Semi-device Independent Protocols for Quantum Key Distribution

José Jesus[1]

[1] *Instituto Superior Técnico, Lisbon, Portugal*

In this work Bell polytopes and quantum correlations were explored for Semi-Device Quantum Key Distribution (SDI QKD). To that end, different new Bell polytope were explored in order to find new Bell inequalities that show promise in quantum communications. We present a first complete description of the polytopes (6,3,2,2) (3,3,3,2) and (3,2,3,3) and an incomplete description of the polytopes (2,2,4,4), (3,3,2,4) and (4,3,3,2). For every inequality generated we provide some properties of interest, namely the quantum bound, the minimum detector efficiency to close the detection loophole and an upper bound on the dimension the states necessary to achieve the maximum quantum score. We explored how these inequalities performed under an SDI QKD setting. This protocol was performed under a dimension bound, where the system shared between Alice, Bob and Eve was limited to a maximum dimension of $d = 64$. The best performing inequalities were $I2244^1$ and $I[[2,2,3,3],[2,2,2]]^2$. $I2244^1$ showed a minimum detector efficiency to distil a secret key rate of $\eta_{QKD} = 0.920$ and a maximum secret key rate of 1.979. $I[[2,2,3,3],[2,2,2]]^2$ showd a minimum detector efficiency to distil a secret key rate of $\eta_{QKD} = 0.912$ and a maximum secret key rate of 1.284. This shows some advantages when compared with the simplest scenario (CHSH) for which we found a minimum detector efficiency to generate randomness of $\eta = 0.706$, a minimum detector efficiency to distill secret keys of $\eta_{QKD} = 0.928$ and a maximum secret key rate of 1.000.

Introduction

The development of quantum computers has the potential to usher a revolution in computation and science. Indeed, a quantum computer can utilize the quantum properties of nature to gain computational advantages. At the same time this poses a new challenge regarding security: the hard computational problems that a quantum computer could potentially solve much faster than a classical computer are the same kind of problems that are the cornerstone of modern day encryption.

A typical example would be the vastly used cryptographic protocol RSA (Rivest–Shamir–Adleman) for secure data transmission that is built upon the assumption that integer factorization is a hard problem for computers and therefore it would take a vast amount of resources and time to decode the data, making it practically impossible. This however, is not true if the attacker has access to a quantum computer as shown by Peter Shor in 1994 [**?**].

Given the recent investment by governments and companies on quantum computers this is a problem that needs to be solved. One possible solution is Quantum Key Distribution (QKD), a collection of protocols that harnesses the potentials of quantum mechanics and are provably secure.

However, it has become clear that we can go even further with device independent (DI) cryptography. In these types of protocols quantum correlations are exploited to achieve QKD even with untrusted devices, a remarkable achievement. This type of security is based only on the assumption that the laws of quantum mechanics are complete and not on time or computational resources. Any potential faults introduced intentionally or unintentionally are detected automatically making these protocols inherently more robust.

There are a few drawbacks to DI cryptography however, namely it's extreme difficulty of implementation in the lab. Therefore, it is more important to take realistic approaches when creating cryptographic protocols whilst trying to preserve the interesting ideas of device independence. Such protocols are known as Semi-Device independent (SDI) protocols and require a well-founded assumption about the measuring devices or the resources used. Common approaches involve imposing an upper bound on the dimensions of the quantum resources used in the protocol, as was used in [**?**], imposing a bound on the information content of the source of the quantum states, as was used in [**?**] or imposing a limit in the energy used by these resources, as was used in [**?**].

The objective of the work here presented is to study these new quantum cryptographic protocols with the ultimate goal of going beyond the established protocols and identifying new quantum scenarios that could be useful for DI and SDI cryptography in the future.

Preliminaries

Approaching Device Independence

To achieve DI and SDI we need a quantum resource that can be used to validate the measuring devices from the statistics obtained from the measurements alone. If we tested a device by using a local/classical resource an evil genius could figure out a way to cheat in the test based solely on the measurements of the device compromising the protocol's security.

To better illustrate this let us consider the following

scenarios: the Bell games (called games in analogy to a quiz - we have participants -Alice and Bob - that are tested with some question to which, depending of their response, they can either win/pass or lose/fail).

A Bell game consist of many rounds. In each round the players are separated, each receives an input and provides an output. The rules of the game and the list of all possible inputs are known by the players in advance. They then work out some common strategy in order to try to beat the game. This strategy is simply what kind of process the players will use in each round. It is also important to know what kind of resources the players have available. These can be classified into 2 categories, (classical) signaling resources which allow communication between the players and no-signaling resources which do not.

A Bell game is won if the statistics produced by the players are nonlocal. Signaling resources allow for the players to beat any kind of Bell game because in this case the game is no longer local and based on the inputs the players can always decide on the right answer. Therefore signaling resources must not be allowed and we need to focus on no-signaling.

