Appendix A
Polytopes

A.1 Definition and Terminology

A *polytope* $\mathcal{P} \subset \mathbb{R}^d$ is the convex hull of a finite number of points $V_i = (V_{i,1}, V_{i,2}, \ldots, V_{i,d}) \in \mathbb{R}^d$

$$\mathcal{P} = \{x = (x_1, x_2, \ldots, x_d) \in \mathbb{R}^d \text{ s.t. } \overline{x} = \sum_i q_i \overline{V_i},\ q_i \geq 0\} \tag{A.1.1}$$

where we denote by $\overline{x} = (1, x_1, x_2, \ldots, x_d)$ the points x completed by an extra component to fit in a space of dimension $d + 1$ for convenience [1].

In general, several sets of points $\{V_i\}_i$ can describe the same polytope $\mathcal{P}$ through (A.1.1). For instance, if a point V_i is not an extremal point of $\mathcal{P}$, i.e. if $\exists\ q_i \geq 0$ such that $\overline{V_j} = \sum_{i \neq j} q_i \overline{V_i}$ for some j, then $\{V_i\}_{i \neq j}$ describes the same polytope $\mathcal{P}$. On the other hand, if V_j is an extremal point of $\mathcal{P}$, then no set of points $\{V_i'\} \not\supset V_j$ can describe the same polytope $\mathcal{P}$. The description of a polytope through (A.1.1) is thus minimal when all point in $\{V_i\}_i$ are extremal points of the polytope, i.e. vertices. We refer to this as the *extremal points* description of a polytope, or *V-representation*. Notice that the condition for extremality of a point V_i is linear. The minimal set $\{V_i\}_{i,min}$ can thus be found from $\{V_i\}_i$ with the help of linear programming.

The *dimension* of a polytope $\dim(\mathcal{P})$ is given by the dimension of the smallest vector space that contains $\mathcal{P}$. It can be computed from the rank of its extremal points as

$$\dim(\mathcal{P}) = \begin{cases} \mathrm{rk}(V_{ij}) & \text{if } \exists\ q_i \leq \mathbb{R} \text{ s.t. } \sum_i q_i \overline{V}_i = (1, 0, 0, \ldots, 0) \\ \mathrm{rk}(V_{ij}) - 1 & \text{else.} \end{cases} \tag{A.1.2}$$

The main theorem on polytopes [1] tells that any polytope $\mathcal{P}$ can also be described as the intersection of finitely many *half-spaces* $\sum_j x_j H_{jk} \geq -H_{0,k}$, namely as:

J.-D. Bancal, *On the Device-Independent Approach to Quantum Physics*, Springer Theses,
DOI: 10.1007/978-3-319-01183-7,

$$\mathcal{P} = \{x \in \mathbb{R}^d \text{ s.t. } \sum_{j=0}^{d} \overline{x_j} H_{j,k} \geq 0 \ \forall k\} \tag{A.1.3}$$

As in the extremal point description of a polytope (A.1.1), the half-spaces description of a polytope can be made unique and minimal by requiring its inequalities to be *irredundant*, i.e. such that no $q_k \geq 0$ can satisfy $H_{j,k} = \sum_{k' \neq k} q_{k'} H_{j,k'}$.

When an inequality is irredundant, it is called a *facet* of the polytope. Its intersection with $\mathcal{P}$ is then of dimension $\dim(\mathcal{P}) - 1$. An inequality satisfied by the polytope which is not a facet might still have a non-null intersection with the polytope. The intersection of this inequality with the polytope is a often called a face of the polytope, and has a dimension strictly less than $\dim(\mathcal{P}) - 1$.

A polytope can thus be described in two equivalent ways (A.1.1), (A.1.3). Transforming one representation of a polytope into its dual one is in general a difficult task [2]. Nevertheless, when the polytopes are not too complicated, it can be possible to perform this transformation exactly with the aid of a computer. Several open-source softwares are available for this, like lrs [3], cdd [4], skeleton [5] or porta [6].

A.2 Some Operations on Polytopes

Polytopes can be manipulated in several ways. Here we describe some of these operations. See also the appendix of [7] for more examples.

A.2.1 Projection

One way to reduce the dimensionality of a polytope is to project it onto a subspace $S \subset \mathbb{R}^d$. For this, consider the linear projection operator $\Pi{:}\mathbb{R}^d \to S$. Without loss of generality, Π can be taken to act as $\Pi(x) = (x_1, x_2, \ldots, x_s, 0, \ldots, 0)$,[1] where $s = \dim(S)$ is the dimension of the projected space.

