No quantum realization of extremal no-signaling boxes

Ravishankar Ramanathan,∗ Jan Tuziemski,‡ Michał Horodecki and Paweł Horodecki

1National Quantum Information Center of Gdańsk, 81-824 Sopot, Poland
2Institute of Theoretical Physics and Astrophysics, University of Gdańsk, 80-952 Gdańsk, Poland
3Faculty of Applied Physics and Mathematics, Technical University of Gdańsk, 80-233 Gdańsk, Poland

Abstract

Pure states are very important in any theory since they represent states of maximal information about the system within the theory. Here, we show that no non-trivial (not local realistic) extremal states (boxes) of general no-signaling theories can be realized within quantum theory. We then explore three interesting consequences of this fact. Firstly, since the pure states are uncorrelated from the environment, the statement forms a no-go result against the most straightforward device-independent protocol for randomness or secure key generation against general no-signaling adversaries. It also leads to the interesting question whether all non-extremal boxes allow for non-local correlations with the adversary. Secondly, in addition to the fact that new information-theoretic principles (designed to pick out the set of quantum correlations from among all non signaling ones) can in consequence be tested on arbitrary non-local vertices to check their validity, it also allows the possibility of excluding from the quantum set any box of no-signaling correlations that can be distilled to a vertex. Finally, it also forms a sufficient condition to identify non-local games with no quantum winning strategy, when one can show that the game has a single unique non-signaling winning strategy. We illustrate each of these consequences with the example of generalized Popescu-Rohrlich boxes.

Introduction. It is well-known that quantum mechanics allows for non-local correlations between spatially separated systems, i.e., correlations that cannot be explained by any local hidden variable theory as shown by the violation of Bell inequalities. The correlations described by quantum theory form a convex set which is sandwiched between the sets of classical correlations and general no-signaling correlations. By how much and why the quantum set is inside the no-signaling set has been the subject of intense research [1–7].

While the classical and no-signaling sets are known to form polytopes, the quantum set is convex but is not a polytope in general. Each point in the set describes a box of correlations, that is a set of conditional probability distributions for outputs given inputs. The extremal boxes (vertices) of the no-signaling polytope are the pure states of the no-signaling theory and their purity implies that they are completely uncorrelated with the environment. Consequently, access to an extremal non-local box would be of great advantage in cryptographic tasks, providing intrinsic certified randomness and keys secure against any eavesdropper even when the latter is limited only by the no-signaling principle. Extremal boxes are also of crucial importance in the program of deriving the set of quantum correlations from purely information-theoretic principles, being essential testbeds for checking the validity of such principles [2–7]. Furthermore, the extremal boxes are the ones that maximally violate Bell inequalities in no-signaling theories; for some Bell inequalities there exists a unique box that gives maximal violation. For instance, for the celebrated CHSH inequality [8], there exists a unique vertex known as the Popescu-Rohrlich (PR) box [9] which maximally violates the inequality. From these considerations, one arrives at the fundamental question: does quantum mechanics allow for the realization of extremal non-local no-signaling boxes? In other words, is there a Bell scenario (for some number of parties, inputs and outputs) for which the quantum set reaches a non-local vertex of the corresponding no-signaling polytope?

Here, we show that the answer to this question is negative: no quantum realization of any extremal non-local no-signaling box exists. To show this, we make use of recently discovered connections between contextuality and Bell scenarios and graph theory [6, 10, 11]. We then consider a few interesting consequences of this fact. Firstly, we consider the important class of Bell inequalities known as multi-player unique games and give a simple condition for identifying when the inequality is maximally violated by a single vertex. Our main result coupled with the fact that all unique games can be won with certainty in general no-signaling theories, then shows that quantum theory does not allow for a winning strategy for this subset of unique games.

Secondly, the non-local vertices being excluded from quantum theory implies that any box that can be distilled to such a vertex by operations (wirings) performed locally by the parties is also excluded. We present a generalization of previously discovered protocols for non-locality distillation to the case of generalized PR boxes with more outcomes and parties, thus excluding new classes of boxes from the quantum set. Finally, the fact that vertices are decoupled from the environment (in particular, eavesdroppers in cryptographic tasks) leads us to consider if any box in the interior of the no-signaling polytope is always non-locally correlated with the environment. We present an extension (into an $n+1$ party box) for the class of $n$ party boxes realized as admixtures of the generalized PR box with the fully mixed box, showing that indeed for any non-zero fraction of

}\end{document}
noise, such a box exhibits non-local correlations with the eavesdropper’s system. We conclude with some open questions.

**Extremal no-signaling correlations.** Consider the $n$-party Bell scenario labeled by $(A_i, \mathcal{X}_i)$ with $i \in [n]$ (with $[n] := \{1, \ldots, n\}$, where the sets $\mathcal{X}_i$ of size $m_i$ denote the respective inputs $x_i$ of the $n$ parties, while the sets $A_i$ of size $k_i$ denote their respective outputs $a_i$. The number of inputs $m_i$ and outputs $k_i$ for each party is arbitrary but for convenience of notation we will consider $m_i = m$ and $k_i = k$, $\forall i \in [n]$, whenever such a simplification does not affect the generality of the argument. A box $\mathcal{P}$ describes a set of conditional probability distributions $P(a|x)$ with $a = \{a_1, \ldots, a_n\} \in A, x = \{x_1, \ldots, x_n\} \in \mathcal{X}$ where $A = A_1 \times \ldots \times A_n$ and similarly $\mathcal{X} = \mathcal{X}_1 \times \ldots \times \mathcal{X}_n$; the Bell scenario corresponding to this box is denoted as $B(n, m, k)$. The box $\mathcal{P}$ is a valid no-signaling box for the Bell scenario if it satisfies: (i) Positivity: $P(a|x) \geq 0$ $\forall a, x$; (ii) Normalization: $\sum_a P(a|x) = 1$ $\forall x$; and (iii) No-signaling:

$$\sum_{a_i} P(a|x^{(i)}) = \sum_{a_i} P(a|x'^{(i)}) \quad \forall a, x^{(i)}, x'^{(i)}, i$$

where $x^{(i)} = \{x_1, \ldots, x_i, \ldots, x_n\}$ and $x'^{(i)} = \{x_1, \ldots, x_{i-1}, x'_i, x_{i+1}, \ldots, x_n\}$. The set of all boxes satisfying the above conditions forms the no-signaling convex polytope

$$\mathcal{NS}(n, m, k) = \{ \mathcal{P} \in \mathbb{R}^{(mk)^n} : A \cdot |\mathcal{P}| \leq |b| \}$$

of dimension $D = \prod_{i=1}^n [m_i(k_i - 1) + 1] - 1$. Here the constraints (i) - (iii) are written in terms of the matrix $A$ and the vector $|b|$, and the box $\mathcal{P}$ is written as a vector of length $(mk)^n$. Boxes that satisfy in addition the integrality constraint: (iv) Integality: $P(a|x) \in \{0, 1\}$ are said to be classical (deterministic) boxes $\mathcal{P}_d$. The convex hull of these deterministic boxes gives rise to the classical polytope $\mathcal{C}(n, m, k) \subseteq \mathcal{NS}(n, m, k)$. The set of quantum correlations $\mathcal{Q}(n, m, k)$ is defined as follows: $\mathcal{P} \in \mathcal{Q}(n, m, k)$ if there exist a state $|\psi\rangle$, sets of measurement operators $\{E_{x_i}^{a_i}\}$ for each party such that for all inputs and outputs

$$P(a|x) = \langle \psi | \otimes_{i=1}^n E_{x_i}^{a_i} |\psi\rangle$$

with the measurement operators satisfying the requirements of hermiticity $(E_{x_i}^{a_i}, E_{x_i}^{a_i}) = E_{x_i}^{a_i}$, $\forall x_i, a_i$, orthogonality $(E_{x_i}^{a_i}, E_{x_i}^{a_i'}) = \delta_{a_i, a_i'} E_{x_i}^{a_i}$, $\forall a_i$ and completeness $(\sum_{a_i} E_{x_i}^{a_i} = 1, \forall x_i)$. This set is convex but in general is not a polytope, and $\mathcal{C}(n, m, k) \subseteq \mathcal{Q}(n, m, k) \subseteq \mathcal{NS}(n, m, k)$.

We are interested in the vertices of the no-signaling polytope, a box $\mathcal{P}$ being a vertex if it cannot be expressed as a non-trivial convex combination of the boxes in $\mathcal{NS}(n, m, k)$. The vertex of a polytope is a point such that the normal cone to the point has full dimension, and every vertex satisfies in a unique way a certain number of the inequality constraints in $A \cdot |\mathcal{P}| \leq |b|$ with equality. Formally the vertex is characterized as follows [12]:

**Fact 1.** A box $\mathcal{P}$ is a vertex of the no-signaling polytope $\mathcal{NS}(n, m, k)$ if any only if $\text{rank}(A) = (mk)^n$ where $A$ denotes the sub-matrix of $A$ consisting of those row vectors $A_i$ for which $A_i \cdot |\mathcal{P}| = |b|$.

For two distinct vertices $\mathcal{P}$ and $\mathcal{P}'$, the corresponding sub-matrices are not equal $(A(\mathcal{P}) \neq A(\mathcal{P'}))$. A non-local vertex is one that does not belong to $\mathcal{C}(n, m, k)$. We use recently discovered connections between contextuality and non-local game scenarios to graph theory [6, 10, 11] to show that such a vertex also does not belong to the quantum set $\mathcal{Q}(n, m, k)$.

**Theorem 1.** For some (arbitrary) $(n, m, k)$, let $\mathcal{P}^{nl}$ be a vertex of the no-signaling polytope $\mathcal{NS}(n, m, k)$ such that $\mathcal{P}^{nl} \notin \mathcal{C}(n, m, k)$. Then $\mathcal{P}^{nl} \notin \mathcal{Q}(n, m, k)$.

**Non-local games with no quantum winning strategy.** An immediate application of Theorem 1 is that if one is able to identify a non-local game that has a single unique winning no-signaling strategy (where by a winning strategy we mean one that achieves maximal value 1), then such a strategy (being a vertex) cannot be realized in quantum theory. So that denoting by $\omega_q(g)$ the quantum value of the game $\omega_q(g)$, we have $\omega_q(g) \neq 1$. Here, we consider a class of Bell inequalities known as total unique games (gU) for multiple players, which are a family of games of great interest in the field of hardness of approximation (in determining the algorithmic complexity of finding close to optimal solutions for optimization problems) as seen in the famous unique games conjecture [13]. A unique game is defined by the following winning condition: for each $x$ and each set of outcomes of any chosen $n - 1$ parties, $a_{j-1}^{(j)} = a \setminus a_j, j \neq i$, the remaining party is required to output a single unique $a_i$ specified by a function $\sigma_j (a_{j-1}^{(j)})$ with $\sigma_j (a_{j-1}^{(j)}) \neq \sigma_j (a_{j-1}^{(j)})$ for $a_{j-1}^{(j)} \neq a_{j-1}^{(j)}$; the term total refers to the fact that such a winning constraint is imposed for every set of inputs $x$. We now introduce the notion of a no-signaling graph associated with any non-local game.

