An Algorithm To Measure The Tightness Of A Bell Inequality

Author: Neil Smith

Supervisors: Dr Mark Howard and Dr Pieter Kok

Dec 2017

Abstract

Extending on previous work, we further develop an algorithm that measures the degree to which a Bell inequality is tight. We generalise the algorithm to work for any Bell inequality of any scenario where the parties can choose from different numbers of measurements and observe different numbers of outcomes for each of these measurements. We explain the theory behind the algorithm in depth and demonstrate the accuracy of the expressions by applying them to the CHSH inequality.

Contents

1 Prelude

Quantum mechanics predicts that particles behave in ways that classical physics tells us is impossible. This quantum mechanical behaviour of particles has already been exploited to create new quantum technologies that perform tasks much more efficiently than current technologies based on classical physics, and there is still a huge interest in the study of this quantum mechanical behaviour for further development of new technologies. One particular feature of quantum mechanics, that of non-locality, has over the past decades become a fruitful topic of research. Non-locality refers to the non-local correlations that can be observed between parties making measurements on entangled quantum systems. Non-locality has the potential to be used in new communication and information-processing devices and enable us to accomplish tasks that are currently either impractical or impossible to do with current technology.

The concept of non-locality originates in a 1935 paper [13] by Albert Einstein, Boris Podolsky and Nathan Rosen (EPR) in which they argued that the theory of quantum mechanics is incomplete. In their argument EPR showed a contradiction in the predictions of quantum mechanics. Heisenberg's Uncertainty Principle tells us that we cannot know simultaneously both the exact position and momentum of a particle, yet EPR argued that we can. They proposed that Quantum Mechanics could be completed through the use of a Local Hidden Variable (LHV) theory. In their argument they made three assumptions about the way the universe behaves, that it has realism, locality and that experimentalists have free will. Later in 1964, John Bell constructed an expression, known as a Bell Inequality, that could be used to experimentally test the correctness of Local Hidden Variable theories through the use of measurable physical quantities [3]. Shortly afterwards, Bell proved that no LHV theory could reproduce all of the predictions of quantum mechanics and be used to complete it, this became known as Bell's Theorem [4].

EPR incorrectly assumed that signals cannot be transmitted between particles at speeds greater than the speed of light, this is known as locality. This seemed like a reasonable assumption to make, otherwise it would be in contradiction with The Theory of Relativity. However, correlations can be observed between distant particles that cannot be explained through a LHV theory. The particles seem to transmit signals between themselves faster than the speed of light, in fact this transmission is instantaneous. This phenomenon is known as Non-locality and arises due to the entanglement of the particles. This caused great concern for Einstein and he called this "Spooky action at a distance". It turns out that these signals transmitted between the particles are in fact random signals, and cannot be used to transmit information faster than the speed of light. Non-locality is not in contradiction with Special Relativity. They cannot be used to transmit signals faster than light, but the phenomenon can still be exploited to perform communication and information processing tasks that were previously unachievable.

In section 2 we remind the reader of the relevant concepts and terminology used in the framework of non-locality. In section 3 we discuss how non-locality can be observed in the lab through a Bell experiment and how noise and technological constraints introduce loopholes into the experimental results. In section 4 we discuss how we quantify the amount of non-locality and why it is difficult to produce a general measure of non-locality. In section 5 we talk about some of the applications of non-local correlations and how they can be used to perform tasks more efficiently and certify the presence of a particular quantum state. In section 6 we explain how we have developed upon our previous work and generalised our algorithm to calculate the facet dimension of a Bell Inequality. In section 7 we explain how our new generalised algorithm functions and how the calculation of the relevant quantities changes as we move to the general scenario. We include a flowchart of the main method of the algorithm. In section 8 we explain which inequalities the algorithm was tested against and reveal the results of the testing. In section 9 we conclude our work and discuss possible further work on the algorithm and how we next intend to apply the algorithm to find tight Bell Inequalities. In the appendix we demonstrate how these general expressions simplify to their previous form in order to convince the reader of their correctness.

2 Preliminaries

2.1 Nonlocality

Here we explain the framework in which we study non-locality. There are n parties who each have access to their own system upon which they can make measurements and observe outcomes. But now, each party k can make a measurement $m_k \in \mathcal{M}_k$ from a set of possible measurements $\mathcal{M}_k = \{1, 2, ..., M_k\}$ out of a total possible M_k measurements. When party k makes measurement m_k they can observe one outcome $d_{m_k,k} \in \mathcal{D}_{m_k,k}$ from a set of possible outcomes $\mathcal{D}_{m_k,k} = \{1, 2, ..., D_{m_k,k}\}$ out of a total possible $D_{m_k,k}$ outcomes. Any party k can also choose not to perform a measurement. We can think of this as them choosing to perform the zeroth measurement, which we denote as $m_k = 0$. The particular form of the measurements the parties perform and outcomes they observe are unimportant, only the number of measurements and outcomes are important.

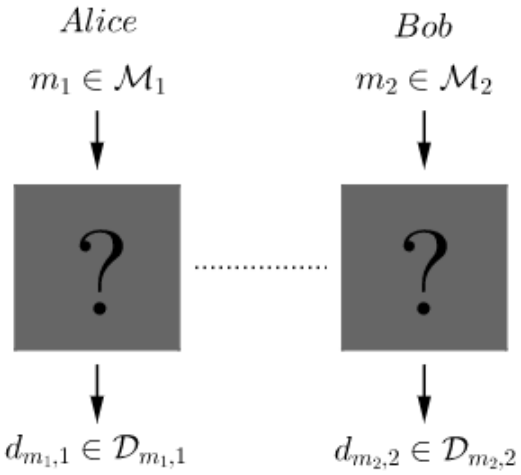


Figure 1: The Alice and Bob scenario, there are two parties who are very far apart from each other and each have access to a system upon which they can make measurements and observe outcomes. Alice can make a measurement $m_1 \in \mathcal{M}_1$ from a set of $\mathcal{M}_1$ possible measurements and observe an outcome $d_{m_1,1} \in \mathcal{D}_{m_1,1}$ from a set of $\mathcal{D}_{m_1,1}$ possible outcomes. Similarly, Bob can make a measurement $m_2 \in \mathcal{M}_2$ from a set $\mathcal{M}_2$ of possible measurements and observe an outcome $d_{m_2,2} \in \mathcal{D}_{m_2,2}$ from a set $\mathcal{D}_{m_2,2}$ of possible outcomes.

The joint probability that party k makes a measurement m_k on their system and observes an outcome $d_{m_k k}$ is now denoted $P(d_{m_1 1} d_{m_2 2} ... d_{m_n n} | m_1 m_2 ... m_n)$. Like before, we can also define a joint probability distribution that can be represented as a vector (1), which is known as a behaviour. The number of elements of this vector will just be the total number of possible ways of getting different outcomes. This can be found by calculating for each party the sum of the total number of possible outcomes for each of their measurements and then taking the product of all these numbers.

$$\vec{P}(d_{m_1,1} d_{m_2,2} ... d_{m_n,n} | m_1 m_2 ... m_n) \in \mathbb{R}^b \qquad b = \prod_{k=1}^{n} \left(\sum_{m_k=1}^{M_k} D_{m_k,k} \right) \tag{1}$$

2.2 Local Behaviours

A Local Hidden Variable (LHV) theory makes the assumption that any correlations observed between distant particles is due to some quantity that predetermines the outcomes we observe when we make measurements upon the particles. This quantity $\lambda \in \Lambda$ is hidden from us and is known as a hidden variable. In particular, a LHV theory makes three assumptions about the way the universe behaves, these are:

1. **Locality**: The systems are influenced only by their local surroundings.
2. **Realism**: The properties of systems have well-defined values independent of external measurements.

3. **Free Will**: The parties can freely choose which measurements to perform.

The first, also known as the assumption of local causality, is the important one here. We assume that the parties are far enough apart that they cannot influence or communicate with each other, by sending a signal. This signal must therefore have a finite speed. In order for the local hidden variable theory to be consistent with the special theory of relativity, the speed of this signal cannot be greater than the speed of light, in order words the systems are unaffected by anything outside their light cones. Another way to phrase this is that each party's choice does not depend on the measurement choices of the other parties and the choice of which measurement to make is made when they are far apart. The local probability distribution of one party's outcome is independent of the experiments performed by the other parties. Mathematically, this can be expressed for party 1 as (2).

$$P(d_{m_1,1}|d_{m_2,2}...d_{m_n,n}m_1m_2...m_n\lambda) = P(d_1|m_1\lambda) \quad \forall\, \lambda \in \Lambda \tag{2}$$

You may ask what is the purpose of the second assumption, isn't this always true? This is what we are used to thinking in classical physics, but in quantum mechanics the properties of systems do not always have well-defined values until they are measured. In fact, the result depends on the specific experimental setup being used to measure it, this is known as quantum contextuality. In the assumption of free will we assume that the common cause λ is not correlated with their choice of measurements. In other words their measurement choices do not depend on the cause of the correlations, either directly or indirectly. This is also known as the assumption of measurement independence.

If we make these three assumptions about how the universe works then there are only a certain set of behaviours that we would be able to observe, these are known as the local behaviours. All the local behaviours can be expressed in the form (3), where $q(\lambda) \geq 0$ is a probability distribution and $\int q(\lambda)\, d\lambda = 1$.

$$P(d_{m_1,1}d_{m_2,2}...d_{m_n,n}|m_1m_2...m_n) = \int_\Lambda q(\lambda)p(d_{m_1,1}|m_1\lambda)p(d_{m_2,2}|m_2\lambda)...p(d_{m_n,n}|m_n\lambda)\, d\lambda \tag{3}$$

Note that not all of these probability distributions represent physically realisable behaviours of systems, what we normally refer to as the local behaviours are infact a subset of these probability distributions (3) that also obey the normalisation (4) and no-signalling conditions (11), these are also known as the local correlations $\mathcal{L}$.

$$\sum_{d_{m_1,1},d_{m_2,2},...,d_{m_n,n}} P(d_{m_1,1}d_{m_2,2}...d_{m_n,n}|m_1m_2...m_n) = 1 \quad \forall \quad m_i \in M_i \quad \forall \quad i \in \{1,...,n\} \tag{4}$$

When we use the term "local behaviours" we are really refering to this subset of local behaviours. Any correlation that cannot be explained through a local hidden variable theory is known as a non-local correlation.

2.3 The Local Polytope

The set of local behaviours $\mathcal{L}$ form a convex set that is also a polytope. A polytope is a convex set with a finite number of extremal points[1], it is a generalisation of a three-dimensional polyhedron, it is an object with "flat" sides. The local behaviours therefore form an shape with "flat" sides in probability distribution space. Figure shows a schematic of the local polytope. The extremal behaviours (5) are those probability distributions that can be expressed as a deterministic[2]product of the local probability distributions of each party. These are the "corners" of this polytope.

$$P(d_{m_1,1}d_{m_2,2}...d_{m_n,n}|m_1m_2...m_n) = D_1(d_{m_1,1}|m_1)D_2(d_{m_2,2}|m_2)...D_n(d_{m_n,n}|m_n) \tag{5}$$

As shown in my previous work it is possible to determine the exact form of each of the extremal behaviours,

[1]For a more detailed explanation of an extremal point see [19] and for polytopes see [45].