At this point it is also important to formalize the definition of locality in the context of a Bell game. This definition follows the one used by Valerio Scarani in [**?**]. By denoting λ as the process we can say that Alice generates a from probability distribution $P_\lambda(a|x)$ and Bob generates b from $P_\lambda(b|y)$. The process is local if the statistics observed by a verifier can be expressed as:

$$P(a,b|x,y) = \int d\lambda Q(\lambda) P_\lambda(a|x) P_\lambda(b|y) \tag{1}$$

where $Q(\lambda)$ describes the strategy used. In an experiment, the statistics $P(a,b|x,y)$ are obtained from Alice's measurement on her system with the output a associated to a Positive Operator Valued Measurement (POVM) Π_x^a and from Bob's measurement on his system with the output b associated to the POVM Π_y^b:

$$P(a,b|x,y) = Tr(\Pi_x^a \otimes \Pi_y^b \rho_{AB}) \tag{2}$$

where ρ_{AB} describes the shared quantum resource between Alice and Bob.

Not all statistics $P(a,b|x,y)$ can be written as in 1 as was proven by John Bell in 1964 [**?**] and that's exactly what will allow for DI, SDI protocols and self-testing of measurement devices.

The Local Polytope

Having identified the need to look for quantum correlations it is now necessary to understand how these can be found in different scenarios and to establish the necessary analysis techniques that allow their identification.

To achieve this it is necessary to study probability distributions and to characterize the set $\mathcal{L}$ of all local behaviours. To this end it is useful to first define the no-signalling conditions that all local processes must obey and define local deterministic processes, given that this class of events plays a crucial role. First and foremost a process λ is called no signaling if the outcome for one player is not affected by the inputs of another player. That is:

$$\begin{aligned} P_\lambda(a|x,y) &= \sum_b P_\lambda(a,b|x,y) = P_\lambda(a|x,y') = P_\lambda(a|x) \\ P_\lambda(b|x,y) &= \sum_a P_\lambda(a,b|x,y) = P_\lambda(b|x',y) = P_\lambda(b|y) \end{aligned} \tag{3}$$

for any input and output. At the same time a process is deterministic if it can be written as $Q(\lambda) = \delta(\lambda - \lambda_d)$ (a probability distribution is deterministic when it takes only values zero and one) and therefore combining the no signaling conditions with 1 we can write:

$$P_\lambda(a|x) = \delta_{a=f(\lambda,x)} \quad P_\lambda(b|y) = \delta_{b=g(\lambda,y)} \tag{4}$$

where f and g are deterministic maps dependent on the process λ and the respective input for each player.

From these, it's possible to extract the properties of $\mathcal{L}$. First, by Fine's theorem [**?**] a behaviour $\mathcal{P}$ will be local if and only if it is a convex mixture of local deterministic processes:

$$P(a,b|x,y) = \sum_{j=1}^{m_A^{M_A}} \sum_{k=1}^{m_B^{M_B}} q_{jk} \delta_{a=f_j(x)} \delta_{b=g_k(y)} \tag{5}$$

At the same time since probabilities are bounded, that is $0 \leq P(a,b|x,y) \leq 1$, the set $\mathcal{L}$ is compact. Since a compact convex set is the convex hull of its extremal points as shown in the Krein-Milman theorem [**?**] the extremal points of $\mathcal{L}$ will be all the deterministic ones. This way, from these points we can construct a geometric structure in which all the local behaviours exist, the Local Polytope.

This geometric construction is incredibly helpful in finding non-local behaviours. Indeed the facets of the polytope (i.e the generalization of the concept of face from 3 dimensions to N dimensions) represent the border between local and non-local sets of behaviours. That is, the inequalities that need to be violated in order to attain DI and SDI will be facets of a polytope. Given that polytopes can be fully identified by either the facets or the extremal points these representations are the dual of each other. Therefore the problem of obtaining the facets from the extremal points, which are easy to obtain, is a feasibility linear program, a simple

instance of convex optimization. This problem, the facet enumeration problem, quickly becomes computationally challenging because the number of vertices and the dimension of the polytope increase very rapidly with the numbers of inputs/outputs.

In this work we use the Collins-Gisin notation, first introduced in 2004 in [**?**]. Indeed in the CG notation we take full advantage of the no signaling conditions and positivity conditions to write the polytope in it's irreducible form. In this notation there are entries for each value of the inputs while one value of the output can be skipped and reconstructed from the rest. This is very convenient for obtaining the extremal points of the local polytope for the values of P_A and P_B simply go from 0 to N-1 in binary (N being the number of marginal probabilities here considered) and the remaining values are simply the product of the respective marginals (i.e $P(00|00) = P_A(0|0) \times P_B(0|0)$. L represents the local bound of the facet.

For a more compact notation, we consider that Alice's outputs are labelled going from 0 to m_A-1 and her inputs go from 0 to $M_A - 1$. The same for Bob. We represent the probabilities in vector form were we first write the coefficients of the joint probabilities between Alice and Bob followed by the coefficients of Alice's marginals and then Bob's. The last term of the vector represents the local bound.

$$[CP(00|00), ..., CP(m_A - 2m_B - 2|M_A - 1M_B - 1), \\ CP_A(0|0), ..., CP_A(m_A - 2|M_A - 1), CP_B(0|0), ..., \\ CP_B(m_B - 2|M_B - 1), L] \tag{6}$$

Equivalent Bell Inequalities

Bell inequalities can be written in many forms. Therefore it is important to divide them into classes where any inequality can be shown to be equivalent to any other inequality. Inside of each class there are 4 types of equivalence between inequalities: positivity conditions, no-signaling conditions, relabeling of inputs and relabeling of outputs conditioned on inputs.

