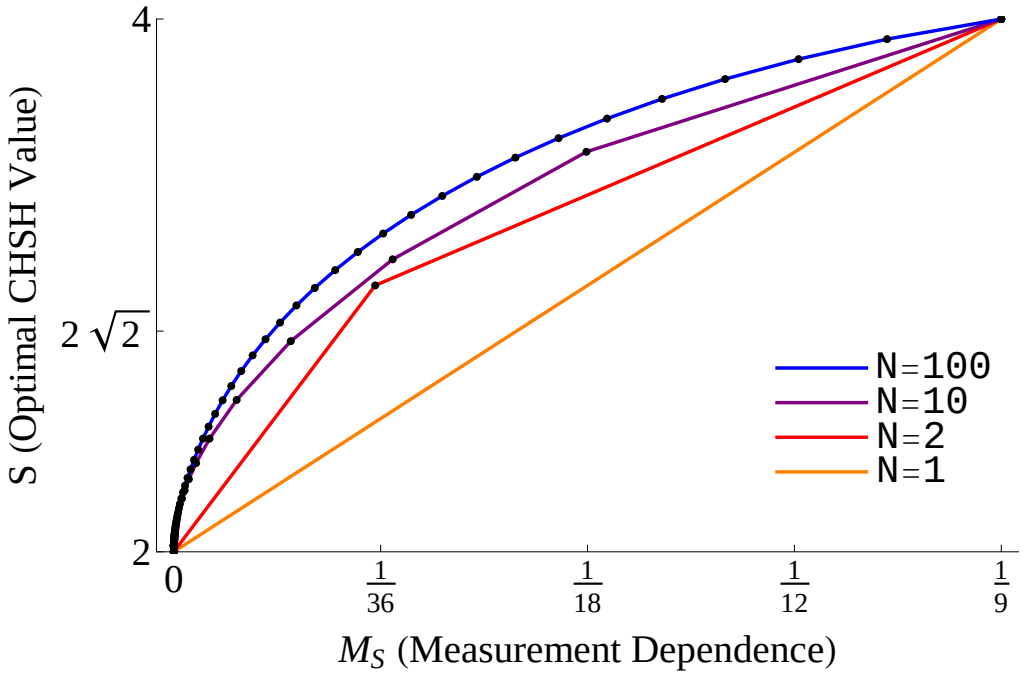

Figure 5.2: Using the Lagrange multipliers method, a plot of S vs M_S for various N. The black dots are crossover points $(S^{(r)}, M_S^{(r)})$ for $r=0,1,\ldots,N$, with straight lines approximating the solution between these points.

Before continuing, we justify the reduction of probabilities to the $N+1$ elements p_k, relevant to this section and the next. Consider the original probability table

$p(\boldsymbol{i}|\boldsymbol{j})$. The above method can still be applied without the reduction, albeit with far more constraints, to obtain a system of equations of the form $K\,|\,v\rangle = |\,b\rangle$. For any matrix Λ_i such that $K\Lambda_i = K$ and $\Lambda_i\,|\,b\rangle = |\,b\rangle$, then if $|\,v\rangle$ is a solution to the equation, so is $\Lambda_i\,|\,v\rangle$, as well as any mixture $\sum_i p_i\Lambda_i\,|\,v\rangle$. Let Λ_i be a permutation of the probabilities $p(\boldsymbol{i}|\boldsymbol{j})$ for a fixed number of correct answers k; this matrix does not change the equations of interest (5.1), (5.4) and (5.6) and therefore qualifies. By taking a uniformly weighted convex combination over all such permutations, the entries of $\sum_i p_i\Lambda_i\,|\,v\rangle$ are just p_k, enabling us to work with the symmetric state consisting of p_k instead, although we must consider that the solution may not be unique.

One advantage to the Lagrange multipliers method compared to the semidefinite programming approach in Section 5.1, is the improvement in efficiency obtained by *a priori* harnessing the ordering on p_k in an optimal model. Despite the advantages, more can be done. Firstly, this method only provides an approximation to the optimal solution for a fixed N. The only precise numerical evaluations for this curve are at the crossover points $(S^{(r)}, M_S^{(r)})$ but even here, except for $r = 0$ and $r = N$, it is difficult to retract a closed-form expression for the model due to the complex structure of K. Secondly, the reliance on the measure M_S makes it difficult to generalise the approach to consider other Bell inequalities.

Despite these problems, the work formulated in this section can be carried forward to the next, where we convert the problem into one requiring only linear constraints in the first place, and explore a more direct comparison with the repeated optimal one-shot model. The methods will investigate the more easily-calculable measure M_K and also allow examination of a more general class of Bell inequalities. In comparison to the Lagrange multipliers method, the next program will be easier to set up, although slower to run.

5.2 Using M_K and Linear Constraints

Corollary 2 confirmed the equivalence of all q-norm variations of the measurement dependence, M_q, for the purposes of maximising S, thus justifying our examination of M_S (i.e. M_2^2) in the previous sections. Our motivation for this was to find a numerical approach that did not have to work with the moduli present in the more accessible measure M_H (i.e. $q = 1$), which can present an obstacle to linear programming techniques. Fortunately, there is a way to overcome this.

In Section 2.2, an argument was made for the measure M_K (2.5) being more intuitive than M_H (2.3) as it conveys the maximum distance between the input dis-

tribution Alice and Bob are expecting (which in the case of nonlocality testing is uniform) and the distribution Eve is actually providing with knowledge of the input made. As a consequence, the improved methods in this section will incorporate this measure, defined using the present N-run notation as

$$M_K = \frac{(m_A m_B)^N}{2((m_A m_B)^N - 1)} \max_{\boldsymbol{i}} \sum_{\boldsymbol{j}} |p(\boldsymbol{j}|\boldsymbol{i}) - p(\boldsymbol{j})|,$$

although with a little more effort the same techniques can be applied to M_H. As mentioned in Section 2.2, M_H appears to be a nice measure because its definition depends only on $p(\boldsymbol{i}|\boldsymbol{j})$ and not on $p(\boldsymbol{i})$. M_K does require a more careful selection of $p(\boldsymbol{i})$, but the upshot is that all rows will be identical when adhering to the relevant symmetry constraints.

We will first continue our investigation of the CHSH inequality, noting that the adaptability of these techniques to examine a more general class of Bell inequalities commonly known as I_{mm22} [37] presents a clear advantage over the Lagrange multipliers method.

5.2.1 CHSH Inequality

Since the definition of M_K includes the probabilities $p(\boldsymbol{j}|\boldsymbol{i})$ of selecting a choice $\boldsymbol{j}$ of measurement inputs given underlying variable $\boldsymbol{i}$, the framework is slightly different from the previous sections, which were concerned with $p(\boldsymbol{i}|\boldsymbol{j})$. Nevertheless, a correspondence can be made between the two via Bayes' rule. The probabilities must satisfy

$$\sum_{\boldsymbol{i}} p(\boldsymbol{i}) p(\boldsymbol{j}|\boldsymbol{i}) = p(\boldsymbol{j}) \qquad \forall \boldsymbol{j}. \tag{5.23}$$

When considering the model for faking CHSH violations under variable free will, it is clear that the probability distribution for $\boldsymbol{j} \in \{0,1,2,3\}^N$ must be uniform ($p(\boldsymbol{j}) = 4^{-N}$) since Alice and Bob should be convinced that their random number generators are working effectively and can test for this after the experiment. The specification for $p(\boldsymbol{i})$ is less restrictive, and indeed we will see in Section 5.2.3 why a non-uniform distribution might be preferred for more general Bell inequalities, however for CHSH the uniform distribution $p(\boldsymbol{i}) = 4^{-N}$, where the outcomes for the nth run are still specified by λ_{i_n} in Table 2.1, will suffice (a motivational argument for this is that the rows are identical to the columns for the correlations in Table 2.1).

The assignment of these distributions interprets (5.23) as $\sum_{\boldsymbol{i}} p(\boldsymbol{j}|\boldsymbol{i}) = 1$. Therefore, the columns of a $p(\boldsymbol{j}|\boldsymbol{i})$ table sum to 1. This condition can also be used to

formulate the CHSH value S in terms of $p(\boldsymbol{j}|\boldsymbol{i})$, which one can obtain by the same method that yielded (5.6) (except summing first over $\boldsymbol{j}$, then $\boldsymbol{i}$) to achieve an almost identical formula

$$\begin{aligned} S &= -4 + \frac{2}{N \cdot 4^{N-1}} \sum_{\boldsymbol{i},\boldsymbol{j}} k(\boldsymbol{i},\boldsymbol{j}) p(\boldsymbol{j}|\boldsymbol{i}) \\ &= -4 + 8 \sum_{\boldsymbol{i}} p(\boldsymbol{i}) S_{\boldsymbol{i}} \end{aligned} \tag{5.24}$$

where

$$S_{\boldsymbol{i}} = \frac{1}{N} \sum_{\boldsymbol{j}} p(\boldsymbol{j}|\boldsymbol{i}) k(\boldsymbol{i},\boldsymbol{j}) \tag{5.25}$$

and $k(\boldsymbol{i},\boldsymbol{j})$ is the number of correct correct answers given by a variable/settings pair. We reduce the probabilities to a smaller set in a similar way to the previous chapter, but the symmetry-based arguments that allow for this reduction must be amended.

$S_{\boldsymbol{i}}$ may be rewritten as

$$S_{\boldsymbol{i}} = \frac{1}{N} \sum_{k=0}^{N} k p_k^{\boldsymbol{i}} \qquad p_k^{\boldsymbol{i}} := \sum_{\boldsymbol{j}:k(\boldsymbol{i},\boldsymbol{j})=k} p(\boldsymbol{j}|\boldsymbol{i}).$$

Since $p(\boldsymbol{j}|\boldsymbol{i})$ can be individually varied, the optimisation can be made on each $S_{\boldsymbol{i}}$ separately. The allowable outcome specifications for an N-run strategy (as illustrated for $N = 2$ in Table 5.2) exhibit the following relation for any $k, \boldsymbol{i}, \boldsymbol{i'}$:

$$\#\{\boldsymbol{j} : k(\boldsymbol{i},\boldsymbol{j}) = k\} = \#\{\boldsymbol{j} : k(\boldsymbol{i'},\boldsymbol{j}) = k\} = \binom{N}{k} 3^k.$$

Thus, variation of the probabilities $p(\boldsymbol{j}|\boldsymbol{i})$ over any $\boldsymbol{j}$ for which $k(\boldsymbol{i},\boldsymbol{j}) = k$ will have no effect on the maximisation, so we may for simplicity set $p(\boldsymbol{j}|\boldsymbol{i}) = p_k^{\boldsymbol{i}}/(\binom{N}{k}3^k)$. Furthermore, $p_k^{\boldsymbol{i}} = p_k^{\boldsymbol{i'}}$ for any $\boldsymbol{i}, \boldsymbol{i'}$ so we may remove the $\boldsymbol{i}$ dependence, defining p_k such that $p_k^{\boldsymbol{i}} = p_k \binom{N}{k} 3^k$. With the reduction to $\{p_k\}$ made, (5.24) becomes

$$S = -4 + 8 \sum_{k=0}^{N} \binom{N-1}{k-1} 3^k p_k \tag{5.26}$$

and similarly the row normalisation (5.23) is converted to

$$\sum_{k=0}^{N} \binom{N}{k} 3^k p_k = 1. \tag{5.27}$$

These two constraints are similar to (5.15) and (5.16), though of course the probabilities here are conditioned on the measurement settings given the underlying variable rather than the converse. By creating the variable vector $\boldsymbol{p} = (p_k)_{k=0,\ldots,N}$ we

can encode these two equations with the vectors $\boldsymbol{s}$ and $\boldsymbol{n}$ where $s_k := 3^k\binom{N-1}{k-1}$ and $n_k := 3^k\binom{N}{k}$. Encoding

$$M_{\boldsymbol{i}} = \sum_{k=0}^{N} \binom{N}{k} 3^k \left| p_k - 4^{-N} \right|, \tag{5.28}$$

such that $M_K = \frac{4^N}{2(4^N-1)} \max_{\boldsymbol{i}} M_{\boldsymbol{i}}$, requires a slightly different tack to dispense with the moduli present. Introduce new non-negative variables $\boldsymbol{w}$ such that

$$w_k \geqslant p_k - 4^{-N} \qquad , \qquad w_k \geqslant 4^{-N} - p_k. \tag{5.29}$$