[2]A deterministic probability is one in which the probability of an outcome is either one or zero $D_k(d_{m_k,k}|m_k) \in \{0,1\}$.

the elements of the probability distribution, by combining the deterministic property of the behaviours with the no-signalling and normalisation conditions into a single set of constraints. Now that the parties can choose from different numbers of measurements and observe different numbers of outcomes this set of constraints is now modified to (6). The derivation of these new constraints is done within the appendix in (A.2).

$$\sum_{d_{m_k,k}} D_k(d_{m_k,k}|m_k) = 1 \quad \forall\, m_k \in \mathcal{M}_k \quad \forall\, k \in \{1,...,n\} \tag{6}$$

The total number of these constraints is denoted n_{con} and can be found by summing the total number of possible measurements M_k that each party k could choose to perform (7).

$$n_{con} = \sum_{k=1}^{n} M_k \tag{7}$$

Using the same argument as I demonstrated in my previous work, we can determine from the constraints (6) the total number of extremal behaviours n_{ex}. This can be calculated by taking the product of the total number of possible outcomes $D_{m_k,k}$ for each measurement m_k of each party k (8).

$$n_{ex} = \prod_{k,m_k} D_{m_k,k} \tag{8}$$

The dimension of the local polytope is now calculated according to (9) and can be found by considering the normalization and no-signalling conditions as shown in Theorem 3.1 of [29].

$$\dim \mathcal{L} = \prod_{k=1}^{n} \left(\sum_{m_k=1}^{M_k} (D_{m_k,k} - 1) + 1 \right) - 1 \tag{9}$$

The local behaviours can also be equivalently defined through (10), where $c_i > 0$ are a series of coefficients that obey $\sum_i c_i = 1$. The probabilities of any local behaviour can be expressed as a convex sum of products of the local deterministic probabilities of each party. More precisely, they are a convex sum of the extremal behaviours. The local polytope is the convex hull of the local behaviours.

$$\mathcal{L} = \left\{ \vec{P}(d_{m_1,1}...d_{m_n,n}|m_1...m_n) \mid P(d_{m_1,1}...d_{m_n,n}|m_1...m_n) = \sum_i c_i D_1(d_{m_1,1}|m_1) D_2(d_{m_2,2}|m_2)...D_n(d_{m_n,n}|m_n) \right\} \tag{10}$$

2.4 No-Signalling Correlations

Local hidden variable theories impose more assumptions upon the scenario than just the assumption that the parties cannot communicate faster than the speed of light. We can also consider what behaviours could occur given just this assumption about the parties, this is known as a no-signalling scenario. We assume that the parties are far enough apart that they cannot get any information about the other parties' experiments, this means that the probability of one party getting a given outcome is independent of any of the other parties' experiments. Mathematically this can be expressed as (11), which is equivalent to requiring that the marginals of the joint probability distribution are well-defined.

$$\sum_{d_k} P(d_{m_1,1}...d_{m_k,k}...d_{m_n,n}|m_1...m_k...m_n) = \sum_{d_k} P(d_{m_1,1}...d_{m_k,k}...d_{m_n,n}|m_1...m'_k...m_n) \tag{11}$$
$$\forall\, m_k, m'_k \in M_K, \quad \forall\, k \in \{1,...,n\}, \quad \forall\, d_i, m_i \in D_i, M_i\ (i \neq k)$$

The behaviours that satisfy these no-signalling conditions form the no-signalling set, this also forms a convex polytope. Since these conditions are less restrictive than the conditions for the local set, the local set of behaviours is contained within the no-signalling set (12), this inclusion is in fact strict [34]. If nature behaved according to just the no-signalling conditions then we would expect to see correlations that are greater than that allowed by the local set. These are called the no-signalling correlations.

$$\mathcal{L} \subset \mathcal{NS} \tag{12}$$

2.5 Quantum Correlations

A quantum behaviour is one that can be written in quantum theory as a trace (13) of a quantum state $\rho \in \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes ... \otimes \mathcal{H}_n$ where $\{M_{m_1}^{d_{m_1,1}}, M_{m_2}^{d_{m_2,2}}, ..., M_{m_n}^{d_{m_n,n}}\}$ are local POVMs acting on the arbitrary Hilbert spaces $\{\mathcal{H}_1, \mathcal{H}_2, ..., \mathcal{H}_n\}$ respectively. The set of all quantum behaviours is denoted $\mathcal{Q}$.

$$P(d_{m_1,1}d_{m_2,2}...d_{m_n,n}|m_1m_2...m_n) = \mathrm{Tr}\left(M_{m_1}^{d_{m_1,1}} \otimes M_{m_2}^{d_{m_2,2}} \otimes ... \otimes M_{m_n}^{d_{m_n,n}}\,\rho\right) \tag{13}$$

The quantum set is more restrictive than the no-signalling set but less restrictive than the local set, for this reason, the local set is contained within the quantum set[3] and the quantum set is contained within the no-signalling set (14), these inclusions are both strict. [34, 9] We can show that the quantum set is contained within the no-signalling set by showing they satisfy the no-signalling conditions (11), this is done in (A.1) in the appendix.

$$\mathcal{L} \subset \mathcal{Q} \subset \mathcal{NS} \tag{14}$$

The quantum set is also a convex set like both the local and no-signalling sets but does not form a polytope, Figure 2 shows this relationship. Quantum behaviours can give rise to correlations greater than that allowed by a local hidden variable theory but less than that allowed by the no-signalling set. States ρ that are separable can only generate local correlations, whereas states that are entangled can generate correlations that cannot be observed in a local hidden variable theory.

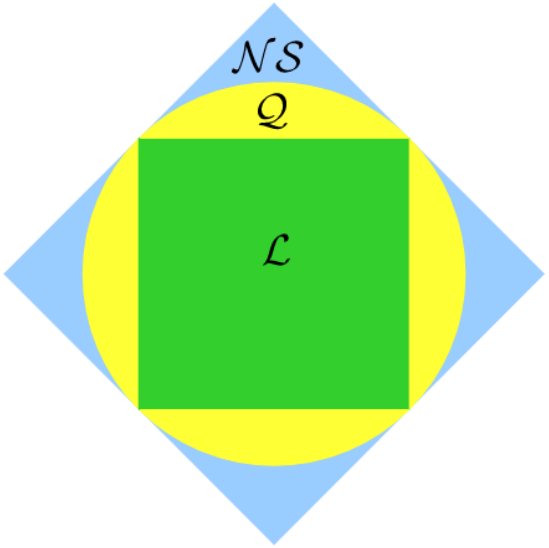


Figure 2: A schematic depicting the local $\mathcal{L}$, quantum $\mathcal{Q}$ and no-signalling $\mathcal{NS}$ sets of correlations. The local set is contained within the quantum set, which is contained within the no-signalling set, they are all convex sets. Both the local and no-signalling sets are polytopes, but the quantum set is not.

Currently, there is no known method to calculate the quantum bound, at least in a finite amount of time, in

[3]This is to be expected since classical physics is contained within quantum physics.

fact there are no set of principles that characterise the quantum set, and it is not known whether such principles exist. This is one of the main unsolved problems in the field on nonlocality. There have been many attempts to characterise the quantum set, one of the best attempts was achieved in 2008 when Navascués, Pironio and Acín found an infinite heirarchy of well characterised sets that converges to the quantum set, known as the NPA heirarchy. [28] The NPA hierarchy has been used to efficiently compute better and better upper bounds on the quantum bound. Methods have also been developed to calculate a lower bound, this is usually attained through the see-saw iterative method. [41]

2.6 Bell Inequalities

Bell Inequalities are expressions that can be used to help distinguish what is and what isn't a local behaviour[4]. Here we consider only those Bell Inequalities that are linear in the probabilities and so represent hyperplanes or half-spaces in probability distribution space. Some correlations will obey the expression and lie on one side of the hyperplane, but others will not. The best such inequalities are those that represent facets of the local polytope, which we call tight Bell Inequalities. But not all Bell Inequalities will represent facets and may either just touch an edge of the polytope or be some distance from it. Correlations that satisfy a Bell Inequality may or may not be a local behaviour but correlations that do not satisfy it are non-local correlations. A violation of such a Bell Inequality is evidence that the universe can exhibit non-local behaviour. The intersection of all the tight Bell Inequalities is the set of local behaviours.

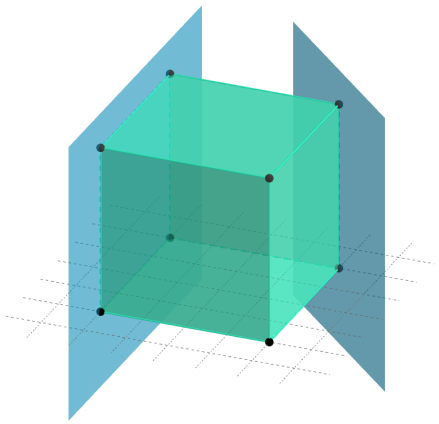


Figure 3: The geometric representation of Bell Inequalities as a series of halfspaces in probability distribution space. Only the corresponding hyperplanes are shown. Tight Bell Inequalities represent the facets of the local polytope. There are an infinite number of Bell Inequalities for each scenario, some represent hyperplanes parallel to the facet and others are not, some are closer to the facet and others are further away.

A Bell Inequality is an inequality involving a sum of probabilities $P_{i_j,j}$ with coefficients $c_{i_j,j}$ as shown in (15). The equality relation defines the hyperplane. In previous work we only considered those Bell Inequalities that could be expressed as a sum of correlators. Now, we consider general Bell Inequalities.

$$S = \sum_{i,j} c_{i_j,j} P_{i_j,j} = \vec{P} \cdot \vec{c} \leq S_{max} \tag{15}$$

We can also express these Bell Inequalities as an inner product of a vector of probabilities $\vec{P}$ that defines the space with a vector of coefficients $\vec{c}$ that determines the orientation of the corresponding set of planes of the Bell Inequality. The vector $\vec{c}$ is the normal vector of these planes.