The projection of a polytope described in terms of extremal points is easily computed by projecting its extremal points:

$$\mathcal{P}' = \Pi(\mathcal{P}) = \left\{x \in \mathbb{R}^d \text{ s.t. } \overline{x} = \sum_i q_i \overline{\Pi(V_i)},\ q_i \geq 0\right\}. \tag{A.2.1}$$

Note that all projected vertices $\{\Pi(V_i)\}_i$ need not be extremal points of the projected polytope anymore. However all extremal points of $\mathcal{P}'$ are necessarily projections of some extremal points of the original polytope. They are thus necessarily contained

[1] A change of variables can be performed on order to let Π take this form if necessary.

in the set $\{\Pi(V_i)\}_i$. Projection of a polytope can thus only reduce the number of its extremal vertices.

When a polytope is specified in terms of half-spaces, finding the H-representation of its projection is more difficult. The Fourier-Motzkin algorithm achieves this without requiring to first transform the description of the polytope into its V-form, but it becomes quickly unpractical for larger problems because of its double-exponential computational complexity.[2]

Still, if one is not interested in the full set of inequalities describing the projected polytope $\mathcal{P}'$, a number of its facets can be found heuristically. Here we describe two linear programs that can be used for this.

The first linear program for finding facets of a projected polytope is similar to the shooting oracle described in [8]. The idea is, starting from a point that belongs to the interior of $\mathcal{P}'$, to travel as far as possible in one direction of the subspace S, until touching the boundary of $\mathcal{P}'$. The point then reached must generically belong to a facet of $\mathcal{P}'$.

Find a facet of a projected polytope. Let x^0 belong to the interior of $\mathcal{P}'$, and let $v \in S$ be a direction in the projected subspace. The linear program

$$\begin{aligned} \min_{z_k} & \sum_k H_{o,k} z_k + \sum_k \sum_{j=1}^{s} x_j^0 H_{j,k} z_k \\ \text{subject to} & \sum_{j=1}^{s} \sum_k v_j H_{j,k} z_k = -1 \\ & \sum_k H_{j,k} z_k = 0 \; \forall \; j = s+1, \ldots, d \\ & z_k \geq 0 \end{aligned} \tag{A.2.2}$$

provides the inequality

$$I_0 + \sum_{j=1}^{s} x_j I_j \geq 0 \tag{A.2.3}$$

with coefficients $I_0 = \sum_k H_{o,k} z_k + \sum_k \sum_{j=1}^{s} x_j^0 H_{j,k} z_k$, $I_j = \sum_k H_{j,k} z_k$ which is satisfied by all points x belonging to the projection of the polytope $\mathcal{P}'$. To see this one can check that the dual of this program is

[2] Note that other algorithms have been proposed, such as the ESP one [8] which is sensitive to the number of facets in the projected polytope $\mathcal{P}'$ rather than in the number of facets of the full polytope $\mathcal{P}$.

$$\max_{\mu, y_{s+1}, \ldots, y_d} \mu$$

$$\text{subject to} H_{0,k} + \sum_{j=1}^{s} (x_j^0 + \mu v_j) H_{j,k} + \sum_{j=s+1}^{d} y_j H_{j,k} \geq 0 \; \forall \, k \tag{A.2.4}$$

which computes the largest value of μ such that $x^0 + \mu v \in \mathcal{P}'$.

In order to find a facet with the above linear program, one needs to choose a direction $v \in S$. Choosing an interesting direction is not necessarily obvious when nothing or just little about the projected polytope is known. Here is a linear program which can provide an interesting direction v to look for a facet when some facets of the projected polytope $\mathcal{P}'$ are known. The idea is that an interesting direction to look for a new facet of the projected polytope is in the direction of a vertex of the polytope described by the known facets of this polytope: if there is a difference between the known polytope and $\mathcal{P}'$, then some of its extremal points need to be outside $\mathcal{P}'$, otherwise the two polytopes are equal and there is nothing left to be found.

