



Convex optimization methods for multipartite quantum experiments

By

GIUSEPPE VIOLA

Supervisor: DR HAB. INŻ. MARCIN PAWŁOWSKI

International Centre for Theory of Quantum Technologies (ICTQT),
UNIVERSITY OF GDAŃSK

Acknowledgement

This work would not have been possible without the personal and financial support of my supervisor, Marcin Pawłowski. In particular, I acknowledge and am grateful for support from CHIST-ERA Call 2022 no. 2023/05/Y/ST2/00005, under the title Modern Device Independent Cryptography (MoDIC) is funded by the National Science Center, Poland.

I would also like to thank Anubhav Chaturvedi and, Piotr Mironowicz for insightful discussions.

Dedication

To my loving parents,

Anna Papaccino & Giovanni Viola

Abstract

Non-locality is one of the properties most exploited by quantum communication protocols to achieve a variety of purposes, such as key generation (QKD) for spatially separated agents or the generation of true random numbers that cannot be predicted by anyone in the universe and which can be exploited for cryptographic purposes.

Since Bell's seminal work, many studies have demonstrated the possibility of using quantum correlation to achieve better performance in the field of communication tasks than can be achieved with classical strategies.

Often the investigation of quantum strategies that offer the highest chance of success in a given task is very arduous and complex, sometimes even impossible with today's knowledge, making numerical approaches useful, and sometimes necessary.

In this thesis I show new contributions in the fields of entanglement witnessing, random number generation and tasks involving multiple agents acting on graphs, achieved with the aid of convex optimisation techniques. This study is carried out through the presentation of three of my articles.

In the *first* article, the quantum experiment proposed involves two trusted agents and an eavesdropping agent. This experiment addresses the problem of distinguishing entangled quantum states from separable quantum states through the use of the entanglement witnessing technique in the presence of imperfect communication and in a context in which the devices used are not fully trusted. In this work convex optimization techniques have been used to establish to what extent an eavesdropping agent can simulate the behavior of entangled quantum states through the use of separable quantum states. To deal with non-detection events, we applied techniques already known and studied in the context of Bell scenarios to the entanglement witnessing technique, and compared the results obtained with different approaches.

In the *second* article, the quantum experiment proposed involves two trusted agents and an eavesdropping agent. In this work we introduced a new algorithm and experimental setup that can be exploited to demonstrate non-local phenomena at very large and, under certain assumptions, arbitrarily large distances, in the presence of imperfect communication. This proposal involves the introduction and implementation of the so-called routed Bell experiment, in which, in one of its formulations, a source sends quantum states to an agent located near the source and to a switch which randomly sends its subsystem to another agent near the source or to one far from the source. The agents placed close to the source perform measurements on the received quantum state trying to obtain correlations that maximally violate the CHSH inequality, while the agent placed further away performs measurements aiming to obtain outcomes which we have demonstrated to be random and non-reproducible through the use of local description in a non-conspiratorial context. In this project we used numerical convex optimization techniques to quantify the maximum predictive power of an adversary who has access to the source of the transmitted quantum states, thus quantifying the randomness obtainable as a function of the

inefficiency of the devices used by the agent placed at large distance from the source.

In the task proposed in the *third* article, we show how sharing quantum states can increase the success probabilities of multiple agents performing communication task. In particular we studied some tasks implemented by mobile agents positioned on the vertices of a graph, focusing on different variants of the graph rendezvous problem and on different variants of a communication task we introduced, taking the graph domination problem as an example. We investigated a possible quantum advantage, i.e. an increase in the probability of victory, or more generally, in the score that agents can obtain when they share quantum states. In this study, convex optimisation methods were used to investigate the optimal quantum strategies that the agents can employ comparing them with what they can do adopting only classical strategies. We considered only tasks for which the success probability or the score is described by a linear function with respect to the distribution of the outputs obtained by the various agents.

Abstrakt

Nielokalność jest jedną z najczęściej wykorzystywanych przez kwantowe protokoły komunikacyjne właściwości, służącą do osiągnięcia różnych celów, takich jak kwantowe generowanie kluczy (Quantum Key Distribution, QKD) dla przestrzennie oddzielonych agentów lub generowanie prawdziwie losowych liczb, których nikt we wszechświecie nie może przewidzieć i które można wykorzystać do celów kryptograficznych.

Od czasu przełomowej pracy Bella, wiele badań wykazało możliwość wykorzystania korelacji kwantowych do osiągnięcia lepszej wydajności w dziedzinie zadań komunikacyjnych niż można byłoby osiągnąć za pomocą klasycznych strategii.

Często badanie strategii kwantowych, które oferują największą szansę na sukces w danym zadaniu, jest bardzo żmudne i złożone, a czasem nawet niemożliwe przy dzisiejszej wiedzy, co sprawia, że podejścia numeryczne są przydatne, a czasem konieczne.

W niniejszej rozprawie pokazuję nowe osiągnięcia w dziedzinie certyfikacji splątania, generowania liczb losowych i zadań z udziałem wielu agentów działających na grafach, uzyskane za pomocą technik optymalizacji wypukłej. Badanie to zostało przeprowadzone w trzech zaprezentowanych artykułach mojego autorstwa.

Zaproponowany w *pierwszym* artykule eksperyment kwantowy obejmuje dwóch zaufanych agentów i agenta podsłuchującego. Eksperyment ten dotyczy problemu rozróżnienia splątanych stanów kwantowych od separowalnych stanów kwantowych poprzez zastosowanie techniki obserwowania splątania w obecności niedoskonałej komunikacji i w kontekście, w którym używane urządzenia nie są w pełni zaufane. W niniejszej pracy zastosowano techniki optymalizacji wypukłej w celu ustalenia, w jakim stopniu agent podsłuchujący może symulować zachowanie splątanych stanów kwantowych za pomocą separowalnych stanów kwantowych. Aby poradzić sobie ze zdarzeniami niewykrycia przez detektor, zastosowaliśmy techniki już znane i badane w kontekście scenariuszy Bella do techniki obserwowania splątania i porównaliśmy wyniki uzyskane przy użyciu różnych podejść.

W artykule *drugim* zaproponowany eksperyment kwantowy obejmuje dwóch zaufanych agentów i agenta podsłuchującego. W tej pracy wprowadziliśmy nowy algorytm i konfigurację eksperymentalną, które można wykorzystać do zademonstrowania zjawisk nielokalnych na bardzo dużych i, przy pewnych założeniach, dowolnie dużych odległościach, w obecności niedoskonałej komunikacji. Propozycja ta obejmuje wprowadzenie i implementację tak zwanego routowanego eksperymentu Bella, w którym, w jednej z jego formuł, źródło wysyła stany kwantowe do agenta znajdującego się w pobliżu źródła i do przełącznika, który losowo wysyła swój podsystem do innego agenta w pobliżu źródła lub do jednego z dala od źródła. Agenci umieszczeni blisko źródła wykonują pomiary na otrzymanym stanie kwantowym, próbując uzyskać korelacje, które maksymalnie łamią nierówność CHSH, podczas gdy agent umieszczony dalej wykonuje pomiary mające na celu uzyskanie wyników, które, jak wykazaliśmy, są losowe i niereprodukowalne przy zastosowaniu lokalnego opisu w kontekście niekonspiracyjnym. W tym projekcie wykorzystaliśmy

techniki numerycznej optymalizacji wypukłej do ilościowego określenia maksymalnej mocy predykcyjnej przeciwnika, który ma dostęp do źródła transmitowanych stanów kwantowych, określając w ten sposób losowość możliwą do uzyskania jako funkcję nieefektywności urządzeń używanych przez agenta umieszczonego w dużej odległości od źródła.

W zadaniu zaproponowanym w artykule *trzecim* pokazujemy, w jaki sposób współdzielenie stanów kwantowych może zwiększyć prawdopodobieństwo sukcesu wielu agentów wykonujących zadanie komunikacyjne. W szczególności zbadaliśmy niektóre zadania realizowane przez mobilnych agentów umieszczonych na wierzchołkach grafu, koncentrując się na różnych wariantach problemu rendezvous na grafie i różnych wariantach wprowadzonego przez nas zadania komunikacyjnego opartego na problemie dominowania w grafie. Zbadaliśmy możliwą przewagę kwantową, tj. wzrost prawdopodobieństwa sukcesu lub, bardziej ogólnie, wyniku, jaki agenci mogą uzyskać, gdy współdzielą splątane stany kwantowe. W tym badaniu wykorzystano metody optymalizacji wypukłej do zbadania optymalnych strategii kwantowych, które agenci mogą zastosować, porównując je z tym, co mogą zrobić, przyjmując tylko strategie klasyczne. Rozważaliśmy tylko zadania, dla których prawdopodobieństwo sukcesu lub wynik jest opisany funkcją liniową w odniesieniu do rozkładu wyników uzyskanych przez różnych agentów.