This overcomes the need for a modulus, however in order to express the problem in the standard linear programming form, we convert all inequalities to a statement on non-negative variables, i.e. introduce variables $\boldsymbol{a}$, $\boldsymbol{b}$ defined by $a_k := w_k - x_k + 4^{-N}$ and $b_k := w_k + x_k - 4^{-N}$ and set $\boldsymbol{a} \geqslant 0$, $\boldsymbol{b} \geqslant 0$ to represent the inequalities (5.29). The measurement dependence condition is then expressible as

$$\sum_{k=0}^{N} \binom{N}{k} 3^k w_k \leqslant \frac{2(4^N-1)}{4^N} M_K, \tag{5.30}$$

but as the aim of the program will be to maximise S for a fixed M_K, note that the maximal strategy will automatically achieve the bound for one of the inequalities (5.29), and thus (5.30) can actually be fixed as an equality in the program. We can now solve the linear problem

$$\begin{aligned} &\text{minimize} && \boldsymbol{c} \cdot \boldsymbol{z} \\ &\text{subject to} && B \cdot \boldsymbol{z} = \boldsymbol{v} \end{aligned}$$

where $\boldsymbol{z}$ is a vector of non-negative variables with the block structure $\boldsymbol{z}^T = (\ \boldsymbol{p} \quad \boldsymbol{w} \quad \boldsymbol{a} \quad \boldsymbol{b}\ )$, $\boldsymbol{c}^T = (\ -\boldsymbol{s} \quad 0 \quad 0 \quad 0\ )$ is used to maximise $S = -4 + 8\boldsymbol{c} \cdot \boldsymbol{z}$ and the row normalisation constraint (5.27), the definitions of $\boldsymbol{a}$ and $\boldsymbol{b}$ and the measurement dependence constraint (5.30) are found within

$$B = \begin{pmatrix} \boldsymbol{n} & 0 & 0 & 0 \\ \mathbb{1} & -\mathbb{1} & \mathbb{1} & 0 \\ -\mathbb{1} & -\mathbb{1} & 0 & \mathbb{1} \\ 0 & \boldsymbol{n} & 0 & 0 \end{pmatrix} \qquad , \qquad \boldsymbol{v} = \begin{pmatrix} 1 \\ 4^{-N} \\ -4^{-N} \\ \frac{2(4^N-1)}{4^N} M_K \end{pmatrix}.$$

As with the M_H measure, M_K is not directly comparable over varying number of runs N. For instance, the model with minimal M_K required to achieve maximum $S = 4$, denoted $M_{\max}(N)$ is given by $p_N = 3^{-N}$, else $p_k = 0$. Inserting this into (5.28) yields $M_{\max}(N) = \frac{4^N}{4^N-1}\left(1 - \left(\frac{3}{4}\right)^N\right)$. Nevertheless, a comparison can be made

between the optimal N-run strategy and the optimal 1-run strategy repeated N times, representing the power of an eavesdropper limited only to independent attacks. A plot of the comparisons for $N = 2$ and $N = 100$ is shown in Figure 5.3. The axes plot S versus $M_K/M_{\max}(N)$, which both run from 0 to 1 regardless of N, for illustrative comparison[4].

In the next section, the preceding work will be applied to a more general class of Bell inequalities known as I_{mm22}[37]. These inequalities involve two users whose devices each have m measurement inputs with two outcome values. At $m = 2$, the inequality reduces to CHSH. For $m \geqslant 3$, a more sophisticated analysis is required due to the fact that not all possible input pairs are queried in evaluating the relevant inequality. A full analysis of $m = 3$ is provided in Section 5.2.3 after introducing the general class; strategies for larger m behave qualitatively the same and are readily generalised.

5.2.2 I_{mm22} Inequalities

The I_{3322} inequality (1.21) was discussed as a notable Bell inequality in Section 1.4.3.2. The generalisation of this inequality to m measurement settings on each side can be written as

$$I_{mm22} := \sum_{j,k=0}^{m-1} \alpha_{jk}^{(m)} P(A_j, B_k) - P(A_0) - \sum_{k=0}^{m-1} (m-1-k) P(B_k) \leqslant 0, \tag{5.31}$$

with the shorthand $P(A_j B_k) = p(a, b|A_j, B_k), P(A_j) = p(a|A_j)$ etc. where $a, b \in \{\pm 1\}$ and defining the coefficients $\alpha_{jk}^{(m)}$ to be $+1$ if $j+k \leqslant m-1$, -1 if $j+k = m-1$ and 0 otherwise (for instance, see Table 5.3 for the coefficients $\alpha_{jk}^{(6)}$). As suggested in [26] (Appendix C), it is convenient to multiply this equation by $1 + ab$ and summing over all a, b to yield an inequality in terms of correlations,

$$S_{mm22} := \sum_{j,k=0}^{m} \alpha_{jk}^{(m)} \langle A_j B_k \rangle \leqslant \binom{m+1}{2} - m + 1. \tag{5.32}$$

This bound is for an LHV model, whereas the no-signalling bound is clearly the number of non-zero coefficients α_{jk}, which is $\binom{m+1}{2} + m - 1$. The LHV bound is derived in Theorem 11.

As with our methods for CHSH, we formulate a variable-free-will model by specifying for a given hidden variable the outcomes of each measurement prescribed by

[4]The specific choices of N in the plots are arbitrary; the important point to take away is that the gap between one-shot and correlated strategies widens with increasing N.

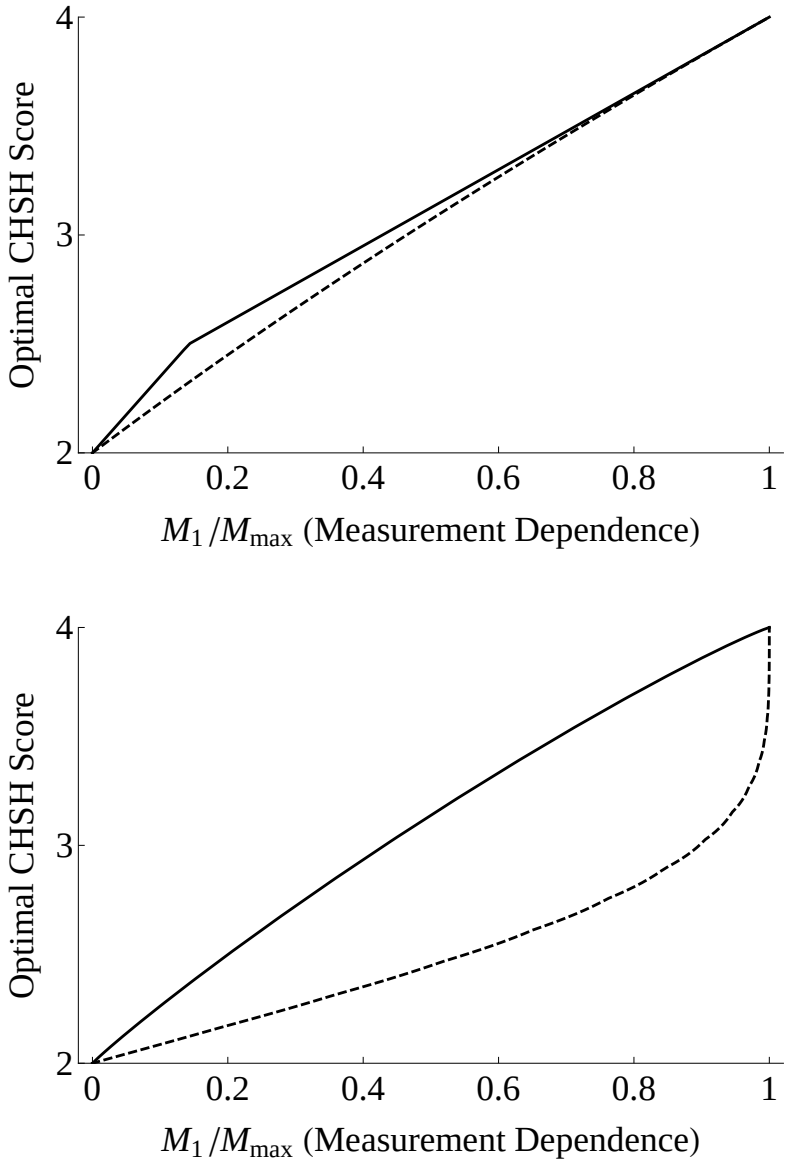

Figure 5.3: Comparison of the optimal correlated attack (solid line) with N repetitions of the optimal one-shot attack (dashed line) for $N = 2$ (top) and $N = 100$ (bottom), using the CHSH inequality. The maximum score $S = 4$ can be simulated classically with a measurement dependence of $M_K = M_{\max} := \frac{4^N}{4^N-1}\left(1 - \left(\frac{3}{4}\right)^N\right)$.

said variable. We find the set of variables that are inequivalent for our purposes. There are 2^{2m} possible outcome sets - since we are only interested in correlations we can disregard 2^m sets which are conjugates of the other 2^m. We then calculate the correlations for each set, deduce the minimum number of incorrect answers over all given outcome sets, and list as variables λ all sets that achieve this minimum. Whilst such a systematic approach can discover these optimal outcome sets, the program

scales exponentially with m so an analytic method is preferred. Whilst the structure is different for $m = 2$ and $m = 3$ (see Tables 2.1 and 5.4 respectively), it is remarkably similar for all $m \geqslant 4$ due to the structure of the coefficients $\alpha_{jk}^{(m)}$.

Theorem 11. *There are eight outcome sets that maximise S_{mm22} for $m \geqslant 4$. These are specified by four underlying variables $\lambda_0, \ldots, \lambda_3$ such that $B_{m-1}(\lambda_1) = A_{m-1}(\lambda_2) = A_{m-1}(\lambda_3) = B_{m-1}(\lambda_3) = -1$, with all other outcomes $+1$, as well as the conjugate variables $\overline{\lambda}_0, \ldots, \overline{\lambda}_3$, which take the negative of these specifications.*

Proof. The following proof applies for $m \geqslant 6$; $m = 4, 5$ can be derived systematically as above. Define a classical strategy by $(a, b) \in \{\pm 1\}^m \otimes \{\pm 1\}^m$, where a_j is the measurement outcome specified when the measurement A_j is made, similarly for b_k. The string consisting entirely of $+1$'s gives the value $S = \binom{m+1}{2} - m + 1$. To prove this is the classical bound for S_{mm22}, consider the table of coefficients $\alpha_{jk}^{(m)}$. We will define $m - 1$ disjoint sets D_n, each of which consist of precisely one (j, k)-pair with $\alpha_{jk}^{(m)} = -1$ and three pairs $(j', k), (j, k'), (j', k')$ with $j' < j, k' < k$ so that the coefficients for these pairs are all $+1$. Table 5.3 shows an example for $m = 6$. Observe that

$$S_{D_n} = \sum_{(j,k) \in D_n} \alpha_{jk}^{(m)} a_j b_k \tag{5.33}$$

is simply a CHSH test classically bounded by 2. Regardless of the specific D_n, there are $\binom{m+1}{2} - 3(m-1)$ pairs (j, k) remaining, each with $\alpha_{jk}^{(m)} = +1$. By fixing the corresponding (a_j, b_k)-pairs to be always correlated, we obtain the bound

$$S \leqslant \sum_{n=1}^{m-1} S_{D_n} + \binom{m+1}{2} - 3(m-1) \leqslant \binom{m+1}{2} - m + 1. \tag{5.34}$$