Again, like before, terms can arise in Bell Inequalities where one or more of the parties do not make any measurements on their system. In this case, the joint probabilities $P_{i_j,j}$ will be replaced with the marginal over the parties that do not make measurements. If there are $n' < n$ parties that make measurements then the joint

[4]There are many different types of inequalities that can be used to distinguish any sets of correlations, which are all given different names. Bell Inequalities are named after John Bell the first to use them.

probability will be a deterministic product of these n' parties that do make measurements. Suppose only party k does not make a measurement, then the marginal probability[5] would be expressed as (16).

$$P(d_{m_1 1}...d_{m_{k-1},k-1}d_{m_{k+1},k+1}...d_{m_n,n}|m_1...m_{k-1}m_{k+1}...m_n) = \\ D(d_{m_1,1}|m_1)...D(d_{m_{k-1},k-1}|m_{k-1})D(d_{m_{k+1},k+1}|m_{k+1})...D(d_{m_n,n}|m_n) \tag{16}$$

Each party k can also choose not to perform a measurement $m_k = 0$.[6] The total number of possible combinations of measurements the parties could choose to perform, or measurement settings n_{set}, is found by calculating the product of the total number of possible measurements each party could choose to perform (17).

$$n_{set} = \prod_{k=1}^{n} (M_k + 1) \tag{17}$$

The dimension of the facet Bell Inequalities (18) will, also like before, be one less than the dimension of the polytope (9).

$$\dim \mathcal{I} = \dim \mathcal{L} - 1 = \prod_{k=1}^{n} \left(\sum_{m_k=1}^{M_k} (D_{m_k,k} - 1) + 1 \right) - 2 \tag{18}$$

We know that the extremal points of the local polytope can be used to characterize the local set, but the set can also be characterised through its facets or the intersection of the corresponding series of halfspaces. If we know the faces of the polytope then we know the form of the local set.

The first Bell Inequality was introduced by Bell in his 1964 paper [3] as a way of providing a test of whether or not quantum mechanics could be completed through the use of hidden variables. A violation of a Bell Inequality provides evidence that at least one of the assumptions made in a local hidden variable theory is incorrect, indeed violations were observed and they showed that no completion in this way was possible. To date, experiments have ruled out realism, showing that nature behaves nonlocally.[7]

An example of a tight Bell Inequality is the CHSH Inequality [10], given in (19), it is one of the most famous and well-studied Bell Inequalities.

$$\begin{gathered} P(11|11) - P(12|11) - P(21|11) + P(22|11) \\ P(11|12) - P(12|12) - P(21|12) + P(22|12) \\ P(11|21) - P(12|21) - P(21|21) + P(22|21) \\ -P(11|22) + P(12|22) + P(21|22) - P(22|22) \leq 2 \end{gathered} \tag{19}$$

It is the simplest tight Bell Inequality for which non-local correlations can be observed. It represents the correlations that can be observed between in a scenario involving two parties who both have a choice of two measurements to perform and can only observe two different possible outcomes for each of these measurements. This is usually denoted the $(2, 2, 2)$ scenario.

Interestingly, Inequalities of more complex scenarios involving more numbers of parties, measurements and outcomes can be generated from Bell Inequalities of simpler scenarios through a process of "lifting". If the original Bell Inequality is tight, the Bell Inequality of the more complex scenario will also be tight [31].

[5] Because terms like these marginal probabilities can arise, in general, there may not be a unique way in which to express a particular Bell Inequality. Two Bell Inequalities are equivalent if they can be obtained from each other by any relabeling of the measurement settings, outcomes and parties.

[6] We can define party k as making no measurement as making measurement zero $m_k = 0$. To be consistent the first outcome of a measurement is denoted with a label 1, outcome zero can be thought of as the outcome that party k observes when they do not make a measurement, they observe nothing.

[7] Free will has not been ruled out but it is in fact scientifically impossible to rule out free will.

3 Bell Experiments And Loopholes

There have been many experiments that have shown that nature does indeed not behave in the manner described by these LHV theories and that non-local correlations are possible. One of the first and most famous of these was Aspect's experiment which was the first to use fast measurement switching [1]. Most experiments are optical and use the entanglement of the polarization of pairs of photons to detect non-locality but others entangle solid-state spins using photons. In optical experiments, single photons are first produced by using the electroluminescence of quantum dots. Entangled pairs of photons are then produced from these that are then sent to two distant observers who each make polarization measurements on the photons. The entangled photons are typically produced by the non-linear effects of firing a high intensity laser pulse through non-linear crystals [25], but they can also be produced through cascade emission. Parametric down conversion of second order non-linear crystals is typically used, but third order non-linear effects can also be used [16]. These photons are then sent down optical fibres to the distant parties. Polarization measurements are made by the distant parties on their individual photons using polarizing filters and waveplates. In light-matter experiments, two solid-state spins are entangled together by transferring the entanglement of the photons to the spin using optical cavities. These optical cavities guide the photons to the spins and increase their coupling to the photon modes and increase the probability of entanglement transfer.

Before the parties can make measurements on their entangled photon on spin they must first be sure that their photon has arrived, the measurement is ready to be made and that the photon is not a stray photon but one of the entangled pairs. This verification of the arrival of the photon is known as Heralding. Non-locality can still be detected without Heralding but the process will take longer as more of the behaviours will be local, entanglement is required for non-locality. One way to Herald the arrival of the photon is to use electronic postselection [33]. We can compare the arrival times of the photons at the detectors of each party and only consider those measurement results for which the times coincide and we can be sure that these photons are the entangled pairs of photons. Another way is to send pairs of photons to each observer, one of these, the idler photon, is used to signal the arrival of the other, the signal photon. The idler photon can be used to control a shutter [5], this is also known as an optical switch. Another way involves using quantum non-demolition (QND) measurements to count photons without destroying them [20], these are measurements that minimise the change in the state of the photon.

Throughout the experiment there will be photon losses and noise due to interactions with the environment, that will inevitably change the state of the photon and possibly disrupt the entanglement. These issues make the implementation of a reliable Bell experiment difficult as they introduce loopholes into the experiment results as additional assumptions have to be made about the system. The first source of error arises in the generation of the single photons. The no-cloning theorem prevents us from creating exact copies of quantum states and the single photon sources generally have a low fidelity, the quantum states produced from trial to trial will be slightly different. There is currently a lot of work in producing efficient single photon sources, not just for Bell Inequality experiments but for other applications including quantum key distribution, quantum cryptography and quantum repeaters in optical fibres. When the photons travel down the optical fibres they interact with the optical fibre or environment, and are either scattered or absorbed, causing them to either be lost or disrupt their entanglement. Despite this, photons are still the best candidates for transmitting quantum information and entanglement over long distances. This noise in optical fibres can be reduced by cryogenically freezing them [12]. The photon signal can also be amplified, but again this is complicated by the no-cloning theorem. Even if the photon does reach the observer, their detector may not be 100% efficient. The noise in the circuits of the detectors can be reduced by using superconductors [12] and very high efficiencies have been achieved, large enough to close the detection loophole. In light-matter systems the spin state can be measured with near perfect efficiency, but the measurements can take a long time. There are also other losses in efficiency due to having to convert the frequency of the photon to match the resonant frequency of the cavity. A recent experiment has achieved 88% fidelity [21]. Noise and photon losses introduce a detection loophole into the Bell experiment. However, if one or more of the parties does not detect a particle at all then the experiment can be improved, as we can safely discard these results if we assume that they were lost because of imperfections and are not lost in an unbiased way.

On top of the detection loophole, technological constraints on the implementation of these experiments can introduce other loopholes by requiring addition assumptions to be made to show that the results are incompatible

with that of a local hidden variable theory. If all of the events of the experiment are not outside the light cones of each other, then we cannot be sure that information does not have time to travel between the different parts of the experiment and that they have not influenced each other. We cannot be sure the experiment is a reliable test of non-locality. This is known as the locality loophole. The measurement apparatus has to be fast enough such that signals traveling at or less than the speed of light do not have time to reach the second observer and transmit information about the measurement results. More thorough tests of non-locality require that the systems involved are separated over larger distances, but only a few Bell experiments have managed to achieve this and most experiments are only over short distances due to the losses in optical fibres. As an example, in order for the random number generators to be independent of each other, one of the random number generators must not exist within the future light cone of the other. One could argue that there could also be an event that exists in the past light cone of both of these random number generators and therefore predetermine their behaviour and influence the measurement results. For this reason, there will always be some loopholes to the experiment that cannot be fully removed. The assumption of free will cannot ever be ruled out, even in principle, because the backwards light cones of the two observers will inevitably intersect.

One of the other requirements of a local hidden variable theory is that the measurement choices of the distant observers are independent. This can be achieved by using a random number generator to randomly select the measurements that the observers perform. It was thought that in order to observe non-locality with a high probability the measurement choices have to be carefully controlled, but it was shown that this is not the case [24]. In fact, randomly chosen measurement bases can still lead to high probabilities of observing non-local correlations and that this increases with the number of parties. Using random measurements can therefore save time and resources in detecting non-locality.

In the literature, many authors report a loophole free experiment, by this they usually mean that their experiment is free of both the locality and detection loopholes, considered the two main loopholes. But their experiment may still consist of other additional assumptions. In fact, almost all experiments have required additional assumptions to be made about the systems involved and introduce loopholes into their results. Recently however, a few true Loophole-free Bell Experiments have successfully been carried out, although only over short distances [36] [18] [38]. In a recent light-matter entanglement experiment, a loop-hole free bell inequality violation was observed between two entangled electrons that were 1.3 km apart [15].

4 Measures Of Nonlocality

The observation of non-local correlations requires that the quantum systems be entangled, but more entanglement does not necessarily imply more non-locality will be observed. In the simplest scenario, the CHSH scenario, the maximally entangled state does produce the maximum quantum correlation, but it is thought that this is not true in general for more higher dimensional and complex scenarios. It is not known what determines the amount of non-locality that will be observed within a quantum system and there is a large ongoing effort to find a measure of non-locality. The degree of non-locality depends not only on the quantum state, but the exact form of the measurements performed upon it and so non-locality cannot be attributed to any particular state. Furthermore, a state that exhibits non-local correlations in one scenario may not necessarily exhibit non-local correlations in another scenario [11]. On top of this, systems that exhibit more non-locality may not necessarily be more useful, as the quantum state may be correlated with the environment.

The violation of a Bell Inequality signifies the presence of non-local correlations and the degree of violation of a Bell Inequality can be used as a measure of non-locality. For this measure to be meaningful the Bell Inequality must be tight and we must know maximum local and quantum correlations possible. A method exists for calculating the maximum local correlation, but it is inefficient and scales exponentially with the size of the system. For this reason, the maximum local correlation has only been calculated for the simplest scenarios. There is currently no known general method of calculating the maximum quantum correlation, but there are iterative methods for calculating better and better upper and lower bounds. A different measure exists that is based on the definition of non-locality. Since non-local correlations require some communication to be classically simulated, one measure of non-locality could be the minimal amount of classical communication required to simulate the correlation. This is known as the communication complexity [26].