**Definition.** For any non-local game $g$, we define the no-signaling graph $G_{NS}(g)$ = $(V, E)$ associated with the game to have set of vertices $v \in V$, each of which is labeled by a set of inputs and outputs that wins the game, $v = (a^{(v)}, x^{(v)})$. Two vertices $v, v' \in V$ are connected by an edge if $\exists S \subseteq [n]$ with $|S| = n - 1$ such that $(a^{(v)} = a^{(v')} \land x^{(v)} = x^{(v')}) \forall i \in S$.

**Lemma 2.** A total multi-player unique game $g^{U}$ is won by a single unique non signaling box if and only if the no-signaling
graph $G_{NS}(g^U)$ associated to the game is connected; for such a game $\omega_q(g^U) \neq 1$.

Proof. By definition for a unique game, only one term from the game constraint appears in each sum in the no-signaling constraint Eq. (1) for any $x(i), x'(i), a$. Hence, two vertices being connected implies that the corresponding probabilities are equal. Consequently, the no-signaling graph $G_{NS}(g^U)$ being connected implies that the box is uniform, with every winning event occurring with probability $\frac{1}{k}$, where $k$ is the number of outputs of the game. Since the total unique game considers all sets of inputs $x$, it is won by this specific no-signaling box alone, which must necessarily therefore be a vertex of the no-signaling polytope. By Theorem 1, we know that such a box cannot be realized by measurements on quantum states, so that $\omega_q(g^U) \neq 1$.

On the other hand, consider that the graph $G_{NS}(g^U)$ is disconnected, being composed of $c \geq 1$ components $G_c$. By definition of the no-signaling graph and the winning constraint of the unique game, each $G_c$ consists of the same number $k_c$ of vertices from each setting $x$, i.e. $k_c(x) = k_c(x')$ for any pair of $x, x'$, where $k_c(x)$ denotes the number of vertices $v$ in graph $G_c$ with associated label $(a(v), x)$. Corresponding to each $G_c$ therefore, we can construct the explicitly non-signaling box $P_c$ with entries $P_c(a^i|x') = \frac{1}{k_c}$ if the vertex $(a^i, x') \in V(G_c)$, and zero otherwise. It is readily seen that each such box $P_c$ wins the game.

An alternative (equivalent) characterization of the total unique game with single maximally violating box is that the block matrix composed of the permutation matrices associated to the functions $\sigma^{(j)}$ defining the unique game in every $n - 1|1$ cut is irreducible. Let us now illustrate the above application with an example of the generalized PR box and show that the corresponding generalized CHSH game cannot be won quantumly.

**Example 1.** The unique game $g^{U,ex}$ for $n$ parties with inputs $x_i \in \{0, 1\}$ and outputs $a_i \in \{0, \ldots, k - 1\}$ defined by the winning constraint: $\oplus_{i=1}^n a_i \mod k = \prod_{i=1}^n x_i$ is won by a single no-signaling vertex for any $n, k$.

Proof. We show that the no-signaling graph $G_{NS}(g^{U,ex})$ is connected so that the game is won by a single no-signaling box by Lemma 2. Firstly, note that the no-signaling graph $G_{NS}(g^U)$ for any unique game of $n$ parties with $m$ inputs each with $k$ outputs is of size $m^n \cdot k^n - 1$ since for each set of inputs $x$ (of which there are $m^n$) there are $k^n - 1$ outputs $a$ that win the game. Therefore, for $G_{NS}(g^{U,ex})$ with vertex set $V$, we have $|V| = 2^n k^{n-1}$. We may group the vertices into two sets $V_j := \{v : \oplus_{i=1}^n a_i^{(v)} \mod k = \prod_{i=1}^n x_i^{(v)} = j\}$ for $j \in \{0, 1\}$.

The edges of the graph $G_{NS}(g^{U,ex})$ can also be grouped into two sets based on $V_0$ and $V_1$:

1. For $u, v \in V_0$, we have the edge $u \sim v$ if $(a^{(v)} = a^{(u)}) \wedge (x^{(v)} = x^{(u)})$ for some $i \in [n]$ where $x^{(u)}_{i+1} = \{x_i^{(u)} , \ldots , x_{i+1}^{(u)} \oplus 1, x_{i+1}^{(u)} , \ldots , x_n^{(u)} \}$, and $\oplus_j$ denotes addition modulo $j$.

2. For $u \in V_1, v \in V_0$, we have $u \sim v$ if $(a^{(v)} = a^{(u)} \oplus 1) \wedge (x^{(v)} = x^{(u)})$ for some $i \in [n]$.

Therefore, we have that the graph is regular with the degree of each vertex (the number of edges incident at each vertex) equal to $n$, so that the total number of edges in the graph is given by $|E| = \frac{2^n k^{n-1}}{2}$. Let us divide the vertex set $V$ into $k^{n-1}$ subsets each of fixed $a_{n-1}$ (outputs of the first $n - 1$ parties) which we denote by $V_{a_{n-1}}$ with $|V_{a_{n-1}}| = 2^n$. From the edge sets above, it is clear that the corresponding subgraphs $G^{a_{n-1}}$ are connected. It remains to be shown that these $k^{n-1}$ subgraphs are connected to each other.

To do this, let us form a new graph $G'_{NS}$ with each connected subgraph $G^{a_{n-1}}$ as a single vertex in the new graph and edges between two vertices in $G_{NS}'$ if there exists an edge between any two vertices in the corresponding subgraphs. Due to the xor structure, the edges in set (2) above with $u \in V_1$ and $v \in V_0$ give rise to cyclic subgraphs of length $k$ in $G_{NS}'$. The vertex set of $G_{NS}'$ (of size $k^{n-1}$) is thus partitioned in $n - 1$ different ways into $k^{n-2}$ sets of vertices belonging to disjoint cyclic subgraphs of size $k$ each. This guarantees that the graph $G_{NS}'$ is connected; and hence that the different subgraphs $G^{a_{n-1}}$ for each $a_{n-1}$ are connected to each other. The graph $G_{NS}(g^{U,ex})$ is thus connected; by Lemma 2 we have that the game $g^{U,ex}$ is won by a unique no-signaling vertex, and hence cannot be won using quantum resources.