Positivity conditions arise from the normalisation of probabilities ($\sum_{a,b} P(a, b|x, y) = 1$) which means equivalent inequalities can be obtained by summing a positivity condition to a previous existent inequality. In the same way we if sum no signaling conditions that add up to zero, (for example: $\sum_b P_\lambda(a, b|x, y) - \sum_b P_\lambda(a, b|x, y') = 0$) we can obtain new inequalities that are equivalent to the original inequality. To solve this problem we simply write the inequalities in spaces that are invariant to positivity and no signaling conditions, the same approach taken in [**?**]. There are many spaces that satisfy such condition including the Collins-Gisin, which we will used to write all inequalities in this work.

Relabeling conditions arise from Alice's and Bob's choices of labeling inputs and outputs. This way from a specific inequality, others can be obtained just by choosing different labels. However this obviously does not produce new inequalities .This way, Alice and Bob can chose any permutation of their inputs, as long as the inputs permuting have the same number of outputs, to produce equivalent inequalities. Specifically if I_{abxy} is an inequality, $\pi(x)$ a permutation of Alice's inputs for some specific number of outputs and $\pi'(y)$ a permutation of Bob's inputs for some specific number of outputs then $I_{ab\pi(x)\pi'(y)}$ is also a valid inequality. The same applies to each output conditioned on the inputs. Indeed, for a given input, Alice is free to label her outputs without generating new classes of inequalities. This way, if $\pi(a|x)$ is a permutation of Alice's outputs given a specific input x and $\pi'(b|y)$ is a permutation of Bob's outputs given a specific input b then $I_{\pi(a|x)\pi'(b|y)xy}$ is also a valid inequality.

Finally the last symmetry that needs to be considered is when the scenario is completely symmetric ($M_A = M_B$ and $m_A = m_B$)) and therefore we can switch Alice and Bob label's. In the script written this was solved using P notation where each probability $P(ab|xy)$ translates to $P(ba|yx)$.

Methods

Polytope Cutting

As previously mentioned the facet enumeration problem is an NP-Hard problem. Therefore the number of Bell polytopes completely solved is extremely limited. However this does not mean that we can not extract useful information and unknown classes of facets from unsolved polytopes.

In this work we use a new approach to these hard to solve polytopes - cutting them into smaller, easier to work with, subpolytopes. This method was first used in [**?**]. Indeed, for this method we take previously known facets of simpler polytopes and we lift them to the dimension of the polytope in which we are interested in. Then, by manipulating the local bound of this lifted facet we can check which vertices will violate this half-plane and which will not, creating this way 2 subpolytopes - the one formed by the vertices that violate the fabricated facet and the ones that don't. By manipulating the local bound, we can construct subpolytopes with less vertices which are much easier to analyse by using software such as $PANDA$ [**?**]. This means that given a vertex description of a polytope, x_k and a half-plane A such as

$A\boldsymbol{x} = c$, then the set of vertices that satisfy:

$$A\boldsymbol{x_k i} \geq c \tag{7}$$

defines the cut polytope.

This way, we can then look for facets in the cut polytope. All facets that are generated by vertices of the original polytope that are also in the cut polytope will obviously be present in the subpolytope and we can extract them much faster. Obviously there will also be new facets of the subpolytope that do not belong to the original polytope but here we can take advantage of the fact that while facet enumeration is an NP-hard problem, checking if half-planes are facets of polytopes given their vertex description is not and is actually quite easy.

Indeed to verify if a half-plane is a facet of a polytope all that is needed is to check that no vertex of the polytope violates the half-plate and that at least d-1 non collinear vertices belong to the half-plane. This way we can then use the symmetry of Bell polytopes to discover all the facets belonging to the same class as the facets extracted from the cut subpolytope and obtain a more complete description of the original object.

This process can then be repeated with as many half-planes as we want to obtain more and more facets. Indeed it is quite easy and quick to perform hundreds and even thousands of cuts and analyse them. Although there is no stopping condition, because to know when the description of the polytope is complete we would have to solve the facet enumeration problem, exactly what we are trying to avoid, this can provide valuable information of large and complex polytopes which would be very hard to obtain otherwise. Additionally, these incomplete descriptions can be provided to software such as $PANDA$ [**?**] in order to speed up the algorithms and obtain complete descriptions of polytopes which otherwise would take much more time.

This way, when no new facets appear after cutting we can then take the ones produced so far and try to solve the Facet Enumeration Problem and check if the description of the polytope is complete .

Semidefinite Programing (SDP)

A key tool to calculate many properties of Bell inequalities is semidefinite programing (SDP) [**?**]. This technique is concerned with the minimization of a linear objective function subject to the constrain that an affine combination of symmetric matrices is positive semidefinite. This restraint is by definition convex, and so SDP belongs to the subfield of convex optimisation and can be considered a generalisation of linear programming (where a linear objective function is maximized or minimized over a polytope). This way, we can define a general SDP problem as :

$$min(c^T \mathbf{x}) \tag{8}$$

subject to:

$$\begin{aligned} F(\mathbf{x}) &\succeq 0 \\ F(\mathbf{x}) &= F_0 + \sum_i^m x_i F_i \end{aligned} \tag{9}$$

Where $x \in \mathcal{R}^m$ and $c \in \mathcal{R}^m$ represents the problem data. Extra constraints can be added on top of the semi-positive definite constraint for the matrix X (for instance one can also constraint its trace $Tr(X)$).