Find an extremal point of a polytope. Let $\{H_k\}_k$ be a set of inequalities defining a polytope $\mathcal{P}''$, and let $w \in \mathbb{R}^d$ be a direction in space. The following linear program yields a point x which lies on the boundary of $\mathcal{P}''$:

$$\begin{aligned} &\min_{x_j} \; \sum_j w_j x_j \\ &\text{subject to} \; \; H_{0k} + \sum_j H_{jk} x_j \geq 0 \; \forall \, k \end{aligned} \tag{A.2.5}$$

If w is chosen at random, the point x is generically an extremal point of $\mathcal{P}''$.

Application to Polytope Representation Conversion

It is possible to find the H-representation of a polytope from its V-representation by performing a polytope slice (defined in the next section) followed by a polytope projection. Indeed, the conditions in Eq. (A.1.1) can be understood as defining a polytope $\tilde{\mathcal{P}} \in \mathbb{R}^{d+n}$, where n is the number of extremal points of $\mathcal{P}$, and $\tilde{\mathcal{P}}$ is defined by the following H-representation:

$$\tilde{\mathcal{P}} = \{(x, q) \in \mathbb{R}^{d+n} \, \text{s.t.} \, \overline{x} = \sum_i q_i \overline{V}_i, \; q_i \geq 0\} \tag{A.2.6}$$

Elimination of the variables q_i, i.e. projection of $\tilde{\mathcal{P}}$ onto the subspace $S = \mathbb{R}^d$ thus defines the set of x such that the conditions in (A.1.1) hold. This projected polytope is thus $\mathcal{P}$, described in terms of inequalities. This is the basic technique used by the software porta [6] to solve a polytope.

A.2.2 Slice

Another way of reducing the dimensionality of a polytope is to consider a slice of it, that is, the intersection of the polytope $\mathcal{P}$ with a subspace $S \subset \mathbb{R}^d$ of dimension s. S can be defined by a set of linear equations: $S = \{x \in \mathbb{R}^d \text{ s.t. } \sum_j \overline{x}_j E_{jl} = 0 \; \forall l = 1 \ldots d - s\}$. The slice of $\mathcal{P}$ which belongs to S is easily defined if $\mathcal{P}$ is specified in the H-representation:

$$\mathcal{P}' = \left\{x \in \mathbb{R}^d \text{ s.t. } \sum_j \overline{x}_j M_{kj} \geq 0 \; \forall k, \sum_j \overline{x_j} E_{jl} = 0 \; \forall l\right\} \tag{A.2.7}$$

Computing the slice of a polytope in its V-representation is more complicated. In fact, on can show through polytope duality [1] that this task is equivalent to a projection of the polytope dual to $\mathcal{P}$ [9]. It can thus be done with the techniques described in the precedent section.

A.2.3 Another Task: Finding Facets Lying Under an Inequality

An inequality satisfied by a polytope is not a facet of the polytope if its dimension is lower than $d - 1$. When this is the case, one can show that the inequality can be expressed as the convex combination of a number of tighter inequalities, the tighter of which are facets of the polytope, sharing an intersection of dimension $d - 1$ with the polytope. Thus, if a point violates a non-facet inequality, it can only violate some of these tighter ones by a larger amount. Given a non-facet inequality, it can thus be interesting to look for these tighter facets.

A method for finding the facets underlying an inequality given a V-description of the polytope is presented in [10]. The idea is that the rank of the set of extremal points saturating the inequality can be augmented by adding more extremal points of the polytope to this set. When the achieved rank is sufficient, and if the hyperplane passing through these points does not cut the polytope into two parts, then it describes a facet of the polytope. By construction, the intersection of this facet with the polytope coincides with the intersection of the original inequality with the polytope since it is generated by the same set of extremal points.

Appendix B
Memoryless Attack on the 6-State Protocol: Proof

Here we provide a proof for the bound (8.1.4) used in the main text.

Proof Without loss of generality, Eve's POVM elements can be written as:

$$F_k = A_k^\dagger A_k = a_k \mathbb{1} + (b_k - a_k) P_k \tag{B.1}$$

where $A_k = \sqrt{a_k} U_k \overline{P_k} + \sqrt{b_k} U_k P_k$ is a Kraus operator associated to the element F_k, $a_k,\ b_k \geq 0$, U_k is a unitary operator, $\overline{P_k} = \mathbb{1} - P_k$ and P_k is a one-dimensional projector.