One of the main reasons why it is difficult to study quantum non-locality is because our knowledge about

the properties of the quantum set is limited. Very little is known about the quantum set other than that it is a convex set and more work needs to be done in investigating these properties. Towards this end, a group of researchers recently used tools from convex geometry to study the features of the quantum set [19] and have found some suprising non-trivial features even in the simplest scenarios. In the CHSH scenario there exists only one type of facet, the tight Bell Inequalities are all equivalent, and since any no-signalling behaviour can violate only up to one of these inequalities, the violation can be seen as a measure of distance from the local set. But defining this measure of distance in other scenarios is more difficult because of the complicated and unfamiliar geometry of the quantum set. One interesting discovery is that the maximal violation may require measurements to be made on mixed states rather than pure states in order to be observed. It is also worth asking whether it is possible for a quantum system to exhibit non-local correlations that are as strong as the extremal points of the no-signalling polytope. It was shown that no quantum behaviour in any scenario can reproduce an extremal nonlocal no-signalling behaviour [35].

5 Applications Of Nonlocality

On top of its importance in the understanding of the fundamentals of quantum mechanics, non-locality has several applications. The four main ones we will describe here are Communication Complexity, Device-Independent Quantum Key Distribution, Device-Independent Random Number Generation and Self-Testing.

5.1 Communication Complexity Tasks

The communication complexity measure of non-locality is the minimal amount of a classical communication that is required to simulate the correlation. For this reason, non-locality is intimately related to communication complexity tasks. In the field of communication complexity we study how successful a group of n parties are in calculating the answer $f(d_1, d_2, ..., d_n)$ to some problem given that each party i only has access to part d_i of the resources $\{d_1, ..., d_n\}$ needed to calculate the answer, and that the communication between the parties is restricted[8]. We try to answer the following questions.

1. Given that the resources are distributed in a certain way, what is the minimal amount of communication necessary in order to guarantee calculation of the correct answer?

2. Given a certain restriction on the amount of communication, what is the probability of calculating the correct answer?

From the phrasing of the first question we can see how these questions are related to non-locality. The second question however is less intuitive, in a classical computation we would get the right answer only if one of the parties has all the resources. But if we use the non-locality of a quantum systems as a resource in the calculation, we can still calculate the correct answer with a certain probability even if one party does not hold all of the resources.

An example of a communication complexity task is in circuit design. Here each of the processors computes the answer to a small part of the overall calculation, we would like to know how we could minimise the communication between the processors in order to reduce the time and energy costs and creating a more efficient circuit design. Other examples of communication complexity tasks include the study of data structures and the optimization of networks. The study of Bell Inequalities and violations also has important applications in cryptography and the security of communication [14].

The simplest and most obvious way to ensure calculation of the correct answer is to just send all of the information to one of the parties, however we are interested in finding methods which result in the answer with less communication. We would also like to know if communication complexity tasks exist where using an entangled system that exhibits non-local correlations would allow us to complete the task with less resources than if we had used a classical system, and by how much this would reduce the resources required. One of the main problems in the field of communication complexity is finding quantum algorithms that are more efficient

[8]We are only interested in the amount of communication necessary, not the number of computational steps involved nor the amount of memory required to store the information.

than classical algorithms. It has been shown that every Bell Inequality is in fact linked to a corresponding communication complexity task [6]. The greater the amount of violation of the Bell Inequality by the quantum bound the larger the advantage of using the quantum system over a classical system. A quantum algorithm is said to have supremacy over a classical algorithm if the quantum algorithm is exponentially faster than the classical algorithm. In other words, it takes the quantum algorithm a polynomial amount of time, but it takes the classical algorithm an exponential amount of time. An example of an algorithm thought to have quantum supremacy is Shor's factorization algorithm, which has important applications in quantum cryptography and secure communications.

5.2 Device-Independent Quantum Key Distribution

Quantum key distribution (QKD) is where we generate a security key, that two parties use to communicate securely, whose security is based on and guaranteed by the laws of quantum physics. Current security protocols are based on factorization of a very large number into their primes. As we have seen in section 5.1, it might soon be possible to factorize such numbers into their primes using Shor's Algorithm and break the security of these systems. However, using non-locality we can also create a new security protocol that not even other quantum computers would be able to break. Such systems have proven to be difficult to implement experimentally due to information losses in the channels used by the parties over long distances, but such systems are already commercially available for use. However, some of these devices are still not completely secure due to loopholes in the experimental implementation of the devices, the design of which still has to be improved. Malicious eavesdroppers can exploit these imperfections of the devices to break the security.

As a result, attention has now shifted to designing a QKD protocol that does not make any assumptions about the inner workings of the devices used in its implementation, this is known as Device-Independent Quantum Key Distribution (DIQKD) [27]. Such protocols do not assume that the quantum systems involved are trustworthy, they could be malicious or noisy. The security of the protocol can be verified by observing the statistics of the systems. We would expect to see certain statistics or correlations between the two systems of the parties that would like to communicate. If the statistics do not match these then we can be sure that our system is not correlated with the system of the other party we would like to communicate with. This tells us that either our system is noisy and working incorrectly or that there is an eavesdropper present. If an eavesdropper listens in to the communication and tries to gain information on it by making a measurement, by the very act of measurement they change the state of the system and influence the statistics of the systems. Some protocols can even account for noisy systems [37]. These devices use the non-local correlations of quantum systems to verify the trustworthiness of the quantum devices used in the protocol. Using the statistics of the measurement outcomes to verify the quantum states is known as self-testing.

For such a device to work the correlations between the systems of the parties must not only violate a Bell Inequality but, it must achieve this without post-selection on the data. This along with the losses in the channels makes the implementation of DIQKD difficult, a few solutions to the channel loss have been proposed however. The first makes use of quantum non-demolition (QND) measurements and heralded noiseless qubit amplification to verify the arrival of the photon without disrupting the quantum state. The second makes use of a third intermediate party that makes measurements to determine whether the state shared between the first two parties is entangled. The former has been demonstrated recently in experiments [23] and the latter has also been implemented successfully closing some loopholes [15].

Because of the difficulty in implementing DIQKD other QKD protocols have also been developed that relax the conditions of DIQKD which are only partially device-independent. In measurement-DIQKD (MDIQKD) the state preparation is device-dependent, it requires the preparation of a specific quantum state, whilst the measurement remains device-independent [44]. There are even one-sided device-independent protocols, that make no assumptions about one of the quantum systems, but do make assumptions about the other [42]. There are also protocols that only require that the dimension of the quantum system used to be bounded. It is also possible to break the security of such systems if the quantum systems are being reused, these are called memory attacks [2].

5.3 Random Numbers

Random numbers have important uses many different fields including cryptography and numerical simulation of physical and biological systems. In cryptography, any imperfections in the random number generator used to encrypt a signal could allow an eavesdropper to intercept and unravel the message. In order for these random numbers to be use in these applications, they must be genuine random numbers and not pseudo-random. Over recent decades research [30] has shown that we can use these random non-local correlations between entangled systems to check or certify that the randomness observed in a system is genuine randomness. This is known as randomness certification. They can be used to help design better random number generators. Current random number generators rely on either complicated algorithms that appear random but are still deterministic underneath or natural physical processes that are unpredictable. It is difficult to control and measure the randomness of a given random number generator. Certain pseudo-random number generators pass current tests for genuine randomness eventhough they are deterministic, because the randomness is due to a lack of knowledge about the system. Quantum systems that are inherently random in nature can also exhibit a deterministic randomness due to their interactions with the environment, this also makes it difficult to quantify the random behaviour of quantum systems. If we use the random number generator in a Bell experiment and observe Bell Inequality violations, then we can guarantee that the randomness is not deterministic and that it arises due to the inherent randomness of quantum systems.

Another application of these random correlations is in random number generation. In device-independent random number generation (DIRNG) we can make a random number generator using the inherent random quantumness of two quantum systems without making any assumptions about how they operate. Randomness is related to entropy which consist of expressions that involve logarithms. From this we can see that one measure of the amount of randomness present in the quantum systems can be found by taking the logarithm of the probability distribution [32]. We start with an initial random seed and source and use the statistics to generate more random numbers, this is known as randomness expansion.

5.4 Self-Testing

We have already mentioned self-testing in section 5.2 when we discussed quantum key distribution, in this section we will discuss it in more detail. Self-testing is where we use the measurement statistics, the probability distribution, of quantum systems to gain information about the form of the quantum states or the measurements that were used to produce the statistics. Suppose we are given some probability distribution and only know the number of possible inputs and outputs, or measurements and outcomes, that were performed on the quantum systems. Self-testing tries to answer the question, what information can we gain about the quantum systems and the measurements performed upon them? This has importance in cryptography and security where we want certify the parties involved in a communication and in quantum technologies where we want to ensure that a device is working correctly. We test the device without making any assumptions about the inner workings of the device or performing any more measurements, hence the name self-testing.

Bell Inequalities are self-test expressions, certain quantum states and measurements violate the inequality whilst others do not. If the non-local correlations we observe, when make certain measurements, violate the Bell Inequality then we know that the quantum state cannot be any of those quantum systems that would not violate it. By studying the statistics we can determine some information about the quantum state. In the extreme case that we observe a maximal violation, then we can gain the most information about the quantum systems and the measurements performed on them. There may only be a few different combinations of states and measurements, related through local isometries, that result in the maximal violation. We would call this a perfect self-test. As an example, in the CHSH scenario there is only one quantum state for a given set of measurements that produce the maximal violation and we can determine precisely what state we have, up to rotations of measurements and states. In this simple scenario there is a unique maximizer of correlations but in more complicated scenarios with more inputs and outcomes this is not true, there may be additional degrees of freedom, see section IV of [19]. There can exist flat boundary regions of the quantum set where there are many quantum states and measurements that result in the same maximal quantum value. There may even be regions where the maximal violation is achieved by different measurements of the same state, this means we could self-test the state but not the measurements. Nevertheless, self-testing provides a powerful tool to certify quantum systems.

The self-tests do not have to be simple linear Bell Inequalities but can take a more complicated form, in recent work, self-tests have been created using commutation relations [22]. Violations of Bell Inequalities and non-local correlations are one example of a self-test but other self-tests also exist that do not use non-local correlations. There are inequalities that allow us to determine the dimension of the quantum systems [40], such expressions are called dimension witnesses. To be experimentally relevant self tests should also take into account noise.

6 This Work

In this work I extend upon previous work [39] on the topic of non-locality, where I created an algorithm which calculates a measure of the tightness of a given Bell Inequality by calculating the degree of intersection of the corresponding plane with the extremal points of the local polytope.