Now to find all optimal strategies which achieve this bound. Define $D_n := \{(n - 1, m - n - 1), (n - 1, m - n + 1), (n, m - n - 1), (n, m - n + 1)\}$ for $n = 1, \ldots, m - 2$ and $D_{m-1} := \{(1, 0), (1, 1), (m - 1, 0), (m - 1, 1)\}$. This choice of sets for $m = 6$ is illustrated in Table 5.3. We require $a_0 = b_l$ for $l = 0, 1, \ldots, m - 4$ and $l = m - 2$, since $(0, l) \notin \cup D_n$ thus correlated outcomes are needed to maximise S. Similarly, the 'symmetrically equivalent' sets defined by $D'_n := \{(m - n - 1, n - 1), (m - n + 1, n - 1), (m-n-1, n), (m-n+1, n)\}$ for $n = 1, \ldots, m-2$ and $D'_{m-1} := \{(0, 1), (1, 1), (0, m - 1), (1, m - 1)\}$ are an equally valid specification (each set D'_n is simply D_n mirrored in the main diagonal of Table 5.3), and necessitate $b_0 = a_l$ for the same range of l. Furthermore,

$$S_{D_1} = a_{m-3}(b_0 + b_1) + a_{m-1}(b_0 - b_1) = 2a_{m-3}b_0$$

Alice (j) \ Bob (k)	0	1	2	3	4	5
0	1	1	1	1	1	1
1	1	1	1	1	1	-1
2	1	1	1	1	-1	0
3	1	1	1	-1	0	0
4	1	1	-1	0	0	0
5	1	-1	0	0	0	0

Table 5.3: The coefficients $\alpha_{jk}^{(6)}$. The coloured sections indicate the sets D_n from $n = 1$ (light) to $n = 5$ (dark).

since $b_0 = b_1$, so we require $a_{m-3} = b_0$ to maximise S_{D_1}, but no restriction is placed on a_{m-1}. Similarly, maximising $S_{D_1'}$ requires $b_{m-3} = a_0$ but places no restriction on b_{m-1}. Therefore the eight outcome sets spanned by the values $a_0, a_{m-1}, b_{m-1} \in \{\pm 1\}$, with $a_j = b_k = a_0$ for all other j, k, are the only candidates to maximise S, and one can easily verify that all of them do. □

The methods for I_{3322} in the following section can be applied here with a small change in the numerics. However, given that I_{3322} has a slightly more difficult structure, and the inequality itself is of greater interest in existing literature, we shall focus our efforts there.

5.2.3 I_{3322} Inequality

The I_{3322} and S_{3322} inequalities are given by (5.31) and (5.32) when $m = 3$, particularly

$$\begin{aligned} S_{3322} &= \langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_0 B_2 \rangle + \langle A_1 B_0 \rangle \\ &+ \langle A_1 B_1 \rangle + \langle A_2 B_0 \rangle - \langle A_1 B_2 \rangle - \langle A_2 B_1 \rangle \end{aligned}$$

which has 4 as an LHV bound, and clearly 8 as a no-signalling bound. In contrast to S_{mm22} for all $m > 3$, where there are only four optimal outcome sets, there are actually six outcome sets for $m = 3$, specified in Table 5.4 using the shorthand jk to mean the resulting correlations $\langle A_j B_k \rangle_\lambda$.

For this inequality (as well as $m \geqslant 4$), use of the M_K measure is preferable to M_H. This is because the columns in the table of correlations do not contain the same number of incorrect answers and therefore the symmetry invoked for CHSH does not apply. Whilst (by definition) the rows do contain an equal number of incorrect answers in a single run and therefore the same structure, up to permutations, in the

	A_0	A_1	A_2	B_0	B_1	B_2	00	01	02	10	11	20	-12	-21
λ_0	1	1	1	1	1	1	1	1	1	1	1	1	-1	-1
λ_1	1	1	-1	1	1	-1	1	1	-1	1	1	-1	1	1
λ_2	1	-1	1	1	-1	1	1	-1	1	-1	1	1	1	1
λ_3	1	-1	-1	-1	1	1	-1	1	1	1	-1	1	1	1
λ_4	1	1	1	1	1	-1	1	1	-1	1	1	1	1	-1
λ_5	1	1	-1	1	1	1	1	1	1	1	1	-1	-1	1

Table 5.4: Optimal ouctome specifications and correlations maximising I_{3322}.

N-run scenario, there is one other important distinction from CHSH to be made; the input pair (A_2, B_2) is not evaluated for the inequality.

Since an eavesdropper wishes to convince Alice and Bob that they are performing a fair experiment with local measurement choices, this pair must still be implemented with probability 1/9 on any given run. Whilst the outcome correlations for this pair are not required for evaluating S_{3322}, the counting structure is now different from CHSH. Our analysis has not only a dependence on the number k of correct answers that an $(\boldsymbol{i}, \boldsymbol{j})$-pair gives (where now $\boldsymbol{i} \in \{0, \ldots, 5\}^N$,$\boldsymbol{j} \in \{0, \ldots, 8\}^N$ and the input pair on the nth run is given by $A^n_{\lfloor j_n/3 \rfloor} B^n_{j_n \mathrm{mod} 3}$), but also the number l of instances of (A_2, B_2), hereby defined as the number of *zero answers*. For a fixed column $\boldsymbol{j}$, this is clearly $l(\boldsymbol{j}) = \#\{n : j_n = 8\}$. The probabilities $p(\boldsymbol{j}|\boldsymbol{i})$ reduce to a set $\{p_{k,l}\}_{k,l=0,\ldots,N}$, and the linear programming technique will begin with a vector of these probabilities $\boldsymbol{p} := (p_{k,l})_{k,l=0,\ldots,N}$, though of course the nature of the experiment intuitively demands $k + l \leqslant N$.

Recall that the probabilities $p(\boldsymbol{j}|\boldsymbol{i})$ must satisfy the column conditions (5.23), where now $p(\boldsymbol{j}) = 9^{-N}$. The choice of $p(\boldsymbol{i})$ is only partially restricted; any assignment for $p(\boldsymbol{i})$ that satisfies (5.23) will be sufficient. One might first consider, as with CHSH, a uniform distribution $p(\boldsymbol{i}) = 6^{-N}$ over all strings $\{0, \ldots, 5\}^N$, which represent all N-fold combinations of the optimal outcome sets specified by $\lambda_0, \ldots, \lambda_5$ in Table 5.4. Whilst this is a possibility, note that some columns in that table give two wrong answers (i.e. the -1's), whereas others give only one. The resulting N-run columns will therefore yield a complicated set of conditions (5.23), since the numbers of $p_{k,l}$ terms in a column will vary depending on the total number of wrong answers contained in that column. It will be helpful to reduce the number of conditions by specifying $p(\boldsymbol{i})$ such that each column contains the same number of wrong answers[5].

[5]This will also be the case for the I_{mm22} inequalities whose single-run outcome sets are given in Theorem 11.

Consider removing the outcome sets specified by λ_4 and λ_5. The resulting table then contains only one wrong answer in each column, and for the N-run equivalent (i.e. $p(\boldsymbol{i}) = 4^{-N}$ for $\boldsymbol{i} \in \{0,1,2,3\}^N$) the structure of each N-run column $\boldsymbol{j}$, up to permutations, differs only according to the number of zero answers $l(\boldsymbol{j})$. There are therefore only $N+1$ column conditions of the form (5.23) to consider depending on the number of zero answers l:

$$\sum_{k=0}^{N-l} \binom{N-l}{k} 3^k 4^l p_{k,l} = \left(\frac{4}{9}\right)^N \qquad , \qquad l = 0, 1, \ldots, N. \tag{5.35}$$

Observe that these constraints *replace* the column normalisation condition (5.26) for CHSH, where l was always 0 and the right-hand side was 1. The new matrix representation for (5.35) is $D \cdot \boldsymbol{p} = \left(\left(\frac{4}{9}\right)^N\right)^T$, where the vector $\left(\left(\frac{4}{9}\right)^N\right)$ has length $N+1$, and D has the block structure $D^T = (\ \boldsymbol{d}^0 \quad \boldsymbol{d}^1 \quad \cdots \quad \boldsymbol{d}^N\ )$, with $\boldsymbol{d}^j$ being a vector of length $(N+1)^2$ defined by

$$d^j_{k,l} = \delta_{l,j} \binom{N-l}{k} 3^k 4^l.$$

Note that for the experimentally impossible cases $k+l > N$, these coefficients vanish due to the presence of the binomial term, so this is not problematic.

Having programmed these conditions, the remainder of the task is similar to the CHSH case. First express S_{3322}, here reduced to S for brevity, from first principles as before.

$$S^{\boldsymbol{j}}_{\boldsymbol{i}} = \frac{1}{N}(1 \cdot k(\boldsymbol{i},\boldsymbol{j}) + 0 \cdot l(\boldsymbol{j}) + (-1) \cdot (N - k(\boldsymbol{i},\boldsymbol{j}) - l(\boldsymbol{j})))$$

$$\begin{aligned} S_{\boldsymbol{i}} = 9 \sum_{\boldsymbol{j}} p(\boldsymbol{j}|\boldsymbol{i}) S^{\boldsymbol{j}}_{\boldsymbol{i}} &= -9 + \frac{9}{N} \sum_{\boldsymbol{j}} p(\boldsymbol{j}|\boldsymbol{i})(2k(\boldsymbol{i},\boldsymbol{j}) + l(\boldsymbol{j})) \\ S = \sum_{\boldsymbol{i}} p(\boldsymbol{i}) S_{\boldsymbol{i}} &= -9 + \frac{9}{N} \sum_{\boldsymbol{i}} p(\boldsymbol{i}) \sum_{\boldsymbol{j}} p(\boldsymbol{j}|\boldsymbol{i})(2k(\boldsymbol{i},\boldsymbol{j}) + l(\boldsymbol{j})). \end{aligned} \tag{5.36}$$

By using the distribution $p(\boldsymbol{i}) = 4^{-N}$ for $\boldsymbol{i} \in \{0,1,2,3\}^N$, and noting that the rows of this table are permutation-invariant[6], counting arguments reduce (5.36) to

$$S = -9 + \frac{9}{N} \sum_{k=0}^{N} \sum_{l=0}^{N-k} \frac{N!}{k!l!(N-k-l)!} 6^k 2^{N-k-l} (2k+l) p_{k,l},$$

which can be encoded by the vector $\boldsymbol{s}$ where $s_{k,l}$ is the coefficient of $p_{k,l}$ in the above sum. Again note that $s_{k,l} = 0$ whenever $k + l > N$.

[6]Indeed, this property justifies our ability to select any distribution for $p(\boldsymbol{i})$, since the latter sum in (5.36) actually has no dependence on $\boldsymbol{i}$, thus $\sum_{\boldsymbol{i}} p(\boldsymbol{i}) = 1$ comes out in the wash.

Finally, a condition for M_K is required. For this inequality, since the rows are permutation invariant, the maximisation in the definition of M_K is unnecessary and the constraint reduces to

$$M_K = \frac{9^N}{2(9^N-1)} \sum_{k=0}^{N} \sum_{l=0}^{N-k} \frac{N!}{k!l!(N-k-l)!} 6^k 2^{N-k-l} \left| p_{k,l} - 9^{-N} \right|.$$

To overcome the modulus, introduce non-negative variables $\boldsymbol{w}, \boldsymbol{a}, \boldsymbol{b}$ as before, where $w_{k,l} \geqslant p_{k,l} - 9^{-N}, w_{k,l} \geqslant 9^{-N} - p_{k,l}$, so that our constraint is $M_K = \frac{9^N}{2(9^N-1)} \boldsymbol{m} \cdot \boldsymbol{w}$ where $m_{k,l} := \frac{N!}{k!l!(N-k-l)!} 6^k 2^{N-k-l}$, and $a_{k,l} := w_{k,l} - x_{k,l} + 9^{-N}$ and $b_{k,l} := w_{k,l} + x_{k,l} - 9^{-N}$. The overall linear programming problem is thus to minimize $\boldsymbol{c} \cdot \boldsymbol{z}$ subject to $B \cdot \boldsymbol{z} = \boldsymbol{v}$, where the block structure of each component is

$$B = \begin{pmatrix} D & 0 & 0 & 0 \\ \mathbb{1} & -\mathbb{1} & \mathbb{1} & 0 \\ -\mathbb{1} & -\mathbb{1} & 0 & \mathbb{1} \\ 0 & \boldsymbol{m} & 0 & 0 \end{pmatrix}, \ \boldsymbol{z} = \begin{pmatrix} \boldsymbol{p} \\ \boldsymbol{w} \\ \boldsymbol{a} \\ \boldsymbol{b} \end{pmatrix}, \ \boldsymbol{v} = \begin{pmatrix} \left(\frac{4}{9}\right)^N \\ 9^{-N} \\ -9^{-N} \\ \frac{2(9^N-1)}{9^N} M_K \end{pmatrix}, \ \boldsymbol{c} = \begin{pmatrix} -\boldsymbol{s} \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

The evaluation for S_{3322} is then given by $S = -9 - \frac{9}{N} \boldsymbol{c} \cdot \boldsymbol{z}$. The program may again be used to plot S vs M_K, as in Figure 5.4, which rescales according to the minimum value of M_K that first achieves $S_{3322} = 8$, this being $M_{\max}(N) = \frac{9^N}{2(9^N-1)} \left(1 - \left(\frac{7}{9}\right)^N\right)$.