Duality theory applies to SDPs. Therefore, given a problem, a primal, in the form 8 a dual can be generated of the form:

$$max(-Tr(F_0 Z)) \tag{10}$$

subject to:

$$\begin{aligned} Tr(F_i Z) &= c_i \\ Z &\succeq 0 \end{aligned} \tag{11}$$

Where $i = 1, ..., m$ and Z is symmetric and $Z \in \mathcal{R}^{n \times n}$. Clearly the dual is also an SDP problem. The Weak Duality theorem [**?**] states that any value of the dual SDP will lower-bound the value of the primal SDP. This can be seen from the duality gap, Δ, the difference between the primal and dual objectives:

$$\begin{aligned} \Delta &= c^T \mathbf{x} + Tr(F_0 Z) = \\ \sum_i Tr(Z F_i x_i) &+ Tr(F_0 Z) = Tr(Z F(\mathbf{x})) \geq 0 \end{aligned} \tag{12}$$

Where the last equality comes from the fact that both Z and F are positive semidefinite. A consequence of this theorem is that any point $\mathbf{x}$ that defines a feasible solution of the primal will define a feasible solution of the dual. This theorem is important, because it establishes a relationship between the solutions of the primal and the dual that can be used to establish primal-dual interior point methods to solve SDPs.

The core idea behind these kind of methods is the usage of already known self-concordant barrier functions based on the constraints imposed on the problem. An example is the logarithmic barrier function:

$$B(\mathbf{x}) = c^T \mathbf{x} - \mu \sum_i^m \log(c_i) \tag{13}$$

Where μ is the barrier parameter and is positive. From the barrier function, one computes its potential ∇B and

minimizes said potential according to some direction δx and δZ. By taking this minimum, x_m and Z_m respectively, we update $\mathbf{x}$ and Z according to the direction chosen, i.e, $\mathbf{x}+x_m\delta x$ and $Z+Z_m\delta Z$. This is iterated until the dual gap Δ is sufficiently small or the problem is deemed unfeasible.

In this work to solved the SDPs that arose, we used a free, academic license of the software $MOSEK$ [**?**] that implements an efficient primal-dual interior point method.

Properties of Interest

Quantum Bound

The first property of interest is the maximum score that one can get by using quantum resources in a Bell Game with respect to a specific facet. To compute this property we use the recently developed NPA hierarchy [**?**] to relax non-commutative polynomial problems to semidefinite programs.

To understand this hierarchy let us consider a finite Hilbert space $\mathcal{H}$, an alphabet of bounded operators $X = (X_1, X_2, ..., X_n)$ and the state $|\psi\rangle \in \mathcal{H}$. We say that each operator in X is a letter and collectively they form strings of length k. The identity I is considered to be the empty string and has length 0.

Given these elements, it is now possible to construct a moment matrix Γ^k based on the set W^k of strings of length lesser or equal than k. Considering 2 elements of this set, W_1 and W_2, the elements of Γ will be indexed by the elements of W:

$$\Gamma^k_{(W1,W2)} = \langle\psi|W_1W_2|\psi\rangle = P(W_1W_2) \tag{14}$$

and

$$\Gamma^k(I, I) = 1 \tag{15}$$

$\Gamma^k_{(W1,W2)}$ is a certificate of level k and on their original paper [**?**], Navascués, Pironio and Acín have shown that it is positive semidifinite for all $k \in \mathbb{N}$. Obviously for each level we have $W^1 \subseteq W^2 \subseteq W^3 \subseteq ... \subseteq W^k \subseteq W^{k+1}$ so we say that each certificate establishes a hierarchy of conditions satisfied by quantum probabilities where each certificate is stronger than the previous (because for each the matrix will be positive semidifinite). Computing the entries of the momentum matrix can be done efficiently with semidinite proraming. Additionally the original authors of [**?**] have shown that for a specific strategy p if there is a momentum matrix Γ that realizes p then p belongs to the quantum set.

For the problem at hand additionally we need a relaxation of non-commuting problems to commuting problems. Indeed, let us consider the following example based on a facet of CHSH where objective is to maximize the score defined by:

$$\begin{aligned} S = \langle\psi|A^0_0 \otimes B^0_0|\psi\rangle + \langle\psi|A^0_0 \otimes B^0_1|\psi\rangle + \langle\psi|A^0_1 \otimes B^0_0|\psi\rangle \\ -\langle\psi|A^0_1 \otimes B^0_1|\psi\rangle - \langle\psi|A^0_0 \otimes \mathbb{I}_B|\psi\rangle - \langle\psi|\mathbb{I}_B \otimes B^0_0|\psi\rangle \end{aligned} \tag{16}$$

where A^a_x and B^b_y represent respectively Alice's and Bob's measurement operators that exist in a finite Hilbert space $\mathcal{H}$ where $\psi \in \mathcal{H}$. Clearly, if we relax the tensor product to a commuting measurement strategy where Alice's and Bob's measurements are projectors then we see that the function to optimize is simply a linear sum of terms of a moment matrix of level $k = 2$ with an alphabet composed by the operators that Alice and Bob apply to the state $|\psi\rangle$:

$$\begin{aligned} S = \langle\psi|A^0_0B^0_0|\psi\rangle + \langle\psi|A^0_0B^0_1|\psi\rangle + \langle\psi|A^0_1B^0_0|\psi\rangle - \\ \langle\psi|A^0_1B^0_1|\psi\rangle - \langle\psi|A^0_0\mathbb{I}|\psi\rangle - \langle\psi|\mathbb{I}B^0_0|\psi\rangle \\ = \Gamma^2_{(A^0_0,B^0_0)} + \Gamma^2_{(A^0_0,B^0_1)} + \Gamma^2_{(A^0_1,B^0_0)} - \Gamma^2_{(A^0_1,B^0_1)} - \Gamma^2_{(A^0_0,\mathbb{I})} - \Gamma^2_{(\mathbb{I},B^0_0)} \\ = p(00|00) + p(00|01) + p(00|10) - p(00|11) - p_A(0|0) - p_B(0|0) \end{aligned} \tag{17}$$

where the following properties are imposed:

- $A^a_x = A^{a\dagger}_x$ and $B^b_y = B^{b\dagger}_y$
- $A^a_xA^{a'}_{x'} = \delta_{xx'}\delta_{aa'}A^a_x$ and $B^b_yB^{b'}_{y'} = \delta_{yy'}\delta_{bb'}B^b_y$
- $\sum_a A^a_x = \mathbb{1}_{\mathcal{H}}$ and $\sum_b B^b_y = \mathbb{1}_{\mathcal{H}}$
- $[A^a_x, B^b_y] = 0$

The first 2 properties are a consequence of considering projectors whilst the third and fourth property impose no-signaling correlations and spacial separation respectively (i.e Alice and Bob each perform their measures separately on the state $|\psi\rangle$ and their marginals are well defined). This relaxation is valid due to 2 reasons: first we have not limited the dimension of the Hilbert space in consideration, we have merely imposed that it is finite. Therefore, given that any POVM can be expressed as a projector on a higher dimension Hilbert space we can go from 16 to by expanding the space in consideration. Secondly, the structure of the tensor imposed in 16 is imposed to denote that the measurements are performed separately which is also imposed by the commutativity. Clearly, if we swap our labels and exchange Alice with Bob the result of our measurements must be the same (because the probabilites can not change if we first consider Alice or Bob i.e $p(a, b|x, y) = \langle\psi|A^a_x \otimes B^b_y|\psi\rangle = \langle\psi|B^b_y \otimes A^a_x|\psi\rangle$. Therefore the quantum Q set used in 16 has to be contained in the quantum set Q' defined in by the algebra above, $Q \subseteq Q'$.

This way, any feasible point of will define a feasible point of 16 with the same objective and we can take full advantage of the NPA hierachy to maximize the score achievable with quantum resources. To that end we define the following problem:

$$\begin{aligned} max(S) = \Gamma^2_{(A^0_0,B^0_0)} + \Gamma^2_{(A^0_0,B^0_1)} + \Gamma^2_{(A^0_1,B^0_0)} \\ -\Gamma^2_{(A^0_1,B^0_1)} - \Gamma^2_{(A^0_0,\mathbb{1})} - \Gamma^2_{(\mathbb{1},B^0_0)} = Tr(C\Gamma^2) \end{aligned} \tag{18}$$

subject to:

$$Tr(X_i\Gamma^2) = b_i \tag{19}$$

$$\Gamma^2 \succeq 0 \tag{20}$$

where the first condition stems naturally from the fact that the entries of Γ^2 being probabilities by construction. This is precisely the definition of a semidefinite program that can be solved using $MOSEK$.

The conversion of the initial problem to a semidefinite problem was made possible through the python package $Ncpol2sdpa$ developed by Prof. Peter Brown and used in [**?**].

Minimum detection efficiency to close detection Loophole

Give the correct state $|\psi\rangle$ the score achieved by a Bell game should in theory be its maximum value S_{max}. However, in practice we are working with detectors that have a limited efficiency η and for a number of measurements the detector will not measure the incoming state. From this arises one question, what is the minimum detection efficiency necessary for a Bell game to detect non-local behaviour, i.e, the minimum efficiency for the score to be above the local bound of a facet?

To determine this we now consider a mixed score composed of the score obtained when both detectors work Q, when Alice's detectors work but Bob's does not fire M_A, when Bob's detectors work but Alice's does not fire M_B and when both parties detectors fail to register XX. This way, in the limit of a game with infinite samples and independent identically distributed rounds the expected score will be:

$$S = \eta^2 Q + \eta(1-\eta)(M_A + M_B) + (1-\eta)^2 XX \tag{21}$$

We can extract an upper bound of the minimum detection efficiency by solving this equation with respect to η when the score matches the local bound $S = L$, one only needs Q, M_A, M_B and XX.

The value of Q can be obtained by following the steps in the previous section (define the commuting polynomial problem associated with the facet, use the NPA hierachy to write the SDP problem and solve it using $MOSEK$). To obtain the values of the remaining quantities we compute the score from the probabilities obtained via the momentum matrix under a specific strategy employed. Indeed, when a detector fails Alice and Bob can choose whether to consider an output of '0' or '1' for that detector. This way there will be $n = A^X \times B^Y$ strategies to be considered for when the detectors fail to trigger (for each input Alice has to choose an output and so does Bob).

This way we can compute for every possible strategy the values of M_A, M_B and XX of each facet and extract the minimum values of η. This value is common for each facet belonging to the same class (for a relabel can not change the properties of the game at hand).