Eve's information on Alice's bit. We consider a given run k of the protocol for which Alice and Bob used the same basis $b = b_k$, and denote by A Alice's bit, B Bob's bit and E the result of Eve's POVM measurement. The total information gained by Eve on Alice's bit after the sifting procedure is given by $I(A : (E, b))$. Since b is independent of A and E, and since the state produced by Alice $\rho = \rho(A, b)$ is a function of A and b, we have:

$$\begin{aligned} I(A : (E, b)) &= H(A) + H(E, b) - H(A, E, b) \\ &= H(A) + H(E) + H(b) - H(A, E, b) \\ &= H(A, b) + H(E) - H(A, E, b) = I((A, b) : E) \\ &= I(\rho : E) = \log(6) - I(\rho|E) \end{aligned} \tag{B.2}$$

Where H is Shannon's entropy, and we assumed that the six states are chosen by Alice with the same probability $\frac{1}{6}$. We thus need to bound the quantity $I(\rho|E)$ which expresses the information that Eve is missing after she learns the result of her measurement, to know which state ρ was prepared by Alice. Using the fact that $\text{Prob}(E = k) = \text{tr}(F_k)/2$, this quantity can be expressed as

$$I(\rho|E) = I(E|\rho) + \sum_k \log(\text{tr}(F_k)) + \log(3) \tag{B.3}$$

J.-D. Bancal, *On the Device-Independent Approach to Quantum Physics*, Springer Theses,
DOI: 10.1007/978-3-319-01183-7,

where $I(E|\rho) = -\sum_{a,s,k} \text{Prob}(A = a, b = s, E = k) \log(\text{Prob}(E = k|A = a, b = s))$.

For every state ρ that Alice can produce, $\overline{\rho} = \mathbb{1} - \rho$ can also be produced by Alice. An attack described by the POVM elements $\{F_k\}$ thus provides Eve with the same information as the attack $\{\tilde{F}_k\}$ where $\tilde{F}_k = A_k \mathbb{1} + (b_k - a_k)\overline{P_k}$. Indeed, as shown above, this information is a symmetric function of $P(E = k|\rho = \rho(a, b))$ and

$$\begin{aligned} \text{tr}(\rho F_k) &= a_k + (b_k - a_k)\text{tr}(\rho P_k) \\ &= a_k + (b_k - a_k)\text{tr}(\overline{\rho}\tilde{F}_k) = \text{tr}(\overline{\rho}\tilde{F}_k). \end{aligned} \tag{B.4}$$

Moreover, the information that can be extracted from a mixture of measurements M_1 applied with probability p_1 and M_2 applied with probability p_2 is

$$I([(p_1, M_1), (p_2, M_2)]) = p_1 I(M_1) + p_2 I(M_2), \tag{B.5}$$

where $I(M_{1,2})$ is the information that can be extracted by using measurement $M_{1,2}$ only. We can thus write

$$\begin{aligned} I(\{F_k\}) &= I\left(\left\{\frac{1}{2}F_k\right\} \cup \left\{\frac{1}{2}\tilde{F}_k\right\}\right) \\ &= \sum_k \frac{a_k + b_k}{2} I\left[\left\{\frac{F_k}{a_k + b_k}, \frac{\tilde{F}_k}{a_k + b_k}\right\}\right] \end{aligned} \tag{B.6}$$

where the factor $1/(a_k + b_k)$ is a normalization coefficient. Thus, the information gained by performing an arbitrary POVM measurement can also be achieved by mixing measurement strategies consisting of only two POVM elements. Let us thus consider a POVM measurement for Eve consisting only of the two elements $\frac{F_k}{a_k+b_k}$ and $\frac{\tilde{F}_k}{a_k+b_k}$.

By direct computation one finds that

$$I(E_k|\rho) = \frac{1}{3}(h(c'_k) + h(d'_k) + h(e'_k)) \tag{B.7}$$

with $c'_k = \frac{a_k+\text{tr}(\rho_2 P_k)(b_k-a_k)}{a_k+b_k}$, $d'_k = \frac{a_k+\text{tr}(\rho_4 P_k)(b_k-a_k)}{a_k+b_k}$, $e'_k = \frac{a_k+\text{tr}(\rho_6 P_k)(b_k-a_k)}{a_k+b_k}$. Since this function is convex in c', d', e', its minimum lies on the boundary of the admissible region

$$\left(\text{tr}(\rho_2 P_k) - \frac{1}{2}\right)^2 + \left(\text{tr}(\rho_2 P_k) - \frac{1}{2}\right)^2 + \left(\text{tr}(\rho_2 P_k) - \frac{1}{2}\right)^2 \leq \frac{1}{4}. \tag{B.8}$$