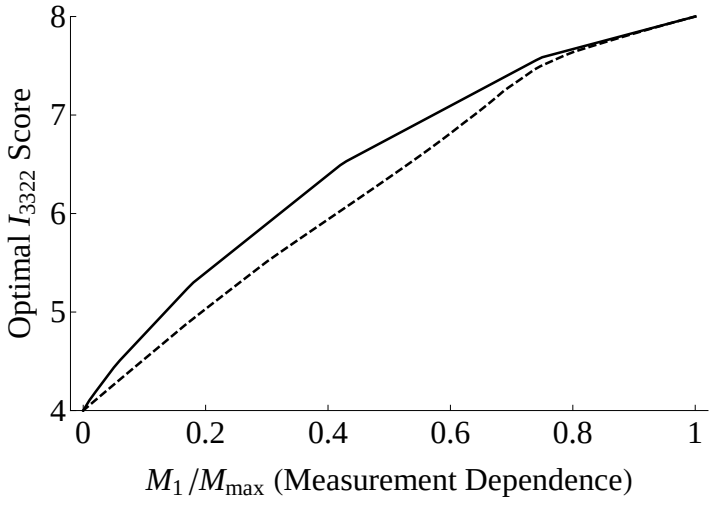

Figure 5.4: Comparison of the optimal correlated attack (solid line) with N repetitions of the optimal one-shot attack (dashed line) for $N = 10$, using the I_{3322} inequality. The maximum score $S_{3322} = 8$ can be simulated classically with a measurement dependence of $M_K = M_{\max} := \frac{9^N}{2(9^N-1)} \left(1 - \left(\frac{7}{9}\right)^N\right)$.

The plot also includes a comparison with N repetitions of the one-shot strategy. Whilst this strategy was not derived prior to the numerical approach above, the numerics determine that the optimal one-shot strategy for a fixed measurement dependence is defined by a single parameter $Q \in [\frac{1}{9}, \frac{4}{27}]$ and assigns probability Q for a correct answer, fixed probability $\frac{1}{9}$ for a zero answer, and therefore probability $\frac{4-27Q}{9}$ for an incorrect answer. The relation between S and M_K for a single run can then be derived as $S = 4 + 16M_K$. The simplicity of this structure suggests that an analytic proof of this model's optimality (akin to Theorem 1) would be fairly easy, yet unnecessary due to the numerical proof. Note that the condition (5.23) for $N = 1$ and $\boldsymbol{j} = 8$ reduces to $p(A_2B_2|\lambda_n) = p(A_2B_2) = \frac{1}{9}$ regardless of n, since our symmetry simplification requires that all probabilities in this column are the same; this justification agrees with the numerical result. The model determined by N runs of this strategy is specified by

$$p_{k,l} = Q^k \left(\frac{1}{9}\right)^l \left(\frac{4-27Q}{9}\right)^{N-k-l}. \tag{5.37}$$

Tables 5.5 and 5.2.3 provide a summary of these optimal strategies.

	$M_{\max}$	Measurement Distribution	Outcomes	S	M	N repetitions
CHSH	$M_H = 1/3$ $M_S = 1/9$ $M_K = 1/3$	Table 2.2 Table 2.3	Table 2.1	$24P - 4$	$M_H = 4P - 1$ $M_S = (4P-1)^2$ $M_K = 4P - 1$	$p_k = P^k(1-3P)^{N-k}$ $M_S(P)$ given by (5.14)
I_{3322}	$M_K = 1/4$	$p_{1,0} = Q$ $p_{0,0} = \frac{4-27Q}{9}$ $\quad Q \in [\frac{1}{9}, \frac{4}{27}]$ $p_{0,1} = \frac{1}{9}$	Table 5.4	$108Q - 8$	$M_K = \frac{1}{4}(27Q - 3)$	$p_{k,l} = Q^k(\frac{1}{9})^l(\frac{4-27Q}{9})^{N-k-l}$ (5.37)

Table 5.5: Summary of optimal one-shot strategies.

	Model	S achieved	M_H	M_K	P
CHSH	$p_k = \frac{1}{4^N}$ $p_k = \delta_{k,N}\frac{1}{3^N}$	$S_{\min} = 2$ $S_{\max} = 4$	0 $\frac{1}{3^{2N}}(3^N - 2^N)$	0 $\frac{4^N-3^N}{2(4^N-1)}$	$\frac{1}{4^N}$ $\frac{1}{3^N}$
I_{3322}	$p_{k,l} = \frac{1}{9^N}$ $p_{k,l} = \delta_{l,N-k}\left(\frac{4}{27}\right)^k\left(\frac{1}{9}\right)^{N-k}$	$S_{\min} = 4$ $S_{\max} = 8$	0 -	0 $\frac{9^N-7^N}{2(9^N-1)}$	$\frac{1}{9^N}$ $\left(\frac{4}{27}\right)^N$

Table 5.6: Summary of N-run threshold models, which both the optimal single-shot and correlated strategies reduce to.

5.3 Using P and Bounds for all N

Whilst the above analysis for the M_K measure have yielded significant results, there are still complexities with this measure that make closed-form solutions difficult to obtain. This is unfortunate because the measure is rather intuitive as to how it interprets free will as the difference in input distributions between an eavesdropper with extra underlying information and the experimenters without. However recall the simpler measure $P = \max_{j,k,\lambda} p(A_j, B_k|\lambda)$, which is actually equivalent to the ∞-norm version of M_K given by (2.8). The definition of P extends to an N-run model by considering all possible combinations of measurement settings $\boldsymbol{j}$ and underlying outcome specifications $\boldsymbol{i}$,

$$P_{(N)} := \max_{\boldsymbol{i},\boldsymbol{j}} p(\boldsymbol{j}|\boldsymbol{i}). \tag{5.38}$$

As shown below, the simplicity of this measure not only allows for an analytic plot of N-run comparisons, but also provides a closed form bound, i.e. for a given value of P, a Bell violation S can only be achieved by a correlated limited-free-will strategy up to some function $S(P)$. Furthermore, this bound is independent of the number N runs of the experiment, and thus is adhered to by all feasible correlated strategies regardless of the number of iterations.

5.3.1 Classical Strategies and General Bound

The focus of this result is again on the CHSH inequality, though it seems reasonable that the consideration of the other Bell inequalities in Section 5.2 could be extended to this work. The equations needed to perform this analysis have already been derived, specifically the equations (5.26) and (5.27) in Section 5.2.1, replicated here. The aim is to maximise

$$S = \frac{8}{N}\sum_{k=0}^{N} k p_k 3^k \binom{N}{k} - 4 \tag{5.39}$$

subject to the normalisation condition

$$\sum_{k=0}^{N} p_k 3^k \binom{N}{k} = 1 \tag{5.40}$$

and fixed measurement dependence $P_{(N)}$.

It is clear that the optimal single-shot strategy given by Table 2.3, when repeated independently for N runs, has MD $P_{(N)} = P^N \in [4^{-N}, 3^{-N}]$. As has already been shown, the optimal correlated attack will obviously perform as well or better than

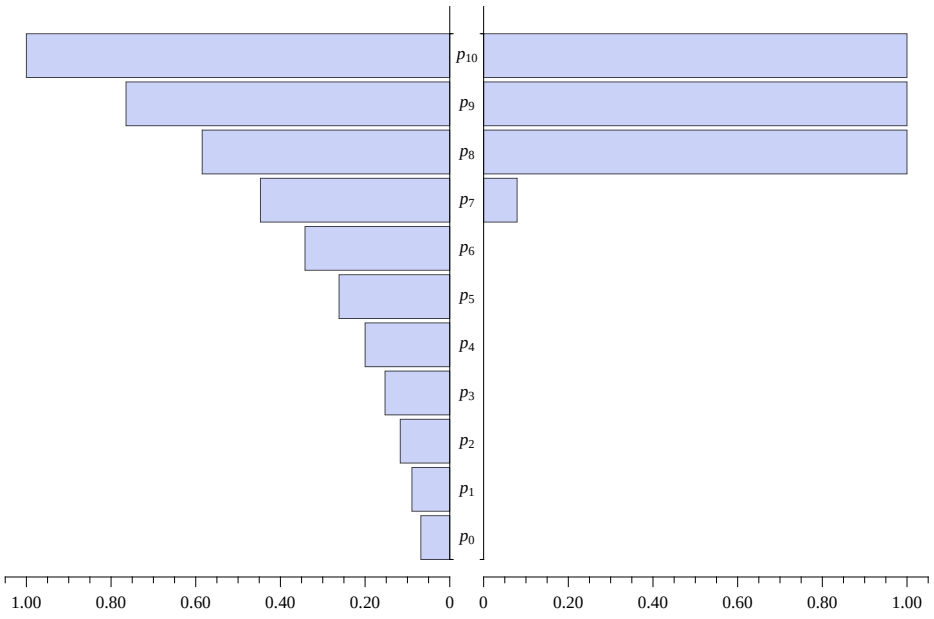

Figure 5.5: The values of p_k/P^N, where $P = 51/192$ and $N = 10$, comparing the repeated optimal one-shot strategy (left) with the optimal correlated strategy (right).

this, and comparison can be made with the repeated single-shot strategy over varying N by taking the Nth root, thus a fixed MD P requires that $p(\boldsymbol{j}|\boldsymbol{i}) \leqslant P^N$ for all $\boldsymbol{i}, \boldsymbol{j}$. We may again invoke symmetry arguments to reduce the conditional probabilities to the set $\{p_k\}$ dependent only on the number k of correct CHSH queries answered. Thus,

$$p_k \leqslant P^N \qquad \forall k. \tag{5.41}$$

The linear programming problem encapsulated by (5.39),(5.40) and (5.41) is simpler than that for M_K, and an equally explicit encoding is not included here. However, the simplicity of the P measure allows for an analytical examination of the optimal attacks.

Intuitively for a CHSH test, obtaining the maximum S value requires more weight to be given to the pairs of measurement settings that answer a larger proportion of the N queries correctly. Therefore we assign $p_N = P^N$. If the normalisation (5.40) allows, set $p_{N-1} = P^N$, and so on. All remaining p_k are set to 0. A comparison of this optimal correlated strategy with the repeated optimal one-shot strategy given by $p_k = P^k(1-3P)^{N-k}$ is illustrated in Figure 5.5. These strategies only coincide when $N = 1$ (i.e. no correlations over runs), $P = 1/4$ ($p_k = 4^{-N}$ for all k) or $P = 1/3$ ($p_k = 0$ for all $k \neq N$ and $p_N = 3^{-N}$).

The curve of maximum S against P^N is piecewise linear, connected by the $N+1$ points defined by a parameter l' such that

$$P = \left(\sum_{k=l'}^{N} 3^k \binom{N}{k}\right)^{-1/N}, \tag{5.42}$$

$$S = \frac{8\sum_{k=l'}^{N} k3^k \binom{N}{k}}{N\sum_{k=l'}^{N} 3^k \binom{N}{k}} - 4. \tag{5.43}$$

The curve is linearly interpolated for P^N, where $P \in [1/4, 1/3]$ between these points by assigning $p_k = 0$ for $k < l' - 1$, $p_k = P^N$ for $k \geqslant l'$, and letting $p_{l'-1}$ fulfil the normalisation (5.40). Figure 5.6 shows such plots for various finite values of N. We see immediately that the eavesdropper gains an advantage with increasing N, outperforming the single-shot attack.

The optimal strategy's behaviour in the large N limit is less clear. Is the limiting curve simply the $S = 4$ line, making perfect measurement independence the singular point at which the CHSH test functions? The following theorem answers this in the negative.

