Aspects of Quantum Non-locality.

David Roberts.

H. H. Wills Physics Laboratory,

University of Bristol.

A thesis submitted to the University of Bristol
in accordance with the requirements of the degree of
Doctor of Philosophy in the Faculty of Science.

June 2004.

Abstract.

In this thesis I will present work in three main areas, all related to quantum non-locality. The first is multipartite Bell inequalities. It is well known that quantum mechanics can not be described by any local hidden variable model, and so is considered to be a *non-local* theory. However for a system of several particles it is conceivable that this non-locality takes the form of non-local correlations within subsets of the particles, but only local correlations between the subsets themselves. This was first considered by Svetlichny [1] who produced a Bell type inequality to distinguish genuine three party non-locality from weaker forms involving only subsets of two particles. In chapter 3 I show that recent experiments to produce three particle entangled states can not yet confirm this three particle non-locality. In chapter 4 I give the generalization of Svetlichny's inequality for n particle systems.

The second main area of research is presented in chapter 5. Entangled quantum systems produce correlations that are non-local, in the sense that they violate Bell inequalities. It is possible to abstract away from the physical source of these correlations and consider sets of correlations that are more non-local than quantum mechanics allows. The only constraint I make is that the joint probabilities can not allow signalling. These correlations form a polytope, which contains the quantum correlations as a (proper) subset. We have become familiar with the idea that entangled quantum states may be viewed as a resource for quantum information processing tasks. In light of this I go on to consider how, when viewed as an information theoretic resource, these maximally non-local correlations are related to the quantum mechanical scenario.

Finally the third area of this thesis concerns entropy inequalities and their relation to multipartite entanglement measures. One way of studying multipartite

states is to consider their reduced entropies. By analyzing the structure of the space of allowed reduced entropies I aim to better understand the constraints on these reduced entropies. If the dimension of the Hilbert spaces of the states is not restricted then the only known constraints come from strong subadditivity, a linear entropy inequality. By analyzing the structure of reduced entropies allowed by strong subadditivity for four particles and considering a classical analogy I conjecture that there are new entropy inequalities, inequivalent to strong subadditivity, yet to be discovered.

I also make a connection with another method for classifying multipartite entanglement - MREGS, or the minimal reversible entanglement generating set. I show how considering the space of allowed reduced entropies shows certain states must belong to the MREGS.

The above is a general picture of the work in this thesis - a more detailed abstract can be found at the start of each chapter.

Acknowledgements.

My greatest thanks go to my supervisor, Sandu Popescu, whose insight and enthusiasm for Physics have been an inspiration. Thanks also to Noah Linden, Dan Collins, Nicholas Gisin, Serge Massar, Ashish Thapilyal, Valerio Scarani, Jonathan Barrett and Stefano Pironio with whom I have collaborated in some of this research.

I would also like to thank my friends and colleagues in the Physics department and Quantum Information group at University of Bristol; Emma Podnieks, Berry Groisman, Jamie Walker, Andy Archer, Maria Thomas, Andy Duff, Danny Jervis, Denzil Rodrigues and Nick Jones.

Declaration.

I declare that the work in this thesis was carried out in accordance with the regulations of the University of Bristol, between July 2001 and June 2004. The work is original except where special reference is made to the work of others. It is the result of the author's investigations under the supervision of Professor Sandu Popescu, in collaboration with other scientists where indicated. No part of this work has been submitted previously for a degree at this or any other University either in the United Kingdom or overseas. Any views expressed in the thesis are those of the author and in no way represent those of the University of Bristol.

List of Papers.

P. Mitchell, S. Popescu. D. Roberts. *Conditions for the confirmation of three party non-locality.* quant-ph/0202009 (2002) (Accepted in Phys. Rev. A.)

D. Collins, N. Gisin, S. Popescu, D. Roberts, V. Scarani. *Bell inequalities to detect true n-party non-separability.* Phys. Rev. Lett. **88** (2002) 170405.

J. Barrett, N. Linden, S. Massar, S. Pironio, S. Popescu, D. Roberts. *Non-local correlations as an information theoretic resource.* quant-ph/0404097 (2004) (Submitted to Phys. Rev. A.)

List of acronyms.

CHSH inequality: Clauser Horne Shimony Holt inequality.

GHZ state: Greenberger Horne Zeilinger state, $|\psi_{GHZ}\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$.

LHV models: Local hidden variable models.

MK polynomials: Mermin-Klyshko polynomials.

MREGS: The minimal reversible entanglement generating set.

SSA: Strong Subadditivity.

W state: $|\psi_W\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle)$.

WM: Weak monotonicity.

Contents

List of Figures

List of Tables

Chapter 1

Introduction.

Since the formalism of quantum mechanics was developed in the 1920's it has become accepted as the most thoroughly tested and widely applied physical theory yet devised. The rules of quantum mechanics are routinely used to predict the results of measurements with stunning accuracy, yet the conceptual foundations for these rules remain a topic for discussion. The characteristics of quantum mechanics which troubled the great scientists in the 1930's were indeterminism and perhaps most counter-intuitive of all, non-locality. In 1935 Einstein, Podolsky and Rosen (EPR) formulated a famous paradox reflecting their dissatisfaction with the new theory [2]. We now understand that they were struggling with the most fundamental departure from classical physics; not the more conspicuous features such as discrete energy levels, but quantum entanglement.

Entangled states are indivisible objects in the sense that even if their component particles are separated, each particle is still affected by actions on other particles. It is as if the particles are able to communicate instantaneously, but we are intrinsically unable to harness this communication to signal faster than light. In 1964 John Bell [3] made the observation that the EPR dilemma could be expressed in the form of assumptions which led to falsifiable predictions. It is hard to understate the importance of this idea, as it allowed the notion of non-locality to move from a domain of meta-physics to that of an experimentally accessible prediction.

In light of technological progress that has allowed experiments to test these ideas, quantum non-locality and entanglement have gradually been accepted. Indeed over the last decade they have been embraced as offering exciting advantages over classical methods in computing and information theory. The new paradigm has been to regard entanglement as a resource which allows us to perform such tasks more efficiently. Thus the emphasis has shifted from demonstrating entanglement to making use of it, and because of this the knowledge we have of entanglement and non-locality has broadened and become more subtle in the distinctions we can make. For example discovering the fundamentally inequivalent ways in which a state can be entangled has been, and remains, the goal of a huge amount of recent work. This thesis is part of the trend to try and understand the non-locality of quantum mechanics, particularly in multipartite systems. I will present work in three main areas.

The first area is generalized Bell inequalities. The aim here is to show that quantum mechanics exhibits genuine n particle non-locality for any number n of particles. This means that the correlations can not be predicted by a model which permits non-local correlations within sub-systems of limited size but only local correlations between sub-systems, in other words a *hybrid* local non-local model. In particular chapter 2 contains a short review of some of the known families of Bell inequalities. I also give a new proof of the CHSH inequality, the most widely known Bell inequality. In chapter 3 I show how recent experiments to demonstrate three party entangled states can not yet be taken as having shown genuine three party non-locality because they do not rule out the possibility of a hybrid local non-local model. Chapter 4 gives the generalization to n parties. The work in chapters 3 and 4 is based on two papers [4, 5].

Bell type inequalities have proven to be one of our most useful tools in understanding quantum non-locality. However it is also known that it is possible to write down sets of correlations that are more non-local than is allowed by quantum mechanics, yet are still non-signalling. If correlations are viewed as an information

theoretic resource, then some of these 'super-quantum' correlations are very powerful. Why does quantum mechanics not allow these powerful correlations? In general we can only understand quantum possibilities fully by placing them within a wider context. With this in mind, I investigate the set of correlations that are constrained only by the no-signalling principle. I show that many of the information theoretic uses for entangled quantum states have close analogies with these maximally non-local (but still non-signalling) probability distributions. This chapter is based on a paper [6].

Finally in chapters 6 and 7 I consider multipartite entanglement measures. Chapter 6 contains an introduction to this area of research, and in chapter 7 I present some new results. One approach to considering multipartite entanglement is to use a measure we understand well from the bi-partite case, and apply it in a multipartite setting. I therefore consider the reduced entropies of multipartite states. I aim to understand the structure of the space of allowed reduced entropies, and in particular the constraints on the allowed reduced entropies. For example, constraints may come from general linear entropy inequalities such as strong subadditivity. They may come from constraints on the states, such as restricting the dimension of the Hilbert space. Finally there may be new entropy inequalities. In chapter 7 I consider all of these possibilities.

If the dimension of the Hilbert space of the states is not restricted then the only known constraints come from strong subadditivity. All of the other entropy inequalities such as weak monotonicity, subadditivity and the triangle inequalities can be deduced form strong subadditivity. By enumerating the reduced entropies allowed by strong subadditivity for four particles and considering a classical analogy I conjecture that there may be new entropy inequalities still to be discovered.

I also make a connection between the space of allowed reduced entropies and MREGS, the minimal reversible entanglement generating set. The MREGS classifies the fundamentally inequivalent types of entanglement possible in multipartite states. In particular I show by considering the space of reduced entropies one may conclude that a certain set of states must belong to the three and four particle MREGS.

Chapter 8 contains conclusions and discusses open questions left by the preceding work.

Chapter 2

Bell inequalities and non-locality.

Abstract.

This chapter contains a short review of Bell inequalities in both bi-partite and multipartite scenarios. I give a new proof of the CHSH inequality, the simplest and most widely known Bell inequality, based on frustrated networks of correlations. Summaries of the known families of Bell inequalities, and some connections between violations of Bell inequalities and entanglement properties are presented. Finally I review loopholes in experiments designed to show violation of Bell type inequalities.

2.1 Historical development.

Bell inequalities [3] consider the strength of correlations between experimental outcomes measured by observers at separate locations. The upper bound for the strength of the correlations detected is determined by the model we use to describe the system. Bell showed that quantum mechanics predicts stronger correlations than any local hidden variable model allows, and *non-locality* has become synonymous with violation of a Bell inequality.

Bell's argument may be seen as the result of 30 years of effort trying to understand just how quantum theory differs from classical mechanics. The debate began with the EPR paper in 1935 [2], and continues to this day. Indeed new papers relating to Bell's theorem appear almost daily, the resurgence of interest in this field inspired by developments in quantum information science. Historically Bell's theorem was inspired by a specific non-local theory; the pilot wave theory of Bohm and de Broglie [8, 9]. This pilot wave theory had been devised as an attempt at reformulating quantum mechanics as a deterministic theory. The theory was non-local, and also contextual - quantum measurements do not reveal the value of a property of the system existing prior to the measurement. It was this property of contextuality which was initially subject to most research.

Suppose we wish to measure an observable $\hat{A}$. Our classical intuition may lead us to believe that the outcome will only depend on the state of the system and $\hat{A}$. Certainly in classical physics the measurement of one property of a system does not interfere with its other properties, so we may imagine that properties of the system exist independently of our experimental set up and in particular which measurements we may choose to perform. If we simultaneously measure $\hat{B}$, which commutes with $\hat{A}$, the result will not change, i.e the result of $\hat{A}$ does not depend on the context of the measurement. For quantum systems, if our state is a simultaneous eigenstate of $\hat{A}$ and $\hat{B}$ then this will be true. However as the following example demonstrates, in general the outcome of a measurement *will* depend on the other

commuting measurements that are made.

Mermin's contextuality proof [10].

Mermin extended a result of Peres [11, 12] to produce the following state independent contextuality proof. Consider the array of Pauli spin operators

$$\begin{array}{ccc} 1 \otimes \sigma_z & \sigma_z \otimes 1 & \sigma_z \otimes \sigma_z \\ \sigma_x \otimes 1 & 1 \otimes \sigma_x & \sigma_x \otimes \sigma_x \\ \sigma_x \otimes \sigma_z & \sigma_z \otimes \sigma_x & \sigma_y \otimes \sigma_y \end{array} \tag{2.1.1}$$

Each of the nine operators in the table has eigenvalues ± 1. The operators in each row and in each column commute and have the property that each operator is the product of the other two, except in the third column where an extra minus sign is needed. Imagine we try to assign a pre-defined value ± 1 for the outcome of each measurement: Because of the minus sign appearing in the third column there is no consistent way to assign these values. The paradox comes from our attempts at assigning the same pre-defined value ± 1 to the operator in each different context. This example shows how quantum mechanically it is impossible to consistently assign values to an observable $\hat{A}$ unless we know the experimental context, i.e which other commuting observables are measured along with $\hat{A}$.

The above example uses a four dimensional Hilbert space. For two dimensional systems Bell [13] showed that we may construct (non-contextual) hidden variable models to reproduce the predictions of quantum mechanics. Using a three dimensional system Kochen and Specken [14], extending an earlier result of Gleason [15] provided the first demonstration of quantum contextuality. However this proof is very much more involved than Mermin's.

Quantum non-locality can be thought of as following from contextuality. Contextuality means that the outcome of observable $\hat{A}$ depends not just on the state, but also on the choice of an observable $\hat{B}$ which is to be measured with $\hat{A}$. This is true even if $\hat{A}$ and $\hat{B}$ commute. If $\hat{A}$ and $\hat{B}$ are performed at locations separated in

space the system exhibits non-locality.

Bell asked if all hidden variable theories that reproduce the predictions of quantum mechanics had to be non-local like pilot wave theory. He subsequently proved that this is indeed the case, and provided the first proof of quantum non-locality in 1964 [3]. His result was extended by Clauser, Horne, Shimony and Holt (CHSH) [16]. The CHSH inequality is the simplest and by far the best studied Bell inequality.

2.2 The CHSH inequality.

There are many derivations of Bell inequalities in the literature. Here I give a new proof based on frustrated networks of correlations. This interpretation shows more clearly how contextuality leads to non-locality. It has also been helpful in understanding other Bell type inequalities and is used in the next chapter.

Bell type inequalities always refer to the correlations between two or more parties at separate sites. For two parties convention dictates that these are referred to as Alice and Bob. Each party receives a particle from a common source and is allowed to perform measurements on it. Alice may choose to make one of the measurements A_1 or A_2 on her particle and Bob may choose to make one of the measurements B_1 or B_2 on his particle. The result of any measurement is labelled ± 1.

To formalize the idea of a local hidden variable theory, let λ be a hidden variable which takes values in the space Λ. λ is assumed to give enough information to allow Alice and Bob to compute their response to any measurement, or at least the probabilities for different outcomes. Let $P(a, b|A, B, \lambda)$ be the probability that Alice finds an outcome a and Bob finds b conditionally on the value of λ given that Alice and Bob measured A and B respectively. Suppose that λ occurs with some probability measure $\rho(\lambda)$, then $P(a, b|A, B, \lambda)$ is defined as being local if it allows a description as

$$P(a, b|A, B, \lambda) = \int \rho(\lambda)\, d\lambda\, P_A(a|\lambda)\, P_B(b|\lambda), \tag{2.2.1}$$

where $P_A(a|\lambda)$ gives the probability that Alice finds outcome a having measured A, and similarly $P_B(b|\lambda)$ gives the probability that Bob will find b having measured B. Then the CHSH inequality is

$$|E(A_1, B_1) + E(A_1, B_2) + E(A_2, B_1) - E(A_2, B_2)| \leq 2, \tag{2.2.2}$$

where $E(A_i, B_j)$ is the expectation value of the product of the outcomes of measurements A_i and B_j.

We can express the CHSH inequality in a different (although equivalent) form. Suppose that A_i and B_j have been measured. Since the outcomes a and b can only take values ± 1 either $a = b$ or $a = -b$. In the first case we can say A_i is correlated with B_j and in the second case that A_i is anti-correlated with B_j. Define $P_c(A_i, B_j)$ to be the probability that A_i and B_j are correlated, and $P_a(A_i, B_j)$ as the probability that A_i and B_j are anti-correlated. i.e,

$$P_c(A_i, B_j) = P(a = 1, b = 1|A_i, B_j) + P(a = -1, b = -1|A_i, B_j), \tag{2.2.3}$$

$$P_a(A_i, B_j) = P(a = 1, b = -1|A_i, B_j) + P(a = -1, b = 1|A_i, B_j). \tag{2.2.4}$$

These probabilities of correlation and anti-correlation are related to the expectation values by

$$E(A_i, B_j) = P_c(A_i, B_j) - P_a(A_i, B_j). \tag{2.2.5}$$

Using the fact that $P_c + P_a = 1$ this may be written

$$E(A_i, B_j) = 2P_c(A_i, B_j) - 1 = 1 - 2P_a(A_i, B_j). \tag{2.2.6}$$

Thus the CHSH inequality is equivalent to

$$1 \leq |\bar{\mathcal{N}}| \leq 3, \tag{2.2.7}$$

where

$$\bar{\mathcal{N}} = P_c(A_1, B_1) + P_c(A_1, B_2) + P_c(A_2, B_1) + P_a(A_2, B_2). \tag{2.2.8}$$

Our task is now to prove eq(2.2.7) under the assumption of a local hidden variable model. In the most general hidden variable model that can be considered for each value of the hidden variable λ the measurements can yield different outcomes according to the associated probabilities such as $P(A = a|\lambda)$. The probabilities of correlation and anti-correlation, and hence the sum of probabilities in eq(2.2.8), are also dependent on λ. We call this sum of conditional probabilities in eq(2.2.8) $\mathcal{N}(\lambda)$, and note that $\bar{\mathcal{N}}$ is the average over $\rho(\lambda)$ of $\mathcal{N}(\lambda)$, i.e

$$\bar{\mathcal{N}} = \int \rho(\lambda)\, \mathcal{N}(\lambda)\, d\lambda. \tag{2.2.9}$$

It can be easily shown that any such model can be re-cast into a deterministic model [20] in which for each value of λ the outcomes are completely determined, and the probabilities of obtaining each of the possible measurements is either 0 or 1. In particular the probabilities of correlation and anti-correlation are either 0 or 1. Then eq(2.2.8) corresponds to the network shown in figure 2.1.

There are only 2^4 deterministic models, each of them satisfying

$$1 \leq |\mathcal{N}(\lambda)| \leq 3. \tag{2.2.10}$$

This may be seen immediately from figure 2.1 as a reflection of the fact that the network is frustrated - it is impossible to satisfy all of the links simultaneously. The best that can be achieved is 3 out of the 4. This inequality is satisfied for every λ, so it will also hold for the average over $\rho(\lambda)$, $\bar{\mathcal{N}}$. This gives the CHSH inequality, in a slightly different form from the usual presentation.

In the next section it is shown that quantum mechanics satisfies

$$2 - \sqrt{2} \leq |\bar{\mathcal{N}}| \leq 2 + \sqrt{2}. \tag{2.2.11}$$

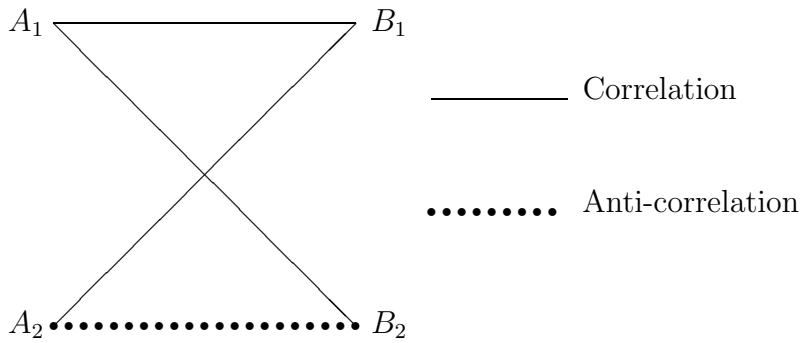

Figure 2.1: Schematic representation of the CHSH inequality.

This diagrammatic method shows more clearly how contextuality leads to non-locality. Because the network is frustrated, any attempt at assigning values to the outcomes independently of the measurement context leads to a contradiction, i.e only a contextual model can violate $1 \leq |\bar{\mathcal{N}}| \leq 3$.

The predictions of quantum mechanics.

Cirel'son [17] found the maximum value of the Bell expression

$$\mathcal{C} = E(A_1, B_1) + E(A_1, B_2) + E(A_2, B_1) - E(A_2, B_2) \tag{2.2.12}$$

to be $\mathcal{C} = 2\sqrt{2}$. For any state $|\psi\rangle$ we may write the sum of expectation values as

$$\mathcal{C} = \langle\psi|A_1(B_1 + B_2)|\psi\rangle + \langle\psi|A_2(B_1 - B_2)|\psi\rangle. \tag{2.2.13}$$

Using Schwarz' inequality we may bound the magnitude of the two terms.

$$\langle\psi|A_1(B_1+B_2)|\psi\rangle \leq \sqrt{|\langle\psi|A_1A_1|\psi\rangle||\langle\psi|(B_1+B_2)(B_1+B_2)|\psi\rangle|} \quad (2.2.14)$$

$$(2.2.15)$$

$$= \sqrt{2+\langle\psi|B_1B_2+B_2B_1)|\psi\rangle} \quad (2.2.16)$$

Using $\langle\psi|A_iA_i|\psi\rangle = 1$, and similarly for B. Let $x = \langle\psi|B_1B_2 + B_2B_1|\psi\rangle$ then

$$|\mathcal{C}| \leq \sqrt{2+x} + \sqrt{2-x}. \quad (2.2.17)$$

Thus $|\mathcal{C}| \leq 2\sqrt{2}$ when $x = 0$. This is equivalent to $2 - \sqrt{2} \leq \bar{\mathcal{N}} \leq 2 + \sqrt{2}$, using eq(2.2.6). To achieve this maximum we may use the singlet state of two spin half particles

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle), \quad (2.2.18)$$

where $|0\rangle$ and $|1\rangle$ are in the z basis, and choose measurements $A_i = \vec{a_i} \cdot \vec{\sigma}$ when $\vec{\sigma}$ is the vector of Pauli spin matrices $\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$, and similarly for B. Then $\vec{a_1} = (0,1,0)$, $\vec{a_2} = (1,0,0)$, $\vec{b_1} = (\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 0)$ and $\vec{b_2} = (-\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 0)$ gives $\mathcal{C} = 2\sqrt{2}$.

2.3 All the Bell inequalities.

The CHSH inequality is just one of an infinite set of Bell type inequalities. Each is based on the assumption that there exists a local hidden variable model to describe the correlations between measurement outcomes at separate locations. We may consider n-partite systems, each subject to a choice of m v-valued measurements. This gives a total of $(mv)^n$ experimentally accessible probabilities. The set of Bell inequalities is then the set of inequalities that bounds this region of probabilities to those accessible with a local hidden variable model. Thus for each value of n, m and v the set of local realist theories is a polytope bounded by a finite set of linear Bell inequalities.

The space would be completely characterized if we could find a minimal set of Bell inequalities, which is complete in the sense that all the inequalities are satisfied if and only if the correlations considered permit a local hidden variable model. This problem is essentially that of enumerating the facets of a convex hull, a problem known to be computationally hard, and is computationally tractable only for problems in low dimension [18]. The result of such a computation is a table of thousands of coefficients that gives little insight unless the local equivalences are removed [19]. Nevertheless various incomplete families of Bell inequalities are known, and also one complete set of families for the case $(n, m, v) = (n, 2, 2)$. The following is a summary of the situation.

The CHSH inequalities are the best studied class of Bell inequalities. They apply to a situation $(n, m, v) = (2, 2, 2)$. Fine [20] showed that any member of a minimal complete set of Bell inequalities for this situation is equivalent to the CHSH inequality up to local relabelling operations. That is Alice may rename her measurement settings, or may relabel her measurement outcomes conditionally on the measurement setting. Bob may perform similar operations.

Gisin [21] has found a family of Bell inequalities for the case with the number of measurements is arbitrary, i.e $(n, m, v) = (2, m, 2)$.

Collins *et al* [22] and Kaszlikowski *et al* [23] have produced inequalities for arbitrarily high dimensional systems, i.e $(n, m, v) = (2, 2, v)$. Such inequalities have the property that they are more resilient against experimental noise than the CHSH inequality.

For the case $(n, m, v) = (2, 3, 2)$ Collins and Gisin [19] performed a computational investigation of the polytope of Bell inequalities. Up to local equivalences they found just one new inequality, and showed that there exist mixed states that violate this new inequality but do not violate any CHSH inequality.

The most complete study of Bell inequalities is for the case $(n, m, v) = (n, 2, 2)$. n-particle generalizations of the CHSH inequality were first proposed by Mermin [24], and Belinskii and Klysko [25], and have been extended by Werner and Wolf

[26], and Zukowski and Brukner [27] to give the complete set for two dichotomic obeservables per site. They found 2^{2^n} such inequalities, complete in the sense that the inequalities are satisfied if and only if the correlations permit a local hidden variable model. All of these inequalities may be summarized in a single non-linear inequality. They found the maximum violation of the inequalities could be achieved using a generalized GHZ state, defined by

$$|\psi_{GHZ}\rangle = \frac{1}{\sqrt{2}}(|00...0\rangle + |11...1\rangle). \tag{2.3.1}$$

There are 2^n different experimental setups labelled by the choice of observables at each site. We can parameterize these choices with binary variables $s_k \in \{0, 1\}$, $k = 1, ..., n$, to indicate the choice of the observable $A_k(s_k)$ on particle number k. A full correlation function is then the expectation of the product

$$\eta(s) = E(\Pi_k A_k(s_k)) \tag{2.3.2}$$

where the string $s = (s_1, ..., s_n)$ labels the setup. For example if $n = 2$, so we consider the CHSH type experiment, $s = (00)$ selects the case when the first measurement of each side is selected, i.e $E(A_1(0)A_2(0))$. $\eta(s)$ may be considered as a component of a vector η in the 2^n dimensional space spanned by the data, so any Bell inequality is of the form

$$\sum_s \beta(s)\,\eta(s) \leq 1. \tag{2.3.3}$$

The coefficients $\beta(s)$ are normalized so that the maximum classical (local) value is 1. So for the CHSH case $\beta = (\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, -\frac{1}{2})$. Such polynomials may be used directly in the quantum case when the variables $A_k(s_k)$ are replaced with operators $\hat{A}_k(s_k)$ acting in the Hilbert space of the kth site. To find the complete set of inequalities Werner and Wolf make a restriction to full correlation functions, i.e correlation functions in all n sites, and consider the extremal cases where the outcomes are deterministic. Their protocol for generating the complete set of Bell inequalities

is as follows. For some number between 0 and $2^{2^n}-1$, express this as a binary expansion with digits ± 1. this defines a vector $f \in \{-1,+1\}^{2^n}$, with components $f(r) \in \{-1,+1\}$. Now $s,r \in \{1,...,2^n\}$ and let $\mathbf{s},\mathbf{r} \in \{0,1\}^n$ be their binary representations (with digits 0 and 1). Then the coefficients in the corresponding Bell inequality are given by

$$\beta(s) = 2^{-n} \sum_r f(r)\,(-1)^{\mathbf{r}.\mathbf{s}}, \tag{2.3.4}$$

where $\mathbf{r}.\mathbf{s}$ is the dot product of the two binary strings $\mathbf{r}$ and $\mathbf{s}$. These coefficients may used to construct a Bell inequality according to eq(2.3.3).

For example, if $n=3$ they find just 5 essentially different inequalities. 2 of these are just trivial extensions of lower order inequalities, the others are

$$\frac{1}{4}\sum_{k,l,m} a_k\, b_l\, c_m - a_1\, b_1\, c_1 \leq 1, \tag{2.3.5}$$

$$\frac{1}{2}[a_1\, b_1(c_1+c_2) - a_2\, b_2(c_1-c_2)] \leq 1, \tag{2.3.6}$$

$$\frac{1}{2}(a_1\, b_1\, c_2 + a_1\, b_2\, c_1 + a_2\, b_1\, c_1 - a_2\, b_2\, c_2) \leq 1. \tag{2.3.7}$$

These polynomials are interpreted as sums of expectation values. We can note that eq(2.3.7) is the Mermin-Klyshko inequality [25].

Although this characterization of the space $(n,m,v) = (n,2,2)$ is complete, it is possible to make more subtle distinctions than simply whether or not these correlations permit a local realistic model. In particular, since we already know that nature has non-local correlations, it is interesting to try and bound the extent of these non-local correlations. We may consider models which allow some non-local correlations but are otherwise local, in other words a hybrid local, non-local model. Bell inequalities of this type will be the subject of the next two chapters.

Bell inequalities are still a very active area of research and the discussion above is by no means exhaustive. In particular some of the more obvious omissions include

Bell inequalities and vacuum states [28, 29, 30], and 'temporal' Bell inequalities [31, 32, 33].

2.4 Bell's theorem without inequalities.

It is possible to demonstrate quantum non-locality without requiring the violation of some inequality, producing 'Bell's theorem without inequalities'. These proofs all show that if we make the assumptions;

(1) - quantum mechanics is correct,

(2) - locality holds,

then we reach a contradiction. The first such proof was provided for a four party maximally entangled state [34], and for three particles in the famous GHZ paradox [35, 36]. Hardy has also given an elegant demonstration of non-locality in the following thought experiment.

Hardy's paradox [37].

This paradox is a variation on the interaction free measurement suggested by Elitzur and Vaidman [38]. We consider two superposed Mach-Zehnder interferometers ($MZ^{\pm}$), one for electrons (MZ^{-}), and one for positrons (MZ^{+}). This situation is shown in figure 2.2.

If we consider each interferometer separately, by adjusting the arm lengths we may arrange specific relative phases between the two possible paths so that the electron is always detected at C^{-} and the positron is always detected at C^{+}. If $|s\rangle_e$ is the state of the electron initially, after the two beam splitters, the new state is

$$|s\rangle_e \rightarrow \frac{1}{\sqrt{2}}(|O\rangle_e + |NO\rangle_e). \tag{2.4.1}$$

Where O labels one arm, and NO the other. The detectors C^{-} and D^{-} measure projectors on the states $\frac{1}{\sqrt{2}}(|O\rangle_e + |NO\rangle_e)$ and $\frac{1}{\sqrt{2}}(|O\rangle_e - |NO\rangle_e)$ respectively. Sim-

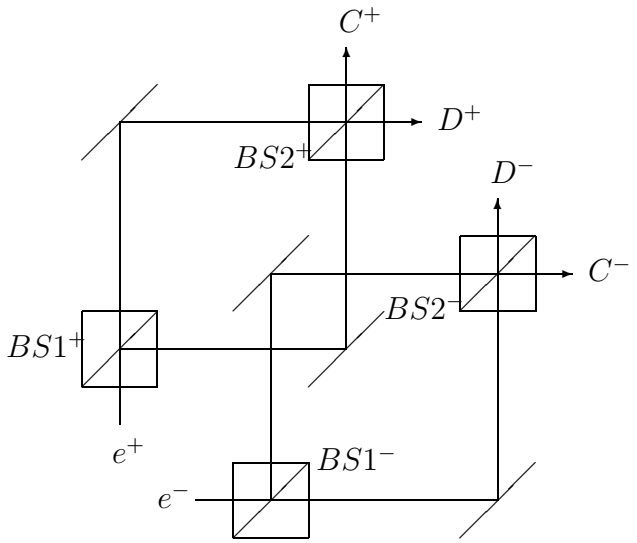

Figure 2.2: Hardy's Paradox. Two superposed Mach-Zehnder interferometers, one for positrons and one for electrons.

ilarly for the positron. Thus when each interferometer is considered separately the detectors D^- and D^+ would never click.