Publications included in the dissertation

- [A] G. Viola, N. Miklin, M. Gachechiladze, M. Pawłowski. *Entanglement witnessing with untrusted detectors*. J. Phys. A: Math. Theor. 2023; 56 425301.
- [B] A. Chaturvedi, G. Viola, M. Pawłowski. *Extending loophole-free nonlocal correlations to arbitrarily large distances*. npj Quantum Inf 2024;10, 7
- [C] G. Viola, P. Mironowicz. *Quantum strategies for rendezvous and domination tasks on graphs with mobile agents*. Phys. Rev. A 2024;109, 042201.

Table of Contents

	Page
1 Introduction	1
2 Summary of dissertation	5
2.1 Preliminaries	5
2.1.1 Notation and definitions	5
2.1.2 Bell inequalities	7
2.1.3 Semidefinite programming	7
2.1.4 The Navascués-Pironio-Acín Method	8
2.1.5 The See-Saw Method	9
2.2 Imperfect communication	9
2.3 Routed Bell experiment	10
2.4 Entanglement witnesses	15
2.5 Tasks on graphs	18
3 Outlook	21
Bibliography	29

Introduction

Since the 20th century, quantum mechanics has caused great progress in terms of technology, enabling the realization and conception of new protocols like device independent (DI) quantum key distribution [1–6] and randomness expansion [7–10].

In particular, one of the most used features for these purposes is the possibility of generating states from which non-classical correlations can emerge, allowing the generation of keys between agents spatially separated, keys which can be exploited to implement various cryptographic protocols in a secure manner, i.e. in such a way that no one can predict the elements that compose them.

Bell’s seminal study [11] also began the study of inequalities that allow us to identify quantum correlations that cannot be reproduced by classical systems, from which several studies followed showing examples of communication tasks for which quantum correlations give to the agents involved greater success probability, with respect to the use of strategies for which a classical description is possible. Among these, one of the most studied examples is the the *Clauser-Horne-Shimony-Holt* (CHSH) Bell inequality [12].

At the same time, thanks to the technological development of recent years and the consequent increase in computing power, the use of computers allows the study and resolution of problems that would require too much time to be solved analytically or, more generally, too many resources, making numerical techniques necessary.

In particular, with the aim of addressing problems related to the investigation of quantum strategies in fields such as entanglement detection and communication tasks, an area of numerical mathematics that proves to be particularly useful is semidefinite programming (SDP) [13–15], exploited in particular in its two applications, the NPA hierarchies [16, 17] and the see-saw method [18].

It is possible to apply these numerical techniques because, as will be explained in more

detail in later sections, in many cases it is possible to formulate problems concerning the investigation of quantum strategies as problems of minimization of linear functions subject to linear constraints, in addition to the requirement that certain operators are positive semidefinite. This last type of constraint is also what distinguishes problems concerning linear programming from problems connected with semidefinite programming. In particular, the reason which makes the use of these techniques feasible, when exploiting a computer, lies in the fact that there are algorithms through which it is possible to solve problems formulated according to semidefinite programming in an efficient manner, and, if used appropriately, can provide precise numerical results up to machine precision.

In the *first* article, taking example from the Bell inequalities approach, when dealing with non-detection events [19], we studied an alternative method to tackle the problem of entanglement detection in a context in which the detectors used can be potentially malicious, when the agents want to perform an entanglement witnessing experiment. In particular, managing no-click events by adopting strategies already studied in the context of Bell experiments, and adapting them to the entanglement witnessing method, with a focus on the discard strategy and the assignment strategy, as will be explained in more detail in later sections.

In this study, in addition to an analytical investigation performed in simpler cases, the use and the adaptation of numerical techniques has proven to be necessary to investigate more complex cases. In particular to study the correlations that untrusted devices can generate when separable quantum states are adopted, trying to reproduce correlations that, in a context of reliable detectors, only non-separable quantum states could achieve.

In the *second* article we introduced and studied the so-called routed Bell experiment, in which a source sends quantum states to an agent located near the source, and to a switch which randomly sends its subsystem to another agent located near the source or to an agent located far from the source, and we looked for the optimal set up for the agents to certify that the outcome of the measurements performed by the agent placed far from the source can't be predicted by a classical model and that they are indeed random.

In this study, numerical techniques have been introduced to study the loophole free violation trade-off in cases where the devices are positioned close to the source and the threshold requirements on the correlations generated by the devices positioned far from the source.

In the *third* article we have exploited convex optimisation techniques to show that it is possible to obtain an advantage in terms of probability of success, or equivalently in terms of a score, when the agents involved in a communication task are distributed over a graph. In particular we studied the following two tasks: the graph rendezvous [20] task and the graph domination task.

In graph rendezvous, as described in more detail in Sec. 2.5, n agents are distributed over a graph and aim to meet at the same node after travelling h edges, in particular they are aware of the structure of the graph in which they will be distributed, they cannot communicate with

other participants once their initial position has been fixed and they can agree on a strategy before being distributed over the graph.

The graph domination task is a task that we introduced by taking example from the domination problem, a problem already studied in the literature [21, 22] in which, in one of its formulations, the objective is to maximize the number of dominated vertices of a graph by deciding where to place a fixed number of dominating vertices. A point in a graph is said to be dominated if it is a dominating vertex or if it is separated by a single edge from a dominating vertex.

In the graph domination task n agents are randomly distributed on the vertices of a graph and these have the objective of maximizing the number of dominated vertices after having traversed each h edges and denoting the final vertices reached as dominating vertices. Also in this case the agents, once positioned on the graph, cannot communicate with each other and can agree on a strategy before being positioned on the graph.

Summary of dissertation

2.1 Preliminaries

This section presents introductory elements and intermediate results that we derived and that are useful to understand the final results that we obtained.

2.1.1 Notation and definitions

Let us consider, for simplicity, two agents Alice and Bob, spatially separated, who receive uniformly distributed inputs, x and y respectively, and each of which generates an output a and b respectively [23]. The set

$$(2.1) \quad \mathbf{P}(A, B|X, Y) = \{p(a, b|x, y)\}_{a \in A, b \in B, x \in X, y \in Y}$$

is called *joint probability distribution function*, where X , Y , A and B are finite non empty sets. While the set

$$(2.2) \quad \mathbf{P}(A|X, Y) = \{p(a|x, y)\}_{a \in A, b \in B, x \in X, y \in Y}$$

is called *marginal probability distribution* of Alice, where

$$(2.3) \quad p(a|x, y) = \sum_b p(a, b|x, y)$$

and similarly for Bob.

A joint probability distribution $\mathbf{P}(A, B | X, Y)$ for which there exist conditional probability distributions

$$(2.4) \quad \mathbf{P}(\Lambda), \mathbf{P}_A(A | X, \Lambda), \mathbf{P}_B(B | Y, \Lambda),$$

where $\mathbf{P}(\Lambda)$ is a probability distribution associated to the possible states of the measured system labeled with λ , satisfying

$$(2.5) \quad p(a, b | x, y) = \sum_{\lambda} p(\lambda) \cdot p(a | x, \lambda) \cdot p(b | y, \lambda)$$

is called a *local* or *classical probability distribution*.

A joint probability distribution $\mathbf{P}(A, B | X, Y)$ is called *no signalling* if, $\forall a \in A, x \in X, y, y' \in Y$,

$$(2.6) \quad p(a | x, y) = p(a | x, y')$$

A joint probability distribution $\mathbf{P}(A, B | X, Y)$ is said to be *quantum* if and only if there exists a Hilbert space \mathbb{H} , on which it is possible to define a state $|\psi\rangle$, and a set of projective measurement operators

$$(2.7) \quad \{E_x^a, F_y^b\}_{a \in A, b \in B, x \in X, y \in Y},$$

for which the following conditions are fulfilled:

1. $E_x^a = E_x^{a\dagger}$ and $F_y^b = F_y^{b\dagger}$ (operators are Hermitian),
2. $E_x^a E_x^{a'} = 0$ and $F_y^b F_y^{b'} = 0$ for $a \neq a'$ and $b \neq b'$ (orthogonality of different results associated with the same setting),
3. $\sum_{a \in A} E_x^a = \mathbb{1}$ and $\sum_{b \in B} F_y^b = \mathbb{1}$ (sum of probabilities of all outcomes for each setting is equal to 1),
4. $[E_x^a, F_y^b] = 0$ (measurements of Alice and Bob commute, i.e. their results do not depend on the time order in which they were performed, which is justified by the no-signaling principle),
- 5.

$$(2.8) \quad p(a, b | x, y) = \langle \psi | E_x^a F_y^b | \psi \rangle = \text{Tr}(|\psi\rangle\langle\psi| E_x^a F_y^b)$$

(the probability distribution is given by measurements on the quantum state).

