Proposta de Projecto Arquitecturas de Elevado Desempenho

Miguel Murça
(Dated: April 12, 2023)

I. PROBLEM CONTEXT

In the context of quantum communications and quantum key distribution, it is important to be able to verify that two parties share non-local resources, that is, a means of generating joint statistics that could not have been achieved by local (independent) behaviour. If no classical signalling is allowed between two parties producing such statistics, one may conclude that the two parties share some form of non-locallity.

Such verification methods may be phrased as a game: two players, Alice and Bob, receive inputs from a verifier, and must reply with some outputs. The players are not allowed to communicate classically, and we will carry the assumption that they do not do so from now onwards. If the players can conjointly generate non-local statistics, they win the game.

In this context, it becomes relevant to characterize both the statistics resulting from local behaviour, as well as the "non-locallity classes", that is, the different families of non-local statistics possible to generate when Alice and Bob share non-locallity.

As an example, take the Clauser-Horne-Shimony-Holt game, where there are two inputs and two outputs for each player; inputs take values $\{0, 1\}$ and outputs take values $\{-1, 1\}$. Denote a_x the output of Alice when given input x, and likewise b_x for Bob. If the verifier computes the score function

$$S = \langle a_0 b_0 \rangle + \langle a_0 b_1 \rangle + \langle a_1 b_0 \rangle - \langle a_1 b_1 \rangle \tag{1}$$

where $\langle \cdot \rangle$ denotes statistical average over multiple rounds of input and output, then one may show that players playing locally are bound to produce

$$-2 \leq S_{\text{local}} \leq 2. \tag{2}$$

A violation of this inequality (in either direction) denotes, as previously said, that the players share a form of non-locallity. Furthermore, even though there are, strictly speaking, two inequalities, they are clearly dual to one another. Take $\mathbb{P}[o_a, o_b \,|\, i_a, i_b]$ to mean "the probability of observing outputs o_a and o_b for Alice and Bob, respectively, when given as respective inputs i_a and i_b." We may rephrase inequality (2) as

$$Cp \geq l \tag{3}$$

where C is a 1×8 matrix of coefficients, p is a vector of 8 probabilities, and l is a single-entry vector. Why isn't p of dimension 2^4 (i.e. of all probabilities $\mathbb{P}[o_a, o_b \,|\, i_a, i_b]$)? Because this would be redundant, as a smaller set of joint and marginal probability distributions is sufficient to describe local behaviour [1] (a notion to be revisited shortly). We may fix a standard ordering for the components of p. Letting

$$\underset{A}{\mathbb{P}}[o_a \,|\, i_a] = \sum_{o_b, i_b} \mathbb{P}[o_a, o_b \,|\, i_a, i_b] \tag{4}$$

and likewise $\mathbb{P}_B[o_b\,|\,i_b]$ be the marginal probabilities for Alice and Bob, we consider the order of the probabilities in p to be first the joint probabilities of Alice and Bob, then the marginal probabilities for Alice, and finally the marginal probabilities for Bob. In the present case, we have

$$p = \begin{pmatrix} \mathbb{P} & [\,-1,\,-1 & | & 0,\,0\,] \\ \mathbb{P} & [\,\;\;1,\,-1 & | & 0,\,1\,] \\ \mathbb{P} & [\,-1,\;\;\;1 & | & 1,\,0\,] \\ \mathbb{P} & [\,\;\;1,\;\;\;1 & | & 1,\,1\,] \\ \mathbb{P}_A & [\,-1 & | & 0\,] \\ \mathbb{P}_A & [\;\;\;1 & | & 1\,] \\ \mathbb{P}_B & [\,-1 & | & 0\,] \\ \mathbb{P}_B & [\;\;\;1 & | & 1\,] \end{pmatrix} \tag{5}$$

and so also we have

$$C = \begin{pmatrix} -1 & -1 & -1 & 1 & 1 & 0 & 1 & 0 \end{pmatrix} \tag{6}$$

$$l = \begin{pmatrix} -1 \end{pmatrix}. \tag{7}$$

The considerations above can, now, be generalized. Instead of considering two inputs and two outputs for Alice and Bob, one may consider m_A, M_A inputs and outputs for Alice, and m_B, M_B inputs and outputs for Bob. This results in a more sophisticated characterization, where multiple classes of non-locallity appear. Equivalently, in this generalized setting, the possible statistics of the game as played by local players are no longer described by a single inequality (as was the case for eq. (2)), but rather by multiple *nonequivalent* inequalities.