Now imagine we bring both interferometers together. Let O label the overlapping arm, and NO the non-overlapping arm for both $MZ+$ and $MZ-$. If both the electron and positron are in the overlapping arm simultaneously they annihilate one another.

$$|O\rangle_e|O\rangle_p \rightarrow |\gamma\rangle. \tag{2.4.2}$$

We are interested in the cases where the electron and positron do not annihilate. In this case the state of the system is

$$|\psi\rangle = \frac{1}{\sqrt{3}}(|NO\rangle_p|O\rangle_e + |O\rangle_p|NO\rangle_e + |NO\rangle_p|NO\rangle_e). \tag{2.4.3}$$

We find that now there are occasions where both the detectors D^- and D^+ do click. Trying to understand this event leads to a paradox. From the clicking of D^- we

should infer that the positron was in the overlapping arm, disturbing the electron which would otherwise arrive at C^-. Similarly from a click at D^+ we infer the electron was in the overlapping arm. However these two statements can not both be true - otherwise the electron and positron would have annihilated each other.

Hardy has also shown that non-locality without inequalities can be demonstrated with two parties in any entangled state except a maximally entangled state in [39]. Hardy's non-locality proof only works for 9% of the runs of the experiment. Cabello has subsequently extended this result to construct an argument that demonstrate non-locality for 100% of the experimental runs [40].

2.5 Bell Inequalities and entanglement.

Violation of Bell inequalities has become synonymous with non-locality, or non-classical correlation. However the issue of which quantum states are non-local in this sense, and which permit a description in terms of local hidden variables remains open. Quantifying entanglement is a huge challenge, and a summary of results in this field is presented in chapter 6. In this section I just give an overview of the main results concerning the relationships between Bell inequalities and some aspects of entanglement.

A n particle state ρ on some Hilbert space $\mathcal{H} = \mathcal{H}^1 \otimes \mathcal{H}^2 \otimes ... \otimes \mathcal{H}^n$ is *separable* (or un-entangled, or classical) if it can be written

$$\rho = \sum_i p_i \, \rho_i^1 \otimes \rho_i^2 \otimes ... \otimes \rho_i^n. \tag{2.5.1}$$

where each $\rho_i^j \in \mathcal{H}^j$ and $\sum_i p_i = 1$. If the state does not permit such an expansion, it is said to be *entangled*. A state is separable if it can be created locally, i.e by each party acting separately. For example to obtain a state of the form (2.5.1), each party j prepares a state ρ_i^j based on an input i. If the numbers i are produced with probability p_i then we have the required state.

Gisin has shown that all pure entangled bi-partite states violate the CHSH inequality [41], and this result was extended by Popescu and Rohrlich [42] to multi-partite entangled states. Thus for pure states a Bell inequality is violated if and only if the state is entangled.

In practical situations, and because of decoherence, we do not have pure states, but mixed states. These may be thought of as classical ensembles of pure states. For mixed states the relationship to Bell inequality violation is far more complex than was the case for pure states; indeed there is at present no complete classification of bi-partite mixed states according to their non-local properties. In 1989 Werner [43] constructed a local hidden variable model which reproduced the predictions of quantum mechanics for a class of entangled states (Werner states) subject to von Neumann measurements. In 1995 Popescu [44] showed that some of these Werner states could violate the CHSH inequality after a sequence of local measurements which are able to reveal the 'hidden' non-locality of the state.

Entanglement has proved to be a useful resource for information processing tasks. Applications such as teleportation [45] and super dense coding [46] consume entangled pure states. In light of this we would like to be able to *distill* from a number of copies of a mixed state a smaller number of maximally entangled pure states [47, 48]. If a state is distillable then the distilled maximally entangled state violates local realism [49]. However the converse; whether Bell inequality violation implies distillability, is an open question. More generally it is an interesting question to find the relationship between distillation properties and Bell inequality violation.

In 1998 the Horodecki's [50] found states which are entangled, but can not be distilled - *bound entangled states*. Because they can not be distilled they are not, by themselves, useful for quantum information processing tasks. It seemed natural to conjecture that Bell inequality violation and distillation were related. The intuition being that if correlations do not permit a classical model, they may be useful for quantum processing [52].

However in a multipartite setting Dür [53, 54] has recently claimed that there exist

bound-entangled states that violate a Bell inequality. However in this multipartite setting there are different ways of defining what it means for a state to be distillable. Dür defines a state as distillable if and only if, by means of local operations and classical communication, given a large number of copies of the state *some* entangled pure state may be created. He then shows that states that can not be distilled in this way may still violate the Mermin-Klysko inequalities [25]. However following on from this work Acín [55] has shown that the states considered by Dür can in fact be used to distill some pure state entanglement, if we consider splitting the parties into two groups.

One further aspect that has received attention is the relationship between positive partial transposition (PPT) and non-locality. Peres [56] has shown that all separable states have positive eigenvalues under the operation of partial transposition (discussed more fully in chapter 6), i.e separability $\Rightarrow$ PPT. The Horodecki's have shown that for a state to be positive under partial transposition is in fact necessary and sufficient for systems of dimension 2×2 and 2×3 [57]. Also PPT states can not be distilled [50]. Peres [58] has conjectured that a PPT state permits a local description, and Werner and Wolf have some partial results in this area [26]. In particular they show that the Mermin-Klyshko class of Bell inequalities are satisfied for PPT states.

2.6 Experimental realizations.

Aspect [59] made beautiful experimental demonstrations of quantum non-locality in the early 1980's. Figure 2.3 shows the essential details of the apparatus that was used.

In any experiment to study violation of a Bell inequality there will be imperfections in the apparatus. Sometimes, if there are a lot of imperfections, local hidden variable models can be devised to reproduce quantum correlations by exploiting these imperfections. Often these models seem contrived or un-physical, nevertheless

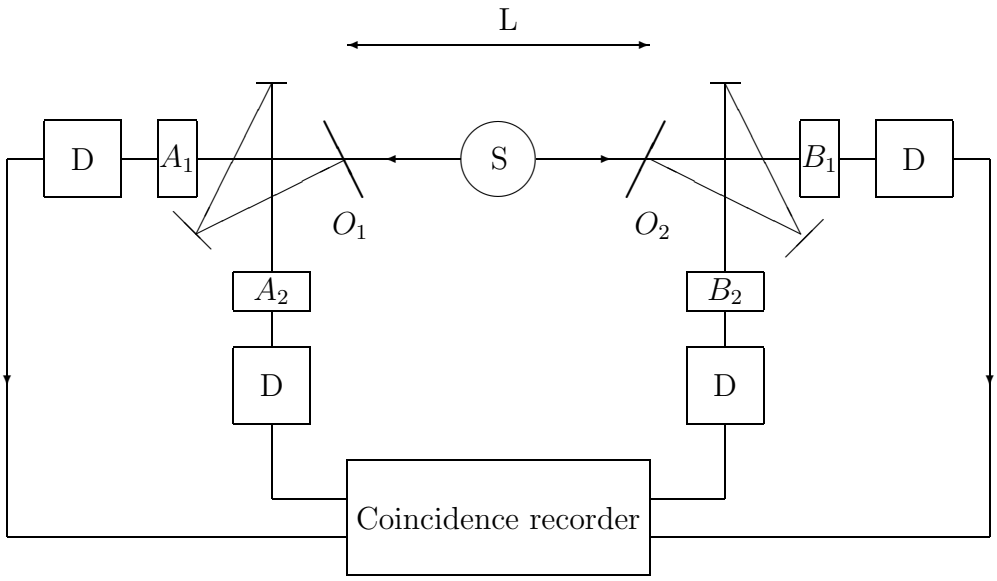

Figure 2.3: Aspects apparatus for demonstrating violation of Bell inequalities. Pairs of photons are emitted from a source S in an atomic cascade. Optical switches O_1 and O_2 redirect these photons to a polarizer with orientation A_1 or A_2 on the left and to a polarizer with orientation B_1 or B_2 on the right. The length L is such that the time taken for the photons to reach the switch is longer than the frequency at which the switch operates (around 10^8 Hz). The detector outputs are checked for coincidences.

because of the fundamental importance of Bell type experiments to our understanding of quantum mechanics such loopholes have received considerable attention. The most famous loopholes are the detection and locality loopholes. As discussed below experiments on photons have recently closed the locality loophole [60], and Rowe *et al* have closed the detection loophole using trapped ions [61], however so far there has been no experiment that closes both loopholes simultaneously.

The detection loophole.

Experiments to detect Bell inequality violations are most often conducted with polarization entangled photons. Photo detectors are at present unreliable: Often they fail to register the passage of a photon. Also photons are absorbed or scattered in the other optical components. Typically of the order of 5% of photons pass successfully through the apparatus and are detected. The detection efficiency which allows loophole free experiments is also related to the amount of background noise in the system.

Let us take as an example the familiar CHSH set up. We may model detector inefficiency as follows: There are two photons a and b, which are subject to one of four possible measurement scenarios A_1B_1, A_1B_2, A_2B_1 and A_2B_2. Now instead of each measurement taking results ± 1 there is a third possibility u - the photon is undetected. This last possibility happens with probability $1-\eta$, where η is the detector efficiency.

Eberhard [62] has shown that with no background noise a loophole free experiment with singlets is possible if $\eta > 0.828$. Surprisingly a lower threshold, $\eta > 0.667$, is possibly if one uses partially entangled states. However such states do not have as large a degree of violation of the inequality as the maximally entangled state.

N. Gisin and B. Gisin [63] have shown that it is possible to construct local hidden variable theories reproducing the quantum mechanical predictions for the singlet state if $\eta < 0.75$. So, despite over 30 years research, this loophole still remains.

The locality loophole.

The assumption of locality in Bell's original derivation requires that the individual measurement processes of the two observers are spacelike separated. An individual measurement has to be completed so quickly that there is not time for any information to travel to the other observer before he has completed his measurement. In Aspects experiment a periodic sinusoidal switching was used to select the analyzer settings. However this is predictable, and so a communication between the two sides of the experiment could still explain the correlations obtained.

In 1998 Weihs *et al* [60] effectively closed this loophole by separating the two measurement locations by 400m, giving them 1.3 μs to select and perform each measurement. Measurements were selected by a physical random number generator, which comprised a light emitting diode illuminating a beam splitter whose outputs were monitored by photomultipliers.

The memory loophole.

In the analysis of Bell type experiments it is usually assumed that any hidden variables associated with the nth photon pair would be independent of the measurement settings and outcomes of the previous $n-1$ pairs. It is possible to exploit such knowledge to produce a model which violates the CHSH inequality, if the data is analyzed in the standard way [64, 65, 66]. However if a different version of the CHSH inequality is used, a violation is no longer possible. Even in the standard analysis the degree of violation becomes small as the number of photon pairs increases. Thus while this loophole suggests a slight flaw in the existing analyzes of Bell type experiments, the data still strongly confirm quantum non-locality against any local hidden variable scheme.

Chapter 3

Conditions for the confirmation of three-particle non-locality.

Abstract.

The notion of genuine three-particle non-locality introduced by Svetlichny [1] is discussed. Svetlichny's inequality, which can distinguish between genuine three-particle non-locality and two-particle non-locality, is analyzed by reinterpreting it as a frustrated network of correlations. Its quantum mechanical maximum violation is derived and a situation is presented that produces the maximum violation. We show that recent beautiful experiments [67, 68] to demonstrate non-locality for a three party state by the GHZ paradox, although demonstrating non-locality, do not allow any violation of the Svetlichny inequality. However we show that with only minor modifications to the measurements performed the experiments would be far more powerful, and able to demonstrate genuine three party non-locality.

3.1 Introduction.

Three particle non-locality was first considered in the famous GHZ paradox [34, 35], and since then generalized Bell inequalities have been derived for n-particle systems which show that quantum mechanics violates local realism in these situations [21, 24, 69]. However, as Svetlichny first showed [1], such results are insufficient to show that all of the particles in a system are acting non-locally - it is possible to imagine a non-local many-particle system as consisting of a finite number of non-local sub-systems, but with only local correlations present between these sub-systems. Svetlichny produced a Bell type inequality to distinguish cases of *genuine* three-particle non-locality from weaker forms involving only two particle non-locality.

Experiments to produce and analyze three particle entangled states are far more difficult than those on two particle entangled states which are now routinely performed. In fact the very first such experiments have only very recently been performed [67, 68]. Unfortunately although the beautiful work of Svetlichny is now more than a decade old, the notion of genuine three particle non-locality that it introduced has not been widely known and the experiments on three particle entanglement have not been specifically designed to verify the existence of such correlations. We show that the particular measurements performed in the experiments of Bouwmeester *et al.* and Pan *et al.* are such that they do not produce (according to quantum mechanics) any violations of Svetlichny's inequality, and can in fact be reproduced by a limited two particle non-local model. Therefore these results cannot be used for the verification of the existence of genuine three-particle non-locality, although they prove non-locality.

To be more specific; a state of three particles $|\Psi\rangle_{123}$ which can be decomposed as $|\psi\rangle_1|\phi\rangle_{23}$ only exhibits non-local correlations between particles 2 and 3. Similarly, a density matrix ρ_{123} which is a mixture of states of the form $|\psi\rangle_1|\phi\rangle_{23}$, $|\eta\rangle_2|\xi\rangle_{13}$ and $|\chi\rangle_3|\theta\rangle_{12}$ contains only two particle non-locality (though it might be very difficult to show this if only the density matrix is given but not the explicit decomposi-

tion). Suppose however that $|\Psi\rangle_{123}$ can not be decomposed - does this necessarily imply that it has three particle non-locality? This was the question first raised by Svetlichny [1]. More precisely, Svetlichny asked the following: We know that the correlations between the results of measurements performed on triplets of particles in the state $|\Psi\rangle_{123}$ cannot be described by local hidden variables. Could they however be described by a *hybrid* local non-local system, in which non-local correlations are present only between two particles (which two particles are non locally correlated can change in different runs of the experiment) while they are only locally correlated with the third? If "yes" then although $|\Psi\rangle_{123}$ can not be decomposed as a direct product of one particle versus a (possible entangled) state of the other two, the non-locality exhibited by this state is still only two particle non-locality.

Although the conceptual ideas in Svetlichny's original paper are very clear, the proof of the inequality is rather complex. In this chapter Svetlichny's inequality is first given a novel interpretation as a frustrated network of correlations. We believe that this new interpretation gives some greater physical intuition into the structure of the Sevtlichny inequality. It is also general enough to be useful when considering other Bell inequalities. We then derive the maximal possible violation of Svetlichny's inequality and a quantum state is then presented which violates it maximally. This also gives the optimum experimental settings for demonstrating a violation. Finally we discuss the experimental status of the verification of genuine three particle non-locality, and suggest simple modifications to the recent experiments by D. Bouwmeester *et al.* [67] and Pan *et al.* [68] which may make such a verification possible.

Formally Svetlichny's model is the following. Let $P(A = a, B = b, C = c)$ be the probability for obtaining a results $A = a$, $B = b$ and $C = c$ when observable A is measured on the first particle, B on the second and C on the third. In a local hidden variables model each particle in the triplet is endowed at source with the same hidden variable λ and later, when subjected to measurements, each particle behaves independently of the others, taking into account only the value of the hidden variable

and the measurement to which it itself is subjected, but not to what measurements the other particles were subjected and/or the results they yield. Hence, $P(A = a, B = b, C = c)$ can be expressed as

$$P(A = a, B = b, C = c)_{local} = \int \rho(\lambda) d\lambda P_1(A = a|\lambda) P_2(B = b|\lambda) P_3(C = c|\lambda), \tag{3.1.1}$$

where $\rho(\lambda)$ describes the probability that the hidden variable has a particular value λ. It is well-known no such local hidden variables model can account for the correlations generated by entangled states.

In the hybrid local non-local hidden variables model considered by Svetlichny, $P(A = a, B = b, C = c)_{Sv}$ is given by:

$$\begin{aligned} P(A = a, B = b, C = c)_{Sv} = \\ q_{12} \int \rho_{12}(\lambda) d\lambda P_{1,2}(A = a, B = b|\lambda) P_3(C = c|\lambda) \\ + q_{23} \int \rho_{23}(\lambda) d\lambda P_{2,3}(B = b, C = c|\lambda) P_1(A = a|\lambda) \\ + q_{13} \int \rho_{13}(\lambda) d\lambda P_{1,3}(A = a, C = c|\lambda) P_2(B = b|\lambda), \end{aligned} \tag{3.1.2}$$

subject to $q_{12} + q_{23} + q_{13} = 1$ and $\int \rho_{ij}(\lambda) d\lambda = 1$.

Thus when repeated measurements are performed on an ensemble, the three terms in eq 3.1.2 correspond to the three possible factorizations of two particle non-locality between the three particles, (1,2)-3, (2,3)-1 and (1,3)-2, with q_{12}, q_{23} and q_{13} the probabilities of each particular factorization being present.

Svetlichny derived an inequality which is obeyed by all such hybrid local two-particle non-local models, and showed that some quantum states violate the inequality, hence they are genuinely three particle non-local.

3.2 Interpreting Svetlichny's inequality as a frustrated network.

Bell-type inequalities are generally expressed in terms of the expectation values of observables. In this section it is shown how it is possible to interpret Svetlichny's inequality as a frustrated networks of correlations. (In fact many presently known Bell type inequalities can be described in such a way and this leads to a better understanding of their physical meaning.) Consider a situation of three spatially separated two dimensional systems. System A is subject to one of the measurements A or A', and similarly for systems B and C. The result of any measurement is labelled ± 1. Let $E(ABC)$ be the expectation value of the product of the outcomes of measurements A, B and C. Then Svetlichny's inequality is;

$$\begin{aligned} &|E(ABC) + E(ABC') + E(A'BC) - E(A'BC') \\ &+E(AB'C) - E(AB'C') - E(A'B'C) - E(A'B'C')| \leq 4. \end{aligned} \tag{3.2.1}$$

We will express this in a different (although equivalent) form. Suppose A, B and C have been measured. Since the outcomes a, b and c can only be equal to ± 1, we have only two possibilities. Either $a = bc$ or $a = -bc$; we refer to the two cases as A being correlated to BC or anti-correlated to BC. Furthermore, when $a = bc$ it is also the case that $b = ac$ and $c = ab$ thus we can talk about correlation without mentioning explicitly between which partitions; similarly for anti-correlation. Define the probability of correlation, $P_c(ABC)$, as the probability that A, B and C are correlated, and $P_a(ABC)$ as the probability that they are anti-correlated. These probabilities of correlation and anti-correlation are related to the expectation values in eq(3.2.1) by

$$E = P_c - P_a = 2P_c - 1 = 1 - 2P_a. \tag{3.2.2}$$

Using eq(3.2.2) Svetlichny's inequality is equivalent to

$$2 \leq \bar{S} \leq 6, \tag{3.2.3}$$

where $\bar{S}$ is defined as

$$\begin{aligned} \bar{S} &= P_a(ABC) + P_a(ABC') + P_a(A'BC) + P_c(A'BC') \\ &+ P_a(AB'C) + P_c(AB'C') + P_c(A'B'C) + P_c(A'B'C'). \end{aligned} \tag{3.2.4}$$

Our task now is to prove eq(3.2.3) under the assumption of a hybrid local non-local model. Suppose initially that limited non-locality takes the form that particles A and B form a non-local subsystem AB and that this subsystem is locally correlated with particle C.

Recall that in our interpretation of Svetlichny's inequality non-locality between A and B means these particles are regarded as a composite system. Hence the outcomes for the paired measurements $AB, AB', A'B$ and $A'B'$ are completely unconstrained from each other. Furthermore, locality of C versus AB means that for any local hidden variable model the choice of which of the paired measurements $AB, AB', A'B$ and $A'B'$ to make is independent of whether C or C' is measured.

In the most general hidden variable model that can be considered, for each value of the hidden variable λ, which occurs with probability $\rho(\lambda)$, the measurements can yield different outcomes according to the associated probabilities such as $P(A = a|\lambda)$. The probabilities of correlation and anti-correlation, and hence the sum of probabilities in eq(3.2.4), are also dependent on λ. We call this sum of conditional probabilities in eq(3.2.4) $S(\lambda)$, and note that $\bar{S}$ is the average over $\rho(\lambda)$ of $S(\lambda)$. It can be easily shown that any such model can be re-cast into a deterministic model [20] in which for each value of λ the outcomes are completely determined, i.e. the probabilities of obtaining each of the possible measurements is either 0 or 1. In particular, for each value of λ we have a given, well-defined assignment of ± 1 values for ab, ab', $a'b$, $a'b'$, c and c', and the probabilities of correlation and anti-correlation are either 0 or 1.

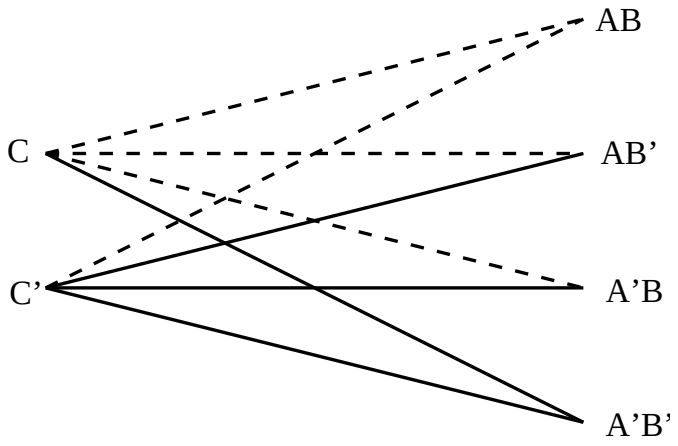

Figure 3.1: Network for the correlations in Svetlichny's inequality. Dotted lines denote anti-correlation, full lines denote correlation.

Then eq(3.2.4) corresponds to the network shown in figure 3.1. The other possible factorizations of the system, A-BC and B-AC, give the same diagram with the particle names permuted.

Referring to eq(3.2.4) and figure 3.1, one can easily check that for no assignment of ± 1 values for the results of measurements can all the eight probabilities be equal to 1, nor can all of them be equal to 0. In fact at least two of the bonds in figure 3.1 must be satisfied by any combination of ± 1 at the vertices, and only a maximum of six out of the total of eight bonds may ever be satisfied. Hence the network is frustrated (in other words not all links can be simultaneously satisfied) and for every value of λ, $2 \leq S(\lambda) \leq 6$. Furthermore, since the the inequality holds for every value of λ, it also holds for the average, $\bar{S} = \int \rho(\lambda)\, S(\lambda)\, d\lambda$.

As a last step, due to the symmetry under permutation of particles, the same inequality holds for all 2 versus 1 partitions, and thus for the grand average over all possible partitions and all assignments of the hidden variable. The values of $S(\lambda)$ for given different partitions or particular values of the hidden variable are not accessible experimentally - only the grand average is experimentally observable.

Thus $2 \leq \bar{S} \leq 6$ for hybrid local non-local models. This is Svetlichny's inequality,

in a slightly different form from originally proposed.

3.3 The predictions of quantum mechanics.

We now derive the maximum possible quantum mechanical violation of Svetlichny's inequality and show a particular case in which the inequality is maximally violated. It is possible to show that $4\sqrt{2}$ is the maximum possible quantum mechanical violation of Svetlichny's inequality. This is the equivalent of Cirel'son's bound for the CHSH inequality. For a state $|\psi\rangle$ the sum of expectations in eq(3.2.1), Sv, can be written as:

$$\begin{aligned} Sv = |\langle\psi|AB(C+C')|\psi\rangle + \langle\psi|AB'(C-C')|\psi\rangle \\ +\langle\psi|A'B(C-C')|\psi\rangle + \langle\psi|A'B'(-C-C')|\psi\rangle|, \end{aligned} \tag{3.3.1}$$

by replacing the expectation values by their quantum expression and grouping the terms. Using Schwarz' inequality we can bound the magnitude of each term:

$$\begin{aligned} |\langle\psi|AB(C+C')|\psi\rangle| \leq \\ \sqrt{|\langle\psi|ABAB)|\psi\rangle||\langle\psi|(C+C')(C+C')|\psi\rangle|} \end{aligned} \tag{3.3.2}$$

$$\leq \sqrt{2+\langle\psi|CC'+C'C|\psi\rangle}, \tag{3.3.3}$$

where the last inequality obtains since $\langle\psi|ABAB|\psi\rangle = \langle\psi|CC|\psi\rangle = \langle\psi|C'C'|\psi\rangle = 1$. Similar results are found for the other three terms. If we now let $x = \langle\psi|CC' + C'C|\psi\rangle$, then

$$|Sv| \leq 2(\sqrt{2+x}) + 2(\sqrt{2-x}). \tag{3.3.4}$$

Thus $|Sv| \leq 4\sqrt{2}$ with the maximum absolute value being attained at $x = 0$.

For a GHZ state of three spin 1/2 particles $|\psi\rangle = \frac{1}{\sqrt{2}}(|\uparrow\uparrow\downarrow\rangle - |\downarrow\downarrow\uparrow\rangle)$, where $\uparrow$ and $\downarrow$ represent spins polarized "up" or "down" along the z axis, Svetlichny's

inequality is violated if, for example, measurements are made in the xy plane along some appropriate directions. In this case $E(ABC) = \langle\psi|\vec{a}\cdot\vec{\sigma}\otimes\vec{b}\cdot\vec{\sigma}\otimes\vec{c}\cdot\vec{\sigma}|\psi\rangle = -\cos(\alpha+\beta-\gamma)$, where we labelled the angles from the x axis and α refers to the measurement on particle A, β to the measurement on particle B, and γ to the measurement on particle C. The inequality will be maximally violated by choosing $\alpha = 0, \alpha' = \frac{-\pi}{2}, \beta = \frac{\pi}{4}, \beta' = \frac{-\pi}{4}, \gamma = 0, \gamma' = \frac{\pi}{2}$. Then $Sv = 4\sqrt{2}$.

3.4 Experiments.

In this section we revisit the experiments of Bouwmeester *et al.* [67] and Pan *et al.* [68], two of the first experiments to test three particle entanglement. We show that the particular measurements performed in these experiments are such that they do not produce (according to quantum mechanics) any violations of Svetlichny's inequality. They can in fact be reproduced by a limited two particle non-local model and therefore do not demonstrate genuine three-particle non-locality.

The two experiments described in [67] and [68] use essentially the same experimental set-up to produce the three-photon entangled state $|\psi\rangle = \frac{1}{\sqrt{2}}(|HHV\rangle - |VVH\rangle)$. Here H represents horizontal polarization and V vertical polarization. They used the set up shown in figure 3.2. The main idea is to transform two pairs of polarization entangled photons into three entangled photons, and a fourth independent photon.

Pairs of polarization entangled photons are produced by short laser pulses passing through a non linear crystal. With some probability the resulting state is

$$\frac{1}{\sqrt{2}}(|H\rangle_a|V\rangle_b - |V\rangle_a|H\rangle_b). \tag{3.4.1}$$

The subscripts a and b refer to the two arms. Each photon continues through polarization independent beam splitters (BS), polarization dependent beam splitters (POL BS), which pass $|H\rangle$ and reflect $|V\rangle$, and a $\lambda/2$ plate which rotates the vertical polarization reflected from the first POL BS to a superposition of $|H\rangle$ and $|V\rangle$ with equal amplitudes. The evolution of the components through the system is such that

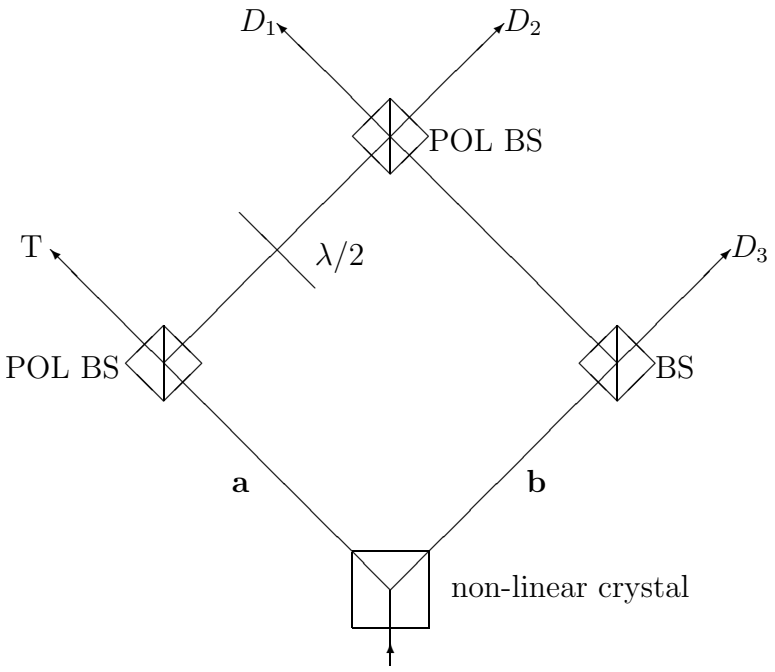

Figure 3.2: The apparatus of Bouwmeester *et al* for producing GHZ states. Conditioned on the detection of a photon at T, the correlations registered at detectors D_1, D_2 and D_3 are consistent with a GHZ state.

$$|H\rangle_a \rightarrow |H\rangle_T \tag{3.4.2}$$

$$|V\rangle_a \rightarrow \frac{1}{\sqrt{2}}(|V\rangle_1 + |H\rangle_2) \tag{3.4.3}$$

$$|H\rangle_b \rightarrow \frac{1}{\sqrt{2}}(|H\rangle_1 + |H\rangle_3) \tag{3.4.4}$$

$$|V\rangle_b \rightarrow \frac{1}{\sqrt{2}}(|V\rangle_2 + |V\rangle_3) \tag{3.4.5}$$

Now suppose that two down conversions have taken place, producing the state

$$\frac{1}{2}(|H\rangle_a|V\rangle_b - |V\rangle_a|H\rangle_b)(|H'\rangle_a|V'\rangle_b - |V'\rangle_a|H'\rangle_b). \tag{3.4.6}$$

If the photons produced from the two down conversions are indistinguishable and we restrict ourselves to terms where only one photon is found in each output the state obtained is

$$\frac{1}{\sqrt{2}}|H\rangle_T(|H\rangle_1|H\rangle_2|V\rangle_3 - |V\rangle_1|V\rangle_2|H\rangle_3). \tag{3.4.7}$$

To verify that indeed such a GHZ state had been produced, different tests were made. It is simpler to represent the state in the z basis writing $|H\rangle = |\uparrow\rangle$ and $|V\rangle = |\downarrow\rangle$. Then $|\psi\rangle = \frac{1}{\sqrt{2}}(|\uparrow\uparrow\downarrow\rangle - |\downarrow\downarrow\uparrow\rangle)$. In [67] measurements (of the optical equivalent) of spin in the z and x directions were performed. Unfortunately, as it is straightforward to check, measurements along x and z do not lead to Svetlichny inequality violations for the GHZ state.

In the subsequent experiment [68] measurements XXX, XYY, YXY and YYX were performed so as to demonstrate the GHZ paradox [34, 35], obtaining values 1,-1,-1,-1 respectively (on the state $\frac{1}{\sqrt{2}}(|\uparrow\uparrow\uparrow\rangle + |\downarrow\downarrow\downarrow\rangle)$). These results can not be reproduced by any local theory. However the GHZ paradox does not demonstrate genuine three party non-locality because the correlations can be described by a hybrid local non-local model. This means that the correlations will not violate any Svetlichny type inequality.