2.1.2 Bell inequalities

One of the most interesting features of quantum mechanics is the prediction of correlation functions which can not be explained and predicted by any classical theory based on an hidden variable model. This disagreement between the predictions of the quantum theory and classical theory was first studied through the so-called Einstein-Podolsky-Rosen paradox, which was formulated in terms of measurable quantities by Bell [11] and by Clauser, Horne, Shimony, and Holt [12], through the so-called CHSH inequality. Many other Bell inequalities have been introduced and studied to date, because of their importance not only in quantum foundations, but also in distinguishing correlations that can be predicted by classical descriptions from correlations that cannot be predicted by classical models in a manner independent of the specific device used, i.e. in the so-called device independent way.

It is possible to write any Bell inequality in terms of a function of the joint probability distribution associated to the given scenario. Although non-linear Bell inequalities have been studied in the literature [24], in this work I focused on the investigation of linear Bell inequalities.

In the two agents scenario, in which the first agent, Alice, receives as input $x \in X$ and generates as output $a \in A$, and the second agent, Bob, receives as input $y \in Y$ and generates as output $b \in B$, the linear function can be written as

$$(2.9) \quad I = \sum_{a \in A} \sum_{b \in B} \sum_{x \in X} \sum_{y \in Y} \alpha_{a,b,x,y} p(a,b | x,y),$$

where $\alpha_{a,b,x,y} \in \mathbb{R}$ [23].

As will be discussed later in this chapter, linearity is a key property which can be exploited, when studying tasks which involves Bell inequalities, letting us to apply numerical techniques in an efficient way.

2.1.3 Semidefinite programming

Semidefinite programming (SDP) is a mathematical optimization technique that extends the concepts of linear programming to handle matrices and, in particular, positive semidefinite matrices. It addresses problems where the objective is to optimize a linear objective function subject to linear equality and semidefinite inequality constraints. SDP finds applications in multiple fields [25], including quantum information [13–15]. Advancements in algorithmic design and improvements in computational power have significantly enhanced the efficiency of SDP solvers. Modern interior-point methods [26], in particular, have proven to be effective in solving large-scale semidefinite programs, making SDP a versatile tool for addressing complex optimization problems [27]. For $m, n \in \mathbb{N}$ the so-called *primal* optimization task of SDP is [23]:

$$(2.10) \quad \begin{aligned} & \text{minimize } c^T \cdot x \\ & \text{subject to } F(x) \succeq 0, \end{aligned}$$

where $c \in \mathbb{R}^m$, $F(x) := F_0 + \sum_{i=1}^m x_i F_i$, $F_i \in \mathbb{R}^{n \times n}$, and $x \in \mathbb{R}^m$ is the variable. The so-called dual of this problem with a symmetric matrix variable $Z \in \mathbb{R}^{n \times n}$ is

$$(2.11) \quad \begin{aligned} & \text{maximize} \quad -\text{Tr}[F_0 Z] \\ & \text{subject to} \quad \text{Tr}[F_i Z] = c_i, \text{ for } i=1, \dots, m, \\ & \quad \quad \quad Z \succeq 0. \end{aligned}$$

2.1.4 The Navascués-Pironio-Acín Method

The Navascués-Pironio-Acín (NPA) method [16, 17] is a powerful mathematical framework for studying quantum correlations and entanglement in quantum information theory. It offers a systematic method to analyse quantum systems' behaviour and correlations.

Let us consider the two agents joint probability distribution $\mathbf{P}(A, B | X, Y) = \{p(a, b | x, y)\}_{a \in A, b \in B, x \in X, y \in Y}$ associated to the quantum state ρ and the projective measurements

$$(2.12) \quad \{E_x^a, F_y^b\}_{a \in A, b \in B, x \in X, y \in Y},$$

with $p(a, b | x, y) = \text{Tr}(\rho E_x^a F_y^b)$, and the following lemma [28]:

Lemma 1. *Let $\{F_1, \dots, F_n\}$ be a collection of operators. The orthogonal matrix M whose entries are*

$$(2.13) \quad [M]_{i,j} = \text{Tr}(\rho F_i^\dagger F_j)$$

is non-negative.

In the NPA method the matrix M is built by selecting the operators F_i as combinations of the operators in the following set: $S = \{\mathbb{1}\} \cup \{E_x^a\}_{a \in A, x \in X} \cup \{F_y^b\}_{b \in B, y \in Y}$ and are investigated all the distributions $\mathbf{P}(A, B | X, Y)$ for which the associated matrix M exists and is positive semidefinite. Level 1 of the NPA method is obtained when the combinations considered are each composed of a single element of S and the set of all distributions $\mathbf{P}(A, B | X, Y)$ for which the associated matrix M exists and is positive semidefinite is denoted by \mathbf{Q}_1 . Similarly, the level n , with $n \in \mathbb{N}_+$, of the NPA method is obtained by considering all the combinations which contain n elements of S and the set of all distributions $\mathbf{P}(A, B | X, Y)$ for which the associated matrix M exists and is positive semidefinite is denoted by \mathbf{Q}_n .

Since at each level $n > 1$ are considered additional constraints with respect to the level $n - 1$, we have that $\mathbf{Q}_1 \supset \mathbf{Q}_2 \supset \mathbf{Q}_3 \supset \dots \mathbf{Q}_n$ and it has been shown that the set of investigated distributions converges to the quantum set \mathbf{Q} , i.e. $\lim_{n \rightarrow \infty} \mathbf{Q}_n = \mathbf{Q}$. Thus, when looking for the maximum violation of a Bell inequality obtainable by investigating quantum probability distributions, the NPA method allows to find upper bounds.

2.1.5 The See-Saw Method

The so-called see-saw [18] method is an alternative approach to optimize over quantum distributions, when we have certain restrictions on the dimensions of operators associated with the setup. Note that the quantum probabilities are given by expressions of the form (2.8). It is easy to see that expressions that are linear combinations of probabilities given by formulas of the form (2.8), such as Bell-type operators, are linear in each term, such as the quantum state, Alice's measurement operators, and Bob's measurement operators. However, since the optimization must be done over all these groups of variables, the whole expression is non-linear.

The key idea of the see-saw method is the alternating use of a series of optimizations for which two of the expressions of the form (2.8) are treated as constants, and the third of them is a variable subjected to optimization by SDP methods with the objective function being the Bell operator. For this purpose, in the first iteration, two of the terms take fixed, often randomly chosen, values.

Note that while the NPA method provides an approximation of the quantum set of probabilities from its exterior, meaning that, when maximizing a function of joint probability distributions, it provides an upper bound, the see-saw method finds direct representations of the quantum state and measurements implementing the found distribution. Thus, any solution obtained by the see-saw method is a lower bound for the exact solution of the quantum optimisation problem.

2.2 Imperfect communication

When applying quantum communication algorithms to real world scenarios, the most commonly used system for encoding quantum states are photons. When photons are transmitted, absorption occurs due to the interaction of the signal with the transmission medium, which causes the so-called no-click event for the detector that should have received the signal. This absorption increases exponentially with the length of the tract over which the photons must travel [29].

In addition to the absorption of photons in the transmission medium, photons may not be detected by the receiving detector due to the use of imperfect detectors. For these reasons, when applying quantum communication algorithms, it is important to adopt strategies to handle no-click events when the transmission medium or detector used is untrusted, i.e. to prevent such events from being exploited by an eavesdropper to obtain information from such photon transmission.

Three strategies have been devised for handling such events in a Bell experiment [19]: the discard strategy, the assignment strategy and the keep everything strategy.

When the parties involved in the Bell experiment employ the discard strategy, they discard every round of the experiment for which at least one of the agent detectors does not click.

In this case, the limit reachable by classical strategies increases, while the limit reachable by purely quantum strategies remains unchanged.

When the agents adopt the assignment strategy, they assign to the no-click event one of the possible outputs for the scenario being studied, e.g. in the case of studying CHSH inequality, the agents will associate the no-click event an element taken from the set $\{0, 1\}$ in a random or predetermined way. In this case, the limit attainable by classical strategies remains unchanged, while the limit attainable by purely quantum strategies decreases.

Finally, when agents opt for the keep everything strategy, they consider the no-click event as an additional outcome of the experiment, allowing them to fully exploit the information gained from the experiment, at the price, however, of having to study a new Bell inequality involving additional outcomes with respect to the inequality initially studied.

In particular, in the first article, we applied the discard strategy and the assignment strategy to the studied entanglement witnessing scenario, and compared their performance. In that scenario, two agents receive a state distributed by a source and then, after performing measurement in the Pauli basis, they evaluate the average value of a particular entanglement witness, as described more in detail in section 2.4.

2.3 Routed Bell experiment

In the routed Bell experiment, in each round, a source sends quantum states to an agent B , located near the source, and based on the value of a random variable $i \in \{0, 1\}$, generated during each round, to an agent A_i , calling A_0 an agent located near the source and A_1 an agent located far from the source.

Practical realization of this experiment can be performed through the use of a switch, which receives the subsystem from the source and resends it to the agent A_i based on the value of the variable i . Equivalently the experiment can be realized in a similar way substituting the two agents A_0 and A_1 and the switch, with a single agent A which, in each round, can be placed randomly near the source, calling them in these rounds A_0 , or far from the source, calling them A_1 .