In fact, already in the above case, one could have derived multiple quantities violated in the presence of non-local behaviour, corresponding to multiple inequalities. In other words, C and l could have taken values

$$C = \begin{pmatrix} -1 & -1 & -1 & 1 & 1 & 0 & 1 & 0 \\ 1 & -1 & 1 & 1 & 0 & -1 & -1 & 0 \\ -1 & 1 & -1 & -1 & 0 & 1 & 1 & 0 \\ 1 & 1 & -1 & 1 & -1 & 0 & 0 & -1 \\ -1 & -1 & 1 & -1 & 1 & 0 & 0 & 1 \\ -1 & 1 & 1 & 1 & 0 & -1 & 0 & -1 \\ 1 & 1 & 1 & -1 & -1 & 0 & -1 & 0 \\ 1 & -1 & -1 & -1 & 0 & 1 & 0 & 1 \end{pmatrix}, \tag{8}$$

$$l = \begin{pmatrix} -1 & 0 & -1 & 0 & -1 & 0 & 0 & -1 \end{pmatrix}^T. \tag{9}$$

However, all of these inequalities can be obtained from each other by one of two symmetries: relabelling of inputs, or relabelling of outputs conditioned on inputs. Naturally, for a verifier to certify the sharing of non-local resources between two players that receive and return the same number of inputs and outputs, it does not matter whether it considers the first player to be Alice or Bob (and vice versa for the second player). Therefore, any inequality that can be obtained from another by permutation of the labels of the players is equivalent to it. Likewise, assigning different labels to the inputs and outputs that can be given to and from Alice and Bob does not fundamentally change the inequalities, i.e., when a player receives a certain input, they are free to permute the labels of the corresponding output (conditioned to the input) without changing the nature of the non-locality test (as long as this permutation is carried out consistently throughout the test). We can summarize this as follows: if there is some inequality for input and output labels a, b, x, y

$$I_{a,b,x,y} \tag{10}$$

then a choice of permutations $\pi_1(x)$, $\pi_2(y)$, $\pi_3(a\,|\,x)$, $\pi_4(b\,|\,y)$ yields equivalent inequalities

$$I_{a,b,\pi_1(x),\pi_2(y)}, \text{ and} \tag{11}$$

$$I_{\pi_3(a\,|\,x),\pi_4(b\,|\,y),x,y}. \tag{12}$$

Returning to the generalization of these non-local games, one may examine the set of joint probability distributions for the inputs and outputs of local players, and conclude it is a polytope in a space of dimension $D = (m_A - 1)M_A(m_B - 1)M_B + M_A(m_A - 1) + M_B(m_B - 1)$, the "local polytope" [2, section 2.5] [1] [2]. Considering that a polytope is a generalization of the notion of a solid of flat faces to D dimensions, we have that each "face" of the local polytope corresponds to an inequality and defines a bound to be violated by non-local players (easy to understand in light of the previous analysis where there was only one such "face"). On the other hand, it is easy to generate a list of vertices of this polytope: consider the possible non-signalling and deterministic distributions. A distribution is said to be non-signalling if the statistics of one player is independent of the other, in the following sense:

$$\text{for some } i_a, o_a \qquad \sum_{o_b} \mathbb{P}[o_a, o_b\,|\,i_a, i_b] = \sum_{o_b} \mathbb{P}[o_a, o_b\,|\,i_a, i'_b] \qquad \text{for all } i_b, i'_b \tag{13}$$

$$\text{for some } i_b, o_b \qquad \sum_{o_a} \mathbb{P}[o_a, o_b\,|\,i_a, i_b] = \sum_{o_a} \mathbb{P}[o_a, o_b\,|\,i'_a, i_b] \qquad \text{for all } i_a, i'_a \tag{14}$$

and a deterministic process is one for which the marginals take values only 0 or 1. The resulting set of distributions form the set of vertices of the local polytope, as any other local process results from a convex combination of these local deterministic processes [3].