The experimental probabilities in the GHZ experiment $P(a,b,c|A,B,C)$, where $a \in \{-1,1\}$ is the outcome of measurement $A \in \{X,Y\}$ and similarly for b and c, are given by

$$p\left(a,b,c|A,B,C\right) = \begin{cases} 1/4 & : \quad abc = -1 \\ 0 & : \quad abc = 1 \end{cases} \tag{3.4.8}$$

when $(A,B,C) \in \{(X,Y,Y),\, (Y,X,Y,),\, (Y,Y,X)\}$, i.e when the product $abc = -1$ then that particular outcome occurs with probability $1/4$.

$$p\left(a,b,c|X,X,X\right) = \begin{cases} 1/4 & : \quad abc = 1 \\ 0 & : \quad abc = -1 \end{cases} \tag{3.4.9}$$

And finally,

$$p\left(a,b,c|A,B,C\right) = \frac{1}{8} \;\; \forall\, a,b,c, \tag{3.4.10}$$

$(A,B,C) \in \{(Y,Y,Y),\, (X,X,Y),\, (Y,X,X),\, (X,Y,X)\}$.

We will construct a hybrid local non-local variable model that reproduces these correlations. Suppose the non-local subsystem is composed of particles 2 and 3, correlated locally with particle 1; we will show that the GHZ correlations in eq(3.4.8) - eq(3.4.10) can be written

$$p\left(a,b,c|A,B,C\right) = \sum_{\lambda=1}^{4} \frac{1}{4}\, p^{\lambda}\left(a|A\right) p^{\lambda}\left(b,c|B,C\right). \tag{3.4.11}$$

Our protocol for constructing the GHZ correlations is the following:

• Each of the $p^{\lambda}\left(a|A\right)$ are deterministic, i.e the probabilities are either zero or 1. All possible deterministic strategies are included in the sum.

• For each of the $p^{\lambda}\left(a|A\right)$ the corresponding $p^{\lambda}\left(b,c|B,C\right)$ is chosen so that

$$p\left(a,b,c|A,B,C\right) = 0 \;\Rightarrow\; p^{\lambda}\left(a|A\right) p^{\lambda}\left(b,c|B,C\right) = 0. \tag{3.4.12}$$

• For each pair B,C the outcomes b, c satisfying the above condition occur with equal probability.

Let $p^1(1|X) = p^1(1|Y) = 1$. Our protocol then gives;

$$p^1(1,1|X,X) = p^1(-1,-1|X,X) = 1/2 \tag{3.4.13}$$

to satisfy the zero probabilities in eq(3.4.9). Similarly, to satisfy the zero probabilities in eq(3.4.8)

$$p^1(1,-1|X,Y) = p^1(-1,1|X,Y) = 1/2 \tag{3.4.14}$$

$$p^1(1,-1|Y,X) = p^1(-1,1|Y,X) = 1/2 \tag{3.4.15}$$

$$p^1(1,-1|Y,Y) = p^1(-1,1|Y,Y) = 1/2 \tag{3.4.16}$$

We also have that $p^2(1|X) = p^2(-1|Y) = 1$, $p^3(-1|X) = p^3(1|Y) = 1$ and $p^4(-1|X) = p^4(-1|Y) = 1$. The protocol then completely specifies $p^\lambda(b,c|B,C)$ in each case. It is then straightforward to check that this hybrid local non-local distribution reproduces the GHZ correlations.

In fact we can extend this model to show any set of measurements chosen to be in the x, y or z direction can be reproduced by a local non-local hybrid model of the form

$$p(a,b,c|A,B,C) = \sum_{\lambda=1}^{8} \frac{1}{8} p^\lambda(a|A)\, p^\lambda(b,c|B,C). \tag{3.4.17}$$

The protocol is exactly the same as before, with $A,B,C \in X,Y,Z$. The following probability distribution characterizes the GHZ correlations. We consider the cases when the set A, B, C contains different numbers of Z measurements separately.

no Z measurements.

$$p(a,b,c|X,X,X) = \begin{cases} 1/4 & : \quad abc = 1 \\ 0 & : \quad abc = -1, \end{cases} \tag{3.4.18}$$

$$p(a,b,c|A,B,C) = \begin{cases} 1/4 & : \quad abc = -1 \\ 0 & : \quad abc = 1, \end{cases} \tag{3.4.19}$$

when $(A,B,C) \in \{(X,Y,Y),\ (Y,X,Y),\ (Y,Y,X)\}$.

Also,

$$p\left(a,b,c|A,B,C\right) = \frac{1}{8}\ \forall\, a,b,c, \tag{3.4.20}$$

when $(A,B,C) \in \{(Y,Y,Y,),\ (X,X,Y,),\ (Y,X,X),\ (X,Y,X)\}$.

1 Z measurement.

When the set A,B,C contains exactly one Z measurement

$$p\left(a,b,c|A,B,C\right) = \frac{1}{8}\ \forall\, a,b,c. \tag{3.4.21}$$

2 Z measurements.

$$p\left(a,b,c|A,B,C\right) = \begin{cases} 1/4 & : \quad a=c \\ 0 & : \quad \text{otherwise}, \end{cases} \tag{3.4.22}$$

when $(A,B,C) \in \{(Z,B,Z) : B \in \{Y,X\}\}$

$$p\left(a,b,c|A,B,C\right) = \begin{cases} 1/4 & : \quad a=b \\ 0 & : \quad \text{otherwise}, \end{cases} \tag{3.4.23}$$

when $(A,B,C) \in \{(Z,Z,C) : C \in \{Y,X\}\}$

$$p\left(a,b,c|A,B,C\right) = \begin{cases} 1/4 & : \quad b=c \\ 0 & : \quad \text{otherwise}, \end{cases} \tag{3.4.24}$$

when $(A,B,C) \in \{(A,Z,Z) : A \in \{Y,X\}\}$

3 Z measurements.

$$p\left(a,b,c|Z,Z,Z\right) = \begin{cases} 1/2 & : \quad a=b=c \\ 0 & : \quad \text{otherwise} \end{cases} \tag{3.4.25}$$

Reproducing the GHZ correlations.

Suppose the non-local subsystem is composed of particles 2 and 3, correlated locally with particle 1. The GHZ correlations above can be written according to eq(3.4.17). Following the same protocol as before: There are eight different deterministic probability distributions $p^{\lambda}(a|A)$, and summing over them according to eq (3.4.17) gives the correct GHZ correlations. For example, suppose $p^{1}(a|A)$ is given by $p^{1}(1|X) = p^{1}(1|Y) = p^{1}(1|Z)$. According to the protocol

$$p^{1}(b,c|X,X) = \begin{cases} 1/2 & : \quad bc = 1 \\ 0 & : \quad \text{otherwise,} \end{cases} \tag{3.4.26}$$

so as to satisfy the zero probabilities in eq (3.4.18). Each of the two possible solutions is taken with probability half.

$$p^{1}(b,c|X,Y) = \begin{cases} 1/2 & : \quad bc = -1 \\ 0 & : \quad \text{otherwise,} \end{cases} \tag{3.4.27}$$

so as to satisfy the zero probabilities in eq (3.4.19). Each of the two possible solutions is taken with probability half.

$$p^{1}(b,c|X,Z) = p^{1}(b,c|Y,Z) = \begin{cases} 1/2 & : \quad b,c = -1,1 \text{ or } 1,1 \\ 0 & : \quad \text{otherwise,} \end{cases} \tag{3.4.28}$$

so as to satisfy the zero probabilities in eq (3.4.22).

$$p^{1}(b,c|Y,X) = p^{1}(b,c|Y,Y) = \begin{cases} 1/2 & : \quad bc = -1 \\ 0 & : \quad \text{otherwise,} \end{cases} \tag{3.4.29}$$

so as to satisfy the zero probabilities in eq (3.4.19).

$$p^{1}(b,c|Z,X) = p^{1}(b,c|Z,Y) = \begin{cases} 1/2 & : \quad b,c = 1,-1 \text{ or } 1,1 \\ 0 & : \quad \text{otherwise,} \end{cases} \tag{3.4.30}$$

so as to satisfy the zero probabilities in eq (3.4.23).

$$p^1(b,c|Z,Z) = \begin{cases} 1 & : \quad b,c = 1,1 \\ 0 & : \quad \text{otherwise,} \end{cases} \tag{3.4.31}$$

so as to satisfy the zero probabilities in eq (3.4.25).

This completely specifies $p^1(b,c|B,C)$. Similar constructions give $p^\lambda(a|A)$ and $p^\lambda(b,c|B,C)$ for $\lambda = 2,...,8$. It is straightforward to check that the probability distribution resulting from eq (3.4.17) gives the GHZ correlations. Therefore the analysis of the data already obtained cannot prove the existence of genuine 3-party correlations.

On the other hand, it is easy to modify the experiments so as to produce a maximum violation of Svetlichny's inequality. It is sufficient to make measurements in the xy plane using the angles listed above in section three. Where to measure a spin component with angle θ in this plane it is necessary to perform a measurement which has eigenvectors $\frac{1}{\sqrt{2}}(|\uparrow\rangle + e^{i\theta}|\downarrow\rangle)$ and $\frac{1}{\sqrt{2}}(|\uparrow\rangle - e^{i\theta}|\downarrow\rangle)$, that is $\frac{1}{\sqrt{2}}(|H\rangle + e^{i\theta}|V\rangle)$ and $\frac{1}{\sqrt{2}}(|H\rangle - e^{i\theta}|V\rangle)$. It should then be possible to confirm that the state produced demonstrates genuine three-particle non-locality.

W state non-locality.

Cereceda has pointed out that the W state also exhibits genuine three party non-locality as demonstrated by a violation of the Svetlichny inequality [70].

$$|W\rangle = \frac{1}{\sqrt{3}}(|\uparrow\uparrow\downarrow\rangle + |\uparrow\downarrow\uparrow\rangle + |\downarrow\uparrow\uparrow\rangle \tag{3.4.32}$$

We can recall that along with the GHZ state, the W state is one of only two types of inequivalent pure three party entangled state of qubits [71] under SLOCC. For such a state the maximum value for the Svetlichny expression is 4.354 [70], as found numerically. Recent experiments have realized the W state [72] but unfortunately the measurements performed do not allow any violation of Svetlichny's inequality[73].

Conclusion.

We conclude that the experiments so far performed on three particle entangled states do not demonstrate three particle non-locality. However with simple modifications they could be adapted to enable a violation of Svetlichny's inequality.

In the next chapter we derive an inequality that plays the role of the generalized Svetlichny inequality for n particle systems. Four and five particle states have recently been created, and we will discuss these experiments in light of the notion of genuine n particle non-locality. We find that in the four particle case a violation of the generalized Svetlichny inequality has been observed, thus demonstrating genuine four particle non-locality.

Chapter 4

Bell inequalities to detect true n-particle non-locality.

Abstract.

This chapter contains a generalization to n particles of the notions of non-locality introduced in the previous chapter. We introduce a classification of correlations based on the concept of non-locality, which is different a priori from the concept of entanglement. Generalizing a result of Svetlichny [1] on three particle correlations, we find an inequality for n particle correlations that holds under the most general separability condition and that is violated by some quantum-mechanical states.

Four and five particle states have recently been created, and we discuss these experiments in light of the notion of genuine n particle non-locality. We find that in the four particle case a violation of the generalized Svetlichny inequality has been observed, thus demonstrating genuine four particle non-locality.

4.1 Introduction.

The remarkable correlations between the outcomes of measurements on entangled quantum systems have been the object of many studies. Usually analyzes of the structure of the correlations are made according to the entanglement properties of the system. In this chapter we propose a complementary classification, in terms of non-locality. This is a generalization to n parties of the concepts of genuine three party non-locality discussed in the previous chapter. To motivate this we can see that the concepts of entanglement and non-locality are a priori different.

Essentially a classification through entanglement pre-supposes that our system under study allows a quantum mechanical description. A classification through non-locality does not assume the system admits a quantum mechanical description. Rather it models the correlations obtained under different types of hybrid local non-local hidden variable models.

To explain this in more detail, let us assume that we are considering a system of three particles. This is a recap of the previous chapter, introducing some new notation which makes generalizing these concepts easier. The classification through entanglement assumes the system admits a quantum mechanical description, and so is completely characterized by some quantum state ρ. To classify ρ through its entanglement properties we must consider all possible decompositions of the state as a mixture of pure states.

$$\rho = \sum_i p_i \, |\Psi_i\rangle\langle\Psi_i| \tag{4.1.1}$$

There are then three possibilities.

(i) If there is a decomposition of ρ so that

$$|\Psi_i\rangle = |\psi_i^1\rangle|\psi_i^2\rangle|\psi_i^3\rangle \tag{4.1.2}$$

for all $|\Psi_i\rangle$, then ρ is a mixture of product states, and so is separable with the property that it can be made by each party acting locally. For this situation we use

the acronym $1/1/1/QM$.

(ii) If all of the $|\Psi_i\rangle$ can be written as $|\psi_i^{12}\rangle|\psi_i^3\rangle$ or $|\psi_i^{13}\rangle|\psi_i^2\rangle$ or $|\psi_i^{23}\rangle|\psi_i^1\rangle$ and at least one of the $|\psi_i^{jk}\rangle$ is not a product state, then ρ is entangled, but does not exhibit any true three-way entanglement. We can say that ρ exhibits two party entanglement, and denote this by $2/1/QM$.

(iii) Finally if there is at least one $|\Psi_i\rangle$ that shows three-way entanglement, i.e can not be written as $|\Psi_i\rangle = |\psi_i^{jk}\rangle|\psi_i^l\rangle$, the ρ exhibits true three-particle entanglement. We will use the acronym $3/QM$ to describe this.

In general it is difficult to decide which class ρ belongs to as it requires a consideration of all possible decompositions. At present no necessary and sufficient criterion is known. We do however have a sufficient criterion, given by the Mermin inequality [10]. Let $\mathcal{M}_3$ be the Mermin operator for three parties. This is described in detail in section 4.2. Then if $\mathrm{Tr}(\rho\mathcal{M}_3) > 1$ the state ρ is entangled. If $\mathrm{Tr}(\rho\mathcal{M}_3) > \sqrt{2}$ the state ρ exhibits true three particle entanglement.

The classification through non-locality does not presuppose that the state permits a description in terms of quantum mechanics. It is based on a classification through different types of hidden variable models. As with the classification through entanglement we distinguish three classes.

(i) Let λ be a hidden variable or script carried by each particle. This value determines the outcome of each measurement made on the particle. When the experiment is repeated many times the scripts can be different, occurring with probability distribution $\rho(\lambda)$. This is an example of a local hidden variable model (LHV), which we will denote by $1/1/1/S$.

(ii) We may imagine a hybrid local non-local model. This was the model used by Svetlichny [1]. We can denote this by $2/1/S$ and note that this is a more general class than $2/1/QM$ because we do not require that the particles are correlated according to quantum mechanics.

(iii) We allow all three particles to share arbitrary correlations without any constraints. We denote this situation $3/S$.

With this new notation we may interpret Svetlichny's work as demonstrated that $3/QM$ is stronger (permits more general correlations) that $2/1/S$. The aim of this chapter is to generalize this idea to n partite systems and show that n/QM is stronger than $k/(n-k)/S$ for all $k < n$. To do this we first introduce the Mermin-Klyshko (MK) inequalities [21, 25, 26] which are the main tool for this study. We show how these can be used to give the Svetlichny inequality for three particles, and that the MK inequality plays the role of the generalized Svetlichny inequality for four particles. Finally the generalization to n particles is made.

In the final section we review recent experimental progress in creating four and five particle entangled states. We find that in the four particle case a violation of the generalized Svetlichny inequality has been observed. Thus this experiment demonstrates four particle non-locality.

Much of the work in this chapter was done in collaboration with N. Gisin and V. Scarani from University of Geneva, and D. Collins and S. Popescu from University of Bristol. It was published in [5].

4.2 The Mermin-Klyshko inequalities.

We consider from now onwards an experimental situation in which two dichotomic measurements A_j and A'_j can be performed on each particle $j = 1, ..., n$. The outcomes of these measurements are written a_j and a'_j, and can take the values ± 1. Letting $M_1 = a_1$, we can define recursively the *MK polynomials* as

$$M_n = \frac{1}{2} M_{n-1} (a_n + a'_n) + \frac{1}{2} M'_{n-1} (a_n - a'_n), \tag{4.2.1}$$

where M'_k is obtained from M_k by exchanging all the primed and non-primed a's. In particular, we have

$$M_2 = \frac{1}{2}\left(a_1a_2 + a_1'a_2 + a_1a_2' - a_1'a_2'\right), \tag{4.2.2}$$

$$M_3 = \frac{1}{2}\left(a_1a_2a_3' + a_1a_2'a_3 + a_1'a_2a_3 - a_1'a_2'a_3'\right). \tag{4.2.3}$$

The recursive relation (4.2.1) gives, for all $1 \leq k \leq n-1$:

$$M_n = \frac{1}{2}\, M_{n-k}\left(M_k + M_k'\right) + \frac{1}{2}\, M_{n-k}'\left(M_k - M_k'\right). \tag{4.2.4}$$

This is shown in appendix A, at the end of this chapter. We shall interpret these ploynomials as sums of expectation values, for example we shall interpret M_2 as

$$\frac{1}{2}\left(E(A_1A_2) + E(A_1'A_2) + E(A_1A_2') - E(A_1'A_2')\right), \tag{4.2.5}$$

where $E(A_1A_2)$ is the expectation value of the product a_1a_2 when A_1 and A_2 are measured. We call quantities such as $E(A_1A_2A_3)$ correlation coefficients. We shall look at the values of these polynomials under quantum mechanics and hybrid local non-local models, and show that they give generalized Bell inequalities.

The MK polynomials under hybrid LHV models.

We can restrict our attention to deterministic versions of hybrid local non-local hidden variable models. It is known that any non-deterministic local model can be made deterministic by adding additional variables [74]. Hence the script λ completely determines the probabilities for the outcomes of any measurement, i.e $P(A_j = a_j|\lambda)$ and similar probabilities are either zero or one.

For any λ the outcomes of all correlation coefficients are fixed, so we can define the fixed quantity M_n^λ. The value M_n is then the average over $\rho(\lambda)$ of M_n^λ. For any LHV model $(1/1/.../1/S)$ [1] $M_n^{LHV} \leq 1$ [21]. This can be seen using a recursive

[1] From now on LHV is taken to mean all particles are uncorrelated, i.e there statistics are described according to $1/1/.../1/S$.

argument and noting that for any LHV script either $a_n = a'_n$ or $a_n = -a'_n$. In particular $M_2 \leq 1$ is the famous CHSH inequality [16]. For models of the type n/S, that is unconstrained models, each M_n can reach its algebraic limit, M_n^{alg}. This can be achieved by setting to +1 (resp. -1) all of the correlation coefficients appearing with positive sign (resp. negative sign). This gives $M_n^{alg} = 2$ for all n.

The MK polynomials under quantum mechanics.

Since we consider dichotomic measurements, we can restrict to the case of two-dimensional systems (qubits)[75]. In this case, the observable that describes the measurement A_j can be written as $\vec{a_j} \cdot \vec{\sigma} \equiv \sigma_{a_j}$, with $\vec{a_j}$ a unit vector and $\vec{\sigma}$ the vector of Pauli spin matrices. The equivalent of M_n is the expectation value of the operator $\mathcal{M}_n$ obtained by replacing all a's by the corresponding σ_a. It is known that quantum mechanics violates the inequality $\mathrm{Tr}(\rho\,\mathcal{M}_n) \leq 1$. More precisely, it is known [21, 25, 26] that:

(i) The maximal value achievable by quantum mechanics is

$$\mathrm{Tr}(\rho\,\mathcal{M}_n) = 2^{\frac{n-1}{2}}, \tag{4.2.6}$$

reached by the generalized Greenberger-Horne-Zeilinger (GHZ) states $\frac{1}{\sqrt{2}}\big(|0...0\rangle + |1...1\rangle\big)$.

(ii) If ρ exhibits m-particle entanglement, with $1 \leq m \leq n$, then

$$\mathrm{Tr}(\rho\,\mathcal{M}_n) \leq 2^{\frac{m-1}{2}}. \tag{4.2.7}$$

In other words, if we have a state of n qubits ρ such that $\mathrm{Tr}(\rho\,\mathcal{M}_n) > 2^{\frac{m-1}{2}}$, we know that this state exhibits at least $(m+1)$-particle entanglement. This means that the MK-polynomials allow a classification of correlations according to entanglement. But do they allow also the classification according to non-locality? The

answer to this question is: yes for n even, no for n odd. However we shall show that a modification to the MK polynomials for n odd does then allow for a classification according to non-locality. We demonstrate this statement first for $n = 3$, then for $n = 4$, and finally for all n.

4.3 Three particles.

Consider the the three particle MK polynomial,

$$M_3 = \frac{1}{2}(a_1 a_2 a_3' + a_1 a_2' a_3 + a_1' a_2 a_3 - a_1' a_2' a_3'). \tag{4.3.1}$$

Then the following bounds have previously been established.

$$M_3^{LHV} = 1 \tag{4.3.2}$$

$$M_3^{2/1/QM} = \sqrt{2} \tag{4.3.3}$$

$$M_3^{3/QM} = M_3^{alg} = 2 \tag{4.3.4}$$

We want to find the bound under $2/1/S$. We can do this by allowing particles one and two to be correlated in the most general way, and setting particle three to be uncorrelated with the other two. M_3 can be re-written,

$$M_3 = \frac{1}{2}M_2(a_3 + a_3') + \frac{1}{2}M_2'(a_3 - a_3'). \tag{4.3.5}$$

For any particular script either $a_3 = a_3'$ or $a_3 = -a_3'$, and without loss of generality we may assume the former. In this case $M_3^{2/1/S} = \max M_2$. Now since particles one and two can share any correlation, they can reach the algebraic maximum of M_2. Therefore $M_3^{2/1/S} = 2$, and

$$M_3^{2/1/S} = M_3^{3/QM} = M_3^{alg} = 2. \tag{4.3.6}$$

Therefore the MK inequality does not distinguish between $2/1/S$ and $3/QM$, i.e the MK inequality can not distinguish between genuine three party non-locality and hybrid local non-local correlations.

However we can easily modify the MK polynomial so that it can. We will consider the properties of the polynomial

$$S_3 = \frac{1}{2}(M_3 + M_3') = \frac{1}{2}(M_2 a_3' + M_2' a_3). \tag{4.3.7}$$

For both LHV and $2/1/S$, without loss of generality we can choose $a_3 = a_3' = 1$, leaving

$$S_3^{\cdots} = \frac{1}{2}\max(M_2 + M_2'). \tag{4.3.8}$$

Now $M_2 + M_2' = a_1 a_2' + a_1' a_2$, which can take a maximum value of 2 for both LHV and $2/1/S$. Therefore

$$S_3^{LHV} = S_3^{2/1/S} = 1, \tag{4.3.9}$$

and also $S_3^{2/1/QM} = 1$, since this is a special case of $2/1/S$ and is more general than LHV. The algebraic limit $S_3^{alg} = 2$, so we are only left with $S_3^{3/QM}$ to find. We can define an operator $\mathcal{S}_3$ by replacing the terms a in the polynomial S_3 with Pauli spin matrices. Now,

$$\mathrm{Tr}(\rho\mathcal{S}_3) = \frac{1}{2}[\mathrm{Tr}(\rho\mathcal{M}_2\sigma_{a_3'}) + \mathrm{Tr}(\rho\mathcal{M}_2'\sigma_{a_3})] \leq \sqrt{2} \tag{4.3.10}$$

since by Cirel'son [17] theorem each term of the sum is bounded by $\sqrt{2}$. As shown in the previous chapter [4], this value is obtained by the GHZ state for a suitable choice of analyzer settings. Therefore $S_3^{3/QM} = \sqrt{2}$, and since this is greater than $S_3^{2/1/S}$ we can say that the GHZ state exhibits genuine three party non-locality. We

	LHV	*2/1QM*	*2/1S*	*3QM*	*3S* (alg.)
M_3	1	$\sqrt{2}$	2	2	2
S_3	1	1	1	$\sqrt{2}$	2

Table 4.1: Maximal values of M_3 and S_3 under different assumptions for the nature of the correlations

can note that $S_3^{2/1/QM} \leq 1$ is one of Svetlichny's original inequalities. The other one (which is actually equivalent under local re-labelling) is associated with $\frac{1}{2}(M_3 - M_3')$.

The results for both the Mermin-Klyshko inequality and Svetlichny's inequality are summarized in table (4.1). We conclude that comparing MK and Svetlichny inequalities allows us to discriminate between the different type of models for correlations in three party states.

4.4 Four particles.

As before we start by considering the properties of the MK polynomial M_4. The following properties of M_4 are already known [21, 25, 26];

$$M_4^{LHV} = 1 \tag{4.4.1}$$

$$M_4^{2/1/1/QM} = M_4^{2/2/QM} = \sqrt{2} \tag{4.4.2}$$

$$M_4^{3/1/QM} = 2 \tag{4.4.3}$$

$$M_4^{4/QM} = 2\sqrt{2} \tag{4.4.4}$$

$$M_4^{alg} = 4. \tag{4.4.5}$$

So we now need the bounds for $2/1/1/S$, $2/2/S$ and $3/1/S$. The last of these may be calculated in the same way as previously.

$$M_4 = \frac{1}{2}[M_3(a_4 + a_4') + M_3'(a_4 - a_4')]. \tag{4.4.6}$$

Setting $a_4 = a'_4 = 1$, $M_4 = \mathrm{Max}\, M_3$. Since we allow any correlations amongst three parties M_3 can take its algebraic limit, giving

$$M_4^{3/1/S} = 2. \tag{4.4.7}$$

For the calculation of $2/1/1/S$ and $2/2/S$: Using (4.2.4), we have

$$M_4 = \frac{1}{2}\, M_{1,2}\, (M_{3,4} + M'_{3,4}) \,+\, \frac{1}{2}\, M'_{1,2}\, (M_{3,4} - M'_{3,4}), \tag{4.4.8}$$

where to avoid confusions we wrote $M_{i,j}$ instead of M_2, with i and j the labels of the particles. Now,

$$M_{3,4} + M'_{3,4} \;=\; a_3 a'_4 + a'_3 a_4 \tag{4.4.9}$$

$$M_{3,4} - M'_{3,4} \;=\; a_3 a_4 - a'_3 a'_4. \tag{4.4.10}$$

For both correlation models we can allow particles three and four to share any correlations, so both $M_{3,4}+M'_{3,4}$ and $M_{3,4}-M'_{3,4}$ can reach there algebraic limits of 2. Therefore under both $2/1/1/S$ and $2/2/S$, $M_4^{\cdots} = \mathrm{Max}\, (M_{1,2} + M'_{1,2}) = \mathrm{Max}\, (a_1 a'_2 + a'_1 a_2)$. In both cases this is 2, so

$$M_4^{2/1/1/S} = M_4^{2/2/S} = M_4^{3/1/S} = 2. \tag{4.4.11}$$

However $M_4^{4/QM} = 2\sqrt{2}$, so for four particles the MK polynomial detects both four particle entanglement and genuine four party non-locality. It is therefore the natural generalization of Svetlichny's inequality.

4.5 Arbitrary numbers of particles.

For n particles we will show that n/QM is stronger that $k/(n-k)/S$, $1 \leq k \leq n-1$, for any bi-partite partition of the set of particles. Partitions of bigger numbers of

smaller subsets are special cases of these bi-partite partitions. We do this by finding a generalized Svetlichny inequality.

Proposition; generalized Svetlichny polynomial.

Define the generalized Svetlichny polynomial S_n as

$$S_n = \begin{cases} M_n & : \ n \text{ even} \\ \frac{1}{2}(M_n + M'_n) & : \ n \text{ odd} \end{cases} \tag{4.5.1}$$

We will show that the correlations $k/(n-k)/S$ all give the same bound S_n^k, and that the bound reached by quantum mechanics is larger by a factor of $\sqrt{2}$ in each case. i.e

$$S_n^{n/QM} = \sqrt{2} S_n^k. \tag{4.5.2}$$

To do this we will use the following properties of the MK polynomials:

(I) The algebraic limit of the MK polynomials is given by

$$M_k^{alg} = \begin{cases} 2^{\frac{k}{2}} = M_k^{k/QM} & : \ k \text{ even} \\ 2^{\frac{k-1}{2}} = M_k^{k/QM} & : \ k \text{ odd} \end{cases} . \tag{4.5.3}$$

(II) For k even, M_k and M'_k each contain all of the correlation coefficients, in different combinations. $M_k + M'_k$ and $M_k - M'_k$ each contain half of the correlation coefficients. The algebraic limit for both is M_k^{alg}

(III) For k odd, M_k and M'_k each contain one half of the correlation coefficients.

These properties can be found in [26]. We will first prove the proposition for n even. In this case the bound for quantum mechanics is known to be $S_n^{n/QM} = 2^{\frac{n-1}{2}}$. There are two cases that can be distinguished; $n-k$ is even, or $n-k$ is odd. We recall that

$$M_n \ = \ \frac{1}{2} M_{n-k} (M_k + M'_k) \ + \ \frac{1}{2} M'_{n-k} (M_k - M'_k) . \tag{4.5.4}$$

- For k and $n-k$ even: In (4.5.4), both $M_k+M'_k$ and $M_k-M'_k$ can be maximized independently because of property (II) above. Therefore, we can replace them by M_k^{alg}. We are left with

$$S_n^k = \frac{1}{2} M_k^{alg} \max(M_{n-k} + M'_{n-k}), \tag{4.5.5}$$

and this maximum is again M_{n-k}^{alg}. So finally

$$S_n^k = \frac{1}{2} M_k^{alg} M_{n-k}^{alg} = 2^{\frac{n-2}{2}}. \tag{4.5.6}$$

- For k and $n-k$ odd: In (4.5.4), M_{n-k} and M'_{n-k} can be optimized independently because of (III) above. We have then $S_n^k = M_{n-k}^{alg} \max M_k = M_{n-k}^{alg} M_k^{alg} = 2^{\frac{n-2}{2}}$.

Thus we have proved the proposition for n even. To prove the proposition for n odd we must calculate both S_n^k and S_n^{nQM}. We begin with S_n^k. Inserting (4.5.4) in the definition of S_n for n odd, we find

$$S_n \;=\; \frac{1}{2}\, M_{n-k}\, M'_k \,+\, \frac{1}{2}\, M'_{n-k}\, M_k\,. \tag{4.5.7}$$

Suppose k odd and $n-k$ even. If we assume correlations $k/(n-k)/S$, M_k and M'_k can both reach the algebraic limit due to property (III). In which case $S_n^k = \frac{1}{2} M_k^{alg} \max(M_{n-k} + M'_{n-k})$ and due to property (II) this maximum is M_{n-k}^{alg}. Thus $S_n^k = 2^{\frac{n-3}{2}}$.

Suppose k even and $n-k$ odd. If we assume correlations $k/(n-k)/S$, M_{n-k} and M'_{n-k} can both reach the algebraic limit due to property (III). In which case $S_n^k = \frac{1}{2} M_{n-k}^{alg} \max(M_k + M'_k)$ and due to property (II) this maximum is M_k^{alg}. Thus $S_n^k = 2^{\frac{n-3}{2}}$.

We now calculate S_n^{nQM}. From the polynomial S_n given by (4.5.7), we define the operator $\mathcal{S}_n$ in the usual way, replacing the a's in the polynomial with Pauli spin matrices. Therefore for the particular case $k=1$ we have

$$\mathrm{Tr}(\rho\mathcal{S}_n) \;=\; \frac{1}{2}\big[\mathrm{Tr}(\rho\,\mathcal{M}_{n-1}\sigma_{a'_n}) + \mathrm{Tr}(\rho\,\mathcal{M}'_{n-1}\sigma_{a_n})\big] \tag{4.5.8}$$

which is bounded by $2^{\frac{n-2}{2}}$ because each of terms in the sum is bounded by that quantity. This bound is reached by generalized GHZ states for the following settings: To maximize $\frac{1}{2}\langle\mathcal{M}_n + \mathcal{M}'_n\rangle_{GHZ}$ for n odd, the σ_{a_j} are taken of the form $\cos\alpha_j\sigma_x + \sin\alpha_j\sigma_y$. One possible choice for the settings is: $\alpha_k = \alpha'_k + \frac{\pi}{2}$ for all k, $\alpha'_1 = ... = \alpha'_{n-1} = 0$, $\alpha'_n = \frac{\pi}{4}$. For such settings, each correlation coefficient becomes equal to $\frac{1}{\sqrt{2}}$ in modulus, with the good sign. Therefore $S_n^{nQM} = 2^{\frac{n-2}{2}}$ for n odd, and we have proved the Proposition also for n odd.