Theorem 12. *The measurement dependence P required to simulate a CHSH score S with a deterministic strategy correlated over N runs, in the $N \to \infty$ limit, has the lower bound*

$$P \geqslant \left(\frac{4+S}{24}\right)^{\frac{4+S}{8}} \left(\frac{4-S}{8}\right)^{\frac{4-S}{8}}. \tag{5.44}$$

Proof. It is enough to consider the $N+1$ points defined by (5.42) and (5.43) and find lower/upper bounds for P/S respectively as functions of the rescaled parameter $l = l'/N \in [3/4, 1]$. To bound P, observe that $P = \frac{1}{4}\Pr(X \geqslant l')^{-1/N}$ where X is a binomial distribution with N trials and success probability $3/4$. The additive form of the Chernoff bound easily recovers

$$P \geqslant (l/3)^l (1-l)^{1-l}. \tag{5.45}$$

We aim to bound S by dividing the region $k = l' \ldots N$ into two runs, split at αN, such that

$$R_1 := \sum_{k=l'}^{\alpha N - 1} 3^k \binom{N}{k} \geqslant 3^{lN} \binom{N}{lN} \geqslant 3^{lN} e^{NH(l)},$$

$$R_2 := \sum_{\alpha N}^{N} 3^k \binom{N}{k} \leqslant 4^N e^{-ND(\alpha \| \frac{3}{4})},$$

where we have used Stirling's approximation and a Chernoff bound respectively. $H(l) = -l\log l - (1-l)\log(1-l)$ is the binary entropy while

$$D(\alpha\|\beta) = \alpha\log\left(\frac{\alpha}{\beta}\right) + (1-\alpha)\log\left(\frac{1-\alpha}{1-\beta}\right)$$

is the Kulback-Leibler divergence between Bernoulli distributed random variables with parameters α and β. For any $\alpha = l + \epsilon$ with finite (but small) ϵ,

$$\frac{R_2}{R_1} \leqslant \frac{4^N e^{-ND(\alpha\|\frac{3}{4})}}{3^{lN} e^{NH(l)}}$$

is exponentially small in ϵN. For increasing $\frac{R_2}{R_1}$,

$$S \leqslant 8\frac{\alpha R_1 + R_2}{R_1 + R_2} - 4$$

is increasing. In the large N limit this yields

$$S \leqslant 8(l+\epsilon) - 4. \tag{5.46}$$

The bound is tight since a lower bound for (5.43) is given by

$$S \geqslant 8\frac{P^N l'}{N}\sum_{k=l'}^{N} 3^k \binom{N}{k} - 4 = 8l - 4, \tag{5.47}$$

substituting the definition of P in (5.42). Substitution for l in the bounds (5.45) and (5.46) yields the result. □

The bound may alternatively be expressed in terms of the CHSH winning probability p_{win} (recall (1.8)) as

$$P \geqslant \left(\frac{p_{\text{win}}}{3}\right)^{p_{\text{win}}} (1-p_{\text{win}})^{1-p_{\text{win}}}. \tag{5.48}$$

The similarity of the bounds (5.45) and (5.48) is not surprising; At the points l' defined by (5.42) and (5.43), $l = l'/N$ is simply the ratio of the N CHSH queries which are answered correctly, which is equivalent to the winning probability when restricted to a game with N rounds. As $N \to \infty$, there become infinitely many points l', and so $l \to p_{\text{win}}$ (this is essentially what the derivation of (5.46) confirms).

The regime of allowable classical correlated attacks described by Theorem 1 is depicted by the solid lines in Figure 5.6. The points $P_\infty \approx 0.258$ and $P_1 \approx 0.285$ are where a CHSH value of $S = 2\sqrt{2}$ can be achieved with (infinitely) correlated strategies and single-shot attacks respectively. In the shaded region (for $P < P_\infty$), the S values are below $2\sqrt{2}$ and therefore achievable with quantum technologies, and yet can never be simulated by any arbitrarily correlated attack without detection from Alice and Bob in their observed measurement choices.

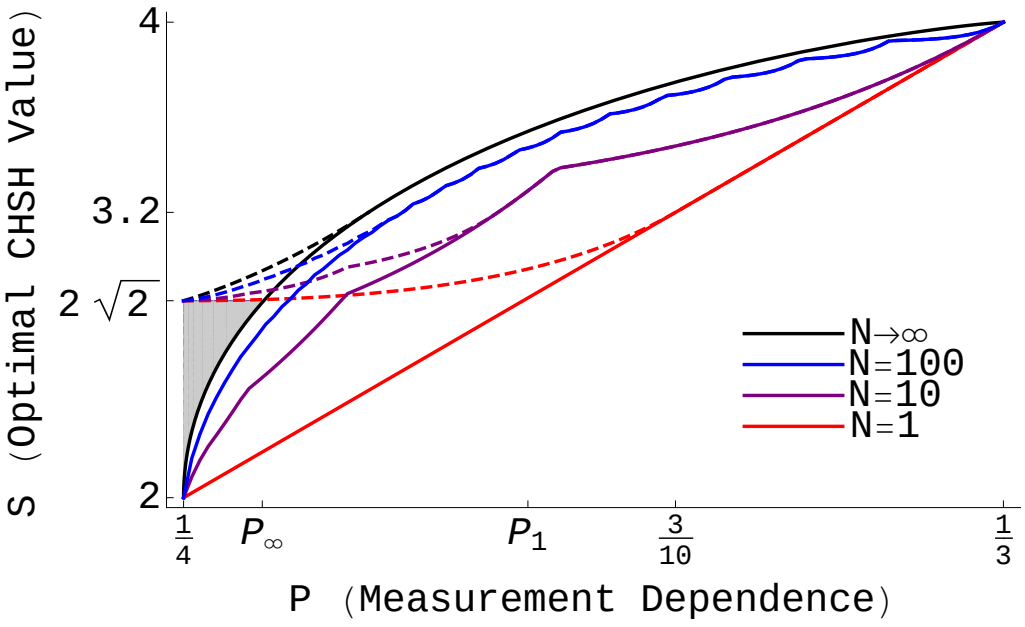

Figure 5.6: S vs P for classical (solid, see (5.42)–(5.43)) and quantum (dashed, see (5.52)) strategies correlated over N runs, and bounded above for all N (black lines, see (5.42)–(5.43)).

5.3.2 Quantum Strategies and General Bound

Tsirelson's bound proves that a test of the CHSH inequality with perfect free will has a maximum possible value of $2\sqrt{2}$, for instance when the experimenters perform quantum measurements on a singlet state [19]. Such quantum strategies are known to be vulnerable to a limited-free-will attack in the single-shot case by optimising over both the measurement input distribution and the measurement operators themselves [1]. Furthermore, as with the classical adversarial strategy above, Eve can enhance a quantum attack by correlating over N runs of the experiment.

Whilst the outcomes of later runs can in principle be allowed to depend on the outcomes of previous runs through use of a quantum state entangled between all of the devices, here we make the common assumption that each run is causally disconnected [77, 55] to exclude the possibility of such dependence. The effective CHSH operator being optimised is of the form

$$\mathcal{S}\otimes\mathbb{1}\otimes\mathbb{1}\ldots+\mathbb{1}\otimes\mathcal{S}\otimes\mathbb{1}\ldots+\mathbb{1}\otimes\mathbb{1}\otimes\mathcal{S}\ldots+\ldots$$

and the state that optimises this operator is separable, corresponding to a tensor product of the states that optimise $\langle\mathcal{S}\rangle$ in (5.49) below, such that $|\langle\mathcal{S}_N\rangle| = N|\langle\mathcal{S}\rangle|$, so it is enough to optimise over the single-shot operator $\mathcal{S}$.

For a specified value of P, determining the optimal quantum strategy (which will typically correspond to no eavesdropping) will yield the maximum realisable CHSH value, which is important in bounding an eavesdropper's knowledge for a given CHSH value.

Using the notation $p_{\boldsymbol{j}}$ for the probabilities of a given set of N measurement settings described by a string $\boldsymbol{j} \in \{0,1,2,3\}^N$, the aim is to maximise the expectation

$$\langle S \rangle = \frac{4}{N} \sum_{n=1}^{N} \langle p_0^n A_0 B_0 + p_1^n A_0 B_1 + p_2^n A_1 B_0 - p_3^n A_1 B_1 \rangle \tag{5.49}$$

where $p_m^n = \sum_{\boldsymbol{j}:j_n=m} p_{\boldsymbol{j}}$ are the marginal probabilities for a given setting m being chosen on run n, and the measurement operators A_j and B_k are two-valued operators. Bounds on S subject to fixed P were derived for an individual run in Section 3.3. Using the same symmetry arguments as above, we reduce the set $\{p_{\boldsymbol{j}}\}$ to $\{p_k\}$ according to the number of correct answers each set $\boldsymbol{j}$ gives. This leaves $p_0^n = p_1^n = p_2^n = R$ and $p_3^n = 1 - 3R$ where, through the symmetry-based reduction, R is simply

$$R = \sum_{k=1}^{N} 3^{k-1} \binom{N-1}{k-1} p_k \tag{5.50}$$

which is equivalent to (5.39) up to constant factors. Therefore, for a fixed degree of free will requiring $p_k \leqslant P^N \ \ \forall k$, R is optimised by the same input distribution (see Eq. (5.42)). The achievable values of S are then, according to Theorem 8 in Section 3.3,

$$|\langle S \rangle| \leqslant \frac{4(1-2R)^{3/2}}{\sqrt{1-3R}}, \tag{5.51}$$

provided $R < 3/10$. This maximal value S_Q can be compared with the value $S_C = 4(6R-1)$ obtained by the optimal classical, deterministic strategy as

$$S_Q = \frac{2(8-S_C)^{3/2}}{3\sqrt{6(4-S_C)}} \tag{5.52}$$

when $S_C < 16/5$. For $R \geqslant 3/10$, hence $S_C \geqslant 16/5$, the two strategies coincide. The quantum strategies are compared with their classical equivalents in Figure 5.6.

It is worth noting that there are Bell inequalities for which the quantum strategy outperforms classical everywhere except for at the algebraic limit. For instance, this chapter's treatment can be applied to the tripartite Mermin inequality (based on the GHZ paradox in Section 1.4.3.1), as sketched in Appendix B.

5.4 Comparison with Randomness Amplification

The correlated attacks investigated in this chapter have strong ties with recent studies of randomness amplification, a task first proposed in [41]. As noted in Section 1.5.1, this task is not the same as the randomness expansion discussed in Chapter 3, where a long sequence of random bits is generated from a relatively short, but perfectly random, seed; The seed in a randomness amplification protocol may be arbitrarily large yet display only imperfect randomness. Whilst such a task has been shown to be impossible in the classical regime [94, 105], Colbeck and Renner [41] proved that by using the imperfect random seed to make measurement selections in a test of chained Bell inequalities (see Section 1.4.3.1), an output bit can be generated that is arbitrarily close to being random[7]. Whilst the randomness of the seed used in their protocol was required to already exhibit a fixed high level of randomness, further work produced alternative protocols amplifying arbitrarily low amounts of randomness using Mermin inequalities between five parties [106] and three parties [107], and recently a protocol based on a four-party Bell inequality was proposed to amplify randomness even within a noisy quantum environment [108]. The efficacy of randomness amplification for more general inequalities has also been studied in terms of the convex combination of no-signalling boxes required to simulate the quantum violation of that inequality [109]. This chapter's results can be seen as a complement to these randomness amplification protocols, with some notable differences.

Since the initial seeds in randomness amplification protocols are used to select measurements in a Bell test, the seed's quality of randomness is inextricably linked to the notion of measurement dependence. Using any one of the proposed measures, a pair of RNGs with full measurement independence will provide uniform outputs, equivalent to both Alice and Bob using a local perfectly random seed to select their measurements. However, all of the above studies required the sources to fulfil a restriction known as the Santha-Vazirani condition [94]. For a source generating a sequence of bits $z_i \in \{0, 1\}$, this condition may be expressed as

$$\frac{1}{2} - \epsilon \leqslant p(z_n|\lambda, z_1, \ldots, z_{n-1}) \leqslant \frac{1}{2} + \epsilon \tag{5.53}$$

for some $\epsilon \in [0, 1/2]$ and any n, where λ encapsulates any underlying variables influencing the source. The generation of bits satisfying this condition may be interpreted

[7]The terminology is slightly different from our results since the quality of randomness available in a source is discussed in the context of the source's correlations (or lack thereof) with outside variables.

as flipping a biased coin, where the bias ϵ is determined by an adversary with access to all previously generated bits.