In order to understand how useful non-locality could be, it is important to be able to calculate the maximum classical and quantum correlations observable in a particular scenario. This project deals with the first of these problems. In order to calculate the maximum classical correlation one needs to derive the tight Bell Inequalities that characterise the local set of correlations, this has only been done for a few very simple systems. However, methods have been developed to derive non-trivial Bell Inequalities, from the calculation of robustness [17], which could still be useful for characterising the local set. Robustness is thought to always produce Bell Inequalities that at least touch the local polytope. They may only intersect one extremal point, or they may intersect an edge or face. We define the facet dimension of the Bell Inequality to be the number of linearly independent extremal points of the local polytope that the plane of the Bell Inequality intersects. This is a measure of how much the plane of the Bell inequality aligns with a facet of the polytope. Tight Bell inequalities will intersect with the most extremal points and therefore have the highest facet dimension; the facet dimension of a tight Bell Inequality will equal its spatial dimension.

Algorithms exist that calculate the maximum classical correlation of a Bell Inequality, but these algorithms are only valid for simple scenarios involving only a few parties and do not calculate the facet dimension of the Bell Inequality. Here we present, for the first time, an algorithm that can calculate both the maximum classical correlation and facet dimension of a general Bell Inequality of any scenario, with any number of parties, inputs or outputs.

In our previous work there were some drawbacks to the algorithm which we have now addressed in this work, these are:

1. The algorithm only worked for Bell inequalities that could be expressed in terms of correlators.
2. The algorithm only worked for scenarios in which each party has an equal number of measurements to choose from and there are an equal number of possible outcomes for each of these measurements.

The goal of this work was to modify the algorithm so that it can deal with an arbitrary Bell inequality as follows:

1. The algorithm should work for Bell inequalities that can be expressed in terms of probabilities.
2. The algorithm should work for scenarios in which all the parties have different numbers of measurements to choose from and have different numbers of outcomes they could observe for each of these measurements.

7 The Algorithm

The algorithm loops over all the possible extremal behaviours by varying the local probabilities and calculates the corresponding Bell value S of the left hand side of (15). It keeps track of the maximum Bell value it has found so far and the corresponding sets of local probabilities that give this maximum. The final maximum Bell value S_{max} will be the maximum classical bound of this Bell inequality. The algorithm then calculates the corresponding behaviours that give this maximum classical bound from the sets of local probabilities. The facet dimension is the number of linearly independent behaviours that lie on the corresponding plane of the inequality, which can be found by calculating the rank of the matrix of these behaviours.

Originally, the algorithm only worked for inequalities that could be expressed as a sum of correlators, and only for scenarios where all of the parties k can choose from an equal number of measurements $M_k = m$ and observe an equal number of possible outcomes $D_{m_k,k} = d$. The algorithm required four things as input in order to accomplish this:

1. The total number of parties involved n.
2. The number of measurements each party could make m.
3. The number of outcomes each party could observe for each of their measurements d.
4. A list of coefficients of correlators that specify the particular Bell inequality c_i.

Now, the algorithm requires only two things as input:

1. A list of the total number of outcomes each party could observe for their measurements $D_{m_k,k}$.
2. A list of coefficients $c_{i_j,j}$ of probabilities $p_{i_j,j}$ that specify the particular Bell inequality.

The list of number of outcomes $D_{m_k,k}$ will be 2-dimensional, the column specifies the party k and the row specifies the particular measurement m_k of that party. The list won't take the form of a simple matrix with dimensions Rows $\times$ Columns as the number of rows m_k of each column k depends on the column k. This list can be thought of as a list of column vectors of different sizes. In order to deal with this, a cell list structure is used. Information about both the number of parties involved n and the number of measurements each party can choose from M_k is contained within this list, they are the number of columns and rows respectively, and so no longer need to be specified independently.

$$D_{m_k,k} = \left(\begin{pmatrix} D_{1,1} \\ D_{2,1} \\ \vdots \\ D_{M_1,1} \end{pmatrix}, \begin{pmatrix} D_{1,2} \\ D_{2,2} \\ \vdots \\ D_{M_2,2} \end{pmatrix}, \cdots, \begin{pmatrix} D_{1,n} \\ D_{2,n} \\ \vdots \\ D_{M_n,n} \end{pmatrix} \right) \tag{20}$$

The list of coefficients of probabilities $c_{i_j,j}$ will also be 2-dimensional and have a form similar to that of the list of number of outcomes $D_{m_k,k}$. Each column j specifies the the measurement settings $\mathcal{M} = \{m_1, m_2, ..., m_n\}$ and the row i_j specifies a particular probability of getting one of the possible outcomes given the parties make those measurements. Since terms can arise where one or more of the parties do not make a measurement, the number of rows R_j also depends on the column j. For this reason, we also use a cell list structure for the list of probability coefficients. The corresponding list of probabilities $p_{i_j,j}$ will have the same dimension as $c_{i_j,j}$.

$$c_{i_j,j} = \left(\begin{pmatrix} c_{1,1} \\ c_{2,1} \\ \vdots \\ c_{R_1,1} \end{pmatrix}, \begin{pmatrix} c_{1,2} \\ c_{2,2} \\ \vdots \\ c_{R_2,2} \end{pmatrix}, \cdots, \begin{pmatrix} c_{1,J} \\ c_{2,J} \\ \vdots \\ c_{R_J,J} \end{pmatrix} \right) \tag{21}$$

The column j of a particular set of measurements $\mathcal{M} = \{m_1, m_2, ..., m_n\}$ can be found through (22). The total number of rows J can be found by subsituting $\mathcal{M} = \{M_1, M_2, ..., M_n\}$ into this expression.

$$j = \sum_{\substack{r=1 \\ m_r \in \mathcal{M}}}^{n} \left(m_r \prod_{k=r+1}^{n} (M_k + 1) \right) + 1 = m_n + m_{n-1}(M_n + 1) + m_{n-2}(M_{n-1} + 1)(M_n + 1) + ... + 1 \tag{22}$$

The number of rows R_j of the jth column of $c_{i_j,j}$ can be found by taking the product of the total number of outcomes $D_{m_r,r}$ for each of these measurements m_r in $\mathcal{M}$ that are non-zero (A.3h).

$$R_j = \prod_{\substack{r \\ \forall \{r \,|m_r \in \mathcal{M}\,,\, m_r \neq 0\}}} D_{m_r,r} \tag{23}$$

$j=$	1	2	...	M_n+1	M_n+2	...	J
$\mathcal{M}=$	$\{0,0,...,0,0\}$	$\{0,0,...,0,1\}$	...	$\{0,0,...,0,M_n\}$	$\{0,0,...,1,0\}$	...	$\{M_1,M_2,...,M_{n-1},M_n\}$

Table 1: The number associated with the measurement settings $\mathcal{M}$ is being incremented as the row j increases. Each digit r of this number can have a different maximum value M_r.

These concepts can be explained more easily through an example. Consider the CHSH inequality, in this scenario there are $n=2$ parties involved and therefore $D_{m_k,k}$ has 2 columns. Each party can choose from only 2 measurements $M_1=M_2=m=2$ and so the length of each column will be 2. Each party can only ever observe 2 possible outcomes when they make a measurement on their system so each element of the outcome list is 2, $D_{m_k,k}=2\,\forall\, m_k,k$.

$$D^{\mathsf{CHSH}}_{m_k,k}=\left(\begin{pmatrix}2\\2\end{pmatrix},\begin{pmatrix}2\\2\end{pmatrix}\right) \tag{24}$$

The total number of possible measurement settings found from (17) is 9 so there are 9 column vectors part of $c_{i_j,j}$ and $p_{i_j,j}$. The CHSH inequality expressed in terms of probabilities is given by (19).

The possible measurement settings in this scenario are $\mathcal{M}=\{0,0\}$, $\{0,1\}$, $\{0,2\}$, $\{1,0\}$, $\{1,1\}$, $\{1,2\}$, $\{2,0\}$, $\{2,1\}$, $\{2,2\}$ and the corresponding form of the list of probabilities is shown in (25). The subscripts 1 and 2 are used to help clarify which party is making the measurement.

$$\begin{aligned}p^{\mathsf{CHSH}}_{i_j,j}=\Bigg(&(1),\begin{pmatrix}P(1|1_2)\\P(2|1_2)\end{pmatrix},\begin{pmatrix}P(1|2_2)\\P(2|2_2)\end{pmatrix},\begin{pmatrix}P(1|1_1)\\P(2|1_1)\end{pmatrix},\begin{pmatrix}P(11|11)\\P(12|11)\\P(21|11)\\P(22|11)\end{pmatrix},\\&\begin{pmatrix}P(11|12)\\P(12|12)\\P(21|12)\\P(22|12)\end{pmatrix},\begin{pmatrix}P(1|2_1)\\P(2|2_1)\end{pmatrix},\begin{pmatrix}P(11|21)\\P(12|21)\\P(21|21)\\P(22|21)\end{pmatrix},\begin{pmatrix}P(11|22)\\P(12|22)\\P(21|22)\\P(22|22)\end{pmatrix}\Bigg)\end{aligned} \tag{25}$$

From (19) we can see that terms only arise where all the parties make measurements and so the only non-zero columns of $c_{i_j,j}$ are those where both parties make a measurement $\mathcal{M}=\{1,1\},\{1,2\},\{2,1\},\{2,2\}$. The corresponding list of coefficients is given in (26).

$$c^{\mathsf{CHSH}}_{i_j,j}=\left((0),\begin{pmatrix}0\\0\end{pmatrix},\begin{pmatrix}0\\0\end{pmatrix},\begin{pmatrix}0\\0\end{pmatrix},\begin{pmatrix}1\\-1\\-1\\1\end{pmatrix},\begin{pmatrix}1\\-1\\-1\\1\end{pmatrix},\begin{pmatrix}0\\0\end{pmatrix},\begin{pmatrix}1\\-1\\-1\\1\end{pmatrix},\begin{pmatrix}-1\\1\\1\\-1\end{pmatrix}\right) \tag{26}$$

As mentioned in my previous work, the algorithm loops over all the extremal behaviours by looping over the possible values of a set of numbers $\mathcal{I}$ which we call the index numbers, shown in (27).

$$\mathcal{I}=\{I_{1,1},I_{1,2},...,I_{m_k,k},...,I_{M_n,n}\} \tag{27}$$

The extremal behaviours are those probability distributions that obey the constraints (6), the number of these constraints is given by (7). Each one of these constraints states that the local probabilities of getting the different outcomes for a particular measurement of a party must sum to unity. Since these local probabilities are deterministic probabilities, probabilities that can only be 0 or 1, only one of these probabilities can be 1 at any given time. Each constraint is independent of the others as no local probability occurs in more than one of the constraints. Together this tells us that the total number of extremal behaviours can be found by calculating the total number of ways of distributing the 1s amongst the probabilities in the constraints. We can

even determine the exact form of these behaviours as we know the form of the local probabilities.

We can use a set of numbers $\mathcal{I}$ to denote which of the probabilities in each constraint is currently 1. We call these the index numbers, they index which of the probabilities are 1. There is one index number for each constraint, and like each constraint, each index number $I_{m_k,k}$ is denoted by the measurement m_k and the party k. The maximum number that these index variables can take is equal to the maximum number of outcomes for that particular measurement of that party $D_{m_k,k}$.