4.6 Experiments.

The four particle GHZ state has recently been produced experimentally with polarization entangled photons in [77], and ions in [78]. Recently Zhao *et al* [79] have shown a violation of the generalized Svetlichny inequality for a four photon GHZ state by 76 standard deviations. This confirms four particle non-locality (and four particle entanglement). Even more recently the same group have produced a five photon GHZ state [80], although they have not yet shown any Bell inequality violation for this state.

The situation is therefore that three particle non-locality remains to be demonstrated (as discussed in the previous chapter), but four particle non-locality has been shown convincingly.

4.7 Conclusion.

We have shown that it is possible to distinguish n party quantum entanglement not just against local hidden variables, but also hybrid local non-local variable models

$k/(n-k)/S$ which allow any correlations within each non-local subset but no correlation between different subsets. This is achieved by a generalized version of the Svetlichny inequality.

Recent experiments on four particles have demonstrated a violation of the MK inequality, playing the role of the generalized Svetlichny inequality, and can be taken as confirmation of four particle non-locality.

M. Seevinck and G. Svetlichny have independently produced inequalities similar to those presented in this chapter [81].

4.8 Appendix A.

We want to show

$$M_n = \frac{1}{2}\, M_{n-k}\,(M_k + M'_k) \;+\; \frac{1}{2}\, M'_{n-k}\,(M_k - M'_k)\,.\;\; 1 \le k \le n-1. \tag{4.8.1}$$

Let us prove this by induction on k [21]. $M_1 = a_1$, so this formula is correct for $k = 1$. Assuming it is true for k, and substituting for M_{n-k} and M'_{n-k},

$$\begin{aligned} M_n = \frac{1}{2}\left(\frac{a_{k+1} + a'_{k+1}}{2}\; M_{n-(k+1)} + \frac{a'_{k+1} - a_{k+1}}{2}\; M'_{n-(k+1)}\right)(M_k + M'_k) \\ +\frac{1}{2}\left(\frac{a'_{k+1} + a_{k+1}}{2}\; M'_{n-(k+1)} + \frac{a'_{k+1} - a_{k+1}}{2}\; M_{n-(k+1)}\right)(M_k - M'_k) \end{aligned} \tag{4.8.2}$$

$$= \frac{M_k\, a'_{k+1} + M'_k\, a_{k+1}}{2}\, M_{n-(k+1)} + \frac{M_k\, a_{k+1} - M'_k\, a'_{k+1}}{2}\, M'_{n-(k+1)} \tag{4.8.3}$$

$$= M_{n-(k+1)}\, \frac{M_{k+1} + M'_{k+1}}{2} + M'_{n-(k+1)}\, \frac{M_{k+1} - M'_{k+1}}{2}. \tag{4.8.4}$$

Hence if (4.8.1) is true for k, it holds for $k + 1$.

Chapter 5

Non-local correlations as an information theoretic resource.

Abstract

It is well known that measurements performed on spatially separated entangled quantum systems can give rise to correlations that are non-local, in the sense that a Bell inequality is violated. They cannot, however, be used for super-luminal signalling. It is also known that it is possible to write down sets of "super-quantum" correlations that are more non-local than is allowed by quantum mechanics, yet are still non-signalling. Viewed as an information theoretic resource, super-quantum correlations are very powerful at reducing the amount of communication needed for distributed computational tasks. An intriguing question is why quantum mechanics does not allow these more powerful correlations. We aim to shed light on the range of quantum possibilities by placing them within a wider context. With this in mind, we investigate the set of correlations that are constrained only by the no-signalling principle. These correlations form a polytope, which contains the quantum correlations as a (proper) subset. We determine the vertices of the no-signalling polytope in the case that two observers each choose from two possible measurements with d outcomes. We then consider how inter-conversions between different sorts of

correlations may be achieved. Finally, we consider some multipartite examples.

5.1 Introduction.

In a typical Bell-type experiment, two entangled particles are produced at a source and move apart to separated observers. Each observer chooses one from a set of possible measurements to perform and obtains some outcome. The joint outcome probabilities are determined by the measurements and the quantum state. One of the more striking features of quantum mechanics is that joint outcome probabilities can violate a Bell-type inequality [3], indicating that quantum mechanics is not, in Bell's terminology, locally causal. This prediction has been confirmed in numerous laboratory experiments [82].

We can abstract away from this scenario and consider two observers who share a black box. Each observer selects an input from a range of possibilities and obtains an output. The box determines a joint probability for each output pair given each input pair. It is clear that a quantum state provides a particular example of such a box, with input corresponding to measurement choice and output to measurement outcome. More generally, boxes can be divided into different types. Some will allow the observers to signal to one another via their choice of input, and correspond to two-way classical channels, as introduced by Shannon [83]. Others will not allow signalling - it is well known, for example, that any box corresponding to an entangled quantum state will not. This is necessary for compatibility between quantum mechanics and special relativity. Of the non-signalling boxes, some will violate a Bell-type inequality. The significance of this can be spelt out in information theoretic terms: separated observers without the box, who have access to pre-shared classical random data but no other resources, and in particular who cannot communicate, will not be able to simulate the box. We refer to any such box (and to the corresponding correlations) as non-local.

In general, these boxes can be viewed as an information theoretic resource. This is obvious in the case of signalling boxes, or classical channels. However, it is also known that non-local correlations arising from an entangled quantum state, even

though they cannot be used directly for signalling, can be useful in reducing the amount of signalling that is needed in communication complexity scenarios below what could be achieved with only shared random data [84]. A local black box is simply equivalent to some shared random data, which in turn (depending on the precise nature of the problem) is better than nothing [85].

An interesting question to ask now is; can any set of non-signalling correlations be produced by measurements on some quantum state? The answer in fact, is no. This was shown by Popescu and Rohrlich [86], who wrote down a set of correlations that return a value of 4 for the Clauser-Horne-Shimony-Holt (CHSH) expression [16], the maximum value logically possible, yet are non-signalling. The maximum quantum value is given by Cirel'son's theorem as $2\sqrt{2}$ [17]. These should be compared with the maximum value obtainable by non-communicating classical observers, which is 2. Popescu and Rohrlich concluded that quantum mechanics is only one of a class of non-local theories consistent with causality. In terms of our boxes, there are some boxes that are non-signalling but are more non-local than is allowed by quantum mechanics. It is interesting to note that from an information theoretic point of view, some of these latter are very powerful. For example, van Dam has shown [87] that two observers who did have access to a supply of Popescu-Rohrlich type boxes would be able to solve essentially any two-party communication complexity problem with only a constant number of bits of communication. This should be contrasted with the quantum case, for which it is known that certain communication complexity problems require at least n bits of communication even if unlimited shared entanglement is available [88].

In this chapter we investigate the set of non-signalling boxes, considering them as an information theoretic resource. Clearly this set includes those corresponding to measurements on quantum states as a subset. The motivation for studying the wider set is partly that it is interesting for its own sake. This is true even though we have no reason to think that correlations other than quantum correlations can be obtained in nature. It is already clear that the set of non-signalling boxes has interesting

structure, and one finds analogies with other information theoretic resources, in particular with the set of entangled quantum states. Another motivation is that a better understanding of the set of quantum correlations can be gained by placing it in the context of a wider set. Only in this way, for example, can one hope to answer Popescu and Rohrlich's original question, of why quantum correlations are not more non-local than they are. More generally, a proper understanding of the information theoretic capabilities of quantum mechanics includes an understanding of what cannot be achieved as well as what can.

This chapter is organized as follows. In Sec. 5.2.1, we introduce the convex polytope that describes the set of non-signalling correlations. In Sec. 5.2.2, we examine more closely the particular case of correlations involving two possible inputs, obtaining all the vertices of the corresponding polytope. We then consider, in Sec. 5.2.3, how inter-conversions between these extreme points may be achieved using local operations. Sec. 5.3 is devoted to three-party correlations and in Sec. 5.3.4, we examine how extremal correlations correlate to the environment. We conclude with some open questions in Sec. 5.4.

This work was done in collaboration with J. Barrett, S. Massar, and S. Pironio from Université Libre de Bruxelles, and N. Linden and S. Popescu from the University of Bristol. It appears as a paper [6].

5.2 Two party correlations

5.2.1 Definitions

A bipartite correlation box (hereafter, just 'box') is defined by a set of possible inputs for each of Alice and Bob, a set of possible outputs for each, and a joint probability for each output pair given each input pair. We denote Alice's and Bob's inputs x and y respectively, and their outputs a and b. The joint probability of getting a pair of outputs given a pair of inputs is $p_{ab|xy}$. This situation is shown in

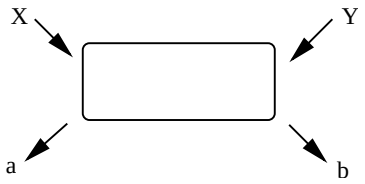

Figure 5.1: A schematic representation of a bipartite correlation box. Alice inputs X and gets a as output. Bob inputs Y and gets b as an output.

Fig 5.1.

A concrete example of a correlation box is an experiment with two spin-half particles, with the inputs x and y labelling Alice's and Bob's analyzer settings and the outputs a and b labelling the experimental outcomes. In a quantum experiment like this one, it is generally the case that the outcome of the measurement is obtained as soon as the measurement is performed. In addition, the entanglement is destroyed after the measurements, so that if the experiment is to be repeated a new entangled state is needed. We define boxes to have the same properties. Alice can select her input at any time and obtains her output immediately, and similarly Bob. There may of course be a time delay between Alice selecting her input and Bob selecting his input, but this makes no difference to the correlations for the case of non-signalling boxes. Further, after a box is used once it is destroyed, and to repeat the experiment a new box is needed.

The no-signalling polytope.

Since $p_{ab|xy}$ are probabilities they satisfy positivity,

$$p_{ab|xy} \geq 0 \qquad \forall\ a, b, x, y \tag{5.2.1}$$

and normalization,

$$\sum_{a,b} p_{ab|xy} = 1 \qquad \forall\ x, y. \tag{5.2.2}$$

Furthermore, in this work we only consider non-signalling boxes, i.e, we require that Alice cannot signal to Bob by her choice of x, and vice versa. This means that the marginal probabilities $p_{a|x}$ and $p_{b|y}$ are independent of y and x respectively:

$$\sum_b p_{ab|x,y} = \sum_b p_{ab|x,y'} \equiv p_{a|x} \qquad \forall\ a, x, y, y' \tag{5.2.3}$$

$$\sum_a p_{ab|x,y} = \sum_a p_{ab|x',y} \equiv p_{b|y} \qquad \forall\ b, y, x, x'. \tag{5.2.4}$$

We shall always consider that the number of possible inputs and outputs is finite. Since the above constraints are all linear, the set of boxes with a given number of inputs and outputs is a polytope, which we denote by $\mathcal{P}$. It is easy to see that the set is convex - if two boxes each satisfy the constraints, then a probabilistic mixture of them will do too.

The local polytope.

In general, the set of non-signalling boxes can be divided into two types, local and non-local. A box is local if and only if it can be simulated by non-communicating observers with only shared randomness as a resource. This means that we can write

$$p_{ab|xy} = \sum_\lambda p_\lambda\, p_{a|x}(\lambda)\, p_{b|y}(\lambda), \tag{5.2.5}$$

where λ is the value of the shared random data and p_λ is the probability that a particular value of λ occurs. We have that $p_{a|x}(\lambda)$ is the probability that Alice outputs a given that the shared random data was λ and the input was chosen to be x, and similarly for $p_{b|y}(\lambda)$.

We recall what is known about the set of local boxes (see for instance [89, 90]). This set is itself a convex polytope, with vertices corresponding to local deterministic boxes (all $p_{a|x}, p_{b|y}$ are 0 or 1). The positivity conditions of Eq. (5.2.1) are trivial facets of this polytope, while non-trivial facets correspond to Bell-type inequalities.

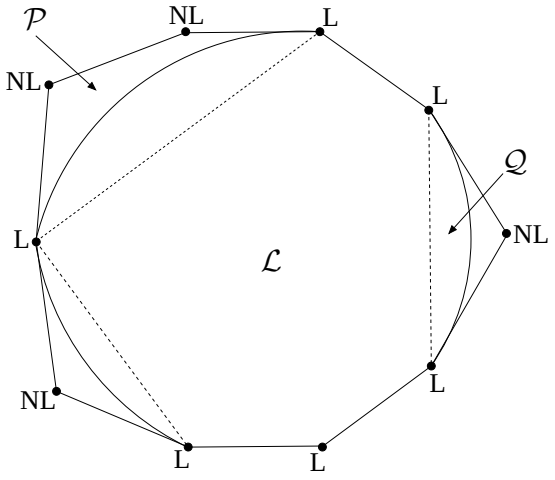

Figure 5.2: A schematic representation of the space of non-signalling correlation boxes. The vertices are labelled L and NL for local and non-local. Bell inequalities are the facets represented in dashed lines. The set bounded by these is $\mathcal{L}$. The region accessible to quantum mechanics is $\mathcal{Q}$. A general non-signalling box $\in \mathcal{P}$.

Violation of the latter implies that a point lies outside the local polytope, and that the corresponding box is therefore non-local. We denote the local polytope by $\mathcal{L}$.

Quantum mechanical correlations.

Finally, there is a third set of interest, the correlations obtainable by measurements on bipartite quantum states. We denote this set $\mathcal{Q}$ (where $\mathcal{Q}$ is defined for a fixed number of measurement settings and outcomes). The set $\mathcal{Q}$ is investigated in Refs. [17, 90, 91, 92, 93]. It is convex but is not a polytope as the number of extremal points is not finite. Since the correlations allowed by quantum mechanics can violate Bell inequalities, $\mathcal{Q}$ is non-local. However, as they violate the CHSH inequality only up to Cirel'son's bound $B = 2\sqrt{2}$ [91, 86], they form a proper subset of the no-signalling polytope. Overall, we have that $\mathcal{L} \subset \mathcal{Q} \subset \mathcal{P}$. This situation is summarized in Fig. 5.2.

5.2.2 The two-inputs no-signalling polytope

Two outputs

Having defined the objects that we are interested in, we begin by considering in detail the simple case in which Alice and Bob are each choosing from two inputs, each of which has two possible outputs. We write $x, y, a, b \in \{0, 1\}$. The probabilities $p_{ab|xy}$ thus form a table with 2^4 entries, although these are not all independent due to the constraints of Sec. 5.2.1. The dimension of the polytope is found by subtracting the number of independent constraints from 2^4, and turns out to be 8. To understand the polytope $\mathcal{P}$, we wish to find its vertices. These will be boxes that satisfy all of the constraints and saturates a sufficient number of the positivity constraints to be uniquely determined. In the next subsection, we present an argument that allows us to find all the vertices of the two-input d-output polytope. Here we simply state the results for the simple two-input two-output case.

We find that there are 24 vertices, which may be divided into two classes, those corresponding to local boxes and those corresponding to non-local boxes. Local vertices are simply the local deterministic boxes, which assign a definite value to each of Alice's and Bob's inputs. There are thus 16 local vertices, which can be expressed as

$$p_{ab|xy} = \begin{cases} 1 & : \quad a = \alpha x \oplus \beta, \\ & \quad\ b = \gamma y \oplus \delta \\ 0 & : \quad \text{otherwise}, \end{cases} \tag{5.2.6}$$

where α, β, $\gamma, \delta \in \{0, 1\}$. Here and throughout, $\oplus$ denotes addition modulo 2. The 8 non-local vertices may be expressed compactly as

$$p_{ab|xy} = \begin{cases} 1/2 & : \quad a \oplus b = x.y \oplus \alpha x \oplus \beta y \oplus \gamma \\ 0 & : \quad \text{otherwise}, \end{cases} \tag{5.2.7}$$

where α, β, $\gamma \in \{0, 1\}$. We will refer to these boxes as Popescu-Rohrlich (PR) boxes.

By using reversible local operations Alice and Bob can convert any vertex in one class into any other vertex within the same class. There are two types of reversible local operations. Alice may relabel her inputs, $x \rightarrow x \oplus 1$, and she may relabel her outputs (conditionally on the input), $a \rightarrow a \oplus \alpha x \oplus \beta$. Bob can perform similar operations. Thus up to local reversible transformations, each local vertex is equivalent to the vertex setting $\alpha = 0$, $\beta = 0$, $\gamma = 0$, $\delta = 0$, i.e,

$$p_{ab|XY} = \begin{cases} 1 & : \quad a = 0 \text{ and } b = 0 \\ 0 & : \quad \text{otherwise.} \end{cases} \tag{5.2.8}$$

Each non-local vertex is equivalent to

$$p_{ab|XY} = \begin{cases} 1/2 & : \quad a \oplus b = x.y \\ 0 & : \quad \text{otherwise.} \end{cases} \tag{5.2.9}$$

We note that if we allow irreversible transformations on the outputs we may convert any non-local vertex into a local vertex.

For the case of two inputs and two outputs, it is well known that the only non-trivial facets of the local polytope $\mathcal{L}$ correspond to the CHSH inequalities [20]. There is an important connection between the CHSH inequalities and the non-local vertices of $\mathcal{P}$. In order to explain this, we first recall explicitly the CHSH inequalities. Let the expectation $\langle i\, j \rangle$ be defined by

$$\langle ij \rangle = \sum_{a,b=0}^{1} (-1)^{a+b}\, p_{ab|X=i,Y=j}. \tag{5.2.10}$$

Then the non-trivial facets of $\mathcal{L}$ are equivalent to the following inequalities.

$$\begin{aligned} B_{\alpha\beta\gamma} \quad \equiv \quad & (-1)^{\gamma} \langle 00 \rangle + (-1)^{\beta+\gamma} \langle 01 \rangle \\ & + (-1)^{\alpha+\gamma} \langle 10 \rangle + (-1)^{\alpha+\beta+\gamma+1} \langle 11 \rangle \leq 2, \end{aligned} \tag{5.2.11}$$

where α, β, $\gamma \in \{0, 1\}$. For each of the 8 Bell expressions $B_{\alpha\beta\gamma}$, the algebraic maximum is $B_{\alpha\beta\gamma} = 4$. We find that for each choice of α, β, γ the correlations

defined by Eq. (5.2.7) return a value for the corresponding Bell expression of $B_{\alpha\beta\gamma} = 4$. Thus there is a one-to-one correspondence between the non-local vertices of $\mathcal{P}$ and the non-trivial facets of $\mathcal{L}$, with each vertex violating the corresponding CHSH inequality up to the algebraic maximum. These extremal correlations describe in a compact way the logical contradiction in the CHSH inequalities.

d outputs.

We now generalize the results of the preceding section. Again we have two parties, Alice and Bob, who choose from two inputs x and $y \in \{0, 1\}$ and receive outputs a and b with a joint probability $p_{ab|xy}$. We denote the number of distinct outputs associated with inputs x and y by d_x^A and d_y^B. If Alice's input is x, for example, then $a \in \{0, \ldots, d_x^A - 1\}$.

Theorem 1 *The non-local vertices of $\mathcal{P}$ for two input settings and d_x^A and d_y^B outputs are equivalent under reversible local relabelling to*

$$p_{ab|xy} = \begin{cases} 1/k & : \quad (b-a) \bmod k = x.y \\ & \quad a, b \in \{0, \ldots, k-1\} \\ 0 & : \quad \text{otherwise,} \end{cases} \tag{5.2.12}$$

for each $k \in \{2, \ldots, \min_{x,y}(d_x^A, d_y^B)\}$.

The proof of this theorem can be found in Appendix B, at the end of this chapter. We note that the case $d_x^A = d_y^B = 2$ gives the PR correlations we found previously. If $d_x^A = d_y^B = k = d$ then the vertex violates the d-dimensional generalization of the CHSH inequality [22] up to its algebraic maximum. We call such a box a d-box (a more complete name would specify that the number of parties and the number of inputs per party are each two).

Resource	Instantiation	Quantitative measure
Shared random data	Random variables	Mutual information
Shared secret data	Random variables	Secrecy rate
Entanglement	Quantum states	Entanglement cost
Non-locality	Boxes	Classical simulation cost, Bell inequality violation

Table 5.1: Comparison of information theoretic resources.

5.2.3 Resource conversions.

In the preceding section we found all the vertices of the no-signalling polytope for bi-partite, two-input boxes. As described in the introduction, the ethos adopted in this work is that boxes, and in particular non-local boxes, can be regarded as an information theoretic resource, and investigated as such. Useful comparisons can be drawn with other information theoretic resources, including shared random data [94], shared secret data [95, 96], and entanglement [97]. In each case, there is a convex set of possible states and a notion of inter-conversion between different states. There is also a notion of inter-conversion between different resources. Each resource is useful for some task(s) and can be quantified via some measure(s). Some of this is illustrated in Table 5.1.

Note that the quantitative measures given are not the only possibilities. Note also that even if the measure given vanishes, a useful resource may still be present. Thus uncorrelated random variables can still be useful (as local randomness), as can local boxes (as local or shared randomness).

In light of this it is natural to ask what inter-conversions between boxes are possible, and what would be a good measure of the non-locality of a box? To the second question, several answers suggest themselves, such as the amount of classical communication needed to simulate the box (given that the only other resource is shared random data), and the degree of violation of Bell inequalities [98]. In this work, however, we concentrate on the first question - an understanding of possible

inter-conversions is a prerequisite for a good understanding of quantitative measures.

The problem that we consider is whether one can simulate one type of box, using one or more copies of another type as a resource. Local operations such as relabelling are allowed. As non-locality is the resource that we have in mind, it is also natural to allow the parties free access to local boxes (i.e., to local and shared randomness). We note, however, that neither local nor shared randomness can help if the box to be simulated is a vertex[1], thus none of the protocols we describe below make use of this. We make the assumption that communication between the parties is not allowed.

In general, outputs for one box can be used as inputs for another box. This allows non-trivial protocols to be constructed. As an interesting logical possibility, we note that the temporal order in which each party uses the boxes need not be the same, and that this allows loops to be constructed that would be ill-defined if it were not for the no-signalling condition. (Thus if signalling boxes were to be considered, our stipulation that outputs are obtained immediately after inputs would have to be altered.) Such a loop is illustrated in Fig. 5.3. In all the protocols presented below, the parties use the boxes in the same temporal order. But protocols of the type illustrated in Fig. 5.3 are an interesting logical possibility.

In the following, we will describe three simple examples. We show that given a d-box and a d'-box, we can simulate a dd'-box. We will also show that given a dd'-box, we can simulate one d-box. Finally, an unlimited supply of d-boxes can simulate a d'-box to arbitrarily high precision. In addition, we will describe a negative result: it is not in general possible to go *reversibly* from n d-boxes to m d'-boxes, where $d \neq d'$. It follows from this that d and d'-boxes are ultimately inequivalent resources

[1]For each value of the local or shared randomness, one can write down the box that is simulated, conditioned on that value occurring. The box simulated by the overall protocol is then the average of these conditional boxes, with the average taken over the possible values of the randomness. But if this box is a vertex, then each of the conditional boxes must be the same vertex, and the protocol could have been carried out without the randomness.

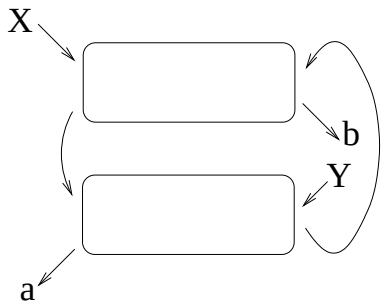

Figure 5.3: An example of how two parties that are given two boxes may process locally their inputs and outputs. They result in simulating another type of box with inputs x,y and outcomes a, b. Note that due to the no-signalling condition, the parties can use their two boxes with a different time ordering.

and that in our context, it is inappropriate to suppose that they can be characterized by a single numerical measure of non-locality[2].

Suppose first, then, that Alice and Bob have one d-box and one d'-box and they wish to simulate one dd'-box. Simulate means that for each value of $x \in \{0, 1\}$, a procedure should be defined for Alice, using the d and d'-boxes, that eventully enables her to determine the value of an output $a \in \{0, \ldots, dd' - 1\}$. Similarly for Bob for each value of y and an output b. The joint probabilities for a and b should satisfy Eq. (5.5.1) (with dd' inserted instead of d where necessary).

[2]Similar considerations apply to the other resources we have mentioned. In the case of entanglement, for example, reversible inter-conversions are not in general possible for mixed states, thus there is no unique measure of entanglement for mixed states. In the case of shared random data, inter-conversions by local operations are rather limited and provide no very meaningful measure of shared randomness. However, if one expands the set of operations that Alice and Bob are allowed, then the picture changes. Thus in the case of shared random data, allowing that Alice and Bob can communicate classically, while demanding that the communication must be subtracted at the end, gives an operational meaning to the mutual information [94]. Inspired by this, it may be interesting to consider conversions between boxes, with classical communication allowed but subtracted at the end, or indeed conversions between entangled quantum states with quantum communication allowed but subtracted at the end. We do not pursue these questions here.

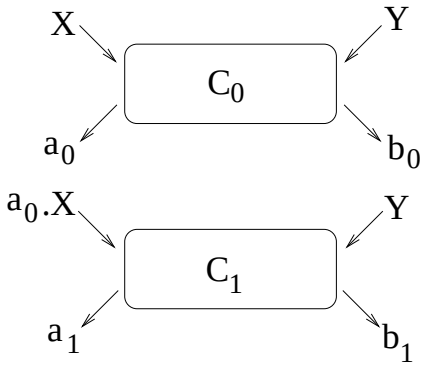

Figure 5.4: Making a 4-box from 2 PR boxes. Alice inputs x into the first box and $a_0.x$ into the second, while Bob inputs y into both boxes. Alice's output a is given in binary by $a_0\, a_1$ and similarly for Bob's output b.

Protocol 1: 1 d-box and 1 d'-box $\rightarrow$ 1 dd'-box

Alice. Alice inputs x into the d-box, obtaining outcome α. She then inputs x into the d'-box if $\alpha = d-1$, and inputs 0 into the d'-box otherwise, obtaining an output α'. Alice's output for the protocol is $a = \alpha' d + \alpha$.

Bob. Bob inputs y into the d-box, obtaining output β, and inputs y into the d'-box, obtaining output β'. His output for the protocol is then $b = \beta' d + \beta$.

Protocol 1 is illustrated in Fig. 5.4 for the case $d = d' = 2$.

We indicate briefly why this protocol works. Recall that a dd'-box satisfies $(b-a) \mod dd' = xy$. Write $a = \alpha' d + \alpha$ and $b = \beta' d + \beta$, where α can take values $\alpha = 0, \ldots, d-1$, and α' can take values $\alpha' = 0, \ldots, d'-1$, and so on. We see that the condition satisfied by a dd'-box is equivalent to

$$\begin{aligned} \beta - \alpha \mod d &= xy \\ \beta' - \alpha' \mod d' &= \begin{cases} xy & : \quad \alpha = d-1 \\ 0 & : \quad \text{otherwise.} \end{cases} \end{aligned} \tag{5.2.13}$$

Protocol 1 is designed precisely to satisfy this condition. We note next that it is

easy to convert one dd'-box into one d-box.

Protocol 2: 1 dd'-box $\rightarrow$ 1 d-box

Alice. Alice inputs x into the dd'-box, obtaining an output α. Her output for the protocol is then $a = \alpha \mod d$.

Bob. Bob inputs y into the dd'-box, obtaining an output β. His output for the protocol is $b = \beta \mod d$.

That Protocol 2 works can be seen from Eq. (5.2.13). Now we show how n d-boxes can be used to simulate a d'-box to arbitrarily high precision. This is done using a combination of Protocols 1 and 2.

Protocol 3: n d-boxes $\rightsquigarrow$ 1 d'-box

Alice and Bob begin by using the n d-boxes to simulate a d^n-box, as per Protocol 1. Call the outputs for the d^n-box α and β. They satisfy $(\beta - \alpha) \mod d^n = xy$. Alice and Bob now use Protocol 2 to obtain something close to a d'-box: the final outputs are $a = \alpha \mod d'$ and $b = \beta \mod d'$.

If $d^n = kd$, this protocol works exactly. Otherwise, one can calculate the errors resulting in Protocol 3. Denote by k the largest integer such that $kd' \leq d^n$. Now we have that if $x = 0$ or $y = 0$, then $(b - a) \mod d' = 0$ as required. However, the probabilities are skewed by an amount $\propto 1/k \approx d'/d^n$. If $x = y = 1$, then the probabilities are skewed in a similar manner. But in addition we have that if $b = d^n - 1$, then $(b - a) \mod d' = 1$ is not satisfied with probability $1/d^n$. The important thing here is that all errors tend to zero exponentially fast as n becomes large.

We have seen several examples of how inter-conversions between non-local extremal boxes are possible using only local operations. It is also interesting to consider how boxes may be simulated using only classical communication (CC) and

shared random data (SR), i.e., without other boxes. For example, we can see that one d-box may be simulated with one bit of 1-way communication and $\log_2 d$ bits of shared randomness.

Protocol 4: 1 bit CC and $\log_2 d$ bits SR $\rightarrow$ 1 d-box
Alice and Bob share a random variable $\alpha \in \{0, \cdots, d-1\}$, where α takes all its possible values with equal probability $1/d$.
Alice. Alice sends her input x to Bob and outputs $a = \alpha$.
Bob. Bob, knowing x and α, outputs $b = (\alpha + x.y) \mod d$.

This protocol is optimal regarding the amount of 1-way communication exchanged. This is a consequence of the following lemma, which places a lower bound on the amount of communication needed to simulate boxes. The lemma is used in the proof of Theorem 2, our final main result for this section.

Lemma 1 *The simulation of n $d-$boxes using 1-way communication requires at least n bits of communication if shared randomness is available, and $n + n\log_2 d$ bits without shared randomness.*

Proof. Note that this bound can be achieved using Protocol 4 for each of the n boxes, replacing if necessary $n\log_2 d$ bits of shared randomness by $n\log_2 d$ bits of communication from Alice to Bob.

Let us show that this amount of communication is necessary. Suppose first that both parties have access to shared random data and that communication is allowed from Alice to Bob. Bob's output is thus $b = b(Y, C, r)$ where $Y = y_1 \ldots y_n$ are the joint inputs for Bob, C is the communication and r the shared data. Note simply that for Alice, there are 2^n possible joint inputs into n d-boxes. If Alice is sending fewer than n bits, there will be at least one pair of joint inputs for which her communication is the same. Call them X_1 and X_2. A careful examination of the definition of a d-box reveals that there will be at least one joint input of Bob's

into the n boxes such that his output must be different according to whether Alice's input was X_1 or X_2. Thus $< n$ bits of communication are not sufficient.

If Alice and Bob do not have access to shared randomness, then Bob's output is of the form $b = b(Y, C)$. The proof then follows by an argument similar to the one used above, noting that for Alice there are $2^{n+n\log_2 d}$ possible joint input-output pairs (X, A). □

These types of considerations will help us to establish the final result of this section.

Theorem 2 *It is in general impossible, using local reversible operations, exactly to transform n d-boxes into m d'-boxes.*

The theorem follows from the following two lemmas.