As noted in [34], the presence of a positive lower bound on the probabilities in (5.53) prevents the predetermined exclusion of a measurement choice. Whilst the users of the devices view the two RNGs as separate entities, and the Santha-Vazirani specification is for individual RNGs, an eavesdropper who is preprogramming both devices has arbitrary access to program them as she wishes, and so effectively considers them as one joint entity. The Santha-Vazirani specification does not exclude such preprogramming strategies (we make no claim that the optimal cheating strategies above cannot be interpreted, at least locally, as satisfying the Santha-Vazirani condition) but does make their presence unclear, both in terms of whether the RNGs are correlated with each other and whether they are correlated with the Bell test outcomes generated by the associated measurement devices.

Furthermore, the randomness amplification procedure is primarily useful as an intermediary step in the process to achieve a particular task such as secure key distribution, and often involves a different Bell inequality to test for, which involves more complexities in the implementation. On the other hand, our analysis can be applied on the fly using the corrupted devices to any of the protocols and experiments that use the CHSH test (and extended to those involving other Bell inequalities), even retrospectively when the experiment has been performed and the data has already been collected.

Our results can nevertheless be interpreted in the context of randomness amplification. For a given MD P, the optimal quantum strategy, in the regime where quantum beats classical (i.e. $S_C < 16/5$), gives perfectly random measurement outcomes on one side. If the players could know the value of the hidden variable in a run, and therefore the measurement selection bias, they can implement the optimal quantum strategy, which has the potential to allow perfect amplification (i.e. procuring perfectly random bits from partially random bits) in this regime. However, there is no obvious reason why honest players would have such knowledge of the hidden variables.

Chapter 6

Conclusions

The rapidly advancing studies of cryptography within the field of quantum information have led to significant claims of security in cryptographic protocols, removing more and more restrictions on the capabilities of an adversary. Quantum cryptography makes such claims against eavesdroppers with unlimited computational power; device-independent cryptography seeks to relinquish trust even within their own experimental apparatus. However, it is important that through all of these significant advancements, every possible pitfall, loophole or experimental imperfection is considered. This thesis has covered one such problem, the free will loophole, and sought to make existing device-independent implementations robust against it.

The emergence of device-independent protocols which remove many assumptions of trust within the experimenters' devices necessitates an analysis of the RNGs that Alice and Bob typically use to select their measurements within a Bell test. We discussed this concept of experimental free will in Chapter 2 and introduced several measures to quantify it. We showed how an eavesdropper programming the RNGs with a hidden model can falsely simulate nonlocality, upon which the security of device-independent protocols is based. The strength of Bell violation is proportional to the amount of measurement dependence in the devices.

Chapters 3 and 4 considered this loophole within the existing device-independent tasks of randomness expansion and key distribution, both based on the CHSH inequality. In the case of randomness expansion, we derived optimality proofs and models to bound the probability of Eve correctly guessing an outcome, which in principle can be used to determine the amount of privacy amplification required to certify the generated randomness as private. However, more work is required in this area, since existing implementations of privacy amplification require some initial randomness to be performed, a quantity considerably under question in limited-free-will scenarios. The cases of general and factorisable no-signalling distributions were considered, as

well as an eavesdropper with quantum technologies. In the case of key distribution, we provided a model with which Eve could simulate nonlocality for a given measurement dependence and key predictability. It would be interesting to find optimality within this regime, as well as make improvements on key generation efficiency.

Finally, we extended the capabilities of Eve in Chapter 5 to consider attacks correlated over multiple runs of a Bell test. We showed that, despite strong advantages to employing such an attack over a single-shot approach, there nevertheless exist Bell violations which Eve cannot simulate using a variable-free-will model, regardless of the number of runs the attack is correlated over. Our investigation was primarily based on the CHSH inequality, though the analysis can also be extended to more general Bell inequalities.

A crucial question for future work is how to experimentally assess the amount of measurement dependence in a pair of RNGs prior to their use in a Bell test. Since the aim of device-independent protocols is to remove knowledge of the inner workings of experimental apparatus, this is a significant problem. In the case of defending against attacks correlated over multiple runs of the Bell test, a method to impose independence between these runs would also be extremely valuable.

References

[1] Dax Enshan Koh, Michael J. W. Hall, Setiawan, James E. Pope, Chiara Marletto, Alastair Kay, Valerio Scarani, and Artur Ekert. Effects of Reduced Measurement Independence on Bell-Based Randomness Expansion. *Physical Review Letters*, 109(16):160404, 2012.

[2] James E. Pope and Alastair Kay. Limited measurement dependence in multiple runs of a Bell test. *Physical Review A*, 88(3):032110, 2013.

[3] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[4] E. Schrödinger. Die gegenwärtige Situation in der Quantenmechanik. *Naturwissenschaften*, 23(49):823–828, 1935.

[5] E. Schrödinger. The Present Situation in Quantum Mechanics: A Translation of Schrödingers Cat Paradox Paper. *Proceedings of the American Philosophical Society*, 124, 1980.

[6] W. Heisenberg. über den anschaulichen inhalt der quantentheoretischen Kinematik und Mechanik. *Zeitschrift für Physik*, 43(3-4):172–198, 1927.

[7] A. Einstein, B. Podolsky, and N. Rosen. Can Quantum-Mechanical Description of Physical Reality Be Considered Complete? *Physical Review*, 47(10):777, 1935.

[8] D.J.A. Welsh. *Codes and Cryptography*. Clarendon Press, 1988.

[9] T.M. Cover and J.A. Thomas. *Elements of Information Theory*. Wiley, 2012.

[10] 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*, pages 175–179.

[11] Artur K. Ekert. Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 67(6):661–663, 1991.

[12] P. W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *35th Annual Symposium on Foundations of Computer Science*, pages 124–134.

[13] John S. Bell. On the Einstein Podolsky Rosen Paradox. *Physics*, 1(3):195–200, 1964.

[14] Itamar Pitowsky. *From George Boole To John Bell The Origins of Bells Inequality*, volume 37 of *Fundamental Theories of Physics*, chapter 6, pages 37–49. Springer Netherlands, 1989.

[15] Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and Stephanie Wehner. Bell nonlocality. *arXiv:1303.2849*, 2013.

[16] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. Proposed Experiment to Test Local Hidden-Variable Theories. *Physical Review Letters*, 23(15):880–884, 1969.

[17] Artur Ekert, Alastair Kay, and James Pope. Turing, ciphers and quanta. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 370(1971):3418–3431, 2012.

[18] Yeong-Cherng Liang. Correlations, Bell Inequality Violation & Quantum Entanglement. *arXiv:0810.5400*, 2008.

[19] Boris S. Tsirelson. Quantum Generalizations of Bell's Inequality. *Letters in Mathematical Physics*, 4:93–100, 1980.

[20] Sandu Popescu and Daniel Rohrlich. Quantum nonlocality as an axiom. *Foundations of Physics*, 24(3):379–385, 1994.

[21] Stuart J. Freedman and John F. Clauser. Experimental Test of Local Hidden-Variable Theories. *Physical Review Letters*, 28(14):938–941, 1972.

[22] Alain Aspect, Philippe Grangier, and Gérard Roger. Experimental Tests of Realistic Local Theories via Bell's Theorem. *Physical Review Letters*, 47(7):460–463, 1981.

[23] Alain Aspect, Philippe Grangier, and Gérard Roger. Experimental Realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: A New Violation of Bell's Inequalities. *Physical Review Letters*, 49(2):91–94, 1982.

[24] Alain Aspect, Jean Dalibard, and Gérard Roger. Experimental Test of Bell's Inequalities Using Time- Varying Analyzers. *Physical Review Letters*, 49(25):1804–1807, 1982.

[25] Roger Colbeck and Renato Renner. No extension of quantum theory can have improved predictive power. *Nature Communications*, 2:411, 2011.

[26] Michael J. W. Hall. Relaxed Bell Inequalities and Kochen-Specker Theorems. *Physical Review A*, 84(2):022102, 2011.

[27] Travis Norsen. Local Causality and Completeness: Bell vs. Jarrett. *Foundations of Physics*, 39(3):273–294, 2009.

[28] L. A. Khalfin and S. B. Tsirelson. Quantum and quasi-classical analogs of Bell inequalities, 1985.

[29] Peter Rastall. Locality, Bell's theorem, and quantum mechanics. *Foundations of Physics*, 15(9):963–972, 1985.

[30] Hermann Minkowski. *Theorie der konvexen Körper, insbesondere Begründung ihres Oberflächenbegriffs*. Teubner Verlag, 1911 (posthumous).

[31] Arthur Fine. Hidden Variables, Joint Probability, and the Bell Inequalities. *Physical Review Letters*, 48(5):291–295, 1982.

[32] Ben Toner. Monogamy of non-local quantum correlations. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Science*, 465(2101):59–69, 2009.

[33] Antonio Acín, Serge Massar, and Stefano Pironio. Randomness vs Non Locality and Entanglement. *arXiv:1107.2754*, 2011.

[34] Le Phuc Thinh, Lana Sheridan, and Valerio Scarani. Bell tests with min-entropy sources. *Physical Review A*, 87(6):062121, 2013.

[35] R. Cleve, P. Høyer, B. Toner, and J. Watrous. Consequences and limits of nonlocal strategies. In *19th IEEE Annual Conference on Computational Complexity*, pages 236–249.

[36] Avis David, Imai Hiroshi, Ito Tsuyoshi, and Sasaki Yuuya. Two-party Bell inequalities derived from combinatorics via triangular elimination. *Journal of Physics A: Mathematical and General*, 38(50):10971, 2005.

[37] Daniel Collins and Nicolas Gisin. A Relevant Two Qubit Bell Inequality Inequivalent to the CHSH Inequality. *Journal of Physics A: Mathematical and General*, 37(5):1775, 2004.

[38] S. L. Braunstein and C. M. Caves. Wringing out better Bell inequalities. *Annals of Physics*, 202(Article):22–56, 1990.

[39] Roger Colbeck and Renato Renner. Hidden Variable Models for Quantum Theory Cannot Have Any Local Part. *Physical Review Letters*, 101(5):050403, 2008.

[40] Jonathan Barrett, Lucien Hardy, and Adrian Kent. No Signaling and Quantum Key Distribution. *Physical Review Letters*, 95(1):010503, 2005.

[41] Roger Colbeck and Renato Renner. Free randomness can be amplified. *Nature Physics*, 8(6):450–454, 2012.

[42] Daniel M Greenberger, Michael A Horne, and Anton Zeilinger. Going beyond Bells theorem. *Bells theorem, quantum theory, and conceptions of the universe*, 37:69–72, 1989.

[43] N. David Mermin. Extreme quantum entanglement in a superposition of macroscopically distinct states. *Physical Review Letters*, 65(15):1838–1840, 1990.

[44] Roger Colbeck. *Quantum and Relativistic Protocols for Secure Multi-Party Computation*. PhD thesis, 2009.

[45] St. Thomas Aquinas. *The "Summa theologica" of St. Thomas Aquinas*. Burns, Oates & Washburne, London, 1920.

[46] J. Beringer et al. Review of Particle Physics. *Physical Review D*, 86(1):010001, 2012.

[47] Walther Gerlach and Otto Stern. Das magnetische Moment des Silberatoms. *Zeitschrift für Physik*, 9(1):353–355, 1922.

[48] S. Pironio, A. Acín, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe. Random numbers certified by Bells theorem. *Nature*, 464(7291):1021–1024, 2010.

[49] Roger Colbeck and Adrian Kent. Private Randomness Expansion with Untrusted Devices. *Journal of Physics A: Mathematical and Theoretical*, 44(9):095305, 2011.

[50] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[51] C. Shannon. Communication Theory of Secrecy Systems. *Bell System Technical Journal*, 28:656–715, 1949.

[52] R. König, R. Renner, and C. Schaffner. The operational meaning of min- and max-entropy. *IEEE Transactions on Information Theory*, 55(9):4337–4347, 2009.