In Fig. 2.1 is depicted a scheme describing the routed Bell experiment as described in the previous paragraph. While in Fig. 2.2 is depicted a scheme describing a generalization of the routed Bell experiment in which, in addition to the Alice's devices, also Bob's devices, in each round, can be randomly positioned near or far from the source.

Let us consider the simplest bipartite Bell scenario entailing a source, \mathcal{S} , distributing *entangled* quantum systems, ideally in a two-qubit pure state, $|\psi\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$, to two spatially separated parties, Alice and Bob. The parties have measurement devices with binary inputs, $x, y \in \{0, 1\}$, specifying the measurement settings, and produce binary outcomes, $a, b \in \{+1, -1\}$, respectively. In ideal circumstances, the measurement devices perform measurements corresponding to binary

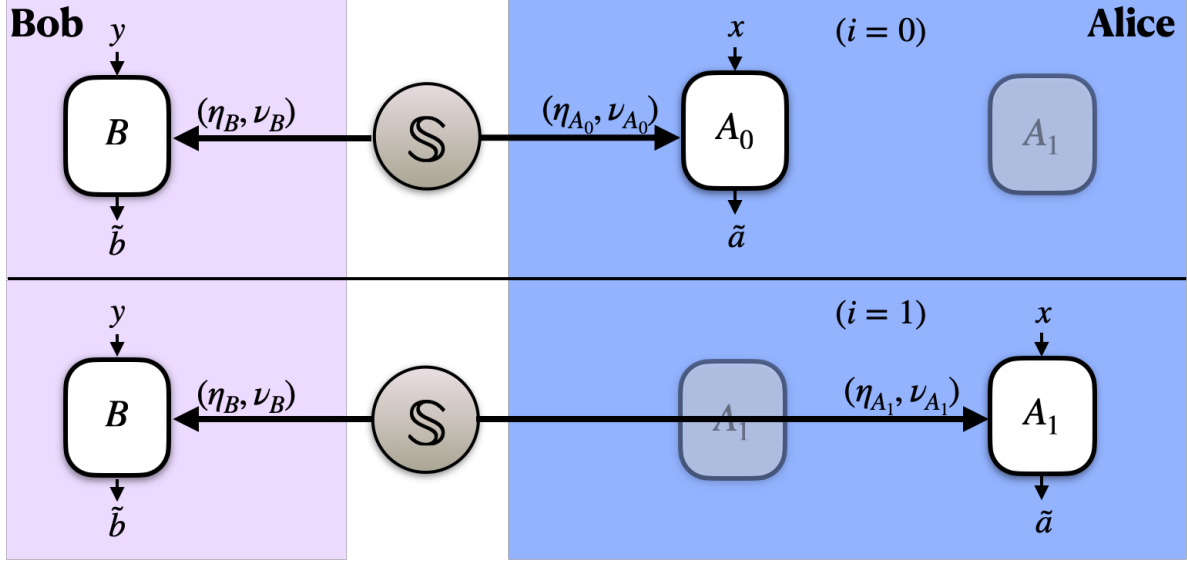


Figure 2.1: The graphic is a schematic depiction of the routed Bell CHSH experiment. In each round of the experiment, the parties choose their respective measurement settings, $x, y \in \{0, 1\}$ and obtain outcomes, $\tilde{a}, \tilde{b} \in \{+1, -1, \perp\}$, where the outcome, \perp , signifies the “no-click” event. While Bob’s measurement device, B , is at a fixed distance from the source throughout the experiment with an unvarying effective detection efficiency and visibility, (η_B, ν_B) , the location of Alice’s measurement device, A_i , depends on a randomly chosen input bit, $i \in \{0, 1\}$. When $i=0$, Alice places her measurement device, A_0 , close to the source with an effective detection efficiency and visibility, (η_{A_0}, ν_{A_0}) , whereas when $i=1$, she places her measurement device, A_1 , further away from the source, with a lower detection efficiency and visibility, (η_{A_1}, ν_{A_1}) , such that, $\eta_{A_1} < \eta_{A_0}$, $\nu_{A_1} < \nu_{A_0}$.

outcome projective observables, $\hat{a}_x \in B(\mathbb{C}^2)$, $\hat{b}_y \in B(\mathbb{C}^2)$. The three tuple, $Q \equiv (|\psi\rangle, \{\hat{a}_x\}_x, \{\hat{b}_y\}_y)$, constitutes a quantum strategy (entailing operational instructions) which ideally results in the experimental behavior, $\mathbf{p} \equiv \{p(a, b|x, y) = \frac{1}{4} \langle \psi | (\mathbb{1} + a\hat{a}_x) \otimes (\mathbb{1} + b\hat{b}_y) | \psi \rangle\} \in \mathbb{R}_+^{16}$. In general, up to local-relabelling, a given behavior, \mathbf{p} , is said to be *nonlocal* if and only if it violates the CHSH inequality,

$$(2.14) \quad C(\mathbf{p}) \equiv \sum_{x,y} (-1)^{x \cdot y} \langle \hat{a}_x \hat{b}_y \rangle_{\mathcal{L}} \leq 2,$$

where $\langle \hat{a}_x \hat{b}_y \rangle = \sum_{a,b} abp(a, b|x, y)$. The inequality (2.14) holds for all behaviors, $\mathbf{p} \in \mathbb{R}^{16}$, which admit *local hidden variable* explanations (\mathcal{L}), such that, $p(a, b|x, y) = \sum_{\lambda \in \Lambda} p(\lambda) p_\lambda^A(a|x) p_\lambda^B(b|y)$, where λ is the local hidden variable, Λ is a measurable hidden variable state space, $p(\lambda)$ specifies the probability of the system occupying the state corresponding to λ , and for a specific λ , the conditional probability distributions, $\{p_\lambda^A(a|x)\}$ and $\{p_\lambda^B(b|y)\}$, represent stochastic response schemes specifying the outcome probabilities for Alice and Bob, respectively.

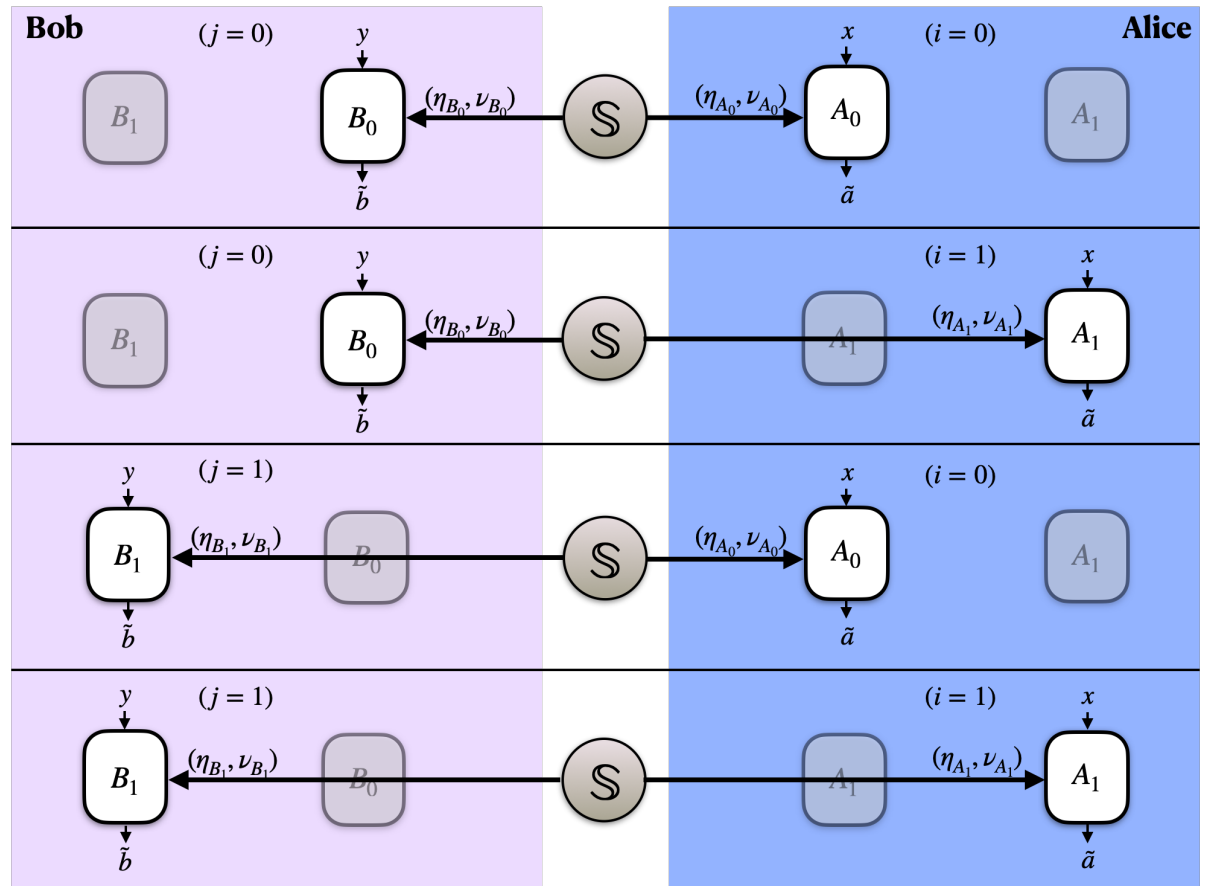


Figure 2.2: The graphic is a schematic depiction of a generalization of the routed Bell experiment depicted in Fig. 2.1. Along with Alice, in each round of the experiment, Bob chooses the location of his measurement device, B_j , based on a randomly chosen input bit, $j \in \{0, 1\}$. When $j=0$, Bob places his measurement device, B_0 , close to the source with an effective detection efficiency and visibility, (η_{B_0}, ν_{B_0}) . When $j=1$, he places his measurement device, B_1 , further away from the source, with a lower detection efficiency and visibility, (η_{B_1}, ν_{B_1}) , such that $\eta_{B_1} < \eta_{B_0}$, $\nu_{B_1} < \nu_{B_0}$. Our results imply that in rounds with $i=j=1$, loophole-free nonlocal correlations can be certified between the measurement devices, (A_1, B_1) , placed arbitrarily far away from each other.