Resistance to Noise

Another very important property to compute is an inequality's resistance to noise. By noise here we mean the introduction of white noise that is mixed with the state shared between Alice and Bob. This way, if an inequality is maximally violated by the state $|\psi\rangle$, its resistance to noise λ will be the maximum amount of white noise that can be mixed into the state such that the inequality is still violated:

$$\rho = \lambda|\psi\rangle\langle\psi| + (1-\lambda)\frac{\mathbb{I}}{d^2} \tag{22}$$

where d is the dimension of the state shared (so if Alice and Bob share qubits, $d = 2$). To obtain this quantity we need to know the optimal measurements A^a_x and B^b_y for which the inequality is maximally violated. From these one can then compute the achievable score with white noise as its state, S_{WN}, and then the extraction of λ is quite triviall:

$$\lambda = \frac{L - S_{WN}}{Q - S_{WN}} \tag{23}$$

To obtain these we need to again construct SDPs, but this time without relying on the NPA hierarchy. Indeed, although the hierarchy allows us to extract the maximally quantum violation for each inequality, we only have access to the resulting probabilities that produce the violation, not the specific measurements that we need. This way, a new program was developed using the Python package $CVXPY$ [**?**], [**?**].

In this program, the first step is the generation random measurements A^a_x and B^b_y From here we can define the necessary SDP as to maximize the score.

Its important to notice that since we are not using the NPA hierarchy here, we can not use a relaxed version of the problem and the tensor product structure must be

imposed. This has the obvious disadvantage of not being dimension agnostic, contrary to the NPA hierarchy, and a dimension of the state and measurements has to be assumed. In this work, we computed an upper bound on the minimum dimension required, d_{min}, for each facet in order to achieve the calculated quantum bounds Q. It must be said, as recently discovered in the works of [**?**] and [**?**], that behaviours that are only observed using higher dimension states could go undiscovered by taking this approach. However, one must take into consideration the limited resources available to the author and that to simulate higher and higher dimensional systems quickly becomes computationally costly.

Having done this first SDP to optimize the state $|\psi\rangle\langle\psi|$, we know take a "seesaw" approach where in each iteration we optimize the state, then Alice's measurements, then Bob's measurements. In each iteration we save the state and the measurements as the starting point for the next iteration.

This iterative process goes on until the maximized score gets close enough to the computed quantum bound. Specifically, we considered as the stopping condition $|Q - S| < 0.01 \times |Q - L|$. If after extensively sampling initial points for the algorithm this stopping condition was not realised then the dimension would increase. This is iterated until the stopping condition is fulfilled and we extract an upper bound on the minimum dimension, d_{min}, required to achieve Q.

Having successfully obtained the optimal measurements, now one just needs to compute the white noise score S_{WN} and follow 23 to compute an inequality's noise resistance.

Scenario Analysis

In this work we analysed the following scenarios: (2,2,2,2), (3,3,2,2), (4,3,2,2), (5,3,2,2), (6,3,2,2), (4,4,2,2), (2,2,3,3), (2,2,3,4), (2,2,3,5), (2,2,4,4), (2,3,3,2), (3,2,3,3), (3,3,3,2), (3,3,4,2) and (4,3,3,2). Of these we present a new complete description of (6,3,2,2), (3,2,3,3) and (3,3,3,2) and conjecture that the description of (2,2,4,4), (3,3,4,2) and (4,3,3,2) is complete. For every facet their properties of interest were calculated.

In the (6,3,2,2) scenario there are 7 classes of facets for a total of 253 872 facets. In the (3,2,3,3) scenario there are a total of 793 854 facets and in the (3,3,3,2) scenario there are 25 classes for a total of 252 558 facets. The completeness of (3,3,3,2) scenario had already been conjectured in [**?**] but as far as the author knows this is the first time that such completeness is proven.

For the (2,2,4,4) scenario we found a total of 11 665 992 facets (64 are positivity facets). They are classified into 34 facets. For the (3,3,4,2) scenario we found 159 classes for a total of 23 973 264 facets and for the (4,3,3,2) we found 80 classes for a total of 9 960 696 facets.

The most important facets found were the ones whose minimum efficiency to close the detection Loophole or resistance to noise is inferior or equal to the CHSH facet. They are presented in table **??**.

To demonstrate the strength of the new cutting method we used the (4,4,2,2) scenario as a performance test. Given the high degree of complexity of the scenario and that the complete list of facets was already known, this poses an excellent benchmark test for our new approach. Indeed, using a single inequality from the $I3322$ class to provide a cut we obtain 40,57% of all the available classes. This cut polytope was solved in less than 20 seconds which clearly shows the strength of this approach.