Lemma 2 *Using n d-boxes, Alice and Bob can exactly simulate at most n d'-boxes, for $d \geq d'$.*

Lemma 3 *Using n d'-boxes, Alice and Bob can exactly simulate at most $n(1 + \log_2 d')/(1 + \log_2 d) < n$ d-boxes for $d' \leq d$.*

Proof. We prove Lemma 2 as follows. We know that we can simulate n d-boxes with n bits of communication and $n \log d$ bits of shared randomness. Suppose that there were a protocol using only local operations that could convert n d-boxes into N d' boxes, for some $d' \leq d$, where $N > n$. As argued above, it follows from the fact that d-boxes are vertices that this protocol would not need any additional shared randomness. But then, by combining the simulation of the d-boxes with the protocol for their conversion, we would have constructed a protocol for simulating N d'-boxes using only n bits of communication, in contradiction with Lemma 1. The proof of Lemma 3 is very similar. Note that we can simulate n d'-boxes with $n + n\log_2 d'$ bits of classical communication and no shared randomness. Suppose that there were a protocol that converts n d'-boxes into N d-boxes, for some $d \geq d'$,

where $N > n(1+\log_2 d')/(1+\log_2 d)$. Then we would have constructed a protocol for simulating N d-boxes using only $n + n\log_2 d'$ bits of communication and no shared randomness, again in contradiction with Lemma 1. □

5.3 Three party correlations.

5.3.1 Definitions.

In this section, we generalize the considerations of the previous sections to consider tripartite correlations. As before, we consider that correlations are produced by a black box with specified inputs and outputs, but now the box is assumed to be shared between three separated parties, A, B and C.

The no-signalling polytope.

A box is defined by joint probability distributions $p_{abc|XYZ}$, which satisfy positivity,

$$p_{abc|XYZ} \geq 0 \qquad \forall\, a, b, c, X, Y, Z \tag{5.3.1}$$

normalization,

$$\sum_{a,b,c} p_{abc|XYZ} = 1 \qquad \forall\ X, Y, Z \tag{5.3.2}$$

and no-signalling. With three parties it is possible to imagine various types of communication, and correspondingly there are different types of no-signalling conditions. Obviously we require that A cannot signal to B or C (and cyclic permutations). We should also, however, require the stronger condition that if the systems B and C are combined, then A cannot signal to the resulting composite system BC. This is expressed by

$$\sum_a p_{abc|X,Y,Z} = \sum_a p_{abc|X',Y,Z} \quad \forall\, b, c, Y, Z, X, X', \tag{5.3.3}$$

where, again, we include cyclic permutations. Finally, note that if systems A and B are combined, the resulting composite system AB should not be able to signal to C. This type of condition does not require a separate statement, however, as it already follows from Eq. (5.3.3). Indeed, using the fact that A cannot signal to BC and that B cannot signal to AC, we deduce

$$\begin{aligned} \sum_{a,b} p_{abc|X,Y,Z} &= \sum_{a,b} p_{abc|X',Y,Z} \quad \forall\, c,\, X,X',Y,Z \\ &= \sum_{a,b} p_{abc|X',Y',Z} \quad \forall\, c,\, X,X',Y,Y',Z, \end{aligned} \tag{5.3.4}$$

which is the condition that AB cannot signal to C. Hence the only conditions we need to impose on a tripartite box are those of Eqs. (5.3.1), (5.3.2) and (5.3.3). The set of boxes satisfying these conditions is the polytope $\mathcal{P}$.

Locality conditions.

In the tripartite case, as well as different types of no-signalling condition, there are different types of locality condition. First, a box is fully local if the probabilities can be written in the form

$$p_{abc|XYZ} = \sum_{\lambda} p_\lambda\, p_{a|X}(\lambda)\, p_{b|Y}(\lambda)\, p_{c|Z}(\lambda). \tag{5.3.5}$$

The set of such boxes is a convex polytope denoted $\mathcal{L}$. Second, we say that a box is two-way local if either there exists a bi-partition of the parties, say AB versus C, such that the composite system AB is local versus C, or if the box can be written as a convex combination of such boxes, i.e.,

$$p_{abc|XYZ} = p_{12} \int p_{ab|XY}(i)\, p_{c|Z}(i)\, \mathrm{d}i \tag{5.3.6}$$

$$+ \; p_{13} \int p_{ac|XZ}(i)\, p_{b|Y}(i)\, \mathrm{d}i \tag{5.3.7}$$

$$+ \; p_{23} \int p_{bc|YC}(i)\, p_{a|X}(i)\, \mathrm{d}i, \tag{5.3.8}$$

where $p_{12}+p_{23}+p_{13}=1$. The set of such boxes is again a convex polytope, denoted $\mathcal{L}2$. Finally, any box that cannot be written in this form demonstrates genuine three-way non-locality. We have that $\mathcal{L} \subset \mathcal{L}2 \subset \mathcal{P}$ and also that $\mathcal{L} \subset \mathcal{Q} \subset \mathcal{P}$.

In the following, we restrict our attention to the case $a, b, c, {}_{X,Y,Z} \in \{0,1\}$. We find the vertices of the polytope $\mathcal{P}$ and point out some connections with three-party Bell-type inequalities. Finally we consider some examples of interconversions, in particular of how to construct tripartite boxes using PR boxes as a resource.

5.3.2 Two inputs and two outputs.

For the tripartite boxes with two inputs and two outputs per observer, Eq. (5.3.2) expresses 8 normalization constraints, and Eq. (5.3.3) expresses $3 \times 12 = 48$ no-signalling constraints. However, as in the bipartite case, there is also some further redundancy; there turn out to be 38 independent constraints. Therefore the dimension of this polytope is $\dim \mathcal{P} = 2^6 - 38 = 26$.

Finding the vertices of a polytope given its facets is the so called "vertex enumeration problem" for which several algorithms are available, although they are efficient only for low dimensional problems. We determined the extreme points of our three-party polytope with *Porta* [99], *cdd* [100] and *l*rs [101]. It turns out that there are 46 classes of vertices, where vertices within one class are equivalent under local relabelling operations and permutations of the parties. These 46 classes of extreme points can be divided into three categories: local, two-way local and three-way non-local.

Local vertices.

This category contains boxes for which A's, B's and C's outputs are all deterministic. They all belong to the same class under reversible local operations, a representative of which is:

$$p_{abc|XYZ} = \begin{cases} 1 & : \quad a = 0,\, b = 0,\, c = 0 \\ 0 & : \quad \text{otherwise.} \end{cases} \tag{5.3.9}$$

Two-way local vertices.

In view of the preceding discussion for bipartite correlations, there is only one class of extremal two-way local correlations that are not fully local. This is because if a box is a vertex, there can be only one term in the decomposition on the right hand side of Eq. (5.3.6). Then it follows from Theorem 1 that this term must describe a PR box shared between two parties, along with a deterministic outcome for the third party. Thus any box of this type is equivalent to

$$p_{abc|XYZ} = \begin{cases} 1/2 & : \quad a \oplus b = X.Y \text{ and } c = 0 \\ 0 & : \quad \text{otherwise,} \end{cases} \tag{5.3.10}$$

Three-way non-local vertices.

This category contains genuine three-party non-local extremal correlations. It is much more complex than the two above, since it comprises 44 different classes of vertices. Out of these, we mention 3 classes of particular interest. The first class can be expressed as

$$p_{abc|XYZ} = \begin{cases} 1/4 & : \quad a \oplus b \oplus c \\ & \qquad = X.Y \oplus X.Z \\ 0 & : \quad \text{otherwise,} \end{cases} \tag{5.3.11}$$

If we imagine that B and C form a composite system with input $Y \oplus Z$ and output $b \oplus c$, then this is a PR box shared between A and BC. We refer to them as

"X(Y+Z)" boxes.

Correlations in the second class are equivalent to

$$p_{abc|XYZ} = \begin{cases} 1/4 & : \quad a \oplus b \oplus c \\ & \qquad = X.Y.Z \oplus \bar{X}.\bar{Y}.\bar{Z} \\ 0 & : \quad \text{otherwise,} \end{cases} \tag{5.3.12}$$

where we define $\bar{x} = x \oplus 1$, and $\bar{y}, \bar{z}$ similarly. We call them "Svetlichny" correlations (for reasons explained below).

Finally, the third class contains what we call "XYZ" correlations.

$$p_{abc|XYZ} = \begin{cases} 1/4 & : \quad a \oplus b \oplus c = X.Y.Z \\ 0 & : \quad \text{otherwise.} \end{cases} \tag{5.3.13}$$

The XYZ correlations are special because, as W. van Dam pointed out to us [102], they can be used to solve any three party communication complexity problem with only 1 bit broadcast by each party. He also pointed out that they have a natural generalization to n parties: $a_1 \oplus a_2 \oplus \cdots \oplus a_n = x_1.x_2 \ldots x_n$, where $x_i \in \{0, 1\}$ is the input of party i and $a_i \in \{0, 1\}$ the output of party i. These n-party correlations can be used to solve any n party communication complexity problem with 1 bit broadcast by each party. They can be constructed from a supply of PR boxes.

We conclude this section with some remarks on these correlation vertices and known multipartite Bell-type inequalities. First, each of the X(Y+Z), XYZ, and Svetlichny boxes violates the Mermin-Klyshko inequality [24, 25] up to the algebraic maximum. Second, we recall that inequalities can be written down that detect genuine three-way non-locality. One such is the Svetlichny inequality [1]. If we define $\langle ijk \rangle$ by

$$\langle ijk \rangle = \sum_{a,b,c} (-1)^{a+b+c} p_{a,b,c|X=i,Y=j,Z=k}, \tag{5.3.14}$$

then the Svetlichny inequality is

$$M = -\langle 000\rangle + \langle 001\rangle + \langle 001\rangle + \langle 011\rangle + \langle 100\rangle + \langle 101\rangle + \langle 110\rangle - \langle 111\rangle \leq 4. \quad (5.3.15)$$

Any local or two-way local box must satisfy this inequality. Quantum mechanically we can obtain $M = 4\sqrt{2}$ using a Greenberger-Horne-Zeilinger (GHZ) state [35]. X(Y+Z) boxes do not violate the Svetlichny inequality (although they must violate some Svetlichny-type inequality as they are three-way non-local). Svetlichny boxes give $M = 8$, the algebraic maximum of the expression (hence their name); XYZ correlations give $M = 6$. From the fact that some quantum states violate the Svetlichny inequality, we can conclude that in the two-input two-output case, $\mathcal{Q} \subseteq \mathcal{L}2$.

5.3.3 Simulating tripartite boxes.

We consider how we may simulate some of these tripartite boxes, using a supply of PR boxes as a resource. We will give three examples, showing how to simulate an X(Y+Z) box with two PR boxes, an XYZ box with three PR boxes and a Svetlichny box with three PR boxes.

First, suppose that two PR boxes are shared with box 1 between Alice and Bob and box 2 between Alice and Charles. The following protocol shows how the three observers may simulate one X(Y+Z) box (see Fig. 5.5).

Protocol 5: 2 PR boxes → 1 X(Y+Z) box

Alice. Alice inputs x into box 1 and box 2, obtaining outcomes a_1 and a_2. She then outputs $a = a_1 \oplus a_2$.

Bob. Bob inputs y into box 1, obtaining an output b.

Charles. Charles inputs z into box 2 obtaining output c.

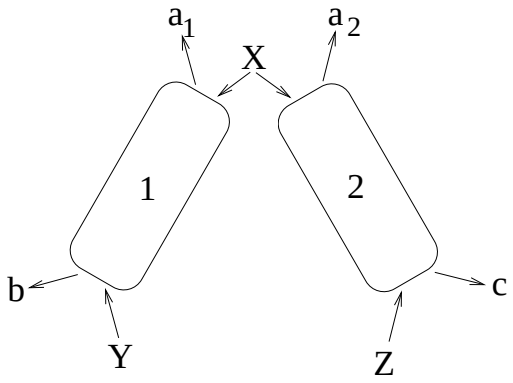

Figure 5.5: Making an X(Y+Z) box from 2 PR boxes.

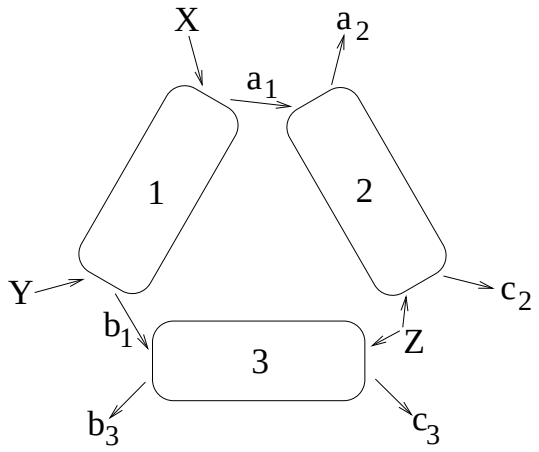

Figure 5.6: Making an XYZ box from 3 PR boxes.

The protocol works because

$$a \oplus b \oplus c = a_1 \oplus a_2 \oplus b \oplus c = x.y \oplus x.z \tag{5.3.16}$$

Suppose now that three PR boxes are shared with box 1 between Alice and Bob, box 2 between Alice and Charles, and box 3 between Bob and Charles. This protocol (summarized in Fig. 5.6) allows them to simulate one XYZ box.

Protocol 6: 3 PR boxes → 1 XYZ box

Alice. Alice inputs x into box 1, obtaining an output a_1. She then inputs a_1 into box 2, obtaining output a_2. Alice's output for the protocol is $a = a_2$.

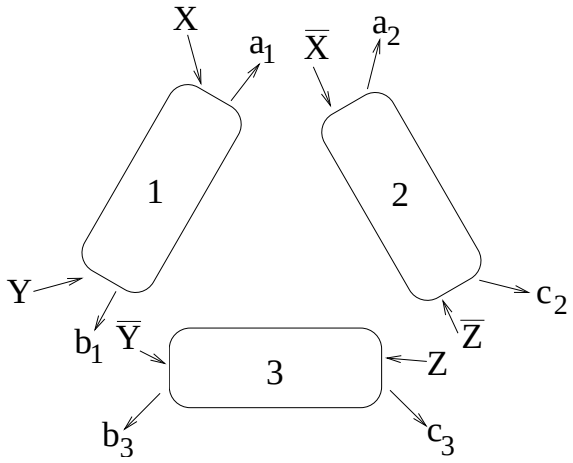

Figure 5.7: Making a Svetlichny box from 3 PR boxes.

Bob. Bob inputs y into box 1, obtaining an output b_1. He then inputs b_1 into box 3, obtaining output b_3. Bob's output for the protocol is $b = b_3$.
Charles. Charles inputs z into both boxes 2 and 3, obtaining outputs c_2 and c_3. Charles' output for the protocol is $c = c_2 \oplus c_3$.

The protocol works because

$$a \oplus b \oplus c = a_2 \oplus b_3 \oplus c_2 \oplus c_3 = z.a_1 \oplus z.b_1 = x.y.z. \tag{5.3.17}$$

It is immediately clear that we may make one Svetlichny box with two XYZ boxes. Into the first XYZ box, Alice, Bob and Charles input x,y,z respectively and into the second $\bar{x},\bar{y},\bar{z}$. For the final output, each person adds (modulo 2) the result of their two outputs. Combining this with Protocol 6, we have shown how to simulate one Svetlichny box with 6 PR boxes. However, one can do better than this.

As before, we suppose that we have three PR boxes, box 1 shared between Alice and Bob with outputs a_1, b_1, box 2 between Alice and Charles with outputs a_2, c_2 and box 3 between Bob and Charles with outputs b_3, c_3. Protocol 7 shows how to construct 1 Svetlichny box. It is summarized in Fig. 5.7.

Protocol 7: 3 PR boxes → 1 Svetlichny box

Alice. Alice inputs $\bar{x}$ into box 1, and x into box 2, obtaining a_1 and a_2. Her final output is $a = a_1 \oplus a_2 \oplus 1$. *Bob.* Bob inputs y into box 1 and $\bar{y}$ into box 3, obtaining b_1 and b_3. His final output is $b = b_1 \oplus b_3$.
Charles. Charles inputs $\bar{z}$ into box 2 and z into box 3, obtaining c_2 and c_3. His final output is $c = c_2 \oplus c_3$.

To see that this works write

$$\bar{x}.\bar{y}.\bar{z} \oplus x.y.z = (x \oplus 1)y \oplus (y \oplus 1)z \oplus (z \oplus 1)x \oplus 1 \tag{5.3.18}$$

in order to obtain

$$a \oplus b \oplus c = \bar{x}.\bar{y}.\bar{z} \oplus x.y.z. \tag{5.3.19}$$

5.3.4 Non-locality and the environment.

Suppose that we have some three party no-signalling distribution $p_{abe|xye}$ with parties A,B and E. We will show that if the reduced probability distribution $p_{ab|xy} = \sum_e p_{abe|xye}$ is a vertex of the bipartite no-signalling polytope, then the composite system AB is local versus E. This is analogous to the result that pure quantum states cannot be entangled with a third party or the environment. It means that extremal non-local correlations cannot be correlated to any other system.

By Bayes' theorem

$$\begin{aligned} p_{abe|xye} &= p_{ab|xyEe}\, p_{e|xye} \\ &= p_{ab|xyEe}\, p_{e|E} \end{aligned} \tag{5.3.20}$$

where we have used the fact that AB cannot signal to E to deduce the second equality. The condition that E cannot signal to AB implies

$$\begin{aligned} p_{ab|XY} &= \sum_e p_{abe|XYE} \qquad \forall E \\ &= \sum_e p_{ab|XYEe}\, p_{e|E} \quad \forall E \end{aligned} \tag{5.3.21}$$

For each value E, the last equality provides a convex decomposition of $p_{ab|XY}$ in terms of non-signalling correlations, with e playing the role of the shared randomness. Since we supposed that $p_{ab|XY}$ is extremal, this decomposition is unique and $p_{ab|XYEe} = p_{ab|XY}\ \forall e, E$. We then deduce

$$p_{abe|XYE} = p_{ab|XY}\, p_{e|E}, \tag{5.3.22}$$

i.e., that AB is uncorrelated with E.

A natural question that we leave as an open problem is whether the converse is true: If $p_{ab|XY}$ is in the interior of the no-signalling polytope, is it always possible to extend it to a tripartite distribution $p_{abe|XYE}$ such that AB is non-local versus E? (It is always possible, if $p_{ab|XY}$ is not a vertex, to write it as $p_{ab|XY} = \sum_e p_{abe|XYE}$, where E takes the single value $E = 0$. One can also require that E take several values, in such a way that $p_{abe|XYE}$ is non-signalling. What is non-trivial is the requirement that $p_{abe|XYE}$ is non-local in the partition AB versus E. We do not know if this is possible in general.)

5.4 Discussion and open questions.

In conclusion, we have defined non-signalling correlation boxes and investigated their potential as an information theoretic resource. Once the structure of the set of such boxes is understood as a convex polytope, it is clear that there are analogies with other information theoretic resources, in particular the resource of shared quantum states (with non-locality taking the place of entanglement). With this in mind, we have shown how various interconversions between boxes are possible. The set of

multipartite boxes in particular appears very rich. Finally, we furthered the analogy with quantum states by demonstrating how non-locality is monogamous, in much the same way that entanglement is monogamous. We finish with some open questions.

Non-local vertices and Bell inequalities.

We saw in Sec. 5.2.2 that for the two-settings two-outcomes polytope there is a one-to-one correspondence between extremal non-local correlations and facet Bell inequalities (non-trivial facets of the local polytope). One might wonder whether this one-to-one correspondence holds in general. It appears that for more complicated situations involving more possible inputs or outcomes, then it does not. It would be interesting to investigate what is the precise relation between non-local vertices and facet Bell inequalities. This might help understand further the geometrical structure of non-local correlations.

Other vertices.

We have given a complete characterization of two-inputs extremal non-local boxes in the bipartite case and presented some examples in the tripartite case. In general, one might also consider extremal boxes involving more inputs, more outcomes or more parties.

For instance, a natural way to generate more complex boxes is by taking products of simpler ones. Suppose Alice and Bob have access to two boxes $p^0_{a_0b_0|X_0Y_0}$ and $p^1_{a_1b_1|X_1Y_1}$, where for simplicity we consider that there are M possible inputs and d possible outputs for each box. If Alice inputs x_0 and x_1 in each of the two boxes and outputs $a = d\,a_1 + a_0$ and similarly for Bob, they have now produced a non-local box with M^2 inputs and d^2 outputs $p_{ab|XY} = p^0_{a_0b_0|X_0Y_0} \cdot p^1_{a_1b_1|X_1Y_1}$, where $X = M\,x_1 + x_0$ and similarly for Y. If the two original boxes were extremal for the (M, d) polytope will the product be extremal for the (M^2, d^2) polytope? In the case of quantum states, the analogous result of course holds - a product of two pure states is itself a pure state. We have not yet been able to show that this result holds in the case of

boxes.

Inter-conversions.

We have so far been able to achieve only a limited set of inter-conversions between extremal boxes. This is especially true for the three party case, where there are 46 classes of vertices and we have investigated only 5 of these. Understanding what kinds of inter-conversions between extremal boxes are possible is necessary to appraise their relative power as an information-theoretic resource.

The motivation is also to answer the general question of whether there exist inequivalent types of non-local correlations. Note for instance that the three-way non-local correlations of eqs. (5.3.11), (5.3.13) and (5.3.12) cannot be reduced to two-way non-local ones using only local operations. This follows from the fact that the outcomes for two out of the three parties are totally independent of one another (unless the outcome of the third party is communicated to them). In this sense genuinely tripartite extremal correlations and bipartite extremal correlations belong to inequivalent classes. Are there inequivalent classes of bipartite extremal correlations? In other words, are there two bipartite extremal boxes, such that one cannot simulate the other even approximately, no matter how many copies are available?

Another problem is whether all bipartite and multipartite correlations can be constructed using PR boxes, as is the case for all the extremal boxes presented in this paper (and thus also for probabilistic mixtures of them). PR boxes could then be viewed as the unit of non-local correlation, in analogy with the bit, qubit and ebit, which are the units of classical and quantum information theoretic resources.

Interior points.

We have only considered conversions between extremal probability distributions. It would be interesting to consider the interior points of the polytope, which comprise quantum correlations. In particular we would like to find out if distillation of such

mixed correlations is possible, i.e., if given a number of copies of a mixed box we can by local operations obtain some number of extremal boxes. Note that Cirel'son's bound [17] shows that the quantum correlations $\mathcal{Q}$, are a proper subset of the set of all non-signalling correlations $\mathcal{P}$. Thus it is impossible to distill correlations in $\mathcal{Q}$ to extremal correlations. But apart from this, we do not know of any constraint on possible distillation of non-local correlations.

Finally, one could consider distillation in a new context, where we allow some communication between the parties but account for it at the end of the protocol (as noted above, an analogous approach was considered in Ref. [94] in the context of classical distillation of shared randomness). Alternatively, following Ref. [96], one could introduce a new element, that of secrecy. Suppose that inputs and outputs are considered to be secret, and that Alice and Bob have a supply of noisy (that is non-extremal) boxes. Can Alice and Bob distill a supply of extremal boxes, whose inputs and outputs are also secret, via public communication?

As we outlined in the introduction, non-local extremal correlations can be a very powerful resource for communication complexity problems. This will also be the case for correlations that can be distilled to these with no or little communication. On the other hand, Cirel'son's bound and results in communication complexity [88] put limits on the power of quantum mechanics as a resource in distributed tasks. A better understanding of the possible inter-conversions between non-local correlations might bring an information theoretic explanation of these limitations.

5.5 Appendix B.

This section contains a proof of theorem 1, derived by S. Massar and S. Pironio.

Theorem 1. *The non-local vertices of $\mathcal{P}$ for two input settings and d_X^A and d_Y^B outputs are equivalent under reversible local relabelling to*

$$p_{ab|XY} = \begin{cases} 1/k & : \quad (b-a) \bmod k = x.y \\ & \quad a, b \in \{0, \ldots, k-1\} \\ 0 & : \quad \text{otherwise,} \end{cases} \tag{5.5.1}$$

for each $k \in \{2, \ldots, \min_{X,Y}(d_X^A, d_Y^B)\}$.

Proof of Theorem 1. A probability table $p_{ab|XY}$ is a vertex of $\mathcal{P}$ if and only if it is the unique solution of Eqs. (5.2.1),(5.2.2),(5.2.3) and (5.2.4) with $\dim(\mathcal{P})$ of the positivity inequalities (5.2.1) replaced with equalities.

It will be useful to distinguish two kinds of extremal points: partial-output vertices and full-output vertices. Partial-output vertices are vertices for which at least one of the $p_{a|X} = 0$ or $p_{b|Y} = 0$. They can be identified with vertices of polytopes $\mathcal{P}'$ with fewer possible outputs: $d'^A_X < d^A_X$ or $d'^B_Y < d^B_Y$. Conversely, the vertices of a polytope $\mathcal{P}'$, with $d'^A_X < d^A_X$ or $d'^B_Y < d^B_Y$ can be extended to vertices of $\mathcal{P}$ by mapping the outcomes of x' and y' to a subset of the outcomes of x and y, and by assigning a zero probability $p_{a|X} = 0$ and $p_{b|Y} = 0$ to extra outcomes. Full-output vertices are vertices for which all $p_{a|X} \neq 0$ and $p_{b|Y} \neq 0$, i.e., for which all outputs contribute non-trivially to $p_{ab|XY}$. Thus the extremal points of a given two-settings polytope consist of the full-output vertices of that polytope and, by iteration, of all the full-output vertices of two-settings polytopes with fewer outcomes. Hence in the following, we need construct only the full-output vertices for a polytope characterized by d_X^A and d_Y^B.

The joint probabilities $p_{ab|XY}$ form a table of $\sum_{X,Y} d_X^A d_Y^B$ entries. These are not all independent because of the normalization and no-signalling conditions. There are 4 normalization equalities expressed by Eq. (5.2.2) and $\sum_X d_X^A + \sum_Y d_Y^B$ no-signalling

equalities expressed by Eqs. (5.2.3) and (5.2.4). But for each value of x, the no-signalling condition for one of Alice's outputs can be deduced from the conditions of normalization and no-signalling for the $d_x^A - 1$ other outputs. A similar argument applies for each value of y and Bob's outputs. Hence Eqs. (5.2.2), (5.2.3) and (5.2.4) form a set of only $4 + \sum_x (d_x^A - 1) + \sum_y (d_y^B - 1) = \sum_x (d_x^A) + \sum_y (d_y^B)$ linearly independent equations. The dimension of the no-signalling polytope is thus

$$\dim(\mathcal{P}) = \sum_{x,y=0}^{1} d_x^A d_y^B - \sum_{x=0}^{1} d_x^A - \sum_{y=0}^{1} d_y^B \ . \tag{5.5.2}$$

This is the number of entries in the table $p_{ab|xy}$ that must be set to zero to obtain a vertex. Moreover, to obtain a full-output vertex, these must be chosen so that neither $p_{a|x} = 0$ nor $p_{b|y} = 0$. If we fix a particular pair of inputs (x, y), then no more than $d_x^A d_y^B - \max(d_x^A, d_y^B)$ probabilities may be set to zero, otherwise there will be fewer than $\max(d_x^A, d_y^B)$ probabilities $p_{ab|xy} > 0$, and thus one of Alice's or one of Bob's outcomes will not be output for these values of x and y. Because of the no-signalling conditions it will not be output for the other possible pairs of inputs, so the vertex will be a partial-output one. Overall, the maximal number of allowed zero entries for a full-output vertex is

$$Z = \sum_{x,y} \left(d_x^A d_y^B - \max(d_x^A, d_y^B) \right) \ . \tag{5.5.3}$$

Such a vertex is thus possible if $\dim(\mathcal{P}) \leq Z$, or

$$\sum_{x=0}^{1} d_x^A + \sum_{y=0}^{1} d_y^B \geq \sum_{x,y=0}^{1} \max(d_x^A, d_y^B) \ . \tag{5.5.4}$$

This condition is fulfilled (with equality) only for $d_x^A = d_y^B = d$, $\forall\, x,y \in \{0,1\}$.

We can thus restrict our analysis to d-outcome polytopes. The extremal points of more general ones, where $d_x^A \neq d_y^B$, will be the full-output extremal points of d-outcomes polytopes for $d = 2, \ldots, \min_{x,y}(d_x^A, d_y^B)$.

Using $d_x^A = d_y^B = d$, $\forall\, x,y \in \{0,1\}$ in the discussion before Eq. (5.5.3), it follows that the dimension of a d-outcome polytope is $4d(d-1)$ and that for a given pair of

inputs exactly $d(d-1)$ probabilities must be assigned the value zero, or equivalently that d probabilities must be > 0. We can therefore write the probabilities as

$$p_{ab|XY} \begin{cases} > 0 & \text{if } b = f_{XY}(a) \\ = 0 & \text{otherwise,} \end{cases} \tag{5.5.5}$$

where $f_{XY}(a)$ is a permutation of the d outcomes. Indeed, if $f_{XY}(a)$ is not a permutation, then at least one of Bob's outcomes will not be output.

We can relabel Alice's outcomes for $x = 0$ so that $f_{01}(a) = a$, we can relabel those of Bob for $y = 0$ so that $f_{00}(a) = a$ and finally those of Alice for $x = 1$ to have $f_{10}(a) = a$. In other words,

$$p_{ab|XY} \begin{cases} > 0 & \text{if } (b-a) \bmod d = 0 \\ = 0 & \text{otherwise,} \end{cases} \tag{5.5.6}$$

for $(x,y) \in \{(0,0),(0,1),(1,0)\}$. It remains to determine f_{11}. It must be chosen so that the probability table $p_{ab|XY}$ is uniquely determined, i.e., so that specific values are assigned to the probabilities different from zero. In fact, it is easy to show that this can only be the case if the permutation f_{11} is of order d, i.e., $f_{11}^k(a) = a$ only for $k = 0 \bmod d$.

The only remaining freedom in the relabelling of the outcomes so that property (5.5.6) is conserved, is to relabel simultaneously the outputs for all four possible inputs. We can relabel them globally so that $f_{11}(a) = (a+1) \bmod d$. This implies that $p_{ab|11} = 1/d$ if $(b-a) \bmod d = 1$. This completes the proof. □

Chapter 6

Quantifying entanglement.

Abstract.

Quantifying entanglement has been the aim of a huge amount of recent research. Except in a few special cases it remains an unsolved puzzle. This chapter contains an overview of the main results in this area, and a framework for interpreting some new results relating to multipartite entanglement which are presented in chapter 7.

6.1 Introduction.

In quantum information applications entanglement is thought to be closely related to the possibilities of gains over classical procedures [104], and applications such as teleportation [45] and super dense coding [46] consume entangled pure states as a resource. This has motivated recent attempts at quantifying entanglement. This task has proven to be extremely challenging but the following chapter presents some of the main results.

6.2 Separability criterion.

A mixed state $\rho \in \mathcal{H}^1 \otimes ... \otimes \mathcal{H}^k$ is separable if it may be written

$$\rho = \sum_i p_i |\phi_i^1\rangle\langle\phi_i^1| \otimes ... \otimes |\phi_i^k\rangle\langle\phi_i^k|. \tag{6.2.1}$$

Where $|\phi_i^m\rangle \in \mathcal{H}^m$ and $\sum_i p_i = 1$. The definition of separability provides no simple way of telling if an arbitrary state is entangled or not [105]. It is therefore important to develop separability criterion which allow us to perform simple tests to assess the entanglement properties of a given state. An important result in this area is the Peres-Horodecki separability criterion for bi-partite states.