In [1, 4], it was shown that for two-player binary games $g^{bin}$ (where the output alphabet of the two players is binary), $\omega_q(g^{bin}) = 1$ if and only if $\omega_q(g^{bin}) = 1$. For the sub-class of binary games known as (total) xor games (where the game winning constraint only depends on the xor of the two players’ outputs), this result can be seen as a consequence of Lemma 2. This is because for total xor games, it is readily seen that the graph $G_{NS}$ is disconnected (and the corresponding block matrix composed of the two possible permutation matrices corresponding to correlations and anti-correlations is reducible) if and only if the game can be won with a classical deterministic strategy.

Exclusion of boxes by distilling many copies to a vertex. The fact that non-local extremal points of the no-signaling set in a single-shot scenario cannot be realized using quantum resources can also be used to exclude from the quantum set those boxes which can be distilled (with many copies in a sequential scenario) to such a vertex. In other words, if there exists a distillation protocol that deterministically maps a certain
number of copies of a box $\mathcal{P}$ to a non-local vertex, then $\mathcal{P} \notin \mathcal{Q}(n, m, k)$.

As an illustration, consider the box presented in the Example [1] defined as

$$\mathcal{P}^{nl,ex}(a|x) = \begin{cases} \frac{1}{k^{n-r}} : \oplus_{i=1}^{n} a_i \ (\text{mod} \ k) = \prod_{i=1}^{n} x_i & \text{if } r \leq n, \\
0 & \text{otherwise} \end{cases}$$

We now examine an admixture of the above non-local vertex with a locally correlated box $\mathcal{P}^{c,ex}$ defined as

$$\mathcal{P}^{c,ex}(a|x) = \begin{cases} \frac{1}{k^{n-r}} : \oplus_{i=1}^{n} a_i \ (\text{mod} \ k) = 0 & \text{if } r \leq n, \\
0 & \text{otherwise} \end{cases}$$

A generalization of the distillation protocols in [15, 16], shows that for any $\varepsilon \in (0, 1)$, many copies of the box

$$\mathcal{P}_{\varepsilon,n} = \varepsilon \mathcal{P}^{nl,ex} + (1 - \varepsilon) \mathcal{P}^{c,ex}$$

can be distilled to the vertex $\mathcal{P}^{nl,ex}$, so that the box $\mathcal{P}_{\varepsilon,n}$ for arbitrary $\varepsilon(> 0)$, $n$ (arbitrarily close to the classical polytope) is immediately excluded from the quantum set.

**Lemma 3.** For any $\varepsilon \in (0, 1)$ there exists a deterministic distillation protocol $\mathcal{D}$ that maps $\mathcal{P}^{\otimes r} \rightarrow \mathcal{P}_{\varepsilon,n}$ for large $r$, i.e., $\mathcal{D}: \mathcal{P}^{\otimes r} \xrightarrow{\mathcal{D}} \mathcal{P}^{nl,ex}$. 

**Proof.** We show a protocol $\mathcal{D}^{(2)}$ that maps $\mathcal{P}^{\otimes 2} \rightarrow \mathcal{P}_{\varepsilon,n}$ with $\varepsilon' > \varepsilon$, the statement then follows by iteration of $\mathcal{D}^{(2)}$. Let us denote by $x_{i}^{(j)}$ and $a_{i}^{(j)}$ the input and outputs of the $i$-th party to the $j$-th copy of the box, where $i \in [n]$ and $j \in [1, 2]$. The protocol $\mathcal{D}^{(2)}$ maps the box with inputs $x_i$ and outputs $a_i$. The inputs to the two boxes are given by $x_{i}^{(1)} = x_i$ and $x_{i}^{(2)} = x_i \cdot I(a_{i}^{(1)} \oplus k 1)$, where $I$ is the indicator $I(b) = 1$ if $b = 1$ and 0 otherwise.

The $i$-th party finally outputs $a_i = a_i^{(1)} \oplus a_i^{(2)}$. We show that with probability $\varepsilon' > \varepsilon$, we have $\oplus_{i=1}^{n} a_i = \prod_{i=1}^{n} x_i$ so that the iteration of the protocol succeeds in distilling the box $\mathcal{P}_{\varepsilon,n}$ to the vertex $\mathcal{P}^{nl,ex}$. Consider the action of the protocol on each of the four terms in $\mathcal{P}^{\otimes 2}$. (i) $\mathcal{P}^{nl,ex} \otimes \mathcal{P}^{nl,ex}$: With the above choice of inputs, we have that $\oplus_{i=1}^{n} a_i^{(1)} = \prod_{i=1}^{n} x_i$ and $\oplus_{i=1}^{n} a_i^{(2)} = 0$ so that once more we have $\oplus_{i=1}^{n} a_i = \prod_{i=1}^{n} x_i$. Therefore, the protocol maps the box $\mathcal{P}^{nl,ex} \otimes \mathcal{P}^{nl,ex}$ to $\mathcal{P}^{nl,ex}$.