From the set of index numbers $\mathcal{I}$ we can calculate the local probabilities and therefore $p_{i_j,j}$ and the behaviours. All the extremal behaviours can be found by varying the values of these index numbers, the search space of the algorithm is represented as a tree diagram. Because the maximum number of these index variables can all be different, the branching factor in the search tree of the algorithm can be different at each depth as shown in Figure 4.

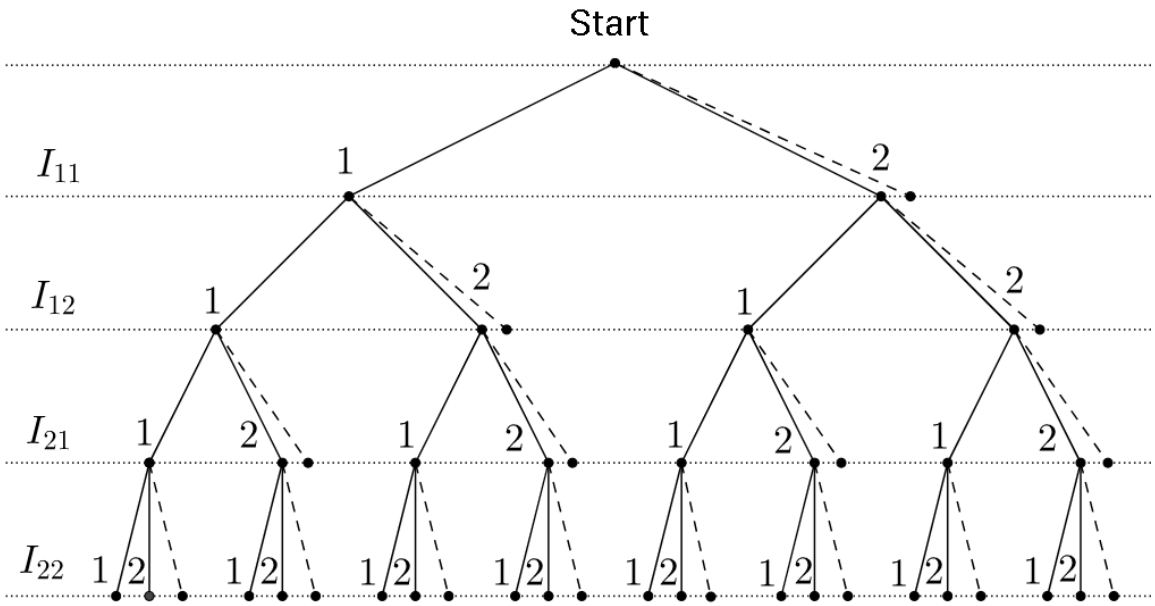


Figure 4: An example of the index number search space of the algorithm. The search space takes the form of a tree diagram. The branching factor at each depth can vary and is given by the numbers $D_{m_k,k}$. Each node represents a particular value of one of the index numbers. Nodes at the same depth represent different values of the same index number. The values of the index numbers at each final node can be used to determine the exact form of one of the extremal behaviours.

As an example, consider the index numbers for the CHSH inequality. There will be 4 index variables in total as there are 2 parties $n = 2$ and they can both make two measurements each $M_1 = M_2 = 2$, so $\mathcal{I}$ will take the form (28).

$$\mathcal{I}^{\text{CHSH}} = \{I_{1,1}, I_{2,1}, I_{1,2}, I_{2,2}\} \tag{28}$$

There are two possible outcomes for each of these measurements $D_{m_k,k} = 2$ so there will be a total of 8 local probabilities which we can also denote as a set $\mathcal{P}_{local}$ as shown in (29). The dashed vertical lines are used to separate the local probabilities that belong to different constraints.

$$\mathcal{P}_{local} = \{P(1|1_1), P(2|1_1) \,\vdots\, P(1|2_1), P(2|2_1) \,\vdots\, P(1|1_2), P(2|1_2) \,\vdots\, P(1|2_2), P(2|2_2)\} \ . \tag{29}$$

Table 2 lists some of the possible values of the CHSH index numbers $\mathcal{I}^{\text{CHSH}}$ and the corresponding values of the local probabilities $\mathcal{P}_{local}$.

Comments have also been added to the code and most of the variables and methods have been renamed for better readability. The new list of methods are given in Table 3. All the functions have just been generalised to deal with the general case. Instead of a method to calculate the correlator we now have a method to calculate the individual probabilities "calcProb".

$\mathcal{I} =$	$\{1,1,1,1\}$	$\{1,1,1,2\}$	...	$\{2,2,2,2\}$
$\mathcal{P}_{local} =$	$\{10 \vdots 10 \vdots 10 \vdots 10\}$	$\{10 \vdots 10 \vdots 10 \vdots 01\}$	...	$\{01 \vdots 01 \vdots 01 \vdots 01\}$

Table 2: The index numbers $\mathcal{I}^{\mathsf{CHSH}}$ determine which local probabilities $\mathcal{P}_{local}$ are 1, the rest are 0.

Method	**Description**
calc	Starts the calculation of the facet dimension and classical bound.
loopExtremalBehaviours	Loops over the extremal behaviours and calculates the Bell value.
getLocalProbIndex	Calculates the index of a particular local probability within the list of local probabilities.
calcProb	Calculates the probability the parties get a particular set of outcomes for the measurements they make.
calcProbDists	Calculates all the behaviours from the sets of local probabilities that give the classical bound.
calcProbDist	Calculates the behaviour of a given set of local probabilities.
calcDim	Calculates the dimension from the behaviours that give the classical bound.

Table 3: The methods part of the class which calculates the classical bound and facet dimension of a Bell Inequality.

Shown in Figure 5 is a flowchart of how the main method loopExtremalBehaviours loops over all the possible extremal behaviours by looping over all the possible values of the index numbers. For each value of the index numbers it loops over all the elements of the probability coefficient list *probCoeffList* and calculates the contribution to the Bell value. Once it has calculated the Bell value for this set of local probabilities *s*, it compares it to the maximum Bell value found so far *sMax* and then either stores this set of local probabilities or discards it. If it has found a new maximum then it discards all of the previous sets of local probabilities that gave the old maximum. At the end of this the program calculates the behaviours from the local probabilities and the facet dimension from these.

8 Testing And Results

The algorithm was tested against eight tight inequalities. Tests 1-4 are the CHSH inequality [10], equation 19 in [11], equation 8 in [43] and example 4 in [7] respectively. Tests 5-7 are equations 11 and 12 in [8] and equation 10 in [11] respectively.

Tests 1-6 are all inequalities involve scenarios where the parties can all perform the same number of measurements and observe the same number of outcomes for each of these measurements. But now, Tests 5 and 6 test that the algorithm works for higher numbers of parties n. Test 7 is an inequality in a scenario where the parties can make different numbers of measurements.

Test	$D_{m_k,k}$	**Expected**		**Calculated**		**Result**
		Dimension	**Bound**	**Dimension**	**Bound**	
1	((2;2),(2;2))	7	2	7	2	Pass
2	((2;2;2),(2;2;2))	14	0	14	0	Pass
3	((2;2),(2;2),(2;2))	25	6	25	6	Pass
4	((2;2;2),(2;2;2),(2;2;2))	62	8	62	8	Pass
5	((2;2),(2;2),(2;2),(2;2))	79	2	79	2	Pass
6	((2;2),(2;2),(2;2),(2;2),(2;2))	241	2	241	2	Pass
7	((2;2),(2;2;2))	10	0	10	0	Pass

Table 4: The Inequalities the program was tested against and the results.

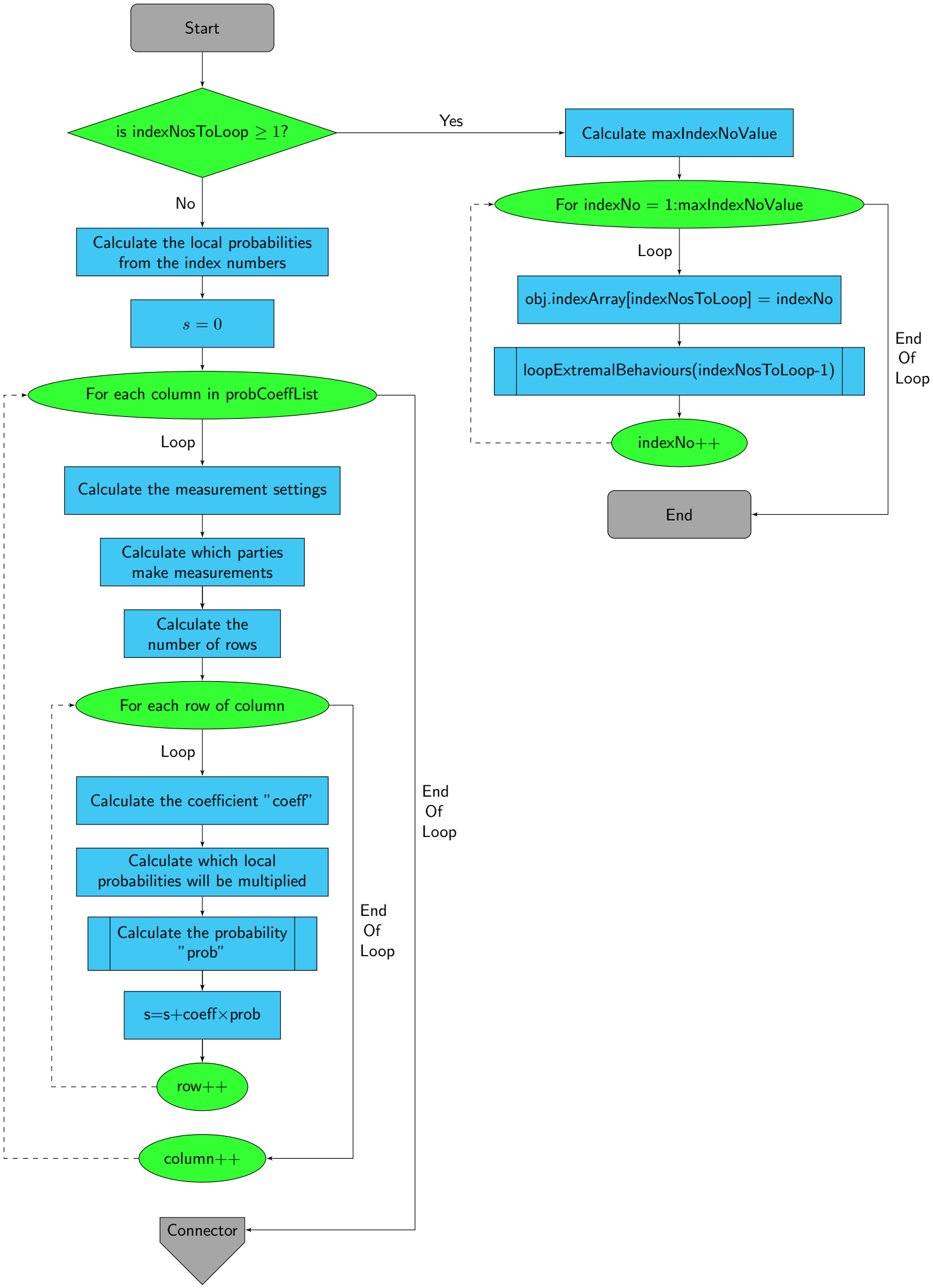
The algorithm successfully produced the correct results for all of these inequalities where the input was a list of probability coefficients. This should convice the reader the algorithm works for scenarios where the parties can choose from different numbers of measurements. There is not much in the literature in terms of inequalities in scenarios in which the parties can observe different numbers of outcomes, this is because we are usually only interested in binary-outcome measurements. For this reason, the algorithm has not been tested against this case.