[53] R. Impagliazzo, L. A. Levin, and M. Luby. Pseudo-random generation from one-way functions, 1989.

[54] Renato Renner. Security of Quantum Key Distribution. *International Journal of Quantum Information*, 06(01):1–127, 2008.

[55] Esther Hänggi and Renato Renner. Device-Independent Quantum Key Distribution with Commuting Measurements. *arXiv:1009.1833*, 2010.

[56] Antonio Acín, Serge Massar, and Stefano Pironio. Efficient quantum key distribution secure against no-signalling eavesdroppers. *New Journal of Physics*, 8(8):126, 2006.

[57] Antonio Acín, 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.

[58] B. G. Christensen, K. T. McCusker, J. Altepeter, B. Calkins, T. Gerrits, A. Lita, A. Miller, L. K. Shalm, Y. Zhang, S. W. Nam, N. Brunner, C. C. W. Lim, N. Gisin, and P. G. Kwiat. Detection-Loophole-Free Test of Quantum Nonlocality, and Applications. *arXiv:1306.5772*, 2013.

[59] J. Silman, A. Chailloux, N. Aharon, I. Kerenidis, S. Pironio, and S. Massar. Fully Distrustful Quantum Bit Commitment and Coin Flipping. *Physical Review Letters*, 106(22):220501, 2011.

[60] D. Mayers and A. Yao. Quantum cryptography with imperfect apparatus. In *Foundations of Computer Science, 1998. Proceedings.39th Annual Symposium on*, pages 503–509.

[61] Julio T. Barreiro, Jean-Daniel Bancal, Philipp Schindler, Daniel Nigg, Markus Hennrich, Thomas Monz, Nicolas Gisin, and Rainer Blatt. Device-independent demonstration of genuine multipartite entanglement. *arXiv:1303.2433*, 2013.

[62] Michele Dall'Arno, Elsa Passaro, Rodrigo Gallego, and Antonio Acín. Robustness of Device Independent Dimension Witnesses. *arXiv:1207.2574*, 2012.

[63] Melvyn Ho, Jean-Daniel Bancal, and Valerio Scarani. Device-independent certification of the teleportation of a qubit. *arXiv:1308.0084*, 2013.

[64] Valerio Scarani. The device-independent outlook on quantum physics (lecture notes on bell inequalities). *arXiv:1303.3081*, 2013.

[65] Philip M. Pearle. Hidden-Variable Example Based upon Data Rejection. *Physical Review D*, 2(8):1418–1425, 1970.

[66] Peter J. Mosley, Jeff S. Lundeen, Brian J. Smith, Piotr Wasylczyk, Alfred B. URen, Christine Silberhorn, and Ian A. Walmsley. Heralded Generation of Ultrafast Single Photons in Pure Quantum States. *Physical Review Letters*, 100(13):133601, 2008.

[67] John F. Clauser and Michael A. Horne. Experimental consequences of objective local theories. *Physical Review D*, 10(2):526–535, 1974.

[68] Philippe H. Eberhard. Background Level and Counter Efficiencies Required for a Loophole-Free Einstein-Podolsky-Rosen Experiment. *Physical Review A*, 47(2):R747–R750, 1993.

[69] Nicolas Brunner, Nicolas Gisin, Valerio Scarani, and Christoph Simon. Detection Loophole in Asymmetric Bell Experiments. *Physical Review Letters*, 98(22):220403, 2007.

[70] G. Garbarino. Minimum detection efficiencies for a loophole-free observable-asymmetric Bell-type test. *Physical Review A*, 81(3):032106, 2010.

[71] Károly F. Pál, Tams Vértesi, and Nicolas Brunner. Closing the detection loophole in multipartite Bell tests using Greenberger-Horne-Zeilinger states. *Physical Review A*, 86(6):062111, 2012.

[72] Serge Massar and Stefano Pironio. Violation of local realism versus detection efficiency. *Physical Review A*, 68(6):062109, 2003.

[73] Tamás Vértesi, Stefano Pironio, and Nicolas Brunner. Closing the Detection Loophole in Bell Experiments Using Qudits. *Physical Review Letters*, 104(6):060401, 2010.

[74] Jonathan Barrett, Daniel Collins, Lucien Hardy, Adrian Kent, and Sandu Popescu. Quantum nonlocality, Bell inequalities, and the memory loophole. *Physical Review A*, 66(4), 2002.

[75] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dusek, Norbert Lutkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Reviews of Modern Physics*, 81(3):1301, 2009.

[76] Matthias Christandl, Renato Renner, and Artur Ekert. A Generic Security Proof for Quantum Key Distribution. *arXiv:quant-ph/0402131*, 2004.

[77] Lluís Masanes, Stefano Pironio, and Antonio Acín. Secure Device-Independent Quantum Key Distribution with Causally Independent Measurement Devices. *Nature Communications*, 2:238, 2011.

[78] Jonathan Barrett, Roger Colbeck, and Adrian Kent. Prisoners of their own device: Trojan attacks on device-independent quantum cryptography. *arXiv:1201.4407*, 2012.

[79] Jian-Wei Pan, Zeng-Bing Chen, Chao-Yang Lu, Harald Weinfurter, Anton Zeilinger, and Marek ukowski. Multiphoton entanglement and interferometry. *Reviews of Modern Physics*, 84(2):777–838, 2012.

[80] Gregor Weihs, Thomas Jennewein, Christoph Simon, Harald Weinfurter, and Anton Zeilinger. Violation of Bell's Inequality under Strict Einstein Locality Conditions. *Physical Review Letters*, 81(23):5039–5043, 1998.

[81] J. G. Rarity and P. R. Tapster. Experimental violation of Bells inequality based on phase and momentum. *Physical Review Letters*, 64(21):2495–2498, 1990.

[82] Alois Mair, Alipasha Vaziri, Gregor Weihs, and Anton Zeilinger. Entanglement of the orbital angular momentum states of photons. *Nature*, 412(6844):313–316, 2001.

[83] J. Brendel, N. Gisin, W. Tittel, and H. Zbinden. Pulsed Energy-Time Entangled Twin-Photon Source for Quantum Communication. *Physical Review Letters*, 82(12):2594–2597, 1999.

[84] M. A. Rowe, D. Kielpinski, V. Meyer, C. A. Sackett, W. M. Itano, C. Monroe, and D. J. Wineland. Experimental violation of a Bell's inequality with efficient detection. *Nature*, 409(6822):791–794, 2001.

[85] Julian Hofmann, Michael Krug, Norbert Ortegel, Lea Grard, Markus Weber, Wenjamin Rosenfeld, and Harald Weinfurter. Heralded Entanglement Between Widely Separated Atoms. *Science*, 337(6090):72–75, 2012.

[86] Wenjamin Rosenfeld, Markus Weber, Jürgen Volz, Florian Henkel, Michael Krug, Adan Cabello, Marek Zukowski, and Harald Weinfurter. Towards a Loophole-Free Test of Bell's Inequality with Entangled Pairs of Neutral Atoms. *Advanced Science Letters*, 2(4):469–474, 2009.

[87] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin. Violation of Bell Inequalities by Photons More Than 10 km Apart. *Physical Review Letters*, 81(17):3563–3566, 1998.

[88] C. Teo, M. Araújo, M. T. Quintino, J. Minář, D. Cavalcanti, V. Scarani, M. Terra Cunha, and M. França Santos. Realistic loophole-free Bell test with atomphoton entanglement. *Nature Communications*, 4, 2013.

[89] Jian-Wei Pan, Dik Bouwmeester, Matthew Daniell, Harald Weinfurter, and Anton Zeilinger. Experimental test of quantum nonlocality in three-photon Greenberger-Horne-Zeilinger entanglement. *Nature*, 403(6769):515–519, 2000.

[90] Manfred Eibl, Nikolai Kiesel, Mohamed Bourennane, Christian Kurtsiefer, and Harald Weinfurter. Experimental Realization of a Three-Qubit Entangled W State. *Physical Review Letters*, 92(7):077901, 2004.

[91] Chun Siong Soon, Marcel Brass, Hans-Jochen Heinze, and John-Dylan Haynes. Unconscious determinants of free decisions in the human brain. *Nature Neuroscience*, 11(5):543–545, 2008.

[92] Michael J. W. Hall. Local Deterministic Model of Singlet State Correlations Based on Relaxing Measurement Independence. *Physical Review Letters*, 105(25):250404, 2010.

[93] Jonathan Barrett and Nicolas Gisin. How Much Measurement Independence Is Needed to Demonstrate Nonlocality? *Physical Review Letters*, 106(10):100406, 2011.

[94] Miklos Santha and Umesh V. Vazirani. Generating quasi-random sequences from semi-random sources. *Journal of Computer and System Sciences*, 33(1):75–87, 1986.

[95] Michel Feldmann. New Loophole for the Einstein-Podolsky-Rosen Paradox. *Foundations of Physics Letters*, 8(1):41–53, 1995.

[96] B. F. Toner and D. Bacon. Communication Cost of Simulating Bell Correlations. *Physical Review Letters*, 91(18):187904, 2003.

[97] Cyril Branciard, Nicolas Brunner, Nicolas Gisin, Christian Kurtsiefer, Antia Lamas-Linares, Alexander Ling, and Valerio Scarani. Testing Quantum Correlations Versus Single-Particle Properties Within Leggett's Model and Beyond. *Nature Physics*, 4(9):681–685, 2008.

[98] Michael J. W. Hall. Complementary Contributions of Indeterminism and Signaling to Quantum Correlations. *Physical Review A*, 82(6):062117, 2010.

[99] Stefano Pironio and Serge Massar. Security of practical private randomness generation. *Physical Review A*, 87(1):012336, 2013.

[100] Serge Fehr, Ran Gelles, and Christian Schaffner. Security and composability of randomness expansion from Bell inequalities. *Physical Review A*, 87(1):012335, 2013. PRA.

[101] Thomas Lawson, Noah Linden, and Sandu Popescu. Biased nonlocal quantum games. *arXiv:1011.6245*, 2010.

[102] Marcus Huber and Marcin Pawłowski. Weak randomness in device-independent quantum key distribution and the advantage of using high-dimensional entanglement. *Physical Review A*, 88(3):032309, 2013.

[103] Antonio Acín, Nicolas Gisin, and Lluis Masanes. From Bell's Theorem to Secure Quantum Key Distribution. *Physical Review Letters*, 97(12):120405, 2006.

[104] Wu-Sheng Lu. *Use SeDuMi to Solve LP, SDP and SCOP Problems: Remarks and Examples*. Dept. of Electrical and Computer Engineering, University of Victoria, 2009. URL: `http://www.ece.uvic.ca/~wslu/Talk/SeDuMi-Remarks.pdf`.

[105] Yevgeniy Dodis, Shien Jin Ong, Manoj Prabhakaran, and Amit Sahai. On the (Im)possibility of Cryptography with Imperfect Randomness, 2004.

[106] Rodrigo Gallego, Lluis Masanes, Gonzalo de la Torre, Chirag Dhara, Leandro Aolita, and Antonio Acin. Full randomness from arbitrarily deterministic events. *arXiv:1210.6514*, 2012.

[107] Piotr Mironowicz and Marcin Pawłowski. Amplification of arbitrarily weak randomness. *arXiv:1301.7722*, 2013.

[108] Ravishankar Ramanathan, Fernando G. S. L. Brandão, Andrzej Grudka, Karol Horodecki, MichałHorodecki, and PawełHorodecki. Robust Device Independent Randomness Amplification. *arXiv:1308.4635*, 2013.

[109] Andrzej Grudka, Karol Horodecki, Micha Horodecki, Pawe Horodecki, Marcin Pawowski, and Ravishankar Ramanathan. Free randomness amplification using bipartite chain correlations. *arXiv:1303.5591*, 2013.

[110] Lluís Masanes, Stefano Pironio, and Antonio Acín. Secure device-independent quantum key distribution with causally independent measurement devices. *Nature Communications*, 2:238, 2011.

[111] Esther Hänggi, Renato Renner, and Stefan Wolf. *Efficient Device-Independent Quantum Key Distribution Advances in Cryptology EUROCRYPT 2010*, volume 6110 of *Lecture Notes in Computer Science*, pages 216–234. Springer Berlin / Heidelberg, 2010.