Peres-Horodecki separability criterion [106, 57].

Let ρ be a bipartite density matrix on $\mathcal{H} = \mathcal{H}^A \otimes \mathcal{H}^B$, which we may write

$$\rho = \rho_{m\mu,\, n\nu} \tag{6.2.2}$$

The Latin indices refer to system A and Greek indices to system B. The partial transposition operation defines a new hermitian matrix σ as follows.

$$\sigma_{m\mu,\, n\nu} = \rho_{n\nu,\, m\mu} \tag{6.2.3}$$

Here the Latin indices have been transposed but not the Greek ones. In the case of separable states this partial transposition operation always results in a physical state, i.e σ is positive. To see this let

$$\rho = \sum_i p_i \, \rho'_i \otimes \rho''_i \tag{6.2.4}$$

where $\rho'_i \in \mathcal{H}_A$ and $\rho''_i \in \mathcal{H}_B$. Then

$$\sigma = \sum_i p_i \, (\rho'_i)^T \otimes \rho''_i. \tag{6.2.5}$$

This is a valid (non-negative) density matrix. Thus the Peres-Horodecki separability criterion may be stated:

Negativity under partial transposition (PPT) $\Rightarrow$ non-separability.

The Horodecki's have shown that this condition is in fact necessary and sufficient for systems of dimension 2×2 and 2×3 [57].

Of course we may be interested in which states are separable, in which case the following criterion may be used [107, 108, 109].

For a bi-partite system ρ of overall dimension d, $\mathbf{Tr}\,\rho^2 < \frac{1}{d-1} \Rightarrow \rho$ is separable.

Single copy and asymptotic conversions.

Because of the incomplete nature of our knowledge in this area it is useful to make distinctions between the different types of systems we may consider. For example pure or general mixed states, bi-partite or multipartite, and continuous or discrete systems. Continuous variable systems are not considered in this review (For a review specific to continuous variable systems, see [110]).

Quantifying entanglement is based on the premise that we can convert an entangled state from one form to another. The resources we are usually allowed are local operations and classical communication (LOCC). There are then two main

approaches, single copy and asymptotic (many copy) conversions. Although within these two main strands there are many more subtle distinctions one can make.

6.3 The single copy approach.

We are interested in what sort of transformations are possible on a single state under LOCC. A key result in this area is Nielson's theorem [111]. This provides necessary and sufficient conditions for exact conversions for bi-partite pure states. First we need the following definition of majorization.

x is majorized by y ($x \prec y$).

If $x = (x_1, x_2, ..., x_d)$ and $y = (y_1, y_2, ..., y_d)$, let $x^{\downarrow}$ mean the reordering of x so that the components are in decreasing order. Then $x \prec y$ if

$$\sum_{j=1}^{k} x_j^{\downarrow} \leq \sum_{j=1}^{k} y_j^{\downarrow} \text{ for } k = 1, ..., d \tag{6.3.1}$$

Where equality holds when $k = d$. Now suppose we are given two bi-partite pure states $|\psi\rangle$ and $|\phi\rangle$. Define the reduced density matrices as

$$\rho_\psi \equiv \mathrm{Tr}_B\left(|\psi\rangle\langle\psi|\right),\ \rho_\phi \equiv \mathrm{Tr}_B\left(|\phi\rangle\langle\phi|\right), \tag{6.3.2}$$

and let λ_ψ and λ_ϕ be the vectors whose components are the eigenvalues of ρ_ψ and ρ_ϕ.

Nielsen's theorem.

A bi-partite pure state $|\psi\rangle$ may be transformed to another bi-partite pure state $|\phi\rangle$ by LOCC with certainty if and only if $\lambda_\psi \prec \lambda_\phi$. We can express this in chemical notation as $|\psi\rangle \rightarrow |\phi\rangle$, and say $|\phi\rangle$ is *exactly reducible* to $|\psi\rangle$. Just as chemical reactions often require catalysts, so too with quantum state conversions. $|\phi\rangle$ is *catalytically reducible* to $|\psi\rangle$ if there exists some state $|\sigma\rangle$ such that

$$|\psi\rangle \otimes |\sigma\rangle \rightarrow |\phi\rangle \otimes |\sigma\rangle \tag{6.3.3}$$

Jonathan and Plenio [112] have found examples where a catalyst allows a transformation to be achieved with certainty, where without the catalyst it may only be done with a chance of failure.

Two states may only be obtained from each other with certainty if they are related by local unitaries (LU)[114, 115]. Even for simple bi-partite systems typical states are not related by LU [116, 117, 118]. Thus a categorization based on exact reducibilities presents a problem in that the number of inequivalent types of entanglement must be labelled by continuous parameters. Because of this the weaker *stochastic* reducibility has been used (SLOCC). Here we no longer require that a conversion be achieved with certainty, only with some non-zero probability. The optimum strategy for converting between any two pure states under SLOCC is presented in [119]. It is optimal in the sense that the probability of a successful conversion is the highest possible. This optimum value may be calculated as follows: Suppose we wish to convert $|\psi\rangle$ into $|\phi\rangle$ under SLOCC. Using the Schmidt decomposition,

$$|\psi\rangle = \sum_{i=1}^{n} \sqrt{\alpha_i} |i\rangle_A |i\rangle_B, \;\; \alpha_i \geq \alpha_{i+1} \geq 0, \;\; \sum_{i=1}^{n} \alpha_i = 1, \tag{6.3.4}$$

$$|\phi\rangle = \sum_{i=1}^{n} \sqrt{\beta_i} |i\rangle_A |i\rangle_B, \;\; \beta_i \geq \beta_{i+1} \geq 0, \;\; \sum_{i=1}^{n} \beta_i = 1. \tag{6.3.5}$$

Then the maximum probability of obtaining state $|\phi\rangle$ from $|\psi\rangle$, $P(\psi \rightarrow \phi)$, is given by

$$P(\psi \rightarrow \phi) = \min_{l \in [1,n]} \frac{\sum_{i=l}^{n} \alpha_i}{\sum_{i=l}^{n} \beta_i}. \tag{6.3.6}$$

Dür, Vidal and Cirac [71] have shown that for 3 party qubit systems there are just two types of inequivalent (under SLOCC) tripartite entanglement. Two representatives of these classes are the GHZ and W states.

The problem of converting to a 2 qubit mixed state from a pure state is considered in [113]. We can also note that other reducibilities are possible, such as stochastic reducibilities with catalysis, and reducibilities without communication.

6.4 The asymptotic approach.

The asymptotic approach to quantifying entanglement means that we are interested in the transformation properties of large numbers of identical copies of our state. This has proved to be a particularly successful approach in the case of bi-partite pure states.

Ideal measures.

There is some consensus about desirable properties any asymptotic entanglement measure should satisfy [114, 120]. Let E be an entanglement measure. Then E should have the following properties.

(a) $\lim_{N\to\infty} E(\rho^{\otimes N}) = NE(\rho)$
(b) $E(\rho) = 0 \Leftrightarrow \rho$ is separable.
(c) Local unitary operations on ρ leave $E(\rho)$ invariant.
(d) $E(\rho)$ can not be increased by local measurements (POVM) and classical communication.

Measures satisfying property (a) are said to be *asymptotically additive*. It is possible to define a stronger additivity; E is *fully additive* if $E(\rho_1 \otimes \rho_2) = E(\rho_1) + E(\rho_2)$ for all ρ_1, ρ_2. Measures satisfying property (d) are said to be *entanglement monotones*.

Two party pure states.

There is a simple and elegant categorization of bi-partite pure state entanglement - the von Neumann entropy of the reduced density matrix. This quantity satisfies all of the conditions above, and is fully additive. For a quantum state ρ defined on $\mathcal{H} = \mathcal{H}^A \otimes \mathcal{H}^B$, the von Neumann entropy is defined as

$$S(\rho) = -\mathrm{Tr}\,(\rho \,\mathrm{Log}\,\rho). \tag{6.4.1}$$

The reduced density matrices are

$$\rho_A = \mathrm{Tr}_B(\rho_{AB}) \tag{6.4.2}$$

and

$$\rho_B = \mathrm{Tr}_A(\rho_{AB}). \tag{6.4.3}$$

Then the reduced entropies are defined as $S_A(\rho_{AB}) = S(\rho_A)$ and $S_B(\rho_{AB}) = S(\rho_B)$. If ρ_{AB} is pure then the *entanglement* of ρ_{AB} is defined

$$E(\rho_{AB}) = S_A(\rho_{AB}) = S_B(\rho_{AB}). \tag{6.4.4}$$

This measure has a physical interpretation as follows. Suppose we have some partially entangled pure state $|\chi\rangle_{AB}$. To measure the entanglement we convert n copies of this state to k copies of the maximally entangled singlet state. We are allowed to perform local operations only, and can communicate classically. We require that the transformation is reversible. Then in the asymptotic limit it can be shown that

$$E(\chi) \equiv \lim_{n\to\infty} \frac{k}{n} = S_A(\chi) = S_B(\chi). \tag{6.4.5}$$

Since the Von Neumann entropy of the reduced state is such a useful entanglement measure, we require that any other entanglement measure reduces to this measure

in the case of pure bi-partite systems. i.e we add condition (e) to the conditions of an ideal entanglement measure.

(e) $E(\rho) = S_A(\rho)$ for pure bi-partite systems.

Two party mixed states.

In contrast to the situation for pure states there exist entangled states ρ which can not be reversibly converted into singlets under asymptotic LOCC [121]. Thus two measures of mixed state entanglement have been proposed; the entanglement cost and the entanglement of distillation. The general scheme is as follows. We wish to convert m copies of a bi-partite state ρ into n copies of σ under LOCC so that the asymptotic ratio $\frac{m}{n}$ is minimal. Generally a perfect transformation

$$\rho^{\otimes m} \rightarrow \sigma^{\otimes n} \tag{6.4.6}$$

is impossible, so we require only that $\rho^{\otimes m}$ approaches $\rho^{\otimes n}$ to arbitrary precision as m is increased. If the final state of $\rho^{\otimes m}$ is ρ', the distance measure used between the two states is the fidelity

$$F(\rho', \sigma^{\otimes n}) = (\mathrm{Tr}(\sqrt{\sigma^{\otimes n}}\,\rho'\,\sqrt{\sigma^{\otimes n}})^{1/2})^2. \tag{6.4.7}$$

If the final state σ desired is the singlet state then the process of conversion is *distillation*, and the *entanglement of distillation*, E_d, is defined

$$E_d(\rho) = \lim_{n\rightarrow\infty} \frac{m}{n} \tag{6.4.8}$$

If the starting state ρ is a singlet state then the *entanglement cost* may be defined

$$E_c(\sigma) = \lim_{n\rightarrow\infty} \frac{m}{n}. \tag{6.4.9}$$

We can also define the entanglement of formation as follows. We may imagine producing some state σ according to the following protocol. σ can be decomposed as

$$\sigma = \sum_i p_i \, |\psi_i\rangle\langle\psi_i|. \tag{6.4.10}$$

Therefore if we make each state $|\psi_i\rangle$ from singlets, and mix them with probability p_i we see that it takes on average $\sum_i p_i \, S_A(\psi_i)$ singlets to make σ. The *entanglement of formation*, E_f, is defined as the average entanglement of the pure states in the decomposition, minimized over all possible decompositions [122]:

$$E_f(\sigma) = \min \sum_i p_i \, S_A(\psi_i). \tag{6.4.11}$$

Concurrence.

For bi-partite mixed states the entanglement of formation involves an optimization over all possible decompositions of the state which is difficult to compute analytically. Wooters [123] proved a result which gives the entanglement of formation for states of two qubits. He did this by defining a quantity called the *concurrence*. Let

$$\tilde{\rho} = (\sigma_y \otimes \sigma_y)\rho^*(\sigma_y \otimes \sigma_y). \tag{6.4.12}$$

The asterisk denotes complex conjugation in the basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. Then the concurrence, $C(\rho)$, is defined

$$C(\rho) = \max\{0, \lambda_1 - \lambda_2 - \lambda_3 - \lambda_4\}, \tag{6.4.13}$$

where the λ_i's are the square roots of the eigenvalues, in decreasing order, of the matrix $\rho\tilde{\rho}$. Now define

$$\mathcal{E}(C) = h\big(\frac{1+\sqrt{1-C^2}}{2}\big), \tag{6.4.14}$$

$$h(x) = -x\log_2 x - (1-x)\log_2(1-x). \tag{6.4.15}$$

The concurrence is an entanglement measure in its own right, ranging from 0 for separable states to 1 for the singlet state. However it is also related to the

entanglement of formation by

$$E_f(\rho) = \mathcal{E}(C(\rho)). \tag{6.4.16}$$

Negativity.

The negativity of a state was introduced by Vidal and Werner [124] as a computationally tractable measure of mixed state bi-partite entanglement. It is based on the Peres separability criterion. Let ρ^{T_A} be the partial transpose of ρ, and let $||\rho^{T_A}||_1$ denote the trace norm of ρ^{T_A}, defined as; $||X||_1 = \mathrm{Tr}\sqrt{X^\dagger X}$. The *negativity* of ρ is defined

$$\mathcal{N}(\rho) \equiv \frac{||\rho^{T_A}||_1 - 1}{2}. \tag{6.4.17}$$

It is also possible to define the *logarithmic negativity*, $E_{\mathcal{N}(\rho)}$, as

$$E_{\mathcal{N}(\rho)} \equiv \log_2 ||\rho^{T_A}||_1. \tag{6.4.18}$$

$\mathcal{N}(\rho)$ is an entanglement monotone, and the logarithmic negativity has the property that it is additive. Vidal and Werner have shown in addition that the logarithmic negativity provides an upper bound on the distillable entanglement on a state.

$$E_d(\rho) \leq E_{\mathcal{N}}(\rho). \tag{6.4.19}$$

Relative entropy of entanglement.

For two mixed states σ and ρ, the relative entropy between σ and ρ is given by

$$D(\sigma||\rho) = \mathrm{Tr}\,\sigma(\log\sigma - \log\rho). \tag{6.4.20}$$

$D(\sigma||\rho)$ can be interpreted as a measure of how difficult it is to distinguish measurement outcomes on ρ from measurements on σ. Vedral *et al* [120] have proposed the *relative entropy of entanglement*, $E_r(\sigma)$ as an entanglement measure.

$$E_r(\sigma) = \min_{\rho \in S} D(\sigma||\rho), \;\; S \text{ is the set of separable states.} \tag{6.4.21}$$

The idea behind this measure is that it quantifies the difference between the state σ and the separable state ρ whose measurement statistics most closely match those of σ. This measure satisfies properties (b), (c), (d) and (e) [120], but is not fully additive [125].

Multipartite pure states and MREGS.

We have seen how bi-partite pure states may be reversibly converted to singlets under LOCC. The MREGS is the generalization of this concept for pure multipartite systems. For these systems it is not possible to reversibly convert every state into singlets shared between the parties, even in an asymptotic sense [115]. It may however be possible to asymptotically reversibly convert any state into some larger set of entangled states. The set of such states with the smallest number of elements is an MREGS, denoted $\mathcal{G}_n$ for a n party system. Thus while for bi-partite pure states entanglement is a scalar, for multipartite systems it would be a vector.

For two pure states ψ and ϕ, ϕ is asymptotically reducible to ψ under local operations and classical communication ($\phi \preceq \psi$) if and only if

$$\begin{aligned} \forall \epsilon,\, \delta > 0 \; \exists\, N, n, \mathcal{L} \, s.t \, |(\frac{n}{N}) - 1| < \delta \, \text{and} \\ F(\mathcal{L}(\psi^{\otimes N}), \phi^{\otimes n}) \geq 1 - \epsilon. \end{aligned} \tag{6.4.22}$$

$\mathcal{L}$ is a locally implementable operator, acting on all N copies of ψ, to convert it to n approximate copies of ϕ. Here $F(\rho, \sigma) = (\mathrm{Tr}(\sqrt{\sigma}\,\rho\,\sqrt{\sigma})^{1/2})^2$ is the fidelity between two states.

Asymptotic reducibilities and equivalences can have non integer yields. We can denote this by allowing tensor exponents to take any non-negative real value. $\phi^{\otimes x}$ is asymptotically reducible to $\psi^{\otimes y}$ under LOCC denotes

$$\forall \epsilon,\, \delta\, > 0\, \exists\, N, n, \mathcal{L}\, s.t\, |(\frac{n}{N}) - \frac{x}{y}| < \delta \,\text{and} \qquad F(\mathcal{L}(\psi^{\otimes N}), \phi^{\otimes n}) \geq 1 - \epsilon. \tag{6.4.23}$$

Pure states $\phi^{\otimes x}$ and $\psi^{\otimes y}$ with $x,\, y \geq 0$ are asymptotically equivalent ($\phi^{\otimes x} \approx \psi^{\otimes y}$) if and only if $\phi^{\otimes x}$ is asymptotically reversible to $\psi^{\otimes y}$ and vice versa.

To formalize the idea of MREGS, given a set of states $\mathcal{G} = \{\psi_1, \psi_2, ..., \psi_t\}$, their entanglement span $\mathrm{Sp}(\mathcal{G})$ is the set of states that $\mathcal{G}$ can generate reversibly under asymptotic LOCC. i.e

$$\mathrm{Sp}(\mathcal{G}) = \{\psi \,|\, \psi \approx \bigotimes_{i=1}^{t} |\psi_i\rangle^{\otimes x_i},\, x_i \geq 0\}. \tag{6.4.24}$$

The set of x_i are entanglement coefficients, which are not unique in general. A set of minimal cardinality able to generate the full class of m party states is an MREGS, which we denote by $\mathcal{G}_m$. For example for two party states $\mathcal{G}_2 = \{|\psi_-\rangle\}$. It is not known if the entanglement coefficients are unique for an MREGS, as is desirable.

Very little is known about MREGS for n-partite systems. Even for the simplest case $n = 3$ it is not known whether $\mathcal{G}_3$ is finite or not. We do however have some lower bounds coming from conditions on the reduced entropies and relative entropies of entanglement. These conditions are reviewed below, but discussion of their implications to specific MREGS sets is postponed until the next chapter.

Constraints on MREGS.

When considering which states may belong to an MREGS we are interested in the type of transformations we may achieve reversibly under LOCC. These transformations are constrained by considerations of reduced entropy and relative entropy of entanglement.

Reduced entropies.

For two states to be asymptotically equivalent they must have the same reduced entropies [115]. For example, by considering the reduced entropies it is possible to show that a four party GHZ may not be reversibly converted into singlets shared between the four parties. This is discussed more fully in the next chapter.

Relative entropy of entanglement.

A consideration of reduced entropies for three party pure states gives no restriction on, for example, the reversible conversion of the GHZ state to singlets. Linden *et al* [126] have found a further restriction based on relative entropy of entanglement. Again suppose that given two pure states ψ and ϕ we wish to convert ψ to ϕ reversibly under LOCC. Then

$$E_r(\psi_{BC}) = E_r(\phi_{BC}). \text{ [126]} \tag{6.4.25}$$

i.e the relative entropy of entanglement for any two parties must remain constant. This shows that it is impossible to convert a GHZ state into singlets reversibly under asymptotic LOCC. To see this we note that the reduced two party state of the GHZ state is the maximally mixed state - which is separable with $E_r = 0$, whereas the the singlet shared between any two parties has $E_r = 1$.

6.5 Other measures.

Three-way tangle.

Coffman, Kundu and Wootters [127] have proposed a generalization of the concurrence for three party pure states of qubits. Firstly to define the *tangle*.

$$\tau_{AB} = (C(\rho_{AB}))^2. \tag{6.5.1}$$

Where $C(\rho_{AB})$ is the concurrence of ρ_{AB} as defined in equation 6.4.13. We can

also consider the quantity $\tau_{A(BC)}$, the tangle between A and the pair BC because although the state space of BC is four dimensional, only two of those dimensions are needed to express the pure state $|\eta\rangle_{ABC}$. So we can treat A and BC as a pair of qubits. The three-way tangle τ_{ABC} can then be defined as

$$\tau_{ABC} = \tau_{A(BC)} - \tau_{AB} - \tau_{AC}. \tag{6.5.2}$$

The idea behind this is that essential three-way entanglement of A is the tangle between A and BC minus the tangle between A and B, and A and C. For example the GHZ state has three-way tangle 1 ($= \tau_{A(BC)}$), whilst the W state has three-way tangle equal to 0.

Schmidt measure.

The Schmidt measure has been proposed as a measure of multipartite entanglement for both pure and mixed states [129]. It has been shown to be an entanglement monotone. For pure states it is a natural generalization of the Schmidt rank. Consider an n particle pure quantum system $|\psi\rangle$. Each party holds a system with dimension d_i, so $|\psi\rangle \in \mathcal{H} = C^{d_1} \otimes ... \otimes C^{d_n}$. We may choose to write

$$|\psi\rangle = \sum_{i=1}^{R} \alpha_i |\psi_1^i\rangle \otimes ... \otimes |\psi_n^i\rangle \tag{6.5.3}$$

where $|\psi_j^i\rangle \in C^{d_j}$ for $j = 1, ..., n$, and $\alpha_i \in C$, $i = 1, ...R$. Let r be the minimal number of product terms R in such a decomposition of $|\psi\rangle$. Then the Schmidt measure, P, is

$$P(|\psi\rangle\langle\psi|) = \log_2 r. \tag{6.5.4}$$

When we consider a bi-partite state this reduces to the Schmidt rank of that state. For mixed states ρ,

$$P(\rho) = \min \sum_i \lambda_i P(|\psi_i\rangle\langle\psi_i|) \tag{6.5.5}$$

where the minimum is taken over all possible decompositions of the form $\rho = \sum_i \lambda_i |\psi_i\rangle\langle\psi_i|$.

The above is a summary of some of the more important ideas in quantifying entanglement, although it is certainly not exhaustive. In the next chapter I present some new work concerning reduced entropies of multipartite states and MREGS.

Chapter 7

Entropy inequalities and MREGS.

Abstract.

In the previous chapter we saw various approaches to understanding multi-partite entanglement. In this chapter we focus on one specific approach; that of considering the reduced entropies of states. This investigation of multipartite entanglement was the original motivation for our work, however we also aim to better understand the constraints on the allowed reduced entropies.

In particular, suppose that we are given a list of reduced entropies - can we find a corresponding quantum state? The reduced entropies could be constrained by general linear inequalities such as strong subadditivity. They may be restricted by constraints imposed on the system, such as restricting the dimension of the Hilbert space. There could also be other constraints from new entropy inequalities.

If the dimension of the Hilbert space is not restricted then the only presently known constraints on the reduced entropies come from strong subadditivity (SSA) - all of the other known entropy inequalities being equivalent to this. SSA is a key result with many important applications in quantum coding theories. In this chapter we identify sets of reduced entropies, which although allowed by SSA can not be achieved by any quantum state [128].

Following Pippinger [132], if we define the *entropy allocation* to be the vector

reduced entropies for every possible subset of the parties, then the linear constraints of SSA mean that these entropy allocations are restricted to a polyhedral cone. In this chapter we enumerate all of the extreme rays of the cone described by SSA for four parties. We find states corresponding to all but two of the extreme rays, and by considering a classical analogy conjecture that no such quantum states exist. This conjecture has subsequently been proven by Linden and Winter [128]. We also suggest a stronger conjecture; that there are new linear entropy inequalities.

Systems associated with Quantum Information applications can often be described by qubit states. We therefore consider the space of reduced entropies under a restriction to pure three party qubit states. We would like to know how the region of allowed entropy allocations is further confined by this restriction. For example, the reduced entropies are now bounded above by 1, but we find that there are also further restrictions on the allowed reduced entropies.

We also make a connection to a proposed method for classifying multipartite entanglement; MREGS, or the minimal reversible entanglement generating set. In particular we show that states corresponding to the extreme rays of the cone of entropy allocations must be included in the MREGS. We show that considerations of reduced entropies mean that a certain set of states must belong to the three and four particle MREGS.

7.1 Introduction.

We have seen how classifying multipartite entanglement is an extremely challenging task. One possible approach is to use a measure we understand well from the bi-partite situation - the reduced entropy - and apply it to the multipartite case. In this multipartite setting we now have several different ways of making the bi-partite division of the parties, and following Pippinger [132] can define the *entropy allocation* to be the vector formed by taking each of the possible reduced entropies as its components. In this chapter we will consider the structure of the space of allowed entropy allocations.

The reduced entropy of a state is defined as follows: Let ρ be an n-particle quantum state. If the parties holding the state are labelled $1, 2, ..., n$, let X denote some non-trivial subset of the parties, and $\bar{X}$ the remaining parties. Then the reduced density matrix of subset X of the parties is

$$\rho_X = \mathrm{Tr}_{\bar{X}}(\rho) \tag{7.1.1}$$

and the reduced entropy of subset X,

$$S_X(\rho) = S(\rho_X). \tag{7.1.2}$$

For a state of n particles there are $2^n - 1$ possible non-trivial subsets of the particles. With each of these subsets we can associate a reduced entropy and write the entropy allocation $\vec{S}$ as the vector of these reduced entropies. For example in the two party case $\vec{S} = (S_1, S_2, S_{12})$.

In analyzing the structure of the space of allowed reduced entropies we would like to be able to answer the question; given a list of reduced entropies - can we find a corresponding quantum state? The constraints which may restrict the set of reduced entropies that can be achieved could take the form of general entropy inequalities such as strong subadditivity (SSA), they could be caused by restrictions on the state, such as a requiring that it can be described by a Hilbert space of finite

dimension for each particle. Finally there could be new entropy inequalities. In this chapter I will consider all of these possibilities.

Suppose initially that the state is not restricted by the dimension of its Hilbert space. What are the constraints on its reduced entropies? In general we know surprisingly little about this. The linear entropy inequalities which provide necessary conditions for a state corresponding to a given set of reduced entropies to exist are based around satisfying SSA.

Derived by Lieb and Ruskai [131] in 1973, SSA is a very important result at the heart of quantum information science. Many familiar results such as subadditivity, weak monotonicity and the triangle inequality follow immediately from SSA. Indeed every presently known result concerning the reduced entropies of a composite quantum system can be derived from SSA [97]. SSA has many applications in quantum coding theories, such as the Holevo Bound on accessible information [133].

Given any state ρ_{123} of three parties SSA may be expressed as follows,

$$S_{123}(\rho) + S_3(\rho) \leq S_{13}(\rho) + S_{23}(\rho). \tag{7.1.3}$$

A familiar consequence of SSA is subadditivity[1],

$$S_{12}(\rho) \leq S_1(\rho) + S_2(\rho). \tag{7.1.4}$$

SSA is also equivalent to weak monotonicity (WM). This is shown in appendix C, at the end of this chapter.

$$S_{12}(\rho) + S_{13}(\rho) \geq S_2(\rho) + S_3(\rho). \tag{7.1.5}$$

The linear constraints of SSA restrict the entropy allocations to belong to a polyhedral cone, which we label B_n. The subscript n gives the number of particles.

[1]We may see this as follows: SSA is true for all states, in particular it is true for pure states. For a pure state of three parties it is well known that $S_{123} = 0$, $S_3 = S_{12}$, $S_{13} = S_2$ and $S_{23} = S_1$. This gives subadditivity.

For one, two, and three party mixed states requiring that the entropy allocation lies inside the cone B_n is a necessary *and sufficient* condition for a corresponding quantum state to exist [132]. If the entropy allocation lies on the boundary of B_n then there is a weaker result - there exists a state that approaches the required entropy allocation to arbitrarily close approximation.

More precisely, if we label the set of entropy allocations allowed for quantum states by A_n, then Pippinger has shown that the topological closure of A_n,[2] denoted $\bar{A}_n$, is a convex cone. This is a remarkable result - it means that if we can find states corresponding to the extreme rays of B_n, then because of this convexity property there must exist a state that approaches any entropy allocation within the set A_n to arbitrarily close approximation.

In this new notation we have that $\bar{A}_n = B_n$, for $n = 1, 2, 3$. If we have more than three particles then there are sets of inequalities, based on SSA, that give necessary conditions for a corresponding quantum state to exist. In this chapter we enumerate all of the extreme rays of B_4, the polyhedral cone formed by the constraints from SSA for four party mixed states. We find states corresponding to all but two classes of these extreme rays, and conjecture that no such states exist. This conjecture is based on the following observations inspired by a classical analogy.

The classical analogy concerns probability distributions in several independent random variables. One may define entropy allocations with components comprising the various Shannon entropies of these probability distributions. As in the quantum case these Shannon entropies are constrained by linear entropy inequalities; classical strong subadditivity and strong monotonicity (SM). However in 1997 Zhang and Yeung [7] found a new classical inequality, inequivalent to classical SSA and SM for systems of 4 random variables.

We note that the quantum version of this Yeung Zhang inequality is violated by the entropy allocations for which we found no corresponding states. Conversely, all of the entropy allocations for which we succeeded in finding corresponding states *do*

[2]The topological closure of A_n is the smallest *closed* set containing every element of A_n

not violate this new inequality. As further support for our conjecture we also show that the quantum analogue of the Yeung Zhang inequality is true for pure quantum states.

Subsequently Linden and Winter [128] have shown the entropy allocations for which we were unable to find any corresponding state *can not* in fact be achieved by any quantum state. This allows us to conjecture that there may be new quantum entropy inequalities, inequivalent to SSA, still to be discovered. This is still an open question, but if true would be the first new entropy inequality for 30 years.

The final type of restriction imposed on the allowed entropy allocations comes from restrictions to the allowed states. Often systems associated with Quantum Information protocols can be described by qubit states. We therefore consider the reduced entropies allowed in the special case of three party pure qubit systems. Because the reduced entropies of qubit systems are bounded above by one, it is immediately clear that the space of allowed entropies is no longer an open ended cone, but must be bounded by a polygon. In fact we find there are further restrictions within this polygon.

In this chapter we also make a connection between the set of allowed reduced entropies A_n and MREGS. MREGS concerns asymptotic equivalences between states under LOCC. The main idea here is that extreme rays of $\bar{A}_n$ are a basis for the space of entropy allocation vectors because the space is convex. For two states to be asymptotically reversibly convertible to one another their reduced entropies must be the same, hence states giving the basis vectors for the space of entropy allocation vectors must be included in MREGS. This allows us to conclude that certain sets of states must belong to the MREGS for 3 and 4 particle states. These arguments are independent of whether or not there are new entropy inequalities.

The plan for this chapter is as follows. In section 7.2 the formal definitions of A_n, B_n and entropy allocations are provided. Pippinger [132] provides us with an algorithm for generating the complete set of entropy inequalities resulting from SSA. In section 7.3 we enumerate the extreme rays of B_n for $n = 2, 3, 4$. In particular in

section 7.3.1 we go on to show $\bar{A}_3 = B_3$. In section 7.3.2 we consider B_4, for which we discuss the classical analogy in section 7.4. Here we show that the quantum analogue of the Yeung-Zhang inequality is true for pure states. In section 7.5 we consider the space of entropy allocations for three party pure qubit systems. In section 7.6 we discuss the connection between the extreme rays of $\bar{A}_n$ and MREGS. Finally we give our conclusions and some open questions in 7.7.

The work in this chapter was done in collaboration with S. Popescu and N. Linden form the University of Bristol, and A. Thapliyal form UC Berkeley.

7.2 Entropy inequalities and convex cones.

In this section we give the definitions of the entropy allocation $\vec{S}$, the space of allowed entropy allocations A_n, and the polyhedral cone B_n. B_n is the space bounded by the constraints given by the linear entropy inequalities of SSA. The cone B_n contains A_n as a subset.