(ii) $\mathcal{P}^{nl,ex} \otimes \mathcal{P}^{c,ex}$: By definition, we have $\oplus_{i=1}^{n} a_i^{(1)} = \prod_{i=1}^{n} x_i$ and $\oplus_{i=1}^{n} a_i^{(2)} = 0$, so that this box is also mapped to $\mathcal{P}^{nl,ex}$. (iii) $\mathcal{P}^{c,ex} \otimes \mathcal{P}^{nl,ex}$: We have that $\oplus_{i=1}^{n} a_i^{(2)} = \prod_{i=1}^{n} x_i$ when $a_i^{(1)} = 0 \forall i$ which happens with probability $\frac{k^{n-r}}{k^n}$ so that this box is mapped to $\frac{1}{k^{n-r}} \mathcal{P}^{nl,ex} + (1 - \frac{1}{k^{n-r}}) \mathcal{P}^{nl,ex}$. (iv) $\mathcal{P}^{c,ex} \otimes \mathcal{P}^{c,ex}$: We have that simply $\oplus_{i=1}^{n} a_i = 0$ so that this box is mapped to $\mathcal{P}^{c,ex}$. Overall, we see that the protocol $\mathcal{D}^{(2)}$ maps $\mathcal{P}^{\otimes 2}$ to $\mathcal{P}^{nl,ex}$ with $\varepsilon' = \frac{1}{k^{n-r}} (k^{n-1} + 1 - \varepsilon) > \varepsilon$. Iterating this protocol for $r = 2^j$ boxes for large $j$ results in the distillation of the initial box $\mathcal{P}_{\varepsilon,n}$ to the non-local vertex $\mathcal{P}^{nl,ex}$. \square

**Extensions of non-extremal boxes.** Perhaps the most crucial consequence of Theorem 1 is that it rules out the most straightforward protocol for obtaining secure keys or random bits, as we now demonstrate. Extremal non-local boxes of the no-signaling polytope cannot be correlated with the environment, i.e., if $\mathcal{P} = \{ \mathcal{P}(a|x) \}$ is an $n$-party box that is a vertex, and $\{ P(a, b | x, y) \}$ is any $n + 1$-party box of which $\mathcal{P}$ is the marginal, then necessarily, one has

$$\{ P(a, b | x, y) \} = \{ P(a| x) \otimes P(b| y) \}.\ (6)$$

To see this, note that

$$P(a|x) = \sum_b P(a, b | x, y) = \sum_b P(a|x, b, y)P(b| y),\ (7)$$

where we have used the no-signaling condition $P(b|x, y) = P(b| y)$. Since $\{ P(a| x) \}$ is a vertex, the decomposition in Eq. (7) can only have a single term, so that for all $b, y$, we have $P(a|x, b, y) = P(a|x)$, which translates to

$$\{ P(a, b | x, y) \} = \{ P(a|x, b, y)P(b| y) \} = \{ P(a|x) \otimes P(b| y) \}.\ (8)$$

Access to an extremal box $\mathcal{P}$ would thus provide a tremendous advantage to the honest parties in cryptographic tasks where one considers the presence of an all-powerful adversary limited only by the relativistic causality constraint imposed by the no-signaling principle. For instance, in a noiseless scenario, one can readily design a protocol where the honest parties check for the presence of the extremal box in a device-independent manner and then obtain the intrinsic randomness from the box or use it to distribute secure keys, knowing that they are uncorrelated with the eavesdropper’s system.

**Theorem 4** is thus a no-go result against this straightforward protocol. On the other hand, if $\mathcal{P}$ is not a vertex, then Eq. (7) shows that there can always be (classical) correlations with the eavesdropper’s system.

A natural question then arises (see [17]) if any box $\mathcal{P}$ that is in the interior of the no-signaling polytope also allows for non-local correlations with an eavesdropper, i.e., if there is an extension into a box $\mathcal{P}(a, e|x, z)$ such that $\mathcal{P}(a|x)$ is obtained as the marginal of $\mathcal{P}$ upon tracing out the eavesdropper’s system, and $\mathcal{P}$ exhibits non-locality in the cut $(A_1, \ldots, A_n)|E$. This is especially interesting not only due to the fact that non-local correlations impart additional power to the eavesdropper, but that the analogous fact in quantum theory holds, namely a mixed state of $n$ systems can always be extended into an
entangled state of $n+1$ systems, i.e., $\rho_n = \sum_i \lambda_i |i\otimes n \rangle \langle i\otimes n|$ can be extended to $|\psi_{n+1}\rangle = \sum_i \sqrt{\lambda_i} |i\otimes n+1 \rangle$ where the $|i\rangle$ constitute an orthonormal basis, and $\lambda_i > 0$ are the corresponding eigenvalues. For the vertices from Example 1 (given in Eq. 3), which correspond to the Bell scenario $B(n,2,k)$, we show that any box obtained by admixing the vertex with the completely noisy box can be extended to a local relabeling of the inputs and outputs. We now examine the isotropic boxes of the form $P_{\varepsilon,n} = \varepsilon P_{n+1,ex}(0) + (1 - \varepsilon) P_1$.

**Lemma 4.** For the Bell scenario $B(n,2,k)$, for any $\varepsilon \in [0,1]$ the box $P_{\varepsilon,n}$ admits a non-local extension to a box $\tilde{P}(a,e|x,z)$, with $a_i, e \in \{0, \ldots, k-1\}$, $x_i, z \in \{0,1\}$ such that the bipartite cut $(A_1, \ldots, A_n) | E$ exhibits non-local correlations. We note that the extremal points of the Bell scenario $B(2,2,k)$ have been characterized in [17] where it was shown that all the extremal boxes are of the form given in Eq. (3) for $n = 2$ up to a local relabeling of the inputs and outputs. We now examine the isotropic boxes of the form $P_{\varepsilon,n} = \varepsilon P_{n+1,ex}(0) + (1 - \varepsilon) P_1$.