To account for imperfections in the source and noise added during transmission from the source, we associated effective visibilities, $\nu_B, \nu_{A_i} \in [0, 1]$ to each measurement device, such that the quantum state shared between the measurement devices, (A_i, B) , is,

$$(2.15) \quad \begin{aligned} \rho(\nu_i) = & \nu_{A_i} \nu_B |\psi\rangle\langle\psi| + \nu_{A_i} (1 - \nu_B) (\rho_B \otimes \frac{\mathbb{1}}{2}) \\ & + (1 - \nu_{A_i}) \nu_B (\frac{\mathbb{1}}{2} \otimes \rho_A) + (1 - \nu_{A_i}) (1 - \nu_B) \frac{\mathbb{1}_4}{4}, \end{aligned}$$

where $\rho_A = \text{Tr}_B(|\psi\rangle\langle\psi|)$, $\rho_B = \text{Tr}_A(|\psi\rangle\langle\psi|)$, $\mathbb{1}$ is the two-dimensional identity operator, and $\mathbb{1}_4 = \mathbb{1} \otimes \mathbb{1}$. Analogously to the detection efficiencies, the effective visibility of Alice's measurement device decreases with the distance from the source, such that $\nu_{A_1} \leq \nu_{A_0}$.

Treating the no-click event as an additional outcome, \perp , the parties observe the experimental behavior in the form of conditional probability distributions, $\mathbf{p}_{(exp)} \equiv \{p(\tilde{a}, \tilde{b}|(x, i), y)\} \in \mathbb{R}^{72}$, where $\tilde{a}, \tilde{b} \in \{1, -1, \perp\}$. A convenient way to post-process the experimental behavior, $\mathbf{p}_{(exp)}$, which avoids considering additional outcomes and as well as the fair-sampling assumption, is the use of the assignment strategy, i.e. to assign a valid outcome, say 1, to each no-click event, such that, the effective distribution reduces to $\mathbf{p}_{(exp)}^{(\perp \mapsto 1)} \equiv \{p(a, b|(x, i), y)\} \in \mathbb{R}_+^{32}$ [19, 30]. One of the benefits of such a post-processing is the applicability of well-studied reliable means of quantifying loophole-free nonlocal correlations such as the observed value of the CHSH expression,

$$(2.16) \quad C_{A_i, B}(\mathbf{p}_{(exp)}^{(\perp \mapsto 1)}) \equiv \sum_{x, y} (-1)^{x \cdot y} \langle \hat{a}_{(x, i)} \hat{b}_y \rangle$$

where $\langle \hat{a}_{(x, i)} \hat{b}_y \rangle = \sum_{a, b} a b p(a, b|(x, i), y)$.

The measurement devices (A_i, B) are said to share loophole-free nonlocal correlations if the behaviour $\mathbf{p}_{(exp)}^{(\perp \mapsto 1)}$ does not allow for a local hidden variable explanation of the form,

$$(2.17) \quad p(a, b|(x, i), y) \stackrel{\mathcal{L}(A_i)}{=} \sum_{\lambda \in \Lambda} p(\lambda) p_\lambda^A(a|x, i) p_\lambda^B(b|y),$$

for all $a, b \in \{+1, -1\}$ and $x, y \in \{0, 1\}$, where λ is a local hidden variable, Λ is a measurable hidden variable state space, $p(\lambda)$ specifies the probability of the shared system occupying the state corresponding to λ , and for a specific λ , the conditional probability distributions, $\{p_\lambda^A(a|x, i)\}$ and $\{p_\lambda^B(b|y)\}$, represent stochastic response schemes specifying the outcome probabilities for Alice and Bob, respectively.

We showed the following theorem:

Theorem 1 (Nonlocality at arbitrary distance). *If the measurement devices close to the source, (A_0, B) , are perfect, i.e., $\eta_B = \eta_{A_0} = \nu_B = \nu_{A_0} = 1$, and witness maximally nonlocal correlations, such that, $C_{A_0 B}(\mathbf{p}_{(exp)}^{(\perp \mapsto 1)}) = 2\sqrt{2}$, then such nonlocal correlations may be operationally extended to Alice's other measurement device placed arbitrarily far away from the source, i.e., loophole-free*

nonlocal correlations between (A_1, B) can be operationally certified for any non-zero values of (η_{A_1}, ν_{A_1}) .

Theorem 2 (A specific analytical trade-off). *If the measurement devices close to the source, (A_0, B) , witness loophole-free nonlocal correlations such that, $C_{A_0B}(\mathbf{p}_{(exp)}^{(\perp \mapsto 1)}) > 2$, then loophole-free nonlocal correlations between (A_1, B) can be certified whenever the following inequality is violated,*

$$(2.18) \quad C_{A_1B}(\mathbf{p}_{(exp)}^{(\perp \mapsto 1)}) \underset{\mathcal{L}(A_1)}{\leq} \sqrt{8 - (C_{A_0B}(\mathbf{p}_{(exp)}^{(\perp \mapsto 1)}))^2}.$$

Given a quantum strategy, Q , and the tuple of experimental parameters, $(\eta_B, \eta_{A_0}, \nu_B, \nu_{A_0})$, we retrieved the experimental behavior, $\mathbf{p}_{(exp)}^{(\perp \mapsto 1)}$, as a function of (η_{A_1}, ν_{A_1}) . Now, the critical parameters, $(\eta_{A_1}^*, \nu_{A_1}^*)$, are simply the ones for which the inequality (2.18) is saturated.

In the second article, we compared the use of the maximally nonlocal isotropic strategy Q_{iso} with the use of tilted strategies $Q_{\eta_{A_0}, \eta_B}$, where $Q_{iso} \equiv (|\phi^+\rangle, \{\sigma_z, \sigma_x\}, \{\frac{1}{\sqrt{2}}(\sigma_z \pm \sigma_x)\})$, where $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and $Q_{\eta_{A_0}, \eta_B}$ is the strategy which attains maximum quantum violation of the following tilted CHSH inequality,

$$(2.19) \quad \begin{aligned} C_{A_0B}^{\eta_{A_0}, \eta_B}(\mathbf{p}) &\equiv \eta_{A_0} \eta_B C_{A_0B}(\mathbf{p}) + 2(1 - \eta_B) \eta_{A_0} \langle \hat{a}_{(0,0)} \rangle \\ &\quad + 2(1 - \eta_{A_0}) \eta_B \langle \hat{b}_0 \rangle + 2(1 - \eta_{A_0})(1 - \eta_B) \\ &\underset{\mathcal{L}}{\leq} 2. \end{aligned}$$

To measure the non-local behaviour of the measurement device A_1 , when we considered the no-click event as an additional outcome, $\mathbf{p}_{(exp)}$, we used the amount of *certifiable randomness*, $H_{min}(G_x(\mathbf{p}_{(exp)}))$, where $H_{min}(\cdot)$ is the min-entropy, and $G_x(\mathbf{p}_{(exp)})$ is maximum guessing probability [31],

$$(2.20) \quad \begin{aligned} G_x(\mathbf{p}_{(exp)}) &= \max_{\mathbf{p}_a} \sum_{\tilde{a} \in \{\pm 1, \perp\}} p_a(\tilde{a}|x, 1) \\ \text{s.t.} \quad &\sum_{\tilde{a} \in \{\pm 1, \perp\}} \mathbf{p}_a = \mathbf{p}_{(exp)} \\ &\forall \tilde{a} \in \{\pm 1, \perp\} : \mathbf{p}_a \in \mathbf{Q}, \end{aligned}$$

where $p_a(\tilde{a}|x, 1) = \sum_{\tilde{b} \in \{\pm 1, \perp\}} p_a(\tilde{a}, \tilde{b}|(x, 1), y)$, $\{\mathbf{p}_a \in \mathbb{R}_+^{72}\}$ are convex decompositions of the raw experimental behavior $\mathbf{p}_{(exp)} \in \mathbb{R}_+^{72}$, wherein we have absorbed the convex coefficients into the respective decompositions, and \mathbf{Q} is the convex set of quantum behaviors, $\mathbf{p} \equiv \{p(\tilde{a}, \tilde{b}|(x, i), y)\} \in \mathbb{R}_+^{72}$.