7.2.1 Entropy allocations.

What we mean by the entopy allocation is most easily seen by example; suppose we have a three particle state ρ_{123}, with particles labelled 1,2,3. The entropy allocation is the vector of reduced entropies, $\vec{S}(\rho) = (S_1, S_2, S_3, S_{12}, S_{13}, S_{23}, S_{123})$.

Definition: $\vec{S}(\rho)$**.**

In general let ρ be an n particle mixed quantum state and $N = \{1, 2, ..., n\}$, where the numbers label the particles. $X \subseteq N$ is some subset of the particles. Let $\bar{X}$ denote the set of particles that are in N but not in X. Then $\rho_X = \mathrm{Tr}_{\bar{X}}(\rho)$. For each possible distinct $X \subseteq N$ we may associate a reduced entropy $S_X(\rho)$. The set of all such reduced entropies $\{S_X(\rho)\}_{X \subseteq N}$ are the components of the entropy allocation $\vec{S}(\rho)$. Thus the entropy allocations are vectors in R^{2^n-1}.

Definition: A_n**.**

Let $A_n \subseteq R^{2^n-1}$ denote the set of entropy allocations for n particle mixed quantum states.

7.2.2 Convex cones.

Definition: Convex cones.

Let Ω be a set of vectors in R^{2^n-1}. Ω is a convex cone if and only if the following two conditions are met.

$$\forall X \in \Omega,\ \forall \lambda \in R,\ \lambda \geq 0 \Rightarrow\ \lambda X \in \Omega \tag{7.2.1}$$

$$\begin{aligned} \forall X \in \Omega,\ \forall Y \in \Omega,\ \forall \lambda \in R;\ 0 \leq \lambda \leq 1 \\ \Rightarrow\ \lambda X + (1 -\ \lambda) Y \in \Omega. \end{aligned} \tag{7.2.2}$$

Theorem.

Let $\bar{A}_n$ denote the topological closure of A_n, i.e the smallest closed set containing every element of A_n. Then $\bar{A}_n$ is a convex cone [132].

This is a remarkable result: It means that if we can find states corresponding to the extreme rays of B_n then by convexity we may achieve any interior point, and approach any point on the boundary to arbitrarily close precision.

7.2.3 Entropy inequalities.

Recall that our aim is to find the constraints on the reduced entropies. Some of these constraints are imposed by SSA. For an n particle quantum system there are various ways of applying SSA, and it is possible to simply write these out by hand

for low numbers of particles. However Pippinger has provided a recipe for generating all of the inequalities as described below.

For technical simplicity weak monotonicity is used as well as SSA, although they are actually equivalent. Suppose $N = \{1, ..., n\}$ and $I,\ J \subseteq N$. Let $I \backslash J$ denote the set of elements that are in I but not in J. Then SSA and WM become

$$S_I(\rho) + S_J(\rho) - S_{I \cup J}(\rho) - S_{I \cap J}(\rho) \geq 0, \tag{7.2.3}$$

$$S_I(\rho) + S_J(\rho) - S_{I \backslash J}(\rho) - S_{J \backslash I}(\rho) \geq 0. \tag{7.2.4}$$

Pippinger [132] provides an algorithm for ensuring that every possible distinct application of these inequalities is achieved. Let $i, j, k = 1, 2, ..., n$. Distinguish instances of SSA where

$$I \backslash J = \{i\},\ J \backslash I = \{j\},\ \text{and } i < j, \tag{7.2.5}$$

and distinguish instances of WM when

$$I \cap J = \{k\},\ I \cup J = N,\ \text{and } k + 1 \in I, \tag{7.2.6}$$

where $k + 1 = 1$ if $k = n$. This algorithm ensures that each possible distinct application of SSA and WM is considered. The combined set of all the distinguished inequalities is also a minimal set in the sense that no equation in this set may be deduced from the others.

Definition: B_n**.**

The set of all the distinguished entropy inequalities describe a cone in $R^{2^n - 1}$ which we label B_n.

We know that $\bar{A}_n \subseteq B_n$, however if $\bar{A}_n \subset B_n$ there must be some other constraints on the reduced entropies of a multipartite quantum system in addition to SSA. We

will go on to enumerate all of the extreme rays of B_2, B_3 and B_4. We note that Pippinger [132] found that for a special case of weakly symmetric states, defined by having reduced entropies which depend only on the number of parties in the partition, then $\bar{A}_n = B_n \; \forall n$.

7.3 The structure of A_n.

$\bar{A}_n$ is a convex cone, contained as a subset of B_n. This means that if we can find states corresponding to all of the extreme rays of B_n this is enough to prove $\bar{A}_n = B_n$. This in turn means that we have necessary and sufficient conditions for a state to exist corresponding to any set of reduced entropies - at least up to arbitrarily good approximation.

To describe B_n we used Pippinger's algorithm to generate the complete set of bounding inequalities. Finding the extreme rays of B_n is then a convex hull problem. There are several well known algorithms for enumerating the extreme rays of a polyhedra; we used *Mathematica* [134] and *lrs* [101].

The following sections describe the results of the calculations for two, three and four particle systems. The results for two and three particles appeared previously in [132]. We include the calculations here as they provide a useful background to the generalizations made in the section on four particle systems. They confirm the validity of the algorithms used, and are rather simpler than the original proofs. We also used these results to draw conclusions about MREGS for three and four particles, as discussed in section 7.6.

Two party mixed states.

We wish to find the extreme rays of B_2. To do this we write out the complete list of entropy inequalities, which in this simple case just result from subadditivity. We use *lrs* and *Mathematica* to compute the extreme rays of the polyhedral cone. We find that the three extremal entropy allocation vectors of B_2 may each be generated

by singlets held between two of the parties, and conclude that $\bar{A}_2 = B_2$. This means that satisfying subadditivity is a necessary and sufficient condition on the set of reduced entropies for a corresponding state to exist that produces this set of reduced entropies up to arbitrarily close approximation.

7.3.1 Three party mixed states.

For the situation of three party mixed states the entropy allocation vectors $\vec{S}$ have components $S_1, S_2, S_3, S_{12}, S_{13}, S_{23}, S_{123}$. The complete set of entropy inequalities from SSA and WM was produced using Pippinger's algorithm. This set of constraints, which bounds B_3, is given by $\mathcal{A}.\vec{S} \geq 0$, where

$$\mathcal{A} = \begin{pmatrix} 1 & 1 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 1 & 1 & -1 \\ 1 & 0 & 1 & 0 & -1 & 0 & 0 \\ 0 & -1 & 0 & 1 & 0 & 1 & -1 \\ 0 & 1 & 1 & 0 & 0 & -1 & 0 \\ -1 & 0 & 0 & 1 & 1 & 0 & -1 \\ 1 & 0 & 0 & 0 & 0 & -1 & 1 \\ 0 & -1 & -1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & -1 & 0 & 1 \\ -1 & 0 & -1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 & 1 \\ -1 & -1 & 0 & 0 & 1 & 1 & 0 \end{pmatrix} \tag{7.3.1}$$

Using *lrs* and *Mathematica* we find eight extremal of rays B_3, given by the rows of $\mathcal{B}$.

$$\mathcal{B} = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 2 & 2 & 2 & 1 \end{pmatrix} \tag{7.3.2}$$

We now identify states which produce each of these entropy allocation vectors. As we are dealing with mixed states we may consider the states to be pure between four parties, labelled A, B, C and D. The first six entropy allocations in $\mathcal{B}$ correspond to singlets, for example, shared between A-B, B-C, B-D, A-D, A-C and C-D respectively. The seventh entropy allocation corresponds to a four party GHZ.

$$|GHZ\rangle_4 = \frac{1}{\sqrt{2}}(|0000\rangle + |1111\rangle). \tag{7.3.3}$$

The eighth entropy allocation corresponds to a maximally entangled 4-party state;

$$|ME\rangle_4 = \frac{1}{3}\sum_{i,j=0}^{2} |i\rangle|j\rangle|i+j \bmod (3)\rangle|i+2j \bmod (3)\rangle. \tag{7.3.4}$$

$$\begin{aligned} |ME\rangle_4 = \frac{1}{3}(&|0000\rangle + |0112\rangle + |0221\rangle \\ &+|1011\rangle + |1120\rangle + |1202\rangle \\ &+|2022\rangle + |2101\rangle + |2210\rangle). \end{aligned} \tag{7.3.5}$$

We conclude that $\bar{A}_3 = B_3$, i.e that SSA and WM are necessary and sufficient conditions on the set of reduced entropies for a corresponding state to exist that produces this set of reduced entropies up to arbitrarily close approximation.

7.3.2 Four party mixed states.

Pippinger's algorithm produces forty distinct inequalities for the four party case. These describe a polyhedral cone in fifteen dimensions, with each entropy allocation vector having components S_1, S_2, S_3, S_4, S_{12}, S_{13}, S_{14}, S_{23}, S_{24}, S_{34}, S_{123}, S_{124}, S_{134}, S_{234}, S_{1234}. As before a numerical computation found the extreme rays.

Because we are considering mixed states we may imagine a pure five part system labelled A,...,E. Of the total of seventy six extremal rays, 10 are singlets, and five are GHZ_4. There is also a GHZ_5 shared between all five parties.

$$|GHZ\rangle_5 = \frac{1}{\sqrt{2}}(|00000\rangle + |11111\rangle). \tag{7.3.6}$$

There are 5 states of the 4-party maximally entangled state, for example

$$|ME\rangle = \frac{1}{3}\sum_{i,j=0}^{2} |i\rangle_A |j\rangle_B |i+j \bmod (3)\rangle_C |i+2j \bmod (3)\rangle_D |0\rangle_E. \tag{7.3.7}$$

For states with entropy allocation vectors of the form

$$\vec{S} = (1,1,1,1,2,2,2,2,2,2,3,3,3,3,2), \tag{7.3.8}$$

there are 5 permutations. To construct a state corresponding to this we will use error correcting codes: Let $|0L\rangle^5$ and $|1L\rangle^5$ be be the logical 0 and 1 for the 5 qubit error correcting codes [97]. i.e

$$\begin{aligned} |0L\rangle^5 = \frac{1}{4}(&|00000\rangle + |10010\rangle + |01001\rangle + |10100\rangle \\ &+|01010\rangle - |11011\rangle - |00110\rangle - |11000\rangle \\ &-|11101\rangle - |00011\rangle - |11110\rangle - |01111\rangle \\ &-|10001\rangle - |01100\rangle - |10111\rangle + |00101\rangle), \end{aligned} \tag{7.3.9}$$

$$|1L\rangle^5 = \frac{1}{4}(|11111\rangle + |01101\rangle + |10110\rangle + |01011\rangle \tag{7.3.10}$$
$$+|10101\rangle - |00100\rangle - |11001\rangle - |00111\rangle$$
$$-|00010\rangle - |11100\rangle - |00001\rangle - |10000\rangle$$
$$-|01110\rangle - |10011\rangle - |01000\rangle + |11010\rangle).$$

Then the following state has the required reduced entropies.

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|0L\rangle^5_{BCDE} + |1\rangle_A|1L\rangle^5_{BCDE}), \tag{7.3.11}$$

where each of the parties A, B, C, D has one qubit and E has two. For states with entropy allocation vectors of the form

$$\vec{S} = (1, 1, 2, 2, 2, 3, 3, 3, 3, 2, 2, 2, 3, 3, 2) \tag{7.3.12}$$

there are 10 permutations. Again we can find a corresponding states based on error correcting codes. Let $|0L\rangle^7$ and $|1L\rangle^7$ be be the logical 0 and 1 for the 7 qubit error correcting codes [97]. i.e

$$|0L\rangle^7 = \frac{1}{\sqrt{8}}(|0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle \tag{7.3.13}$$
$$+|0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle),$$

$$|1L\rangle^7 = \frac{1}{\sqrt{8}}(|1111111\rangle + |0101010\rangle + |1001100\rangle + |0011001\rangle \tag{7.3.14}$$
$$+|1110000\rangle + |0100101\rangle + |1000011\rangle + |0010110\rangle).$$

Then the following state has the required reduced entropies.

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|0L\rangle^7_{BCDE} + |1\rangle_A|1L\rangle^7_{BCDE}), \tag{7.3.15}$$

where each of the parties A, B has one qubit and C, D, E have two. This accounts for 36 of the 76 extremal rays. Of the remaining extremal entropy allocations 30 are permutations of

$$\vec{S}_1 = (3, 3, 3, 3, 6, 4, 4, 4, 4, 4, 5, 5, 5, 5, 2), \tag{7.3.16}$$

and 10 are permutations of

$$\vec{S}_2 = (2, 2, 2, 3, 4, 4, 3, 4, 3, 3, 4, 3, 3, 3, 3). \tag{7.3.17}$$

Based on the other states corresponding to extreme rays it was tempting to think that these entropy allocations might be achieved for states of 14 and 12 qubits, grouped amongst the 5 parties A,...,E. However considering the classical analogue of the entropy inequalities led us to conjecture that these entropy allocations can not be achieved for any quantum state. The evidence for this is discussed in the following section. Whilst the arguments are not conclusive, the conjecture has turned out to be correct, and it has subsequently been shown by Linden and Winter [128] that no quantum state exists with entropy allocation vectors $\vec{S}_1$ or $\vec{S}_2$.

7.4 The classical analogy.

In this section we review the classical analogy of the entropy inequalities. Yeung and Zhang have discovered a new inequality (Y-Z inequality), inequivalent to classical SSA and SM. We show that entropy allocations $\vec{S}_1$ and $\vec{S}_2$ violate a quantum version of this inequality. Furthermore, all of the entropy allocations for which we succeeded in finding corresponding states do not violate this new inequality. We also show that the quantum Y-Z inequality is true for pure states.

In the classical setting we are now concerned with entropy allocation vectors for probability distributions in n independent random variables. The components of the entropy allocation vectors are given by the Shannon entropies. Yeung and

Zhang have shown that classical SSA and strong monotonicity are insufficient to characterize the space of reduced entropies for systems of four or more random variables. They did this by deriving a new entropy inequality, which we discuss below.

Definition: $\vec{H}(X)$**.**

Here we give the formal definitions of the classical entropy allocation $\vec{H}(X)$. This is of the same form as the quantum state entropy allocations, but with the reduced von Neumann entropies replaced by Shannon entropies. Let $X = (X_1, ..., X_n)$ be an n-component random variable and $N = \{1, ..., n\}$. For $I \subseteq N$, let X_I denote the random variable formed by tracing over the variables not in I. For each $I \subseteq N$ we may associate an entropy $H_I(X) = H(X_I)$, where $H(X)$ is the Shannon entropy defined as follows: Let p_x be the probability $\Pr(X = x)$, then

$$H(X) = -\sum_x p_x \mathrm{Log}\, p_x. \tag{7.4.1}$$

The collection of entropies $\{H_I(X)\}_{I \subseteq N}$ is the entropy allocation. Thus the entropy allocations are vectors in R^{2^n-1}.

Definition: A_n^c**.**

Let $A_n^c \subseteq R^{2^n-1}$ denote the set of classical entropy allocations for n component probability distributions.

Theorem.

Yeung and Zhang [137] have shown that $\bar{A}_n^c$ is a convex cone, where $\bar{A}_n^c$ is the topological closure of A_n^c.

Polymatroid inequalities.

Polymatroid inequalities are the classical equivalent of the SSA and WM inequalities. Suppose $N = \{1, ..., n\}$ and $I,\ J \subseteq N$. Classical SSA becomes

$$H_{I\cup J}(X) + H_{I\cap J}(X) \leq H_I(X) + H_J(X). \tag{7.4.2}$$

Let $I\backslash J$ denote the set of elements that are in I but not in J. Strong monotonicity (SM) gives

$$H_{I\backslash J}(X) \leq H_I(X). \tag{7.4.3}$$

Definition: B_n^c.

By applying every possible instance of these inequalities we obtain a convex cone B_n^c.

Yeung and Zhang have shown that $\bar{A}_n^c \neq B_n^c$ for $n \geq 4$. They did this by constructing a new inequality, which can not be deduced from the polymatroid inequalities.

The Yeung-Zhang inequality.

For a system of four independent random variables X_1, X_2, X_3 and X_4 Yeung and Zhang derived the following inequality

$$I(X_1; X_2) + I(X_1; X_3, X_4) + 3I(X_3; X_4|X_1)$$

$$+I(X_3; X_4|X_2) - 2I(X_3; X_4) \geq 0.$$

Where $I(X, Y)$ is the mutual information for independent random variables X and Y. We will expand the terms so that the inequality is given in terms of the Shannon entropies. We have the following definitions

$$I(X_1;X_2) = H(X_1) - H(X_1|X_2) = H(X_1) + H(X_2) - H(X_1,X_2), \tag{7.4.4}$$

$$I(X_1;X_3,X_4) = I(X_1;X_3) + I(X_1;X_4|X_3), \tag{7.4.5}$$

$$\begin{aligned} I(X_1;X_4|X_3) &= H(X_1|X_3) - H(X_1|X_4,X_3) \\ &= H(X_1,X_3) - H(X_3) - H(X_1,X_3,X_4) + H(X_3,X_4). \end{aligned} \tag{7.4.6}$$

Expanding the terms gives

$$-H_1 - 2H_3 - 2H_4 - H_{12} + 3H_{13} + 3H_{14} + H_{23} + H_{24} + 3H_{34} - 4H_{134} - H_{234} \geq 0 \tag{7.4.7}$$

We define the quantum version of this inequality by replacing the Shannon entropies H_I with reduced von Neumann entropies S_I. We can make the following remarks about the quantum analogue of the Y-Z inequality.

The Quantum Y-Z inequality is true for pure states.

We do not presently know whether the quantum version of the Y-Z inequality is true in general. We can however perform a check where we consider pure states, and show that the quntum Y-Z inequality for four party pure states is a consequence of SSA. Any three party state satisfies strong subadditivity and weak monotonicity. In particular

$$-S_3 + S_{13} + S_{23} - S_{123} \geq 0 \tag{7.4.8}$$

$$-S_2 + S_{12} + S_{23} - S_{123} \geq 0 \tag{7.4.9}$$

$$-S_2 - S_3 + S_{12} + S_{13} \geq 0 \tag{7.4.10}$$

$$-2S_1 - 2S_2 + 2S_{13} + 2S_{23} \geq 0. \tag{7.4.11}$$

Summing these inequalities implies

$$-2S_1 - 4S_2 - 2S_3 + 2S_{12} + 4S_{13} + 4S_{23} - 2S_{123} \geq 0. \tag{7.4.12}$$

Now we may always consider a three party mixed state as a pure state of four parties. For this state $S_1 = S_{234}$ etc so we may expand (7.4.12) as

$$-S_1 - 2S_3 - 2S_4 - S_{12} + 3S_{13} + 3S_{14} + S_{23} + S_{24} + 3S_{34} - 4S_{134} - S_{234} \geq 0. \tag{7.4.13}$$

This is the quantum analogue of the Y-Z inequality (7.4.7).

Extreme rays of B_4 and the quantum Y-Z inequality.

The two entropy allocation vectors $\vec{S}_1$ and $\vec{S}_2$ for which we have been unable to find corresponding states are precisely those which violate (7.4.13). Substituting the entropy values in $\vec{S}_1$ (7.3.16) into (7.4.13) gives -2, a violation of the inequality. To see that $\vec{S}_2$ (7.3.17) gives a violation of the quantum Y-Z inequality we need to take a permutation of (7.4.13) where we have renamed the parties as follows;

$$A \to A,\ B \to B,\ C \to D,\ D \to E,\ E \to C. \tag{7.4.14}$$

The inequality then reads

$$-S_1 - 2S_4 - S_{12} - S_{13} + 3S_{14} - 4S_{23} + S_{24} + 3S_{123} + S_{134} + 3S_{234} - 2S_{1234} \geq 0, \tag{7.4.15}$$

and this inequality is violated by $\vec{S}_2$.

We also checked that all of the extreme rays for which we could find corresponding states did not violate the new inequality, or any version of the new inequality with the particle names permuted.

These observations allowed us to conjecture that states corresponding to $\vec{S}_1$ or $\vec{S}_2$ do not exist. This has subsequently been proven [128]. This opens the possibility that there may be new quantum entropy inequalities, along the lines of the Yeung Zhang inequality.

7.5 The entropies of a three qubit pure state.

In the above section we demonstrated that $\bar{A}_2 = B_2$. Now we may always imagine a mixed state of two particles as a pure state of three particles. We may therefore interpret this result as demonstrating that for three party pure states if we are given a list of reduced entropies, we know whether or not a closely corresponding state exists. This state is subject to no constraints however, and in particular is allowed to be of any dimension. In fact the only constraints on the reduced entropies come from subadditivity. Here we consider a different type of restriction on the possible reduced entropies of a state. Often systems associated with Quantum Information protocols can be described by qubit states, and in this section we consider a restriction to pure three party qubit states. In the previous unrestricted case the reduced entopies belonged to an open cone, and we would like to know how this region of allowed entropies is further confined by the new restriction. For example, the reduced entropies are now bounded above by 1, so the allowed region is now bounded by a closed polygon. In fact we find that there are also further restrictions on the allowed reduced entropies as shown below.

The entropy inequalities applicable to this situation are

$$S_1 + S_2 - S_3 \geq 0 \tag{7.5.1}$$

$$S_1 - S_2 + S_3 \geq 0 \tag{7.5.2}$$

$$-S_1 + S_2 + S_3 \geq 0. \tag{7.5.3}$$

A recent paper by Sudbery *et al* [135, 136] characterizes qubit states in an alter-

native way. This characterization is based on the eigenvalues of the reduced states of the system, and provides necessary and sufficient conditions for a qubit state with a given list of reduced state eigenvalues to exist. These conditions are based on the satisfaction of a set of *polygon inequalities*.

For a pure state ρ_{123} of three parties, let λ_1, λ_2, and λ_3 be the smallest eigenvalues of ρ_1, ρ_2 and ρ_3 respectively. Then the necessary and sufficient conditions on the $\lambda' s$ to characterize the reduced density matrices for three party states are the following polygon inequalities:

$$\begin{aligned} \lambda_1 &\leq \lambda_2 + \lambda_3 \\ \lambda_2 &\leq \lambda_1 + \lambda_3 \\ \lambda_3 &\leq \lambda_1 + \lambda_2. \end{aligned} \tag{7.5.4}$$

We require each λ to be greater than or equal to zero. Because these are the smallest eigenvalues λ_1, λ_2, $\lambda_3 \leq \frac{1}{2}$.

This eigenvalue description is related to the reduced entropies as follows: Let $S(\lambda)$ be defined as

$$S(\lambda) = -\lambda \operatorname{Log}(\lambda) - (1-\lambda)\operatorname{Log}(1-\lambda) \tag{7.5.5}$$

so that $S_i(\rho) = S(\lambda_i)$.

This characterization implies subadditivity is satisfied. If $\lambda_2 + \lambda_3 \leq \frac{1}{2}$ then $S(\lambda_2 + \lambda_3)$ is monotonic and hence

$$S(\lambda_1) \leq S(\lambda_2 + \lambda_3) \leq S(\lambda_2) + S(\lambda_3). \tag{7.5.6}$$

The last inequality comes from concavity of the entropy. If $\lambda_2 + \lambda_3 > \frac{1}{2}$ then $S_2 + S_3 \geq 1$ and since $S_1 \leq 1$ this implies subadditivity.

The converse is not true, i.e satisfaction of subadditivity (7.5.1)-(7.5.3) does not imply satisfaction of the polygon inequalities (7.5.4). For example $S_1 = 1$, $S_2 = 0.5$, $S_3 = 0.5$ satisfies the entropy inequalities (7.5.1)-(7.5.3), but the corresponding

eigenvalues $\lambda_1 = 0.5$, $\lambda_2 = 0.11$, $\lambda_3 = 0.11$ violate the polygon inequalities, showing there is no qubit state with these reduced entropies. Other regions are also unobtainable. Suppose $S_1 = S_2 + S_3$; a plane in the three dimensional space. We can show only the lines $S_1 = S_2$ and $S_1 = S_3$ are obtainable.

$$S_1 = S_2 + S_3 \Rightarrow \qquad (7.5.7)$$
$$\lambda_1 = S^{-1}(S(\lambda_2) + S(\lambda_3)).$$

From concavity we have $S^{-1}(S(\lambda_2) + S(\lambda_3)) \geq \lambda_2 + \lambda_3$ with equality if and only if $\lambda_2 = 0$ or $\lambda_3 = 0$, i.e if $S_2 = 0$ or $S_3 = 0$.

It is not known how the set of allowed entropy allocations is restricted for qubits in general. For a projection to two dimensions, where we consider the ratios of the reduced entropies, we have the following results: We may achieve any point in this new space to arbitrary precision, though not every point exactly. This is shown in the following section.

Entropy Ratios.

We consider ratios of the reduced entropies. Define the new variables $Y = S_3/S_1$ and $X = S_2/S_1$ for $S_1 \neq 0$. Without loss of generality we can ensure that this last condition is met for generic states by requiring that

$$S_1 \geq S_2, \ S_1 \geq S_3. \qquad (7.5.8)$$

$S_1 = 0$, and hence $S_2 = 0$ and $S_3 = 0$, only if the state is a product state. This also gives the following ordering condition on the eigenvalues of the reduced states.

$$\lambda_1 \geq \lambda_2, \ \lambda_1 \geq \lambda_3. \qquad (7.5.9)$$

The set (X, Y) allowed by subadditivity is now bounded by a triangle with vertices (0,1), (1,0) and (1,1), i.e

$$\begin{aligned} X + Y &\geq 1, \\ X &\leq 1, \\ Y &\leq 1. \end{aligned} \tag{7.5.10}$$

The vertices correspond to a product state of one party verses an entangled state of the other two, and for example, a GHZ state at (1,1). The W state is also at this vertex. As a consequence of our earlier result that $S_1 = S_2 + S_3 \Rightarrow S_1 = S_2$ or $S_1 = S_3$ no qubit system can achieve the line $Y = -X + 1$ unless $X = 0$ or $X = 1$.

Although there is a line of inaccessible relative entropies ratios, we can in fact generate any point in the space to arbitrary precision using a very restricted subset of possible states - states that are an arbitrarily small distance from product states. Let $\mathcal{L}(X, Y)$ be the set of (X, Y) which can actually be achieved to arbitrary precision for two dimensional quantum states. We can choose to write

$$\lambda_1 = \frac{1}{\epsilon}\lambda_2, \tag{7.5.11}$$

$$\lambda_1 = \frac{1}{\delta}\lambda_3, \tag{7.5.12}$$

for some $\epsilon,\ \delta \in R_{>0}$. The conditions on the eigenvalues to be consistent with a qubit state are $\lambda_1 \geq \lambda_2$ and $\lambda_1 \geq \lambda_3$ and $\lambda_1 \leq \lambda_2 + \lambda_3$. These are implied directly by the following conditions on ϵ and δ.

$$\begin{aligned} \epsilon + \delta &\geq 1, \\ \epsilon &\leq 1, \\ \delta &\leq 1. \end{aligned} \tag{7.5.13}$$

Now,

$$\frac{S(\lambda_2)}{S(\lambda_1)} = \frac{-\lambda_2 \operatorname{Log} \lambda_2 - (1-\lambda_2) \operatorname{Log} (1-\lambda_2)}{-\frac{\lambda_2}{\epsilon} \operatorname{Log} \frac{\lambda_2}{\epsilon} - (1-\frac{\lambda_2}{\epsilon}) \operatorname{Log} (1-\frac{\lambda_2}{\epsilon})}, \tag{7.5.14}$$

$$\frac{S(\lambda_3)}{S(\lambda_1)} = \frac{-\lambda_3 \operatorname{Log} \lambda_3 - (1-\lambda_3) \operatorname{Log} (1-\lambda_3)}{-\frac{\lambda_3}{\delta} \operatorname{Log} \frac{\lambda_3}{\delta} - (1-\frac{\lambda_3}{\delta}) \operatorname{Log} (1-\frac{\lambda_3}{\delta})}. \tag{7.5.15}$$

If we take the limits of these functions we find that $\lim_{\lambda_2 \to 0} \frac{S_2}{S_1} = \epsilon$, and similarly $\lim_{\lambda_3 \to 0} \frac{S_3}{S_1} = \delta$. These limits mean that the state is approaching a product state. Thus $\mathcal{L}(X, Y) \cong (\epsilon,\ \delta)$ where ϵ and δ obey exactly the conditions on the entropy ratios (7.5.10).

7.6 Extreme rays of $\bar{A}_n$ and MREGS.

In this section we show how considering the extreme rays of $\bar{A}_n$ allows us to conclude that certain sets of states must belong to the $n+1$ particle MREGS. The essential idea is that the extreme rays of $\bar{A}_n$ are a basis for the space of entropy allocation vectors because the space is convex. For two states to be asymptotically reversibly convertible to one another their reduced entropies must be the same, hence states giving the basis vectors for the space of entropy allocation vectors must be included in MREGS. We show that considerations of reduced entropies mean that a certain set of states must belong to the three and four particle MREGS.

Pure states and mixed states.

The above results on $\bar{A}_n$ and B_n all refer to n part mixed states, but the concept of an MREGS is only valid for pure states. However we can use the following well known results to convert between the spaces of entropy allocations for pure and mixed states. The first result is that for a pure state ψ_{12}, $S_1(\psi) = S_2(\psi)$. The second is that for any density matrix ρ_1 there exists a purification to a pure state ρ_{12} such that $\rho_1 = \mathrm{Tr}_2\, \rho_{12}$.

Lemma.

These results mean that if a mixed state is an extreme ray of $\bar{A}_n$ then its purification will be an extreme ray of the space of entropy allocations for pure states of $n+1$ particles.

A more detailed description of MREGS was given in the previous chapter, in section 6.4, however we begin by recalling that the crucial concept in MREGS is that of asymptotic reducibility between two states, and that given a set of states $\mathcal{G} = \{\psi_1, \psi_2, ..., \psi_t\}$, their entanglement span $\mathrm{Sp}(\mathcal{G})$ is the set of states that $\mathcal{G}$ can generate reversibly under asymptotic LOCC. i.e

$$\mathrm{Sp}(\mathcal{G}) = \{\psi \,|\, \psi \approx \bigotimes_{i=1}^{t} |\psi_i\rangle^{\otimes x_i},\ x_i \geq 0\}. \tag{7.6.1}$$

The set of x_i are entanglement coefficients, which are not unique in general. A set of minimal cardinality able to generate the full class of m party states is an MREGS, which we denote by $\mathcal{G}_m$. We will now show how characterizing $\bar{A}_n$ allows us to conclude that certain states must belong to MREGS. First we need the following definitions.

Definition: isentropic.

states ρ and σ (mixed) are *isentropic* if and only if $\vec{S}(\rho) = \vec{S}(\sigma)$.

Definition: scaled isentropic.

states ρ and σ (mixed) are *scaled isentropic* if and only if $\vec{S}(\rho) = \lambda\vec{S}(\sigma)$ for some real λ.

Theorem.

If $\exists$ a pure state $|\psi\rangle$ of n particles s.t $\vec{S}(\psi)$ is an extreme ray of $\bar{A}_{n-1}$, then a state scaled isentropic to $|\psi\rangle$ is in $\mathcal{G}_n$.

Proof.