**Proof.** Define the non-local box $\tilde{P}_{\varepsilon,n+1}$ as $\tilde{P}_{\varepsilon,n+1} := \varepsilon P_{n+1,ex}(0) \otimes P_1 + (1 - \varepsilon) P_{n+1}$. Where $P_1$ is a deterministic box with entries $P_1(0|z) = 1$ and $0$ otherwise, and $P_{n+1,ex}(0)$ is a slightly modified form of the non-local vertex from Eq. (3), obeying $a_i^{n+1} a_i = x_1 \cdot (x_2 + 2) \cdots (x_n + 2) : x_{n+1}$. It is then readily seen that $P_{\varepsilon,n}$ is obtained from $\tilde{P}_{\varepsilon,n+1}$ by tracing out the $(n+1)$-th system.

We now show that for any $\varepsilon \in [0,1]$, the box $\tilde{P}_{\varepsilon,n+1}$ in the cut $(A_1, \ldots, A_n) | E$ violates the bipartite Bell inequality defined for $P_{n+1,ex}(0)$, i.e., with the winning constraint $a \oplus e = x \cdot z$ which is achieved by the following choice of inputs for the $n+1$ parties: $(x_1 = x, x_2 = \ldots = x_n = 0, x_{n+1} = z)$ and the outputs $(a = a_i^{n+1} a_i, e = a_{n+1})$. With this choice of inputs and outputs, the box $\tilde{P}_{\varepsilon,n+1}$ achieves the cut $(A_1, \ldots, A_n) | E$ the value $4 - \varepsilon$ for the bipartite inequality which beats the local bound of $3$ for any $\varepsilon \in [0,1]$.

**Conclusions.** We have seen that the non-local vertices of the no-signaling polytope of correlations admit no quantum realization and explored some consequences of this fact. An interesting question for future study is how close the quantum set can get to such a vertex, and whether a finite separation always exists. In this regard, it is pertinent to note that for Bell inequalities with algebraic violation (such as the GHZ paradoxes in [18]) or close to algebraic violation (such as the chained Bell inequalities in [19]), the quantum set only reaches the corresponding facet of the no-signaling polytope. Another question for further research is to identify other interesting classes of vertices than the one illustrated here, and construct novel distillation protocols for these. Finally, an open problem is whether all points in the interior of the no-signaling set allow for non-local correlations with the environment, and its consequences for cryptographic tasks.

**Acknowledgements.** This work is supported by the ERC grant QOLAPS, the EU grant RAQUEL (No. 323970), and the Foundation for Polish Science TEAM project co-financed by the EU European Regional Development Fund. R. R. acknowledges useful discussions with G. Murta, P. Mironowicz and M. Pawłowski.
(1984).
[24] T. Fujie and A. Tamura, J. Op. Res. Soc. of Japan 45, 3 (2002).
[25] F. B. Shepherd, In Perfect graphs, Wiley-Intersci. Ser. Discrete Math. Optim., 261, Wiley, Chichester (2001).
[26] M. K. de Carli Silva and L. Tunçel, arXiv: 1309.7415 (2013).
[27] M. K. de Carli Silva, PhD Thesis, University of Waterloo (2013).
[28] R. A. Horn and C. R. Johnson, Matrix Analysis, Cambridge University Press, Cambridge (1987).

Supplemental Material

Here we present the proof of the Theorem stated in the main text. To do this, we first present some background information on recently discovered relations between contextuality and non-local game scenarios to graph theory.

In [20], a hierarchy of semi-definite programs was formulated for optimization with non-commuting variables, that is used to identify when a box $P$ does not belong to the quantum set; it was also shown that the hierarchy converges to a set $Q^{pr}(n, m, k)$. Note that the set $Q^{pr}(n, m, k)$ described in this hierarchy can be in fact larger than $Q(n, m, k)$ since the former set is defined for the probabilities given by

$$P(a|x) = \langle \psi | \prod_{i=1}^{n} E_{x_i, a_i} | \psi \rangle$$

with commutativity imposed on the measurements of different parties, i.e., $[E_{x_i, a_i}, E_{x_j, a_j}] = 0$ for $i \neq j$.

In other words, the strict requirement of a tensor product structure of the operators of different parties is replaced with the requirement of only commutation between these operators. Since $Q(n, m, k) \subseteq Q^{pr}(n, m, k)$, the exclusion of the non-local vertices from $Q^{pr}(n, m, k)$ is sufficient to exclude them from the quantum set.

In the hierarchy, one considers sets of sequences of products of projection operators $S_1 = \{1 \} \cup \{ E_{x_1, a_1} \} \cup \cdots \cup \{ E_{x_n, a_n} \}$, $S_2 = S_1 \cup \{ E_{x_{i_1}, a_{i_1}} E_{x_{i_2}, a_{i_2}} : i_1, i_2 \in [n] \}$, etc. The convex sets $Q_l$ corresponding to different levels of the hierarchy are then constructed by testing for the existence of a certificate $\Gamma^l$ associated to the set of operators $S_l$ using a semi-definite program. The certificate $\Gamma^l$ corresponding to level $l$ is a $|S_l| \times |S_l|$ matrix whose rows and columns are indexed by the operators in set $S_l$ and is a complex Hermitian positive semi-definite matrix that satisfies the following constraints on its entries

$$\Gamma^l_{i,j} = 1,$$

as well as constraints resulting from operator relations, $\Gamma^l_{Q,R} = \Gamma^l_{S,T}$ if $Q,R \subseteq S,T$. The lack of existence of a positive semi-definite certificate corresponding to any level of the hierarchy implies the exclusion of the box from the quantum set. Recently, one of the levels of the hierarchy labeled $Q(n, m, k)$ has been highlighted as the almost quantum set [21], owing to the fact that it was proven to satisfy most (all but the principle of information causality [4], there being numerical evidence in support of this too) of the reasonable information-theoretic principles designed to pick out quantum theory from among all no-signaling theories. The set $\hat{Q}$ is an intermediate level of the hierarchy associated to the set of operators $\hat{S} = 1 \cup \{ E_{x_1, a_1} \} \cup \cdots \cup \{ E_{x_n, a_n} : a_i \in A_i, x_i \in X_i \}$. As we shall see, $\hat{Q}(n, m, k)$ already excludes all the non-local no-signaling vertices.