9 Conclusions And Further Work

Extending on previous work, we generalised our algorithm which calculates a measure of how tight a given Bell Inequality is. Previously our algorithm worked only for those inequalities that could be expressed in terms of correlators and only involved scenarios where the parties could choose from an equal number of measurements and observe the same number of outcomes for each of these measurements. Now, the algorithm has been developed to work for any Bell inequality in general scenarios where the parties can choose from different numbers of measurements and observe different numbers of outcomes for each of these measurements.

The algorithm was tested against an array of different tight Bell inequalities and successfully calculated the correct dimension and classical bound. It successfully calculates these quantities for inequalities in probability form and for inequalities where the parties can make different numbers of measurements. However, it still needs to be tested against inequalities involving scenarios with different numbers of outcomes.

In our next work, we are going to use another program which calculates a Bell inequality through robustness from a given quantum state and measurements and apply this algorithm to study how the facet dimension of these Bell inequalities varies for different states and measurements and search for useful tight Bell inequalities and try to maximise the facet dimension.


Start
is indexNosToLoop ≥ 1?
Yes
No
Calculate maxIndexNoValue
For indexNo = 1:maxIndexNoValue
Loop
obj.indexArray[indexNosToLoop] = indexNo
loopExtremalBehaviours(indexNosToLoop-1)
indexNo++
End Of Loop
End
Calculate the local probabilities from the index numbers
$s = 0$
For each column in probCoeffList
Loop
Calculate the measurement settings
Calculate which parties make measurements
Calculate the number of rows
For each row of column
Loop
Calculate the coefficient "coeff"
Calculate which local probabilities will be multiplied
Calculate the probability "prob"
s=s+coeff×prob
row++
End Of Loop
column++
End Of Loop
Connector

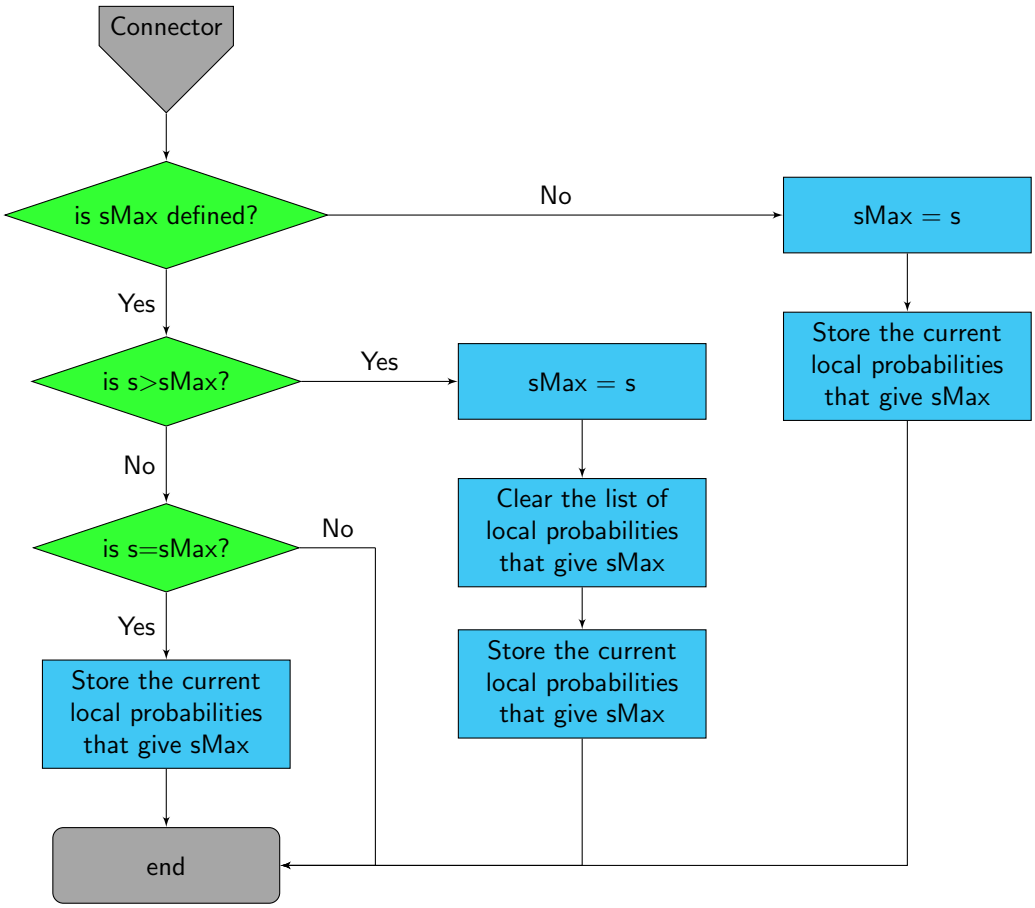


Figure 5: A flowchart of the function loopExtremalBehaviours which calculates the classical value achievable for each extremal behaviour.

A Appendix

The no-signalling conditions require that the marginals of the joint probability distribution be well defined. It can be shown that the quantum behaviours satisfy the no-signalling conditions as follows.

$$\begin{aligned}\sum_{d_n} P(d_{m_1,1}d_{m_2,2}...d_{m_n,n}|m_1m_2...m_n) &= \mathrm{Tr}\left(M_{m_1}^{d_{m_1,1}} \otimes M_{m_2}^{d_{m_2,2}} \otimes ... \otimes \left(\sum_{d_n} M_{m_n}^{d_{m_n,n}}\right) \rho\right) \\ &= \mathrm{Tr}\left(M_{m_1}^{d_{m_1,1}} \otimes M_{m_2}^{d_{m_2,2}} \otimes ... \otimes \mathbb{1}\, \rho\right) \\ &= \mathrm{Tr}\left(M_{m_1}^{d_{m_1,1}} \otimes M_{m_2}^{d_{m_2,2}} \otimes ... \otimes M_{m_{n-1}}^{d_{m_{n-1},n-1}} \rho_{1,..,n-1}\right) \\ &= P(d_{m_1,1}d_{m_2,2}...d_{m_{n-1},n-1}|m_1m_2...m_{n-1})\end{aligned} \tag{A.1}$$

Where $\rho_{1,...,n-1}$ is the reduced state found by tracing out over the nth party. This was done by marginalizing over the nth party, but a similar derivation can be done for any party or set of parties.

We can combine the fact that the joint probability distributions of the extremal behaviours can be expressed as a product of the single party local deterministic probabilities with no the no-signalling conditions to end up

with a simpler constraint to check.

$$\begin{aligned}
&\forall\ m_k, m_k' \in M_K, \quad \forall\ k \in \{1,...,n\}, \quad \forall\ d_{m_i,i}, m_i \in D_{m_i,i}, M_i\ (i \neq k) \\
&\sum_{d_{m_k,k}} P(d_{m_1,1}...d_{m_k,k}...d_{m_n,n}|m_1...m_k...m_n) = \sum_{d_{m_k,k}} P(d_{m_1,1}...d_{m_k,k}...d_{m_n,n}|m_1...m_k'...m_n) \\
&\sum_{d_{m_k,k}} D_1(d_{m_1,1}|m_1)...D_k(d_{m_k,k}|m_k)...D(d_{m_n,n}|m_n) = \sum_{d_{m_k,k}} D_1(d_{m_1,1}|m_1)...D_k(d_{m_k,k}|m_k')...D(d_{m_n,n}|m_n) \\
&\sum_{d_{m_k,k}} D_k(d_{m_k,k}|m_k) = \sum_{d_{m_k,k}} D_k(d_{m_k,k}|m_k') \quad \forall\ m_k, m_k' \in M_k \quad \forall\ k \in \{1,...,n\}
\end{aligned} \tag{A.2a}$$

We can also combine the fact that the joint probability distributions can be expressed as products with the normalisation conditions to end up with a second constraint.

$$\begin{aligned}
&\sum_{d_{m_1,1},...,d_{m_n,n}} P(d_{m_1,1}...d_{m_n,n}|m_1...m_n) = 1 \quad \forall\ m_1,...,m_n \\
&\sum_{d_{m_1,1}} \sum_{d_{m_2,2}} ... \sum_{d_{m_n,n}} D_1(d_{m_1,1}|m_1) D_2(d_{m_2,2}|m_2)...D_n(d_{m_n,n}|m_n) = 1 \quad \forall\ m_1,...,m_n \\
&\sum_{d_{m_1,1}} D_1(d_{m_1,1}|m_1) \cdot \sum_{d_{m_2,2}} D_2(d_{m_2,2}|m_2) \cdot ... \cdot \sum_{d_{m_n,n}} D_n(d_{m_n,n}|m_n) = 1 \quad \forall\ m_1,...,m_n
\end{aligned} \tag{A.2b}$$

The products of the sums over each individual party's local deterministic probabilities must be unity. However, if we study this more closely we can reduce this further. Consider the values that each of these sums could take, we know that each of these sums can in principle take any integer value from 0 to d, the number of items summed over, since each deterministic probability must be either zero or one. However, suppose one of them does take a value greater than 1, say 2, then in order for the overall expression to be unity the rest of the products must be a fraction, here $1/2$. But this is impossible since as we just mentioned each sum can only take integer values. This implies that none of the sums can take a value greater than 1. Also, if one of the sums takes a value 0 then the whole expression would be invalid, these together imply that each of the sums must individually be unity.

$$\sum_{d_{m_k,k}} D_k(d_{m_k,k}|m_k) = 1 \quad \forall\ m_k \in M_k \quad \forall\ k \in \{1,...,n\} \tag{A.2c}$$

Comparing this to the previous constraint found (A.2a) we can see that this second one (A.2c) is more restrictive than the first and so the first can be discarded. Therefore, in order to check that the behaviours satisfy both the normalisation and no-signalling conditions and so represent real physical extremal behaviours, one only needs to check they obey (A.2c).