Converting between a vertex representation and a facet representation, which is its dual form, is an NP-complete problem. Per the discussion above, however, we are most interested in the facet representation. For this reason, significant effort has been made to tackle concrete instances of the problem [2, 4]. The result is that this stage (of converting between the vertex representation and the facet/half-space representation) is not the bottleneck of finding classes of non-locallity for a given choice of (m_A, M_A, m_B, M_B). Instead, due to the large amount of inequalities produced, the bottleneck is the previously discussed identification of equivalences, in order to determine the unique classes of non-locallity for that non-local game.

II. PROBLEM STATEMENT

Input: m_A, M_A, m_B, M_B, the number of inputs and outputs for Alice and Bob, respectively.
The extended matrix $\big(C\,|\,l\big)$, given as a text file.

Output: The *nonequivalent* row entries of C.

The order of the symbolic entries of p for a particular (m_a, m_B, M_A, M_B) is known and given, namely

$$p = \Big(\mathbb{P}[0,0\,|\,0,0], \ldots, \mathbb{P}[m_A - 2, m_B - 2\,|\,M_A - 1, M_B - 1], \\ \underset{A}{\mathbb{P}}[0\,|\,0], \ldots, \underset{A}{\mathbb{P}}[m_A - 2\,|\,M_A - 1], \underset{B}{\mathbb{P}}[0\,|\,0], \ldots, \underset{B}{\mathbb{P}}[m_B - 2\,|\,M_B - 1] \Big)^T. \tag{15}$$

---

[1] Assuming that the number of possible outputs is the same regardless of the input received for both players.
[2] The previous remark that 8 probabilities sufficed is now justified by taking $m_A = m_B = M_A = M_B = 2$.

The main challenge of the problem is throughput. There are $m_A!$ permutations of Alice's input labels, $m_B!$ permutations of Bob's input labels, $m_A(M_A!)$ permutations of Alice's output labels conditioned on input, and $m_B(M_B)!$ permutations of Bob's output labels conditioned on input. However, even this does not dominate the size of the problem, which is mainly fixed by the number of inequalities produced in the half-space description of the polytope. Although the scaling relation of the number of faces of the polytope with the number of inputs and outputs is not known, we have that, for example, for $(m_A, m_B, M_A, M_B) = (3, 3, 3, 3)$, the local polytope is described by $\sim 10^8$ inequalities.

There is no known algorithm for this problem other than brute-force checking.

$C \leftarrow \{\text{inequalities}\}$

$I \leftarrow \{\}$

For inequality $I_{a,b,x,y}$ in C:

seen $\leftarrow$ False

For each input permutation π_1, π_2:

For each output permutation conditioned on input π_3, π_4:

$x' \leftarrow \pi_1(x)$, $y' \leftarrow \pi_2(y)$, $a' \leftarrow \pi_3(a\,|\,x')$, $b' \leftarrow \pi_4(b\,|\,y')$.

If $I_{a',b',x',y'}$ is in I, set seen to True.

If seen is False, insert $I_{a,b,x,y}$ into I.

Output I.

---

[1] D. Collins and N. Gisin, A relevant two qubit bell inequality inequivalent to the CHSH inequality, Journal of Physics A: Mathematical and General **37**, 1775 (2004).

[2] J. D. da Costa Jesus, *Semi-device Independent Protocols for Quantum Key Distribution*, Master's thesis, Instituto Superior Técnico, Universidade de Lisboa (2023).

[3] J. Halliwell, Two proofs of Fine's theorem, Physics Letters A **378**, 2945 (2014).

[4] S. Lörwald and G. Reinelt, PANDA: a software for polyhedral transformations, EURO Journal on Computational Optimization **3**, 297 (2015).