Recently, a relationship was discovered between Bell scenarios, more general contextuality scenarios, and graph theory via the use of orthogonality graphs [3,10] and hypergraphs [11]. The orthogonality graph $G_B$ corresponding to the Bell scenario $B(n, m, k)$ is constructed as follows. Each event $(a|x')$ of the Bell scenario corresponds to a vertex of $G_B$, and a pair of vertices is connected by an edge if the corresponding events are locally orthogonal [6], i.e.

$$u \sim v \iff \exists i \in [n] \ s.t. \ x_i^u = x_i^v \land a_i^u \neq a_i^v.$$  

(12)

Equivalently, each operator of the form $E_{x_1, a_1} \cdots E_{x_n, a_n}$ in the $n$-party Bell scenario corresponds to a vertex of $G_B$, and a pair of vertices is connected by an edge if

$$\exists i \in [n] \text{ such that } E_{x_i, a_i} E_{x_i, a_i'} = 0.$$  

The graph $G_B$ therefore has $D := (mk)^n$ vertices (in general the number of vertices is $\prod_{i=1}^{n} m_i k_i$). An orthonormal representation of a graph $G$ with vertex set $V$ and edge set $E$ is a set of unit vectors $\{ |u_i| : i \in V \}$ where $|u_i| \in \mathbb{C}^V$ for some $N, ||u_i|| = 1$ for all $i \in V$ and $\langle u_i | u_j \rangle = 0$ for $(i, j) \in E$ (note that this differs from the original representation in [22] where non-adjacent vertices were assigned orthogonal vectors). Based on orthonormal representations, one constructs the theta body $\mathrm{TH}(G)$ of the graph which is
Definition (22). For any graph $G = (V, E)$, $TH(G) := \{P = (|\psi u_i|^2 : i \in V) \in \mathbb{R}^V_+: ||\psi|| = ||u_i|| = 1, \{u_i\}\}$ is an orthonormal representation of $G$.

We are now ready to provide the proof for the main theorem stated in the text.

Theorem 1. For some (arbitrary) $(n, m, k)$, let $P^{\text{nl}}$ be a vertex of the no-signaling polytope $\text{NS}(n, m, k)$ such that $P^{\text{nl}} \notin C(n, m, k)$. Then $P^{\text{nl}} \notin Q(n, m, k)$.

Proof. We first examine the precise relation between $P$

$$\sum_{a_j} P(a_1, \ldots, a_j, \ldots, a_n|x_1, \ldots, x_j, \ldots, x_n) + \sum_{a_j'} P(a_1, \ldots, a_j', \ldots, a_n|x_1, \ldots, x_j', \ldots, x_n) = 1$$

$$\forall j, x_j, x'_j, x_i (i \neq j) \tag{13}$$

Now, it is readily seen that all the events occurring in the above expression are locally orthogonal, so that the no-signaling constraints are maximum clique inequalities that are saturated for the orthogonality graph $G^*_B$; however we also note that not every maximum clique inequality of $G^*_B$ corresponds to a no-signaling or a normalization condition. We now define the subset $TH^{(c)}(G) \subset TH(G)$ as the set of boxes in $TH(G)$ for which the maximum cliques $c$ corresponding to the normalization and no-signaling constraints have $\sum_{i \in c} |\langle \psi u_i | \rangle| = 1$, i.e., defining $C_{n, ns}$ as the set of maximum cliques corresponding to the normalization and no-signaling constraints, we have the following definition for $TH^{(c)}(G)$.

Definition. For the orthogonality graph $G_B$ corresponding to the Bell scenario $B(n, m, k)$, define the set $TH^{(c)}(G)$ as $TH^{(c)}(G) := \{P = (|\psi u_i|^2) \in TH(G) : \forall c \in C_{n, ns}, \sum_{i \in c} |\langle \psi u_i | \rangle| = 1\}$.

Theorem 5. For any $n$-party Bell scenario $B$, $\tilde{Q} = TH^{(c)}(G_B)$.

Proof. The set $\tilde{Q}$ of boxes $P = \{P(a|x)\}$ is characterized by the existence of a certificate $\Gamma^{\tilde{Q}}$ which is a $D \times D$ complex Hermitian positive semi-definite matrix with the following constraints on its entries

$$\Gamma^{\tilde{Q}}_{1,1} = 1,$$

$$\Gamma^{\tilde{Q}}_{1, E_{a_1} \ldots E_{a_n}, a_n} = \Gamma^{\tilde{Q}}_{E_{a_1} \ldots E_{a_n}, a_n, 1} = \Gamma^{\tilde{Q}}_{E_{a_1} \ldots E_{a_n}, a_n, E_{a_1} \ldots E_{a_n}, a_n} = P(a|x) \quad \forall (a, x)$$

as well as constraints resulting from any operator relations $\Gamma^{\tilde{Q}}_{L,M} = \Gamma^{\tilde{Q}}_{N,O}$ if $L^\dagger M = N^\dagger O$. Crucially, the only constraints from this set of operators are those that impose the Hermiticity of the matrix by the identity

$$(E_{a_1} \ldots E_{a_n} a_n)(E_{a_1} \ldots E_{a_n} a_n)^\dagger \equiv \{(E_{a_1} \ldots E_{a_n} a_n)(E_{a_1} \ldots E_{a_n} a_n)^\dagger\}$$