In order to convince the reader of the accuracy of these newly derived expressions, in this section, we will demonstrate that they reduce to their previous forms and produce the correct results for CHSH. We assume that all of the parties k can choose from $M_k = m$ measurements and observe $D_{m_k,k} = d$ possible outcomes for each of these measurements.

The dimensions of the behaviours are

$$b = \prod_{k=1}^{n} \left(\sum_{m_k=1}^{M_k} D_{m_k k} \right) = \prod_{k=1}^{n} \left(\sum_{m_k=1}^{m} d \right) = (md)^n \tag{A.3a}$$

The number of constraints is

$$n_{con} = \sum_{k=1}^{n} M_k = \sum_{k=1}^{n} m = nm \tag{A.3b}$$

The number of extremal behaviours is

$$n_{ex} = \prod_{k,m_k} D_{m_k,k} = \prod_{k=1}^{n} \left(\prod_{m_k=1}^{m} d \right) = d^{nm} \tag{A.3c}$$

The dimension of the polytope is

$$\dim \mathcal{L} = \prod_{k=1}^{n} \left(\sum_{m_k=1}^{M_k} (D_{m_k k} - 1) + 1 \right) - 1 = \prod_{k=1}^{n} \left(\sum_{m_k=1}^{m} (d-1) + 1 \right) - 1 = (m(d-1)+1)^n - 1 \tag{A.3d}$$

Similarly, the dimension of the Bell inequalities is one less than this.

The number of measurement settings is

$$n_{set} = \prod_{k=1}^{n} (M_k + 1) = \prod_{k=1}^{n} (m+1) = (m+1)^n \tag{A.3e}$$

Now, we will demonstrate that the expressions for the number of columns (22) and rows (A.3h) in the coefficient list $c_{i_j,j}$ are correct for the CHSH inequality. In this case, we have $M_k = 2$ and $n = 2$. For the number of columns, When every party doesn't make a measurement $m_r = 0$, we end up with the first column $j = 1$ as the expression disappears. Now consider the case that both parties make their second measurement $m_r = 2$, we expect the last of the 9 columns.

$$j = \sum_{\substack{r=1 \\ m_r \in \mathcal{M}}}^{n} \left(m_r \prod_{k=r+1}^{n} (M_k + 1) \right) + 1 = \sum_{r=1}^{2} \left(2 \prod_{k=r+1}^{2} (2+1) \right) + 1 = 2 \cdot 3 + 2 \cdot 1 + 1 = 9 \tag{A.3f}$$

Now consider the case that the first party makes their first measurement $m_1 = 1$ and the second party makes their second measurement $m_2 = 2$. This represents column 6.

$$j = \sum_{\substack{r=1 \\ m_r \in \mathcal{M}}}^{2} \left(m_r \prod_{k=r+1}^{2} (2+1) \right) + 1 = 1 \cdot 3 + 2 \cdot 1 + 1 = 6 \tag{A.3g}$$

Since all the parties have the same number of outcomes, the number of rows of the coefficient list for CHSH depends only on the number of parties that make measurements $n' \leq n$.

$$R_j = \prod_{\forall \{r \,|m_r \in \mathcal{M}\,,\, m_r \neq 0\}}^{r} D_{m_r,r} = \prod_{k=1}^{n'} d = d^0 \text{ or } d^1 \text{ or } d^2 = 1 \text{ or } 2 \text{ or } 4 \tag{A.3h}$$

References

[1] Alain Aspect, Jean Dalibard, and Gérard Roger. Experimental test of bell's inequalities using time-varying analyzers. *Phys. Rev. Lett.*, 49:1804–1807, Dec 1982.

[2] Jonathan Barrett, Roger Colbeck, and Adrian Kent. Memory attacks on device-independent quantum cryptography. *Phys. Rev. Lett.*, 110:010503, Jan 2013.

[3] J. S. Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1:195–200, 1964.

[4] J.S. Bell. *Speakable and unspeakable in quantum mechanics*. Cambridge University Press, 1987.

[5] G. Brida, I. P. Degiovanni, M. Genovese, A. Migdall, F. Piacentini, S. V. Polyakov, and I. Ruo Berchera. Experimental realization of a low-noise heralded single-photon source. *Opt. Express*, 19(2):1484–1492, Jan 2011.

[6] Časlav Brukner, Marek Żukowski, Jian-Wei Pan, and Anton Zeilinger. Bell's inequalities and quantum communication complexity. *Phys. Rev. Lett.*, 92:127901, 2004.

[7] Jing-Ling Chen and Dong-Ling Deng. Bell inequality for qubits based on the cauchy-schwarz inequality. *Phys. Rev. A*, 79:012115, 2009.

[8] Jing-Ling Chen and Dong-Ling Deng. Tight correlation-function bell inequality for multipartite d-dimensional systems. *Phys. Rev. A*, 79:012111, Jan 2009.

[9] B. S. Cirel'son. Quantum generalizations of bell's inequality. *Letters in Mathematical Physics*, 4(2):93–100, 1980.

[10] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23:880–884, 1969.

[11] Daniel Collins and Nicolas Gisin. A relevant two qubit bell inequality inequivalent to the chsh inequality. *Journal of Physics A: Mathematical and General*, 37(5):1775, 2004.

[12] Shellee D. Dyer, Burm Baek, and Sae Woo Nam. High-brightness, low-noise, all-fiber photon pair source. *Opt. Express*, 17(12):10290–10297, Jun 2009.

[13] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47:777–780, 1935.

[14] Artur K. Ekert. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.*, 67:661–663, 1991.

[15] Hensen B et al. Loophole-free bell inequality violation using electron spins separated by 1.3 kilometres. *Nature*, 526:682, Jun 2015.

[16] Robert J A Francis-Jones and Peter J Mosley. Fibre-integrated noise gating of high-purity heralded single photons. *Journal of Optics*, 19(10):104005, 2017.

[17] Joshua Geller and Marco Piani. Quantifying non-classical and beyond-quantum correlations in the unified operator formalism. *Journal of Physics A: Mathematical and Theoretical*, 47(42):424030, 2014.

[18] Marissa et al Giustina. Significant-loophole-free test of bell's theorem with entangled photons. *Phys. Rev. Lett.*, 115:250401, Dec 2015.

[19] Koon Tong Goh, J edrzej Kaniewski, Elie Wolfe, Tamás Vértesi, Xingyao Wu, Yu Cai, Yeong-Cherng Liang, and Valerio Scarani. Geometry of the set of quantum correlations. *Phys. Rev. A*, 97:022104, Feb 2018.

[20] B. R. et al Johnson. Quantum non-demolition detection of single microwave photons in a circuit. *Nature Physics*, 6:663, June 2010.

[21] Norbert Kalb, Andreas Reiserer, Stephan Ritter, and Gerhard Rempe. Heralded storage of a photonic quantum bit in a single atom. *Phys. Rev. Lett.*, 114:220501, Jun 2015.

[22] J edrzej Kaniewski. Self-testing of binary observables based on commutation. *Phys. Rev. A*, 95:062323, Jun 2017.

[23] Xiang G. Y. Ralph T. C. Pryde G. J. Kocsis, S. Heralded noiseless amplification of a photon polarization qubit. *Nature Physics*, 9(23), 2016.

[24] Yeong-Cherng Liang, Nicholas Harrigan, Stephen D. Bartlett, and Terry Rudolph. Nonclassical correlations from randomly chosen local measurements. *Phys. Rev. Lett.*, 104:050401, Feb 2010.

[25] Nobuyuki Matsuda, Hidetaka Nishi, Peter Karkus, Tai Tsuchizawa, Koji Yamada, William John Munro, Kaoru Shimizu, and Hiroki Takesue. Generation of entangled photons using an arrayed waveguide grating. *Journal of Optics*, 19(12):124005, 2017.

[26] Alberto Montina and Stefan Wolf. Information-based measure of nonlocality. *New Journal of Physics*, 18(1):013035, 2016.

[27] Alejandro Mttar and Antonio Acn. Implementations for device-independent quantum key distribution. *Physica Scripta*, 91(4):043003, 2016.

[28] Miguel Navascués, Stefano Pironio, and Antonio Acín. A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. *New Journal of Physics*, 10(7):073013, 2008.

[29] S. Pironio. *Aspects of quantum non-locality*. PhD thesis, Université Libre de Bruxelles, 2004.

[30] S. et al Pironio. Random numbers certified by bells theorem. *Nature*, 464:1021, Apr 2010.

[31] Stefano Pironio. Lifting bell inequalities. 2005.

[32] Mataj Pivoluska and Martin Plesch. Device independent random number generation. 64:600–663, 02 2015.

[33] Raphael C. Pooser, Dennis D. Earl, Philip G. Evans, Brian Williams, Jason Schaake, and Travis S. Humble. Fpga-based gating and logic for multichannel single photon counting. *Journal of Modern Optics*, 59(17):1500–1511, 2012.

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

[35] Ravishankar Ramanathan, Jan Tuziemski, Michał Horodecki, and Paweł Horodecki. No quantum realization of extremal no-signaling boxes. *Phys. Rev. Lett.*, 117:050401, Jul 2016.

[36] Wenjamin Rosenfeld, Daniel Burchardt, Robert Garthoff, Kai Redeker, Norbert Ortegel, Markus Rau, and Harald Weinfurter. Event-ready bell test using entangled atoms simultaneously closing detection and locality loopholes. *Phys. Rev. Lett.*, 119:010402, Jul 2017.

[37] Valerio Scarani and Christian Kurtsiefer. The black paper of quantum cryptography: Real implementation problems. *Theoretical Computer Science*, 560:27 – 32, 2014.

[38] Lynden K. et al Shalm. Strong loophole-free test of local realism. *Phys. Rev. Lett.*, 115:250402, Dec 2015.

[39] Neil C. Smith. An algorithm to calculate the facet dimension of a bell inequality. July 2017.

[40] Armin Tavakoli, Jedrzej Kaniewski, Tamas Vertesi, Denis Rosset, and Nicolas Brunner. Self-testing quantum states and measurements in the prepare-and-measure scenario. *arXiv preprint arXiv:1801.08520*, 2018.

[41] Reinhard F. Werner and Michael M. Wolf. Bell inequalities and entanglement. *Quantum Info. Comput.*, 1(3):1–25, 2001.

[42] Erik Woodhead. Semi device independence of the bb84 protocol. *New Journal of Physics*, 18(5):055010, 2016.

[43] Chunfeng Wu, Jing-Ling Chen, L. C. Kwek, and C. H. Oh. Correlation-function bell inequality with improved visibility for three qubits. *Phys. Rev. A*, 77:062309, 2008.

[44] Liang-Yuan et al Zhao. Loss-tolerant measurement-device-independent quantum private queries. *Scientific Reports*, 7:39733, Jan 2017.

[45] G.M. Ziegler. *Lectures on Polytopes*. Graduate Texts in Mathematics. Springer New York, 2012.