Recall that $\bar{A}_{n-1}$ is the closure of the set of entropy allocation vectors for mixed $n-1$ part states, or equivalently pure n part states. Now for two states ϕ and ψ to be asymptotically reducible they must have the same reduced entropies [115] ,

$$\phi \approx \psi \;\Rightarrow\; S_X(\phi) = S_X(\psi)\ \forall X \subseteq N \tag{7.6.2}$$

$$\Rightarrow\; \vec{S}(\phi) = \vec{S}(\psi). \tag{7.6.3}$$

In particular

$$\phi^{\otimes x} \approx \psi^{\otimes y} \;\Rightarrow\; x\, S_X(\phi) = y\, S_X(\psi)\ \forall X \subseteq N \tag{7.6.4}$$

$$\Rightarrow\; x\, \vec{S}(\phi) = y\, \vec{S}(\psi). \tag{7.6.5}$$

Suppose $\mathcal{G}_n = \{\mu_1, \mu_2, ..., \mu_w\}$. Now for any state $|\rho\rangle \in \mathrm{Sp}(\mathcal{G}_n)$

$$\vec{S}(\rho) = \sum_i x_i\, \vec{S}(\mu_i),\ x_i \in R_{\geq 0}. \tag{7.6.6}$$

Let $\{\chi_1, \chi_2, ..., \chi_s\}$ be a set of states so that each χ_i produces an entropy allocation vector which is a scaled isentropic to the ith extremal ray of $\bar{A}_{n-1}$. Suppose χ_i or any state scaled isentropic to χ_i were not in the MREGS $\mathcal{G}_n$. Therefore we know $\chi_i \notin \mathrm{Sp}(\mathcal{G}_n)$ because $\vec{S}(\chi_i)$ is an extreme ray, and hence $\mathcal{G}_n$ is not an MREGS. □

MREGS for three and four particles.

In the previous sections we found states corresponding to the extreme rays of $\bar{A}_n$ for $n = 2, 3$. Here we summarize the implications of this for the three and four party MREGS.

We found that the extreme rays of B_2 corresponded to three pairs of singlets shared between the parties. We conclude that this analysis based on reduced entropies gives a MREGS for three party states which must include states scaled isentropic to $|\psi_-\rangle_{AB}$, $|\psi_-\rangle_{AC}$ and $|\psi_-\rangle_{BC}$. This result was found in by Linden *et al* [**?**].

By enumerating the extreme rays of B_3 and finding a state corresponding to each extreme ray we conclude that a state scaled isentropic to each element of the set

$$\{6 \times |\psi_-\rangle, |GHZ_4\rangle, |ME\rangle_4\} \tag{7.6.7}$$

must be included in $\mathcal{G}_4$.

Arguments based on reduced entropies provide a 'lower bound' on the size of $\mathcal{G}_n$ but we already know that these are not sufficient conditions because of the stronger considerations of relative entropy of entanglement. For example, an argument based only on reduced entropies shows that $\mathcal{G}_3$ must contain singlets. However by showing that the relative entropy of entanglement between two states must remain constant during any reversible transformation Linden *et al* [**?**] demonstrated that the GHZ state can not be generated reversibly under asymptotic LOCC by just these singlets.

The next conjecture, that

$$\mathcal{G}_3 = \{3 \times |\psi_-\rangle, |GHZ\rangle\} \tag{7.6.8}$$

constitutes the three particle MREGS, was disproved by Acin, Vidal and Cirac [138].

Moving on to the four party MREGS, the situation is even less clearly understood. The conjecture that $\mathcal{G}_4 = \{6 \times |\psi_-\rangle, 4 \times |GHZ\rangle_3, |GHZ\rangle_4\}$ is an MREGS for four party pure states was disproved by Wu and Zhang [139] (again using relative entropy of entanglement). They found that the state

$$|\psi\rangle = \frac{1}{2}(|0000\rangle + |0110\rangle + |1001\rangle - |1111\rangle) \tag{7.6.9}$$

can not be generated by $\mathcal{G}_4$ by asymptotically reversible LOCC.

7.7 Conclusion.

In this chapter we considered different types of restrictions on the space of reduced entropies of multipartite states. We know that for three or fewer particles SSA is necessary and sufficient condition on the reduced entropies that a closely corresponding quantum state exists. By considering the space of reduced entropies allowed by SSA

for four particles we conjecture that there are new inequalities, similar to the classical inequalities discovered by Yeung and Zhang, which further restrict this space. We also considered the restrictions imposed on the reduced entropies by requiring the Hilbert space of each particle to be two dimensional, i.e for qubit systems. Finally we showed how the space of allowed entropy allocations is related to MREGS. In particular we showed certain sets of states must belong to the three and four particle MREGS. We finish with some open questions.

Entropy inequalities.

For mixed states of two and three parties, the fact that we can find states corresponding to all of the extreme rays of B_2 and B_3 demonstrates that $\bar{A}_2 = B_2$, and $\bar{A}_3 = B_3$.

For four party mixed states the fact that there are extreme rays of $\bar{A}_4$ which can not be achieved by quantum states [128] supports the conjecture $\bar{A}_4 \neq B_4$, and this is of course the main open question remaining from this work. In general the issue of whether $A_n = \bar{A}_n$ remains open, but we can note Yeung and Zhang have shown that classically $A_n^c \neq \bar{A}_n^c$ for $n \geq 3$.

For classical random variables Yeung and Zhang have *not* claimed that their new inequality, combined with SSA and SM completely characterizes the space of reduced entropies, even for 4 particles. i.e let C_n^c be the space of entropy allocations bounded by the complete set of SSA, SM, and all distinct applications of the Y-Z inequality. Then it is not presently known if $\bar{A}_n^c = C_n^c$ for $n \geq 4$.

Similarly, in the quantum setting even if we take the quantum version of the Y-Z inequality and use it to further restrict the space B_n to a new space C_n, we do not know the relationship between $\bar{A}_n$ and C_n.

One possible avenue for future work is to consider a slightly different question: Given the largest set of rays for which we know corresponding quantum states exist, what is the set of bounding inequalities? In this way it may be possible to guess the form of new inequalities which provide sufficient conditions for states with a given

entropy allocation to exist.

MREGS.

We have shown how consideration of the space of reduced entropies allows us to conclude that a certain set of states must belong to the MREGS. This argument is quite general and is independent of the issue of whether $\bar{A}_n = B_n$. By finding the extreme rays of $\bar{A}_n$ for the specific cases $n = 2, 3$ we were able to conclude that certain states must be included in the 3 and 4 particle MREGS. While the arguments given in this chapter can give a 'lower bound' on MREGS, they certainly do not represent a definitive classification. For example, it is not even known if $\mathcal{G}_3$ is finite. Also there are stronger constraints imposed by considering the relative entropy of entanglement.

7.8 Appendix C.

Strong subadditivity and weak monotonicity are in fact equivalent. To see this we use two well known facts: For any density matrix ρ_1 there exists a pure state ρ_{12} such that $\rho_1 = \mathrm{Tr}_2\, \rho_{12}$. Also if ρ_{12} is pure then $S(\rho_1) = S(\rho_2)$.

To show that SSA implies WM. For some ρ_{123} there is a purification ρ_{1234}. For this pure state

$$S(\rho_1) + S(\rho_2) = S(\rho_{234}) + S(\rho_2). \tag{7.8.1}$$

Now from SSA we have;

$$S(\rho_{234}) + S(\rho_2) \leq S(\rho_{23}) + S(\rho_{24}) = S(\rho_{23}) + S(\rho_{13}) \tag{7.8.2}$$

The result is WM. Now to show that WM implies SSA; For some ρ_{123} there is a purification ρ_{1234}.

$$\begin{aligned} S(\rho_{123}) + S(\rho_3) &= S(\rho_4) + S(\rho_3) \\ &\leq S(\rho_{14}) + S(\rho_{13}) = S(\rho_{23}) + S(\rho_{13}). \end{aligned}$$

This is strong subadditivity. □

Chapter 8

Conclusion.

Summary and future directions.

In this thesis I have tried to understand different aspects of quantum non-locality, particularly for multipartite systems. If we perform experiments on quantum systems then a signature of non-locality is violation of a Bell inequality. These were the subject of the first part of this thesis. In particular, I considered Bell type inequalities that reveal not just non-locality, but a more specific type of non-local correlation that must involve every single particle in a system. This was an idea first suggested by Svetlichny [1], and I give the generalization of his inequality for n particles. I showed that quantum mechanics exhibits this type of n-particle non-locality, by demonstrating that the GHZ states violate the generalized Svetlichny inequality.

If we imagine an abstract experiment, then regardless of the details, the information we hope to extract is a set of probabilities for different outcomes, conditionally on the measurement settings we may select. If we think in terms of these probability distributions then Bell inequalities describe the boundaries between the probability distributions which are local, and those which are non-local. Quantum mechanics famously produces non-local correlations, but can not be used for super-luminal

communication. In understanding this quantum non-locality it is interesting to consider why the correlations obtainable are not 'more non-local' than quantum mechanics predicts. We might imagine that the restriction that we can not use spacially separated states to signal would mean only a limited form of non-locality was allowed. Whilst a no-signalling constraint does restrict the space of allowed probability distributions, it still allows sets of correlations which are more non-local than quantum mechanics. This was first noted by Popescu and Rohrlich who concluded that quantum mechanics is only one of a class of non-local theories consistent with causality [86].

The second part of this thesis concerns this class of non-local theories. We aim to shed light on why quantum mechanics does not allow these more powerful correlations by placing them within this wider context.

The non-local nature of quantum mechanics is a consequence of the possibility of *entangled* states. For bi-partite states the nature of this entanglement is reasonably well understood, but for multipartite systems we only have a very limited understanding at present. A possible approach to this problem is to use a concept that has proved very successful in the bi-partite case - the reduced von Neumann entropy - and apply it in the multipartite setting. Then will now be several ways of making a bi-partite division of the state, and so our measure of entanglement will be a vector - the *entropy allocation.*

The third subject of this thesis concerns these entropy allocations. By analyzing the structure of the space of allowed entropies we aim to better understand the constraints on the reduced entropies. In particular this approach allows us to place a 'lower bound' on the fundamentally inequivalent types of multipartite entanglement by showing certain sets of states must belong to MREGS, the minimal reversible entanglement generating set.

In the following paragraphs I outline in more detail the results found in these three areas of study. In each case I also suggest some open questions remaining from this work, and possible avenues for future research.

Multipartite Bell inequalities.

Bell inequalities allow us to distinguish between local and non-local correlations. However as Svetlichny first discovered [1], in a multipartite setting we can make more subtle distinctions. We may imagine that the correlations in a system could be described by a number of non-local subsystems, but with only local correlations present between the subsystems themselves. Svetlichny produced an inequality for three parties that is able to distinguish the case of *genuine* three party non-locality from weaker forms.

In chapter 3 we revisited Svetlichny's inequality. Experiments to produce three particle entangled states have only recently been achieved [67, 68]. Although quantum mechanics predicts Svetlichny's inequality can be violated, we showed that the particular measurements performed in these experiments are such that they will not exhibit genuine three particle non-locality between the measurement outcomes. However we show that a simple modification to the experiments would make such a demonstration possible.

In chapter 4 we gave a generalization of Svetlichny's inequality for n particle systems. We show that for even number of particles the Mermin-Klysko (MK) inequality plays the role of the generalized Svetlichny inequality, and that for odd numbers of particles a simple modification to the MK inequality gives the generalized Svetlichny inequality.

The four particle GHZ state has recently been produced experimentally [77, 78]. Recently Zhao *et al* [79] have shown a violation of the generalized Svetlichny inequality for a four photon GHZ state by 76 standard deviations. This confirms four particle non-locality. Even more recently the same group have produced a five photon GHZ state [80], although they have not yet shown any Bell inequality violation for this state.

The set of Svetlichny inequalities is not complete in the sense that we do not have a set of inequalities which, if they are all satisfied, allow us to conclude that the

state exhibits only a limited form of non-locality. Rather we have only a sufficient condition to demonstrate genuine non-locality. This is in contrast to the situation where we are only concerned with whether a state exhibits *any* non-locality. In this case Werner and Wolf, and Zukowski and Bruckner [26, 27] have found a set of inequalities which are complete in the sense that the inequalities are satisfied if and only if the correlations permit a local hidden variable model (we consider only pure states). It would be interesting to achieve something similar for Svetlichny's notion of limited non-locality. This problem is essentially that of enumerating the facets of a convex hull. It is likely that this problem would be computationally tractable for three parties.

Non-local correlations as an information theoretic resource.

An interesting question one can ask is; why is quantum mechanics not *more* non-local than it is? With this in mind Chapter 5 presents a different, more abstract, notion of non-locality. We imagine that the source of non-local correlations is a box with a set of possible inputs. Each observer selects one of these inputs and receives an output. The box determines a joint probability for each set of outputs, given the inputs. A quantum state provides an example of such a box, with input corresponding to measurement settings and output to measurement outcome.

These boxes may be classified as signalling or non-signalling. In general our intention is to regard these boxes as an information theoretic resource. This is immediately clear in the case of the signalling boxes - They can be used to send a message. However these are ruled out by special relativity, so we confine our attention to the non-signalling boxes. This class of boxes can be further categorized as local or non-local. A local box is equivalent to shared random data, and so may be useful in some tasks. However, the most interesting cases are the non-local boxes. If we consider these boxes as an information theoretic resource we find that they are very powerful. For example, van Dam has found that they are able to solve communication complexity problems more efficiently than any quantum, or classical

strategy [102].

The set of non-signalling boxes has an interesting structure, and can be understood as a convex polytope. We can make several analogies between these non-local boxes and quantum mechanics. For example, we find there are analogies to monogamy of entanglement. We can make inter-conversion between boxes just as we can make inter-conversions between states.

There remain many open question arising from this work. In particular we may consider the following questions.

Vertices and Bell inequalities. For the polytope of two-input two-output boxes there was a one to one correspondence between the vertices of the polytope and the Bell inequalities which bound the region of local probability distributions. This relationship does not seem to hold in general however, and it would be interesting to establish the precise relationship.

New vertices. We do not yet have a complete characterization of the vertices if we allow more parties, inputs and outputs.

Inter-conversions. Understanding the types of inter-conversions that are possible between boxes is important to quantify their relative power as information theoretic resources. For the two party case we have considered quite a wide range of inter-conversions, but for the three party case we only considered a limited set of possible inter-conversions.

One non-local vertex seemed particularly important in these inter-conversions. This is the PR box [86]. We found that all of the correlations we considered could be constructed using these PR boxes. It is tempting to think of these boxes as the unit of non-local correlation, just as ebits are the units of quantum correlations. It would be interested to see if we can extend this analogy to cover all possible non-local correlations.

Interior points and distillation. We only considered inter-conversions between the vertices of the polytope of no-signalling correlations. Quantum correlations are a subset of this polytope, so it may well be worthwhile to consider interior points.

These interior points may be thought of as mixed boxes because they can be obtained by probabilistic mixtures of the vertices. In particular we would like to find an analogy of distillation, i.e given a number of copies of a mixed box (an interior point) can we *distill* with local operations any extremal correlations?

Having set up a framework in which we can understand non-local correlations, we hope that by thinking about some of the above questions we may find an information theoretic explanation for the limited power of quantum correlations.

Entropy inequalities.

In chapter 7 we used the reduced entropies as a method of characterizing multipartite states, and were particularly interested in the constraints on the allowed reduced entropies. If we consider a situation where there are no constraints on the states, then we know that for three or fewer particles strong subadditivity (SSA) provides necessary and sufficient conditions on the reduced entropies for a closely corresponding state to exist. By enumerating the extreme rays of the space of reduced entropies allowed by SSA for four parties we were able to make two conjectures. The first is that two classes of extreme ray are unobtainable for any quantum state - this has subsequently turned out to be true [128]. The second is that there may be new entropy inequalities. These conjectures were based on an analogy with a new classical inequality derived by Yeung and Zhang [7]. If true this second conjecture would be a very interesting result - SSA has proved to be a very useful tool in quantum information science, and no new entropy inequalities have been discovered for 30 years. Of course this is the main open question left by this work, and is currently the subject of active research.

We also made a connection between the extreme rays of the space of allowed reduced entropies and MREGS. This allowed us to conclude that a certain set of states must belong to the MREGS for three and four particles. This is independent of the question of whether or not there may be new entropy inequalities. Arguments based on reduced entropy provide necessary but not sufficient conditions for states

to be in MREGS, so the arguments presented give a 'lower bound' on the set of states to be included. By considering relative entropy of entanglement it has been shown that other states must be in MREGS.

The above paragraphs contain a summary of the main results that I have found in the areas of multipartite Bell inequalities, non-local correlations, and entropy inequalities. They also contain a review of some of the open questions arising directly from this work.

Entanglement, particularly for multipartite systems, has proved to have an extremely rich structure. The most important questions in this area remain unsolved despite the considerable attention they have received over the last decade or so. For example, we do not yet know the inequivalent classes of entangled states, nor do we understand the precise role of entanglement in quantum computation. Finally, there are deeper question that remain unanswered - no satisfactory physical mechanism for non-locality has been proposed. Nevertheless, as many authors have [140, 141, 142, 143] noted, Quantum Information has given us new insight into questions about the foundations of quantum mechanics; hopefully a trend which will continue in the future.

Bibliography

[1] G. Svetlichny. Phys. Rev. D **35** (1887) 3066

[2] A. Einstein, B. Podolsky, N. Rosen. Phys. Rev. **47** (1935) 777

[3] J. Bell. Physics. **1** (1964) 195

[4] P. Mitchell, S. Popescu, D. Roberts. quant-ph/0202009 (2002)

[5] D. Collins, N. Gisin, S. Popescu, D. Roberts, V. Scarani. Phys. Rev. Lett. **88** (2002) 170405.

[6] J. Barrett, N. Linden, S. Massar, S. Pironio, S. Popescu, D. Roberts. quant-ph/0404097 (2004)

[7] Z. Zhang, R. Yeung. Transaction on Information Theory **43** (1997) 1982

[8] D. Bohm. Phys. Rev. **85** (1952) 166

[9] D. Bohm. Phys. Rev. **85** (1952) 180

[10] N. Mermin. Phys. Rev. Lett. **65** (1990) 3373

[11] A. Peres. Phys. Lett. A. **151** (1990) 107

[12] A. Peres. *Quantum theory: Concepts and methods.* Kluwer Academic, Dordrecht. (1993)

[13] J. Bell. Rev. Mod. Phys. **38** (1966) 447

[14] S. Kochen, E. Specken. J. Math. and Mech. **17** (1967) 59

[15] A. Gleason. J. Math. and Mech. **6** (1957) 885

[16] J. Clauser, M. Horne, A. Shimony, R. Holt. Phys. Rev. Lett. **23** (1969) 880

[17] B.S. Cirel'son. Lett. Math. Phys. **4** (1980) 83

[18] I. Pitowsky, K. Svozil. Phys. Rev. A **64** (2001) 014102

[19] D. Collins, N. Gisin. J. Phys. A **37** (2004) 1775

[20] A. Fine. Phys. Rev. Lett. **48** (1982) 291

[21] N. Gisin, H. Bechmann-Pasquinucci. Phys. Lett. A **246** (1998) 1

[22] D. Collins, N. Gisin, N. Linden, S. Massar, S.Popescu. Phys. Rev. Lett. **88** (2002) 040404

[23] D. Kaszlikowski, P. Gnacinski, M. Zukowski, W. Miklaszewski, A. Zeilinger. Phys. Rev. Lett. **85** (2000) 4418

[24] D. Mermin. Phys. Rev. Lett. **65** (1990) 2838

[25] A.V. Belinskii, D.N. Klyshko. Phys. Usp. **36** (1993) 653

[26] R. Werner, M. Wolf. Phys. Rev. A. **61** (2000) 062102

[27] M. Zuckowski, C. Brukner. Phys. Rev. Lett. **88** (2002) 21041

[28] B. Reznik, A. Retzker, J. Silman. J Mod Optic **51** (2004) 833

[29] S. Summers, R. Werner. Phys. Lett. A. **110** (1985) 257

[30] H. Halvorson, R. Clifton. J. Math. Phys. **41** (2000) 1711

[31] C. Brukner, S. Taylor, S. Cheung, V. Vedral. quant-ph/0402127

[32] A. Leggett, A. Garg. Phys. Rev. Lett. **54** (1985) 857

[33] J. Paz, G. Mahler. Phys. Rev. Lett. **71** (1993) 3235

[34] D. Greenberger, M. Horne, A. Shimony, A. Zeilinger. Am. J. Phys. **58** (1990) 1131

[35] D. Greenberger, M. Horne, A. Zeilinger. *Bells theorem, Quantum Theory, and conceptions of the Universe*. (ed. M. Kafatos) 73-76 Kluwer Academic, Dordrecht. (1989)

[36] D. Mermin. Physics Today. **43** (1990) 13

[37] L. Hardy. Phys. Rev. Lett. **68** (1992) 2981

[38] A. Elitzur, L. Vaidman. Foundations of Physics **23** (1993) 987

[39] L. Hardy. Phys. Rev. Lett. **71** (1993) 1665

[40] A. Cabelo Phys. Rev. Lett. **86** (2001) 1911

[41] N. Gisin. Phys. Lett. A. **154** (1991) 201

[42] S. Popescu, D. Rohrlich. Phys. Lett. A. **166** (1992) 293

[43] R. F. Werner, Phys. Rev. A **40** (1989) 4277

[44] S. Popescu, Phys. Rev. Lett. **74** (1995) 2619

[45] C. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, W. Wooters. Phys. Rev. Lett. **70** (1993) 1895

[46] C. Bennett, S. Wiesner. Phys. Rev. Lett. **69** (1992) 2881

[47] C. Bennett, H. Bernstein,S. Popescu, B. Schumacher. Phys. Rev. A. **53** (1996) 2046

[48] C. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. Smolin, W. Wooters. Phys. Rev. Lett. **76** (1996) 722

[49] A. Acin, V. Scarini, M. Wolf. J. Phys. A: Math. Gen. 36, L21 (2003)

[50] M. Horodecki, P. Horodecki, R. Horodecki, Phys. Rev. Lett. **80** (1998) 5239

[51] R. Werner, M. Wolf. Phys. Rev. A. **61** (2000) 062102

[52] B. Terhal. Phys. Lett. A. **271** (2000) 319

[53] W. Dür. Phys. Rev. Lett. **87** (2001) 230402

[54] R. Augusiak, P. Horodecki. quant-ph/0405187 (2004)

[55] A. Acin. Phys. Rev. Lett. **88** (2002) 027901

[56] A. Peres. Phys. Rev. Lett. **77** (1996) 1423

[57] M. Horodecki, P. Horodecki, R. Horodecki. Phys. Lett. A. **223** (1996) 1

[58] A. Peres. Found. Phys. **29** (1999) 589

[59] A. Aspect, J. Dalibard, G. Roger, Phys. Rev. Lett. **49** (1982) 1804

[60] G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, A. Zeilinger. Phys. Rev. Lett. **23** (1998) 5039

[61] M. Rowe, D. Kielpinski, V. Meyer,C. Sackett, W. Itano, C. Monroe, D. Wineland. Nature **409** (2001) 791

[62] P. Eberhard. Phys. Rev. A. **47** (1993) R747

[63] N. Gisin, B. Gisin. Phys. Lett. A. **260** (1999) 323

[64] J. Barrett, D. Collins, L. Hardy, A. kent, S. Popescu. Phys. Rev. A. **66** (2002) 042111

[65] R. Gill. *Mathematical Statistics and Applications: Festschrift for Constance van Eeden.* (ed. M. Moore, S. Froda) 133-154 IMS lecture notes - Monograph series **42** (2003) Institute of Mathematical Statistics, Beachwood, Ohio. Also quant-ph/0110137 (2001)

[66] L. Accardi, M. Regoli. quant-ph/0007005

[67] D. Bouwmeester, J. Pan, M. Daniell, H. Weinfurther, and A. Zeilinger, Phys. Rev. Lett. **82** (1999) 1345

[68] J. Pan, D.Bouwmeester, M. Daniell, H. Weinfurther, and A. Zeilinger, Nature **403** (200) 515

[69] S. Popescu, D. Rohrlich, Phys. Lett. A, **166** (1992) 293

[70] J. Cereceda. Phys. Rev. A. **66** (2002) 024102

[71] W. Dur, G. Vidal, J. Cirac. Phys. Rev. A. **62** (2000) 062314

[72] M. Eibl, N. Kiesel, M. Bourennane, C. Kurtsiefer, H. Weinfurther. Phys. Rev. Lett. **92** (2004) 077901

[73] J. Cereceda. quant-ph/0402198 (2004)

[74] I. Percival. Phys. Lett. A **244** (1998) 495

[75] R. Werner and M. Wolf. Phys. Rev. A. **64** (2001) 032112

[76] V. Scarani, N. Gisin. J. Phys. A: Math. Gen. **34** (2001) 6043

[77] J. Pan, M. Daniell, S. Gasparoni, G. Weihs, A. Zeilinger. Phys. Rev. Lett. **86** (2001) 4435

[78] C. Sackett, D. Kielpinski, B. King, C. Langer, V. Meyer, C. Myatt, M. Rowe, Q. Turchette, W. Itano, D. Wineland, C. Munroe. Nature **404** (2000) 256

[79] Z. Zhao, Y. Chen, A. Zhang, M. Zukowski, J. Pan. Phys. Rev. Lett. **91** (2003) 180401

[80] Z. Zhao, Y. Chen, A. Zhang, M. Zukowski, J. Pan. quant-ph/0402096 (2004)

[81] M. Seevinck, G. Svetlichny. Phys. Rev. Lett. **89** (2002) 060401

[82] A. Aspect. Nature **398** (1999) 195

[83] C. Shannon. *Two-way communication channels.* Preceedings of the Fourth Berkeley Symposium on Mathematical Statistics and Probability. (ed. J. Neyman) 611-644 University of California Press, Berkely CA. (1961)

[84] R. Cleve, H. Buhrman. Phys. Rev. A. **56** (1997) 1201

[85] E. Kushilevitz, N. Nisan. *Communication Complexity.* Cambridge University Press, Cambridge. (1997).

[86] S. Popescu, D. Rohrlich, Foundations of Physics **24** (1994) 379.

[87] W. van Dam. PhD Thesis. *Nonlocality and Communication Complexity.* University of Oxford, Department of Physics. (2000). Available at http://web.mit.edu/vandam/www/publications.html

[88] R. Cleve, W. van Dam, M. Nielsen. Lec.Notes Comput.Sci 1507 (1998) 61

[89] M. Werner, M. Wolf. Quant. Inf. Comp. **1** (2001) 1

[90] I. Pitowsky. *Quantum Probability, Quantum Logic.* Springer, Heidleberg. Lecture notes in Physics 321 (1989)

[91] B.S. Cirel'son. Journal of Soviet Mathematics. **36** (1987) 557

[92] L. Masanes. Quant. Inf. Comp. **3** (2003) 345

[93] L. J. Landau. Found. Phys. **18** (1988) 449

[94] R. Ahlswede, I. Csiszár. IEEE Transactions on Information Theory. **44** (1998) 225

[95] R. Ahlswede, I. Csiszár. IEEE Transactions on Information Theory. **39** (1993) 1121

[96] D. Collins, S.Popescu. Phys. Rev. A. **65** (2002) 032321

[97] M. A. Nielsen, I. Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press. (2000)

[98] S. Pironio. Phys. Rev. A. **68** (2003) 062102

[99] T. Christof, A. Löbel. http://www.zib.de/Optimization/Software/Porta/index.html

[100] K. Fukuda. http://www.cs.mcgill.ca/ fukuda/soft/cdd_home/cdd.html

[101] *lrs* is available at http://cgm.cs.mcgill.ca/ avis/C/lrs.html

[102] W. van Dam. private communication.

[103] J. Barrett, L. Hardy, A. Kent. in preparation.

[104] N. Linden, R. Jozsa. P. Roy. Soc. Lond. A. Mat. **459** (2003) 2011

[105] L. Ioannou, B. Travaglione, D. Cheung, A. Ekert. quant-ph/0403041

[106] A. Peres. Phys. Rev. Lett. **77** (1996) 1423

[107] L. Gurvits, H. Barnum. Phys. Rev. A. **66** (2002) 062311

[108] S. Braunstein, C. Caves, R. Jozsa, N. Linden, S. Popescu, R. Schack. Phys. Rev. Lett. **83** (1999) 1054

[109] K. Zyczkowski, P. Horodecki, A. Sanpera, M. Lewenstein. Phys. Rev. A. **58** (1998) 883

[110] J. Eisert, M. Plenio. Int. J. Quant. Inf. **1** (2003) 479

[111] M. Nielson. Phys. Rev. Lett. **83** (1999) 436

[112] D. Johnathan, M. Plenio. Phys. Rev. Lett. **83** (1999) 1455

[113] G. Vidal. Phys. Rev. A. **62** (2000) 062315

[114] G. Vidal. J. Mod. Optics. **47** (2000) 355

[115] C. Bennett, S. Popescu, D. Rohrlich, J. Smolin, A. Thapliyal. Phys. Rev. A **63** (2000) 012307

[116] N. Linden, S. Popescu. Fortsch. Phys. **46** (1998) 567. Also quant-ph/9711016 (1997)

[117] A. Sudbery. J. Phys. A. **34** (2001) 643

[118] J. Kempe. Phys. Rev. A. **60** (1999) 910

[119] G. Vidal. Phys. Rev. Lett. **83** (1999) 1046

[120] V. Vedral, M. Plenio, M. Rippon, P Knight. Phys. Rev. Lett. **78** (1997) 2275

[121] G. Vidal, J. Cirac. Phys. Rev. lett. **86** (2001) 5803

[122] C. Bennett, D. DiVincenzo, J. Smolin, W. Wootters. Phys. Rev. A. **54** (1996) 3824

[123] W. Wooters. Phys. Rev. Lett. **80** (1998) 2245

[124] G. Vidal, R. Werner. Phys. Rev. A. **65** (2002) 032314

[125] K. Vollbrecht, R. Werner. Phys. Rev. A. **64** (2001) 062307

[126] N. Linden, S. Popescu, B. Schumacher, M. Westmoreland. quant-ph/9912039 (1999)

[127] V. Coffman, J. Kundu, W. Wootters. Phys. Rev. A. **61** (2000) 052306

[128] N. Linden, A. Winter. quant-ph/0406162

[129] J. Eisert, H. Briegel. Phys. Rev. A. **64** (2001) 022306

[130] H. Araki, E. Lieb. Comm. Math. Phys. **18** (1970) 160

[131] E. Lieb, M.B. Ruskai. J. Math. Phys **14** (1973) 1938

[132] N. Pippinger. Transactions on Information Theory **49** (2003) 773

[133] A. Holevo. Problems of Inf. Transm. **5** (1979) 247

[134] *Mathematica* (version 5.0) available from Wolfram Research. Vertex enumeration package.

[135] A. Higuchi, A. Sudbery and J. Szulc. Phys. Rev. Lett. **90** (2003) 107902

[136] S. Bravyi. quant-ph/0301014 (2003)

[137] R. Yeung. *A First Course in Information Theory* Kluwer Academic (2002)

[138] A. Acin, G. Vidal, J. Cirac. Quant. Inf. Comp **3** (2003) 55

[139] S. Wu, Y. Zhang. Phys. Rev. A. **63** (2001) 012308

[140] R. Clifton, J. Bub, H. Halverson. Found. Phys. **33** (2003) 1561

[141] C. Fuchs. Proceedings of the NATO Advanced Research Workshop. *Decoherence and its implications in Quantum Computation and Information transfer.* (ed. A. Gonis) (2001). Also quant-ph/0106166 (2001)

[142] L. Hardy. Proceedings of the NATO Advanced Research Workshop. *Modality, Probability and Bells Theorem.* (2001). Also quant-ph/0111068 (2001)

[143] D. Deutsch. *It from Qubit.* Science and Ultimate reality. Cambridge University Press. (2003)