More precisely, this is found for $\text{tr}(\rho_2 P_k) \in \{0, 1\}$, $\text{tr}(\rho_4 P_k) \in \{0, 1\}$, or $\text{tr}(\rho_6 P_k) \in \{0, 1\}$. In this case, since $\log\left(\text{tr}\left(\frac{F_k}{a_k+b_k}\right)\right) = 0$, we find

$$I(\rho|E_k) = \frac{2 + h\left(\frac{b_k}{a_k+b_k}\right)}{3} + \log(3) \tag{B.9}$$

where $\epsilon_k = \frac{a_k}{b_k}$.

All in all, this gives the following bound on Eve's information about Alice's bit:

$$I(A : (E, b)) \leq 1 - \sum_k \frac{a_k + b_k}{2} \cdot \frac{2 + h\left(\frac{1}{1+\epsilon_k}\right)}{3}. \tag{B.10}$$

Perturbation on Bob's system. The attack of Eve delivers the state $\rho_i' = \sum_k A_k \rho_i A_k^\dagger$ to Bob instead of the expected ρ_i. This creates some errors in the outcomes of Bob, which are measured by the QBER:

$$Q = 1 - \sum_{i=1}^{6} P(A = i, B = i) = 1 - \frac{1}{6} \sum_i \mathrm{tr}(\rho_i' E_i) \tag{B.11}$$

where $E_i, i = 1, \ldots, 6$ are the six possible measurement operators of Bob and

$$\rho_i' = \sum_k \sqrt{a_k b_k} U_k \rho_i U_k^\dagger + \sqrt{a_k}(\sqrt{a_k} - \sqrt{b_k}) U_k \overline{P}_k \rho_i \overline{P}_k U_k^\dagger + \sqrt{b_k}(\sqrt{b_k} - \sqrt{a_k}) U_k P_k \rho_i P_k U_k^\dagger. \tag{B.12}$$

Note, that the attack $\{A_k\}$ has the same effect as $\{\tilde{A}_k\}$ for $\tilde{A}_k = \sqrt{a_k} U_k P_k + \sqrt{b_k} U_k \overline{P}_k$. Indeed, for all i there is a j such that $\overline{\rho}_i = \rho_j$ and $\overline{E}_i = E_j$, and one can check that:

$$\begin{aligned} \mathrm{tr}(U_k \rho_i U_k^\dagger E_i) &= \mathrm{tr}(U_k \overline{\rho}_i U_k^\dagger \overline{E}_i), \\ \mathrm{tr}(U_k P_k \rho_i P_k U_k^\dagger E_i) &= \mathrm{tr}(U_k \overline{P}_k \overline{\rho}_i \overline{P}_k U_k^\dagger \overline{E}_i). \end{aligned} \tag{B.13}$$

So we can assume that both A_k and $\tilde{A}_k$ are present in the attack. In this case the perturbed state is

$$\rho_i' = \sum_k \sqrt{a_k b_k} U_k \rho_i U_k^\dagger + \frac{(\sqrt{a_k} - \sqrt{b_k})^2}{2} (U_k \overline{P}_k \rho_i \overline{P}_k U_k^\dagger + U_k P_k \rho_i P_k U_k^\dagger). \tag{B.14}$$

To bound the second part of this expression, one can show by direct computation that

$$\begin{aligned}\sum_i &\mathrm{tr}(U_k\overline{P}_k\rho_i\overline{P}_kU_k^\dagger E_i)+\mathrm{tr}(U_kP_k\rho_iP_kU_k^\dagger E_i)\\ &=\sum_i \mathrm{tr}(\overline{P}_k\rho_i)\mathrm{tr}(\overline{P}_kU_k^\dagger E_iU_k)+\mathrm{tr}(P_k\rho_i)\mathrm{tr}(P_kU_k^\dagger E_iU_k) \qquad \text{(B.15)}\\ &=2((1-c)(1-\tilde{c})+c\tilde{c}+(1-d)(1-\tilde{d})+d\tilde{d}+(1-e)(1-\tilde{e})+e\tilde{e})\end{aligned}$$