The most interesting facets found were:

TABLE I – continued from previous page

Name	Scenario	Q	η	λ	d_{min}
CHSH	(2,2,2,2)	0.2071	0.8284	0.7071	2
F_6	(4,4,2,2)	0.2879	0.8179	0.8128	4
F_{57}	(4,4,2,2)	1.6430	0.8021	0.7917	3
F_{72}	(4,4,2,2)	0.4554	0.8245	0.7935	2
F_{79}	(4,4,2,2)	1.6056	0.8281	0.7676	2
F_{80}	(4,4,2,2)	0.4353	0.8179	0.7751	2
F_{146}	(4,4,2,2)	1.5932	0.8261	0.7468	2
$I2233$	(2,2,3,3)	0.3050	0.8139	0.6861	3
$I2244^{1}$	(2,2,4,4)	0.3648	0.8044	0.6728	4
$I2244^{7}$	(2,2,4,4)	0.4485	0.8156	0.7316	3
$I2244^{8}$	(2,2,4,4)	0.4681	0.8185	0.7062	4
$I2244^{9}$	(2,2,4,4))	0.4733	0.8074	0.7039	4
$I2244^{10}$	(2,2,4,4)	0.4564	0.8142	0.7088	3
$I[[2,2,3],[3,3]]^{2}$	(3,2,3,3)	0.3038	0.8190	0.6976	3
$I[[2,3,3],[3,3]]^{2}$	(3,2,3,3)	0.4448	0.8151	0.7141	3
$I3233^{2}$	(3,2,3,3)	0.4448	0.8151	0.7141	3
$I[[2,2,3],[2,2,2]]^{2}$	(3,3,3,2)	1.3913	0.8255	0.7616	2
$I[[2,3,3],[2,2,2]]^{4}$	(3,3,3,2)	0.3913	0.8255	0.7616	2
$I[[2,3,4],[2,2,2]]^{1}$	(3,3,4,2)	0.4771	0.8170	0.7774	3
$I[[2,3,4],[2,2,2]]^{2}$	(3,3,4,2)	1.3913	0.8255	0.7616	2
$I[[2,2,2,3],[2,2,2]]^{3}$	(4,3,3,2)	0.3944	0.8259	0.7601	2
$I[[2,2,3,3],[2,2,2]]^{2}$	(4,3,3,2)	1.4866	0.8189	0.7740	3

New Semi-Device Independent Protocols

For the most interesting facets we investigate how they performed in an SDI QKD setting. To that end we lower bound the secret key rate achievable by using the Devetak-Winter bound [**?**]:

$$r \geq H(A|X=0,E) - H(A|B) \tag{24}$$

The entropy $H(A|X=0,E)$ can be lower bounded by calculating the min entropy between Alice and Eve:

$$H(A|X=0,E) \geq H_{min}(A|X=0,E) = -log_2(P_g) \tag{25}$$

Where P_g is the guessing probability of Eve over Alice's results. This relations is established due to the fact that the min entropy is the smallest entropy of the Rényi family [**?**]. We take an SDI approach where we use $CVXPY$, and bound the dimension of the available system. This way, we take as the dimension of Alice and Bob's measurements the minimum dimension, d_min, to achieve the expected maximum score and we use the same optimal measurements as the ones obtained before and limit the dimension of Eve's Hilbert space to some d_E. This follows the same approach as the works in [**?**]. Here we considered that $d_E = 4$, where Eve performs qutwart measurements.

$H(A|B)$ on the other hand can be calculated by applying the following equation:

$$H(A|B) = H(AB) - H(B) \tag{26}$$

Where the first term represents the entropy obtained from the joint probabilities between Alice and Bob and the second term the entropy obtained from Bob's marginals. Given a set of probabilities $p = \{p(ab|xy)\}$ the entropy of this is:

$$H(p) = -\sum_{abxy} log_2(p(ab|xy)) \tag{27}$$

So to obtain $H(A|B)$ we simply need the joint probabilities between Alice and Bob and Bob's marginals for when they select the correct inputs to produce a secret key. To obtain these we consider a scenario where Bob has an extra input for key producing. This way, if we for example consider a CHSH facet, then in our QKD setting Alice will have its typically 2 inputs each with 2 outputs but Bob will have 3 inputs - an extra for key generation. Therefore, every time that Alice selects the input $X = 0$ and Bob selects the extra input, $Y = 3$, then the results from this measurements are used for key generation.

We know need to choose Bob's strategy for the extra input. With the ultimate goal of minimizing the uncertainty between Alice and Bob, we can intuitively chose for him to have the same measurements that Alice has when $X = 0$. This way the probability outcomes for Alice given that $X = 0$ will be the same as the ones obtained by Bob when $Y = 3$. Alice's results in turn can be extracted by computing the expected score for some η using the NPA hierarchy and so we have all the necessary ingredients to extract device independent rates for a given facet and detector efficiency. We also maintain the same binning strategy for Alice when the minimum detection efficiency was calculated. For Bob however, the work in [**?**] has shown that we can achieve a lower entropy (and therefore a higher key rate) if he does not bin the non detection results and instead storage them as an extra measurement.

Of the results obtained the facets that performed better were facet $I2244^1$ and facet $I[[2,2,3,3],[2,2,2]]^2$. These results were

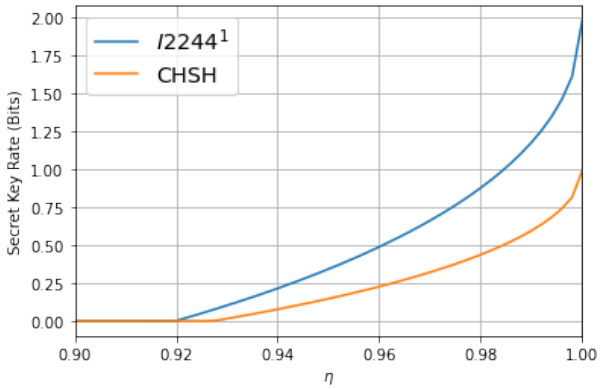

FIG. 1. Comparison between secret key rate obtained using the dimension bound for the $I2244^1$ facet and CHSH in terms of detector efficiency η