The optimization problem (2.20) is extremely arduous to solve because of the constraint $\mathbf{p}_a \in \mathbf{Q}$. Instead, to retrieve progressively tightening upper-bounds on the maximum guessing

probability, $G_x(\mathbf{p}_{(exp)})$, and the estimation of the critical parameters $(\eta_{A_1}^*, \nu_{A_1}^*)$, we employ the *Nieto-Silleras* hierarchy of semi-definite programs [31, 32], which relaxes the constraint $\mathbf{p}_a \in \mathbf{Q}$, to $\mathbf{p}_a \in \mathbf{Q}_L$, where \mathbf{Q}_L are the convex relaxations of the quantum set, \mathbf{Q} , corresponding to NPA hierarchy, $L \in \mathbb{N}_+$ denotes the level of the relaxation, such that, $\mathbf{Q} \subset \mathbf{Q}_{L+1} \subset \mathbf{Q}_L$ for all $L \in \mathbb{N}_+$, and $\lim_{L \rightarrow \infty} \mathbf{Q}_L = \mathbf{Q}$.

2.4 Entanglement witnesses

An entanglement witness is a linear Hermitian operator W , such that $\langle W \rangle_{\rho_s} := \text{Tr}[W \rho_s] \geq 0$ for all separable states ρ_s and $\langle W \rangle_{\rho} < 0$ for the entangled state ρ under investigation. In the first article we studied an experiment in which two spatially separated agents perform measurements on states distributed by a source, and then, calculating the average value of the Bell witness, they want to establish if the states distributed by the source are entangled. This is done under the assumption that the detectors are untrusted i.e. that the detector can click or not click based on an hidden variable model constructed by the provider of the states, who tries to reproduce the behaviour of entangled states while distributing only separable states.

In the first article, we focused on two-qubit states for which the typical observables are the Pauli operators, i.e., we consider witnesses W of the form

$$(2.21) \quad W = w_{0,0} \mathbb{1} \otimes \mathbb{1} + \sum_{i=1}^3 w_{i,0} \sigma_i \otimes \mathbb{1} + \sum_{j=1}^3 w_{0,j} \mathbb{1} \otimes \sigma_j + \sum_{i,j=1}^3 w_{i,j} \sigma_i \otimes \sigma_j,$$

with $w_{i,j} \in \mathbb{R}$ being coefficients of the decomposition, and $\{\sigma_1, \sigma_2, \sigma_3\} = \{\sigma_x, \sigma_y, \sigma_z\}$ being the set of Pauli operators.

We demonstrated our findings on the example of pure entangled two-qubit states, for which we use a notation

$$(2.22) \quad |\Psi_{\theta}\rangle := \sin(\theta)|0,0\rangle + \cos(\theta)|1,1\rangle$$

with $\theta \in (0, \frac{\pi}{4}]$. The corresponding witness for $|\Psi_{\theta}\rangle$ reads

$$(2.23) \quad W_{\theta} := \cos(\theta)^2 \mathbb{1} \otimes \mathbb{1} - |\Psi_{\theta}\rangle \langle \Psi_{\theta}|.$$

The non-zero coefficients of the decomposition of W_{θ} into Pauli observables are $w_{0,0} = \frac{1}{2} \cos(2\theta) + \frac{1}{4}$, $w_{0,3} = w_{3,0} = \frac{1}{4} \cos(2\theta)$, $w_{1,1} = -w_{2,2} = -\frac{1}{4} \sin(2\theta)$, and $w_{3,3} = -\frac{1}{4}$. We refer to $|\Psi_{\frac{\pi}{4}}\rangle$ and $W_{\frac{\pi}{4}}$ as the Bell state and the Bell witness, respectively.

In Fig. 2.6 there is a schematic representation of the experiment we studied, underlining the parts of the experimental apparatus which we assumed to be trusted.

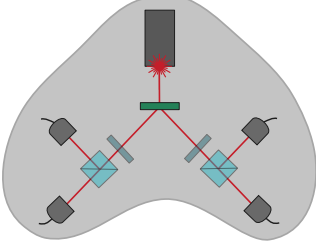


Figure 2.3: Bell test

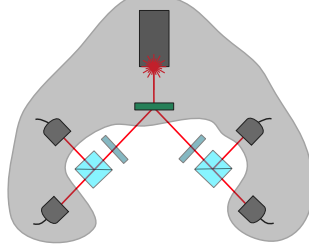


Figure 2.4: Our scenario

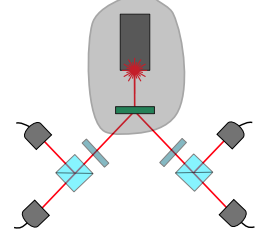


Figure 2.5: Entanglement witnessing

Figure 2.6: A schematic representation of a two-photon experiment with polarization qubits. Parts of the experimental apparatus covered in grey are assumed to be untrusted. 2.3: the Bell test. 2.4: scenario considered in this work; the detection part of the measurement devices and the entanglement source are assumed to be untrusted. 2.5: the entanglement witnessing scenario.

When the agents use the discard strategy to deal the non detection events we derived that the SDP problem that must solved to find which values of the average of the Bell witness can be achieved when separable states are employed is

$$\begin{aligned}
 \min_{\rho_\lambda} \quad & w_{0,0} + \frac{1}{\eta} \sum_{i=1}^3 w_{i,0} \sum_{\lambda \in \Lambda_i^A} \langle \sigma_i \otimes \mathbb{1} \rangle_{\rho_\lambda} + \frac{1}{\eta} \sum_{j=1}^3 w_{0,j} \sum_{\lambda \in \Lambda_j^B} \langle \mathbb{1} \otimes \sigma_j \rangle_{\rho_\lambda} \\
 & + \frac{1}{\eta^2} \sum_{i,j=1}^3 w_{i,j} \sum_{\lambda \in \Lambda_i^A \cap \Lambda_j^B} \langle \sigma_i \otimes \sigma_j \rangle_{\rho_\lambda}, \\
 \text{s.t.} \quad & \sum_{\lambda \in \Lambda_i^A} \text{Tr}[\rho_\lambda] = \sum_{\lambda \in \Lambda_j^B} \text{Tr}[\rho_\lambda] = \eta, \quad \sum_{\lambda \in \Lambda_i^A \cap \Lambda_j^B} \text{Tr}[\rho_\lambda] = \eta^2, \quad \forall i, j \in \{1, 2, 3\},
 \end{aligned}
 \tag{2.24a}$$

$$\rho_\lambda \geq 0, \quad \rho_\lambda^{\text{T}^A} \geq 0, \quad \forall \lambda \in \Lambda,
 \tag{2.24b}$$

$$\rho_{\text{observed}} \geq 0, \quad \sum_{\lambda \in \Lambda} \text{Tr}[\rho_\lambda] = 1.
 \tag{2.24c}$$

In the above SDP, we have introduced an operator ρ_{observed} , which corresponds to the physically observed state, and is defined as

$$\begin{aligned}
 \rho_{\text{observed}} := & \frac{\mathbb{1} \otimes \mathbb{1}}{4} + \frac{1}{\eta} \sum_{i=1}^3 \left(\sum_{\lambda \in \Lambda_i^A} \langle \sigma_i \otimes \mathbb{1} \rangle_{\rho_\lambda} \right) \frac{\sigma_i \otimes \mathbb{1}}{4} + \frac{1}{\eta} \sum_{j=1}^3 \left(\sum_{\lambda \in \Lambda_j^B} \langle \mathbb{1} \otimes \sigma_j \rangle_{\rho_\lambda} \right) \frac{\mathbb{1} \otimes \sigma_j}{4} \\
 & + \frac{1}{\eta^2} \sum_{i,j=1}^3 \left(\sum_{\lambda \in \Lambda_i^A \cap \Lambda_j^B} \langle \sigma_i \otimes \sigma_j \rangle_{\rho_\lambda} \right) \frac{\sigma_i \otimes \sigma_j}{4},
 \end{aligned}
 \tag{2.25}$$

with

$$(2.26) \quad \Lambda_i^A = \{\lambda \in \Lambda \mid p(\mathbf{c}^A|i, \lambda) = 1\}, \quad \Lambda_j^B = \{\lambda \in \Lambda \mid p(\mathbf{c}^B|j, \lambda) = 1\},$$

where $p(\mathbf{c}^A|i, \lambda)$ denotes the probability that Alice's device performing the measurement associated with the observable σ_i clicks when receiving the state, labelled with λ , sent by the source (similarly for Bob). We investigated, without loss of generality, only deterministic clicking strategies.