[112] 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.

Appendix A

Estimating Guessing Probability from CHSH Violation

Within device-independent protocols for both randomness expansion and key distribution, the amount of information available to the adversary is related directly to the degree of violation of a Bell inequality. A relation between the single-round guessing probability and the degree of violation of the CHSH inequality has been derived in [48] and alternatively in [110]. We present here a proof of this relation, in a similar manner to [48], assuming Alice and Bob have complete experimental free will (of course, Chapters 3 and 4 are dedicated to investigating when this is not the case). We also assume that Eve's strategy is restricted to collective attacks where she acts independently on each round of testing, although this restriction has been lifted in more recent work [77, 111].

Theorem 13. *In a CHSH test using two-valued inputs and two-valued outcomes, observing a CHSH expectation value of S, Alice and Bob can bound Eve's guessing probability G on a generated bit by*

$$G \leqslant \frac{1}{2}\left(1+\sqrt{2-\frac{S^2}{4}}\right). \tag{A.1}$$

Proof. Consider the CHSH inequality in operational terms – the outcomes A_0, A_1, B_0 and B_1 that Alice and Bob may obtain are the results of single-qubit measurements represented by 3-dimensional unit vectors on the Bloch sphere, $\hat{a}_0, \hat{a}_1, \hat{b}_0$ and $\hat{b}_1$ respectively, so that $A_0 = \hat{a}_0 \cdot \sigma$ where σ is a vector of Pauli matrices. In the device-independent scenario, Eve preselects these measurements as well as the quantum state to be distributed between Alice and Bob on each round (for the CHSH scenario, we may restrict the shared state to being two entangled qubits). We wish to calculate

the largest possible violation $S_{\max}$, defined to be the maximum of $\langle\psi\,|\,\mathcal{S}\,|\,\psi\rangle$ over all two-qubit states $|\,\psi\rangle$ and all measurements $\hat{a}_0, \hat{a}_1, \hat{b}_0, \hat{b}_1$, where $\mathcal{S}$ is the CHSH operator

$$\mathcal{S} = (\hat{a}_0 \cdot \sigma) \otimes (\hat{b}_0 + \hat{b}_1) \cdot \sigma + (\hat{a}_1 \cdot \sigma) \otimes (\hat{b}_0 - \hat{b}_1) \cdot \sigma. \tag{A.2}$$

By unitary freedom, Eve can select $|\,\psi\rangle = \sin\theta\,|\,00\rangle + \cos\theta\,|\,11\rangle$ where $0 \leqslant \theta < \pi/4$. Rewriting $|\,\psi\rangle$ in the form of equation (1) in [112], we see that

$$S_{\max} = \max_{\hat{a}_0,\hat{a}_1,\hat{b}_0,\hat{b}_1} \Big(\hat{a}_0 \cdot t \cdot (\hat{b}_0 + \hat{b}_1) + \hat{a}_1 \cdot t \cdot (\hat{b}_0 - \hat{b}_1)\Big) \tag{A.3}$$

where t is a 3×3 diagonal matrix with diagonal entries $(\sin 2\theta, -\sin 2\theta, 1)$. Now define the unit vectors $\hat{c}, c'$ and scalars l, l' by

$$\hat{b}_0 + \hat{b}_1 = l\hat{c}, \tag{A.4}$$

$$\hat{b}_0 - \hat{b}_1 = l'c'. \tag{A.5}$$

Taking the dot product of (A.4) and (A.5) tells us that $\hat{c}$ and c' are orthogonal. Squaring them yields $l^2 + l'^2 = 4$, suggesting we write $l = 2\cos\phi$ and $l' = 2\sin\phi$ for some ϕ. We then ascertain the maximum achievable CHSH value to be

$$S_{\max}(\theta) = \max_{\hat{a}_0,\hat{a}_1,\hat{c},c',\phi} 2\,(\hat{a}_0 \cdot t \cdot \hat{c}\cos\phi + \hat{a}_1 \cdot t \cdot c'\sin\phi) \tag{A.6}$$

$$= \max_{\hat{c},c',\phi} 2\,(\|t \cdot \hat{c}\|\cos\phi + \|t \cdot c'\|\sin\phi) \tag{A.7}$$

$$= \max_{\hat{c},c'} 2\sqrt{\|t \cdot \hat{c}\|^2 + \|t \cdot c'\|^2} \tag{A.8}$$

$$= 2\sqrt{1 + \sin^2 2\theta} \tag{A.9}$$

where the steps for maximization are choosing $\hat{a}_0$ and $\hat{a}_1$ to be parallel to $t \cdot \hat{c}$ and $t \cdot c'$ respectively in (A.6), defining ϕ in (A.7) by $\tan\phi = \|t \cdot c'\|/\|t \cdot \hat{c}\|$, and selecting $\hat{c}$ and c' in (A.8) as the eigenvectors of t with largest eigenvalues (remembering $\hat{c}$ and c' must be orthogonal). Note that this maximization has selected Alice's measurements to be the Pauli operations $A_0 = Z$ and $A_1 = X$. Eq. (A.9) is further maximized by selecting $\theta = \pi/4$, yielding the familiar $S_{\max} = 2\sqrt{2}$, but we shall see that varying θ allows us to find a trade-off between $S_{\max}(\theta)$ and the probability with which an eavesdropper can guess the measurement outcome.

The guessing probability G is the maximum probability that Eve guesses the outcome of the key bit generated by the pair (A_0, B_2) (in a key distribution protocol that differs from the above one only in that Bob, not Alice, has the third measurement setting). Since the measurements have only ± 1 outcomes, we have that $G =$

$\frac{1}{2}(1+\mathrm{Tr}(A_0\rho_A))$, where ρ_A is the reduced density matrix on Alice, $\rho_A = \cos^2\theta\,|\,0\rangle\,\langle 0\,| + \sin^2\theta\,|\,1\rangle\,\langle 1\,|$. Choosing $A_0 = Z$ gives the highest expectation $\mathrm{Tr}(\rho_A A_0) = \cos^2\theta - \sin^2\theta$, yielding $G = \cos^2\theta$. Since the optimal strategies for calculating G and maximizing S are compatible by selecting $A_0 = Z$, the maximum guessing probability has therefore been bounded above according to (A.1). □

Appendix B

Limited Measurement Dependence in a GHZ Test

The GHZ test [42] is an important test of nonlocality because it can be satisfied on every run by the correlations produced from an optimal quantum strategy, as described in Section 1.4.3.2. Therefore, the best strategies adhering to generic no-signalling do no better than those achievable with quantum technologies. Here, we investigate the role of measurement dependence when testing the closely related tripartite Mermin inequality [43]. We show that a classical adversarial strategy can be improved when incorporating limited measurement dependence, whereas a quantum strategy cannot. The results are a natural extension of the CHSH-based work in Chapters 2 and 5 and no formal optimality proofs will be given.

As with CHSH, we consider a modified form of the tripartite Mermin inequality,

$$S = p_{00}A_0B_1C_1 + p_{01}A_1B_1C_0 + p_{10}A_1B_0C_1 - p_{11}A_0B_0C_0, \tag{B.1}$$

where the notation p_{jk} has been chosen simply to compare to the CHSH test, with $\sum p_{jk} = 1$. Since an optimal quantum strategy such as the one specified in Section 1.4.3.2 produces the desired correlations on every run of an experiment, it is clear that variation of p_{jk} and describing a new quantum strategy accordingly will not provide an advantage, since the algebraic limit of $p_{00} + p_{01} + p_{10} + p_{11} = 1$ has already been reached. However, the classical strategy, which under a free will only reproduces the correct correlation 75% of the time (since only three of the four relations in (1.23) can be simultaneously satisfied), can be improved.

For the classical strategy, we consider as before a model specified by underlying variables λ, which in turn specify a set of outcomes $a_0(\lambda), a_1(\lambda), b_0(\lambda), b_1(\lambda), c_0(\lambda)$ and $c_1(\lambda)$ and a measurement selection distribution $p(A_jB_kC_l|\lambda)$. There are 32 optimal outcome sets, i. e. those which satisfy three of the four relations in (1.23), which

are grouped according to the relations which they satisfy in Table B.1 (where the notation $\pm$ is shorthand for ± 1), producing the correlations described in Table B.2.

In Definition 1 we described a conjugate-inclusive model for the CHSH test in order to avoid suspicion of fixed outcomes; the same motivation applies here where, conditioned on drawing λ_n from the underlying variables, one of the eight possible outcome sets is drawn with equal probability. By inspection of Table B.1, this will over many runs approximate a uniform output of $+1$ or -1 for each local measurement input.

λ	Possible outcome specifications $(a_0(\lambda), a_1(\lambda), b_0(\lambda), b_1(\lambda), c_0(\lambda), c_1(\lambda))$
λ_0	$(+,+,+,+,+,+)$, $(+,+,-,-,-,-)$, $(+,-,+,-,+,-)$, $(+,-,-,+,-,+)$ $(-,+,+,-,-,+)$, $(-,+,-,+,+,-)$, $(-,-,+,+,-,-)$, $(-,-,-,-,+,+)$
λ_1	$(+,+,+,+,-,+)$, $(+,+,-,-,+,-)$, $(+,-,+,-,-,-)$, $(+,-,-,+,+,+)$ $(-,+,+,-,+,+)$, $(-,+,-,+,-,-)$, $(-,-,+,+,+,-)$, $(-,-,-,-,-,+)$
λ_2	$(+,+,+,-,-,-)$, $(+,+,-,+,+,+)$, $(+,-,+,+,-,+)$, $(+,-,-,-,+,-)$ $(-,+,+,+,+,-)$, $(-,+,-,-,-,+)$, $(-,-,+,-,+,+)$, $(-,-,-,+,-,-)$
λ_3	$(+,+,+,-,-,+)$, $(+,+,-,+,+,-)$, $(+,-,+,+,-,-)$, $(+,-,-,-,+,+)$ $(-,+,+,+,+,+)$, $(-,+,-,-,-,-)$, $(-,-,+,-,+,-)$, $(-,-,-,+,-,+)$

Table B.1: Optimal outcome specifications maximising GHZ, divided according to equivalence of correlations.

	$\langle a_0 b_1 c_1 \rangle_\lambda$	$\langle a_1 b_0 c_1 \rangle_\lambda$	$\langle a_1 b_1 c_0 \rangle_\lambda$	$-\langle a_0 b_0 c_0 \rangle_\lambda$
λ_0	1	1	1	-1
λ_1	1	1	-1	1
λ_2	1	-1	1	1
λ_3	-1	1	1	1

Table B.2: Optimal outcome correlations maximising GHZ.

	$p(A_0 B_1 C_1 \vert \lambda)$	$p(A_1 B_0 C_1 \vert \lambda)$	$p(A_1 B_1 C_0 \vert \lambda)$	$p(A_0 B_0 C_0 \vert \lambda)$
λ_0	P	P	P	$1-3P$
λ_1	P	P	$1-3P$	P
λ_2	P	$1-3P$	P	P
λ_3	$1-3P$	P	P	P

Table B.3: Optimal outcome specifications and correlations maximising GHZ.

The remarkably similar structure of the optimal correlations to the CHSH case allow us to similarly express the degree of violation of the Mermin inequality in terms of the measure of measurement independence P. When restricted to having the rows sum to 1 and not having any probability exceed a certain maximum value

$1/4 \leqslant P \leqslant 1/3$, we use the measurement selection distribution described in Table B.3, delivering a value of $S = 6P - 1$. Thus, for all $P < 1/3$, there is a gap between the optimal classical and quantum strategies.

We can also extend this attack to be correlated over many runs, using a similar approach to Section 5.3, discovering that

$$P \geqslant \left(\frac{1+S}{6}\right)^{(1+S)/2} \left(\frac{1-S}{2}\right)^{(1-S)/2}. \tag{B.2}$$

This only allows $S \to 1$ in the limit $P \to 1/3$. This tells us that even in the model correlated over infinitely many runs, there is a gap between the optimal classical and quantum strategies for all $P < 1/3$. This is in contrast to the results derived for the CHSH test, where there was a threshold value of the inequality ($S > 16/5$) for which the quantum strategy could do no better than classical.