where $c=\mathrm{tr}(P_k\rho_2)$, $d=\mathrm{tr}(P_k\rho_4)$, $e=\mathrm{tr}(P_k\rho_6)$, $\tilde{c}=\mathrm{tr}(U_kP_kU_k^\dagger E_2)$, $\tilde{d}=\mathrm{tr}(U_kP_kU_k^\dagger E_4)$ and $\tilde{e}=\mathrm{tr}(U_kP_kU_k^\dagger E_6)$. The maximum value of (B.15) under the constraints $\left(c-\frac{1}{2}\right)^2+\left(d-\frac{1}{2}\right)^2+\left(e-\frac{1}{2}\right)^2\le\frac{1}{4}$, $\left(\tilde{c}-\frac{1}{2}\right)^2+\left(\tilde{d}-\frac{1}{2}\right)^2+\left(\tilde{e}-\frac{1}{2}\right)^2\le\frac{1}{4}$ can be checked to be 4.

Finally, the first part of (B.14) can also be bounded since $\mathrm{tr}(U_k\rho_iU_k^\dagger E_i)\le 1$. Thus we find that

$$Q\ge\sum_k\frac{a_k+b_k}{2}\cdot\frac{(1-\sqrt{\epsilon_k})^2}{1+\epsilon_k}. \qquad \text{(B.16)}$$

Putting the two bounds together. Let us consider equations (B.10) and (B.16) together. Keeping the sum a_k+b_k constant for all k, we choose two values of k if possible: $k1$ and $k2$ such that $\epsilon_{k1}<\epsilon_{k2}$. Following [11] one can show that increasing ϵ_{k1} in such a way that keeps the bound on the QBER (B.16) unchanged, can only decrease ϵ_{k2} and increase Eve's information as given by (B.10). It is thus always better to have $\epsilon_k=\epsilon\ \forall\ k$. In this case both bounds become:

$$I(A:(E,S))\le\frac{1-h\left(\frac{1}{1+\epsilon}\right)}{3},\quad Q\ge\frac{(1-\sqrt{\epsilon})^2}{3(1+\epsilon)} \qquad \text{(B.17)}$$

which can be summarized as

$$I(A:(E,S))\le\frac{1}{3}\left[1-h\left(\frac{1-\sqrt{3Q(2-3Q)}}{2}\right)\right]. \qquad \text{(B.18)}$$

Tightness of the bound. To show that the above bound is tight, consider the attack in which Eve uses the two POVM elements $F_k=\frac{1-\gamma}{2}\mathbb{1}+\gamma|k\rangle\langle k|$ for $k=0,1$. This gives $P(\rho=\pm z|k)=(1\pm(-1)^k\gamma)/6$, $P(\rho=\pm x|k)=P(\rho=\pm y|k)=1/6$, and so $I(A|E)=\frac{2}{3}+\log 3+\frac{1}{3}h\left(\frac{1-\gamma}{3}\right)$. Since $I(A)=1+\log 3$, this attack proved Eve with a mutual information with Alice of $I(A:E)=I(A)-I(A|E)=\frac{1}{3}\left[1-h\left(\frac{1-\gamma}{2}\right)\right]$. Moreover, the QBER induced by this attack is $Q=\frac{1-\sqrt{1-\gamma^2}}{3}$. Thus Eve can choose an attack that saturates Eq. (8.1.4): the bound is tight.

References

1. G.M. Ziegler, *Lectures on Polytopes, Graduate Texts in Mathematics 152*, Revised edn. (Springer, Berlin, 1998)
2. D. Bremner, On the complexity of vertex and facet enumeration for convex polytopes, PhD thesis (1998)
3. http://cgm.cs.mcgill.ca/~avis/C/lrs.html
4. http://www.ifor.math.ethz.ch/~fukuda/cdd_home/index.html
5. http://www.uic.unn.ru/~zny/skeleton/
6. http://typo.zib.de/opt-long_projects/Software/Porta/
7. T. Fritz, Polyhedral duality in Bell scenarios with two binary observables. J. Math. Phys. **53**, 072202 (2012) arXiv:1202.0141
8. http://www-control.eng.cam.ac.uk/~cnj22/research/projection.html
9. N.Yu. Zolotykh, private communication
10. J.-D. Bancal, N. Gisin, S. Pironio, J. Phys. A: Math. Theor. **43**, 385303 (2010)
11. N. Lütkenhaus, Phys. Rev. A **54**, 97 (1996)