The condition $\rho_{\text{observed}} \geq 0$ in Eq. (2.24c) requests that the observed statistics corresponds to some physical state, which otherwise could lead to the parties realizing that the behavior of their detectors is malicious.

While, when the agents use the assignment strategy to deal with the non detection events, given assignments (a_1, a_2, a_3) and (b_1, b_2, b_3) and detection efficiency η , we derived that the SDP problem that must solved is:

$$(2.27a) \quad \begin{aligned} \min_{\rho_\lambda} \quad & w_{0,0} + \sum_{i=1}^3 w_{i,0} \left(\sum_{\lambda \in \Lambda_i^A} \langle \sigma_i \otimes \mathbb{1} \rangle_{\rho_\lambda} + \sum_{\lambda \in \bar{\Lambda}_i^A} \text{Tr}[\rho_\lambda] a_i \right) \\ & + \sum_{j=1}^3 w_{0,j} \left(\sum_{\lambda \in \Lambda_j^B} \langle \mathbb{1} \otimes \sigma_j \rangle_{\rho_\lambda} + \sum_{\lambda \in \bar{\Lambda}_j^B} \text{Tr}[\rho_\lambda] b_j \right) \\ & + \sum_{i,j=1}^3 w_{i,j} \left(\sum_{\lambda \in \Lambda_i^A \cap \Lambda_j^B} \langle \sigma_i \otimes \sigma_j \rangle_{\rho_\lambda} + \sum_{\lambda \in \Lambda_i^A \cap \bar{\Lambda}_j^B} \langle \sigma_i \otimes \mathbb{1} \rangle_{\rho_\lambda} b_j \right. \\ & \quad \left. + \sum_{\lambda \in \bar{\Lambda}_i^A \cap \Lambda_j^B} \langle \mathbb{1} \otimes \sigma_j \rangle_{\rho_\lambda} a_i + \sum_{\lambda \in \bar{\Lambda}_i^A \cap \bar{\Lambda}_j^B} \text{Tr}[\rho_\lambda] a_i b_j \right) \\ \text{s.t.} \quad & \sum_{\lambda \in \Lambda_i^A} \text{Tr}[\rho_\lambda] = \sum_{\lambda \in \Lambda_j^B} \text{Tr}[\rho_\lambda] = \eta, \quad \sum_{\lambda \in \Lambda_i^A \cap \Lambda_j^B} \text{Tr}[\rho_\lambda] = \eta^2, \quad \forall i, j \in \{1, 2, 3\}, \end{aligned}$$

$$(2.27b) \quad \rho_\lambda \geq 0, \quad \rho_\lambda^{\text{T}^A} \geq 0, \quad \forall \lambda \in \Lambda,$$

$$(2.27c) \quad \rho_{\text{observed}} \geq 0, \quad \sum_{\lambda \in \Lambda} \text{Tr}[\rho_\lambda] = 1,$$

$$(2.27d) \quad \begin{aligned} \sum_{\lambda \in \Lambda_i^A \cap \bar{\Lambda}_j^B} \langle \sigma_i \otimes \mathbb{1} \rangle_{\rho_\lambda} &= (1 - \eta) \sum_{\lambda \in \Lambda_i^A} \langle \sigma_i \otimes \mathbb{1} \rangle_{\rho_\lambda}, \\ \sum_{\lambda \in \bar{\Lambda}_i^A \cap \Lambda_j^B} \langle \mathbb{1} \otimes \sigma_j \rangle_{\rho_\lambda} &= (1 - \eta) \sum_{\lambda \in \Lambda_j^B} \langle \mathbb{1} \otimes \sigma_j \rangle_{\rho_\lambda} \quad \forall i, j \in \{1, 2, 3\}. \end{aligned}$$

where ρ_{observed} is defined in Eq. (2.25),

$$(2.28) \quad \bar{\Lambda}_i^A = \{\lambda \in \Lambda \mid p(\mathbf{c}^A|i, \lambda) = 0\}, \quad \bar{\Lambda}_j^B = \{\lambda \in \Lambda \mid p(\mathbf{c}^B|j, \lambda) = 0\}.$$

When discussing detection efficiency, one is often focused on the critical values that must be exceeded in order to observe a violation of a Bell inequality, or in our case an entanglement

witness. At the same time, these theoretical limits must be adjusted in experiments due to inevitable noise. The relevant figure of merit in this discussion is the critical visibility, which we define here for a witness W as follows

$$(2.29) \quad v_\rho = \min [v \langle W \rangle_\rho + (1-v) \langle W \rangle_{\frac{1 \otimes 1}{4}} \leq \langle W \rangle_\lambda],$$

with $0 \leq v \leq 1$, where $\langle W \rangle_{\frac{1 \otimes 1}{4}}$ is the value of the witness W with respect to the maximally mixed state $\frac{1 \otimes 1}{4}$, and $\langle W \rangle_\lambda$ is the minimal value attainable by malicious strategies, in which the detectors can be controlled by a hidden variable λ . Critical visibility, as defined by Eq. (2.29), is directly connected to white noise robustness, but has the opposite interpretation. Namely, values of visibility close to 1 mean that little amount of noise can be tolerated in the experiment.

The definition in Eq. (2.29) is applicable to both, the discard and the assignment strategy. For the former, $\langle W \rangle_\rho$ is independent of η and $\langle W \rangle_\lambda$ gets more negative as η decreases, as shown in Fig. 3.1. For the latter, $\langle W \rangle_\rho$ increases as η decreases, while $\langle W \rangle_\lambda$ remains zero for η above the critical value, as shown in Fig. 3.2. In both situations, for the critical value of η , the visibility v_ρ is equal to 1 for the state ρ giving the minimal value of the witness W . For η above critical, some amount of white noise can be tolerated, resulting in the required visibility values going below 1.

2.5 Tasks on graphs

In the third article, we used the following definitions:

Definition 2.1. Given a graph, and a number $h \geq 1$, the **rendezvous task** is defined as the task in which $r \geq 2$ agents, placed uniformly randomly among the vertexes of the graph, move along edges of the graph h times. They are successful if, after crossing the edges h times, they are all positioned in the same vertex. They can establish a strategy before being placed on the graph, but they are not allowed to communicate before each of the agents has completed their move.

If $h=1$ then the rendezvous task is called **single-step**.

One variant of the rendezvous problem is the symmetric rendezvous where both players have equal capabilities and constraints or are following the same strategy [33–36].

Definition 2.2. Given a graph, and a number $h \geq 1$, the **domination task** is defined as the task in which $r \geq 2$ agents, placed uniformly randomly among the vertexes of the graph, move along edges of the graph h times. They try to dominate as many vertexes as they can, counting the dominated points only after all the agents completed their moves.

A vertex is said to be dominated when an agent occupies it or it is connected with an edge to a vertex where there is an agent.