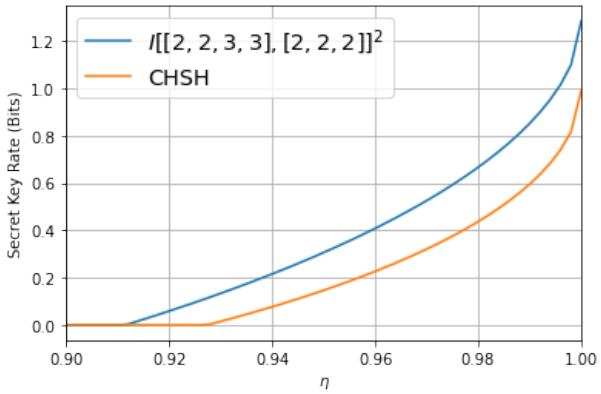

FIG. 2. Comparison between secret key rate obtained using the dimension bound for the $I[[2,2,3,3],[2,2,2]]^2$ facet and CHSH in terms of detector efficiency η

Facet $I2244^1$, as expected from equation **??**, possesses the highest maximum secret key rate, 1.979. For the CHSH facet this value was limited to 1.000. The minimum detector efficiency to extract secret key rates also improved: it went from $\eta_{QKD} \approx 0.928$ for the CHSH facet to $\eta_{QKD} \approx 0.920$. All in all, this facet outperforms the CHSH facet for all detector efficiencies.

On the other hand the maximum secret key rate achieved by facet $I[[2,2,3,3],[2,2,2]]^2$ was smaller than the one obtained for $I2244^1$, it was only 1.284, but this

was the facet with the smallest minimum detector efficiency to extract secret key rates, $\eta_{QKD} \approx 0.912$. This facet also outperforms the CHSH facet for all detector efficiencies.

Conclusion

In this work, we explored the world of bell correlations with the objective of finding new bell inequalities that can be used for DI and SDI QKD. To achieve this goal we looked at previously unsolved Bell polytopes of high dimensions under a new framework - polytope slicing. We demonstrated the capacities of this technique with the (4,4,2,2) scenario, a single slice provided 40.7% of all the classes of this scenario and could be solved in a few seconds. This allowed us to solve previously unsolved polytopes: (6,3,2,2); (3,3,3,2); (3,2,3,3); and (2,2,3,5) confirming previously estabelished conjectures regarding the (6,3,2,2) and (3,3,3,2) scenarios and giving a first full description of (3,2,3,3) and (2,2,3,5).

We didn't stop at these scenarios however, and also looked at even more complex Bell polytopes: the (2,2,4,4); (3,3,4,2) and (4,3,3,2) scenarios. For these, although we could not solve the facet enumeration problem with the resources at our disposal, we conjecture that the list of facets presented is complete given that no new classes of inequalities appeared with increasing slices.

For each class identified we also tried to understand its fundamental properties. To this end, new computational techniques such as Semi-Definite programming were used. The new NPA hierarchy was also defined and used to establish tight quantum bounds for each class presented. Additionally, with the focus of qkd implementations, we also identified in a complete measurement agnostic setting a minimum detection efficiency necessary to close the detection loophole for each class.

The resistance to noise of each class was also explored, although in this case we could no longer work in the same setting as before. Indeed, for this property it was necessary to define the dimensions used by Alice and Bob. Nonetheless, this also allowed us the opportunity to explore what the minimum dimension of the states shared between Alice and Bob should be in order to achieve the quantum bounds previously found via the NPA hierarchy.

Based on these properties, and in comparison with the most simple scenario of all (the CHSH cenario) we identified 22 inequalities, including the CHSH inequality, that should be useful for QKD settings and can be found in table **??**. Of these, to the best knowledge of the author, 12 were found in the most complex scenarios analysed and were previously unknown in the literature.

For each of the I22441 inequality we then explored how well it preformed at tasks like Randomness and Secret Key generation in settings with inefficient detectors. For the cases studied, the inequality demonstrated the advantages already expected of looking beyond the simplest case scenario by dis- playing higher secret key rates and lower experimental requirements

To conclude, we reinforce just how important these new results are. Indeed, the field of Bell inequalities and correlations, despite being more than 50 years old, still has many open questions that could provide new insights and practical technologies to the second quantum revolution. Indeed, this field is such a cornerstone of physics that the 2022 Nobel prize was awarded to Alain Aspect, John Clauser and Anton Zeilinger "for experiments with entangled photons, establishing the violation of Bell inequalities and pioneering quantum information science" [**?**]. Therefore, the hope is that this work can actively contribute to the field and answer some questions regarding high dimension Bell polytopes and their uses.

Nonetheless, there are still many questions unanswered. For instance, one could consider multi-partite Bell inequalities with more than 2 players like in [**?**] or sequential Bell inequalities, where new correlations arise from multiple sequential measurements, like in [**?**]. Another interesting direction would be to consider the inequalities that required a dimension higher than 2 to achieve the maximum expected score and explore their applications in dimension witnessing [**?**] where by verifying a certain score for certain facets we can certify the dimension of the states and measurements used. These directions could inspire new research projects in the future.