due to the commutativity of the operators $E_{a_1} \ldots E_{a_n}$ acting on the systems of different parties $i_1$ and $i_2$. As noted in [20], the question of existence of the complex Hermitian positive semi-definite matrix $\Gamma^{\tilde{Q}}$ is equivalent to the existence of a real symmetric positive semi-definite matrix defined as $\frac{1}{2}(\Gamma^{\tilde{Q}} + \Gamma^{\tilde{Q}}^\dagger)$. The set $\tilde{Q}$ then consists of those boxes for which the certificate
\begin{align}
\Gamma^Q \text{ exists, and the normalization and no-signaling constraints are satisfied.}
\end{align}

\begin{align}
TH(G) = \left\{ [P] \in \mathbb{R}^{|V|} : \exists \Pi \in \mathbb{S}^{|V|} \mid |P| \leq 0 \text{ } \forall \Pi \right\}
\end{align}

where $\mathbb{S}^{|V|}$ denotes the set of symmetric matrices of size $|V| \times |V|$ and we view the box $P$ as a vector in $\mathbb{R}^{|V|}$ (for our graphs, we have $|V| = D = (mk)^n$). While there are other equivalent definitions of this set, the above definition is most suitable to recognize the similarities between this set and $\tilde{Q}$.

By inspecting the characterization of $TH^{(c)}(G)$ above, it can be seen that the set $TH^{(c)}(G_B)$ of the orthogonality graph corresponding to the Bell scenario $B$ is just the set $\tilde{Q}$ of the hierarchy. This is seen by considering the requirement of the real symmetric positive semi-definite matrix $(\frac{1}{2})(\Gamma^Q + \Gamma^{Q^*})$ in $\tilde{Q}$ and identifying it with the requirement of the real symmetric positive semi-definite matrix $(\frac{1}{2})(\Pi^Q + \Pi^{Q^*})$ which by the use of Schur complements [28] is equivalent to the condition that $\Pi - |P\rangle\langle P| \succeq 0$ in Eq. (14).

The proof now follows analogously to a similar statement in [24–27]. To show this, we use the following alternative characterization of $TH(G)$ in [24],

\begin{align}
TH(G) = \left\{ [P] \in \mathbb{R}^{|V|} : \langle P|M|P \rangle - \sum_{i \in |V|} M_{i,i} |P\rangle_i \leq 0 \text{ } \forall M \in \mathcal{M}, \right\}
\end{align}

with

\begin{align}
\mathcal{M} := \{ M \in \mathbb{S}^{|V|} : M_{u,v} = 0 \text{ } (u \neq v, v \sim v, M \succeq 0) \}.
\end{align}

Consider a non-local vertex $\mathcal{P}^{nl}$ of the no-signaling polytope $\mathcal{NS}(n, m, k)$. From Fact 1, we know that there is an associated matrix $\hat{A}$ such that $\langle \mathcal{P}^{nl} \rangle_i = |b\rangle$, i.e., such that

\begin{align}
|\mathcal{P}^{nl}\rangle_i = 0 \text{ } \forall i \in \text{Pos},
\end{align}

where Pos is the set of positivity constraints which are set to equality in the vertex box, and the number of independent positivity constraints is $|\text{Pos}|_{\text{ind}} = D = (m(k-1)+1)^n - 1$ (in general $\prod_{i=1}^{n} [m_i(k_i - 1) + 1] - 1$) is the dimension of the no-signaling polytope $\mathcal{NS}(n, m, k)$. In other words, the vertex of $\mathcal{NS}(n, m, k)$ has $D$ independent probabilities that are assigned value 0. Moreover, the box also obeys normalization and no-signaling constraints which are written as maximum clique equalities

\begin{align}
\sum_{i \in c} |\mathcal{P}^{nl}\rangle_i = 1, \text{ } \forall c \in C_{n, ns}
\end{align}

and the number of such independent constraints is $|C_{n, ns}|_{\text{ind}} = D - D$. Consider the matrix $\hat{M} := \hat{A}^T \hat{A}$, which can be written as

\begin{align}
\langle \mathcal{P}^{nl}|\hat{M}|\mathcal{P}^{nl}\rangle - \sum_{i=1}^{D} \hat{M}_{i,i} |\mathcal{P}^{nl}\rangle_i = 0.
\end{align}

Since $\mathcal{P}^{nl}$ is a non-local vertex of a rational convex polytope, it has some entry $|\mathcal{P}^{nl}\rangle_j$ which is non-integer (and rational), i.e., $\exists j \in [\tilde{D}] \text{ s.t. } |\mathcal{P}^{nl}\rangle_j \notin \{0, 1\}$. Now, one can construct the matrix $\tilde{M}' := M - \varepsilon I_{\tilde{D}}$ which is guaranteed to be positive semi-definite for some finite $\varepsilon > 0$ since $\tilde{M}$ is positive definite. Moreover, we also have $\hat{M}' := \hat{M} - \varepsilon I_{\tilde{D}}$ which is guaranteed to be positive semi-definite for some finite $\varepsilon > 0$ since $\hat{M}$ is positive definite. Therefore, $\langle \mathcal{P}^{nl}|\tilde{M}'|\mathcal{P}^{nl}\rangle - \sum_{i=1}^{\tilde{D}} \tilde{M}'_{i,i} |\mathcal{P}^{nl}\rangle_i = -\varepsilon |\mathcal{P}^{nl}\rangle_j (|\mathcal{P}^{nl}\rangle_j - 1) > 0$, so that $\mathcal{P}^{nl} \notin TH(G)$ due to the characterization of $TH(G)$ in Eq. (15). As we have seen in Theorem 5 for any Bell scenario $B(n, m, k)$, $Q(n, m, k) \subseteq \tilde{Q}(n, m, k) = TH^{(c)}(G_B) \subset TH(G_B)$. Therefore, $\mathcal{P}^{nl} \notin Q(n, m, k)$. □