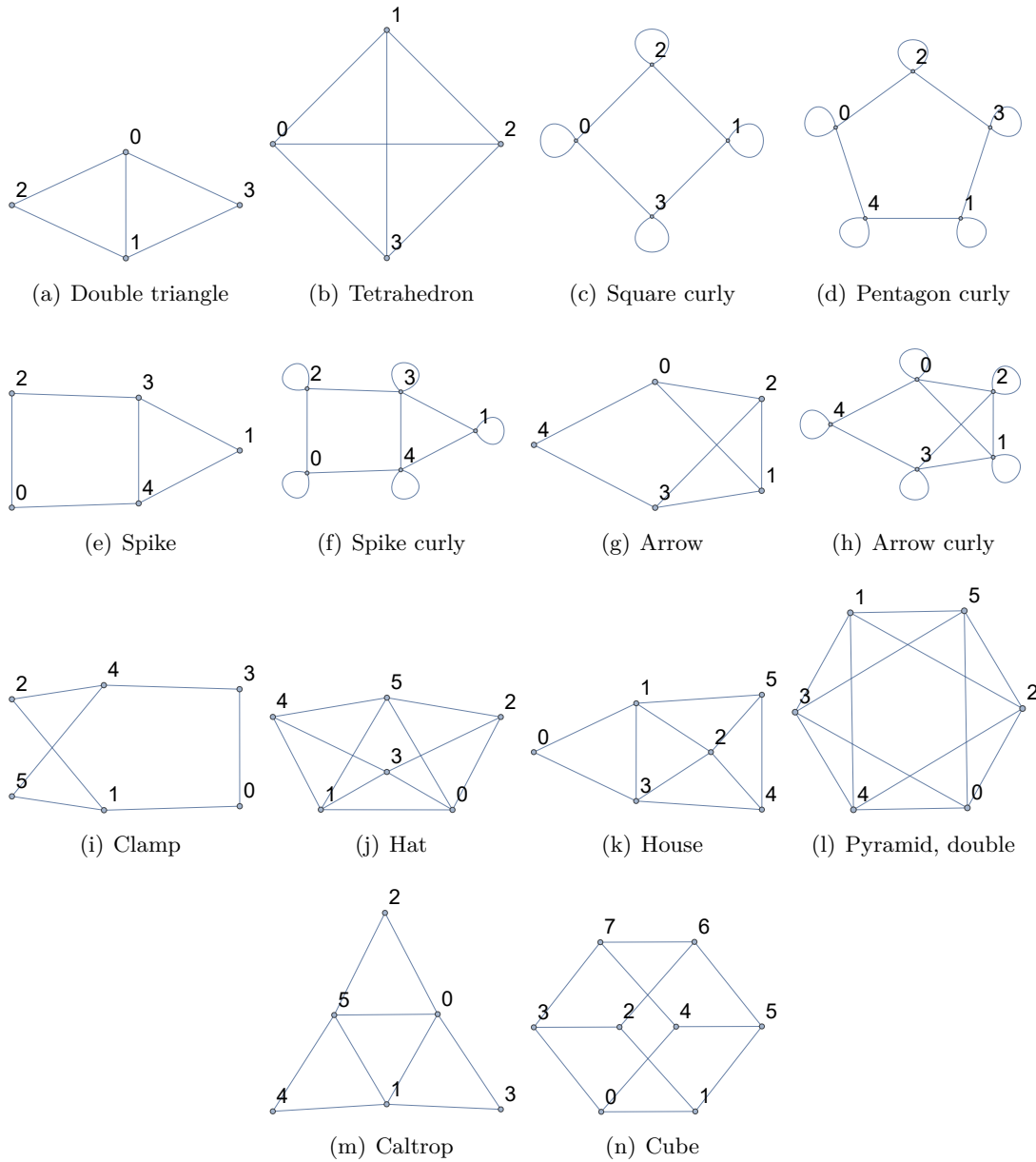


Figure 2.7: Some of the graphs analysed.

The agents can establish a strategy before being placed on the graph, but they are not allowed to communicate before each of the agents has completed their move.

If $h=1$ then the domination task is called **single-step**.

In Fig. 2.7 we present some of the graph scenarios with which we dealt. With the name n -gon we refer to the graphs described by a polygon with n vertexes, with the name n -line we refer to the graphs described by a line connecting n vertexes, while with the name n -line curly we refer to a n -line graph where the extrema are connected with themselves.

At exception of the n -line curly graphs, for which we provided a specific definition, for all the other graphs we included the word "curly" in their name when each of their vertexes is connected with itself.

In the quantum version of these tasks the agents share a quantum state before being placed on the graph, and, after performing a measurement on their subsystem, determined by the starting position, they decide to which accessible node they will move.

In addition to the standard cases, we studied also the symmetric cases in which the agents are constrained to use the same strategy. In the symmetric quantum case the agents are constrained to receive subsystems described by the same quantum state and they all decide in the same way which measurement to perform based on the starting position.

The results were found through the application of see-saw method and NPA hierarchy method.

Outlook

The articles in this dissertation aim to bring out the usefulness and versatility of numerical optimisation approaches applied to problems directly related to quantum experiments and communication tasks, aiming in particular to show examples of application of already known and analysed tools and their adaptation and extension to particular problems, to the point of generating new algorithms with which to approach more complex problems, making it possible to obtain new results and increase the researcher's understanding in situations not yet explored, favouring the emergence of insights that can help in the search for more elegant analytical solutions.

In the first article we have applied the discard strategy and assignment strategy techniques to a particular entanglement witness experiment with faulty and potentially malicious detectors, deriving formulations (2.24) and (2.27) which can be solved through convex optimization.

Through convex optimisation, we then derived the plots in Fig. (3.1) where we show the solutions of Eq. (2.24) for the witness W_θ for $\theta \in \{\frac{\pi}{6}, \frac{\pi}{5}, \frac{\pi}{4}\}$. Additionally, we provided an explicit solution for the Bell witness, and show that in that for the discard strategy the critical detection efficiency is $\frac{1}{\sqrt{3}}$. This value is significantly smaller than $\sqrt{\frac{2}{3}}$, which is the critical detection efficiency of detecting the Bell state device-independently in a Bell experiment [37].

In Fig. 3.2 (left) we demonstrated the solution to the SDP in Eq. (2.27) for the witness W_θ and the assignment $(0,0,0)$. This particular assignment preserves the property $\langle W \rangle_{\rho_s} \geq 0$ for all separable states. In Fig. 3.2 (left) by the dashed lines we depicted values of the witness W_θ with respect to the corresponding state $|\Psi_\theta\rangle$. These values increase as η decreases due to the assignment strategy selected. The points where the dashed lines intersect the solid lines are the critical detection efficiencies for the chosen assignment.

In Fig. 3.2 (right) we also compared different assignments for the Bell witness. One can see that the property of $\langle W \rangle_{\rho_s} \geq 0$ is not preserved for any of the selected assignments. At

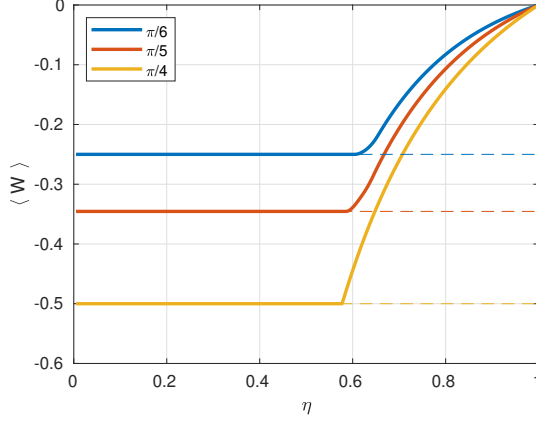


Figure 3.1: Minimal values that the witness $\langle W_\theta \rangle$ can take in the discard strategy as a function of detection efficiency η (solid lines), and the corresponding values of the witness $\langle W_\theta \rangle$ for the entangled state $|\Psi_\theta\rangle$ (dashed lines).

the same time, one can still detect entanglement if the expectation value with respect to an entangled state is lower than the calculated bound on $\langle W_{\frac{\pi}{4}} \rangle_{\rho_s}$ due to untrusted detectors, as we demonstrate in Fig. 3.2. Notably, the minimal expectation values that the witnesses can take with respect to entangled states (dashed lines) do not correspond to the Bell state.

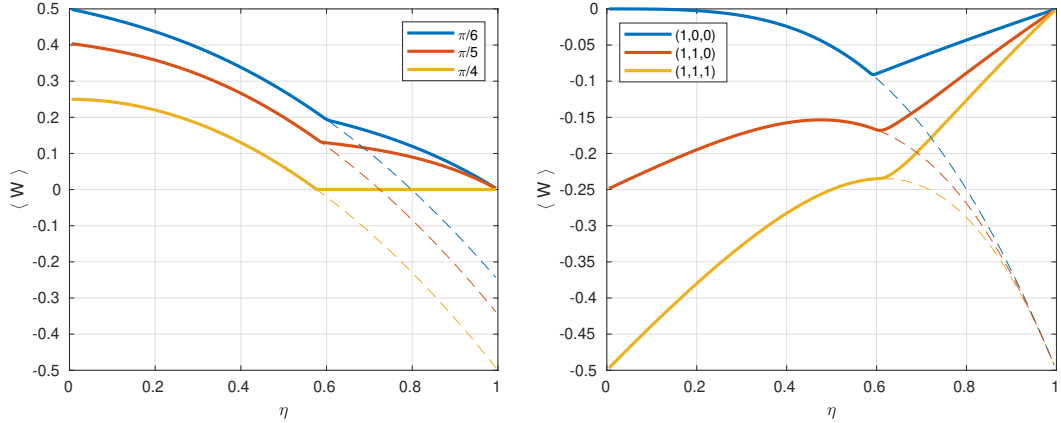


Figure 3.2: Left: Minimal values of the witness $\langle W_\theta \rangle$ in the assignment strategy with $a_i=0$ and $b_j=0, \forall i, j, \in \{1, 2, 3\}$ as a function of detection efficiency η (solid lines) and the corresponding values of the witness for the entangled state $|\Psi_\theta\rangle$ (dashed lines). Right: Minimal values of the Bell witness for the assignments $(a_1, a_2, a_3) \in \{(1, 0, 0), (1, 1, 0), (1, 1, 1)\}$ and $b_i = (-1)^{i+1} a_i \forall i$ (solid lines), and the corresponding minimal values of the witness over entangled states (dashed lines).

The critical detection efficiency for the Bell witness for the assignment strategy $\alpha=\beta=\frac{1}{2}$ is again $\eta=\frac{1}{\sqrt{3}}$ as for the discard strategy. And, although we have studied different other assignment strategies, we never found a critical detection efficiency smaller than $\frac{1}{\sqrt{3}}$. So remains

open the question whether it is possible to further reduce the value of critical detection efficiency with a more suitable assignment strategy.

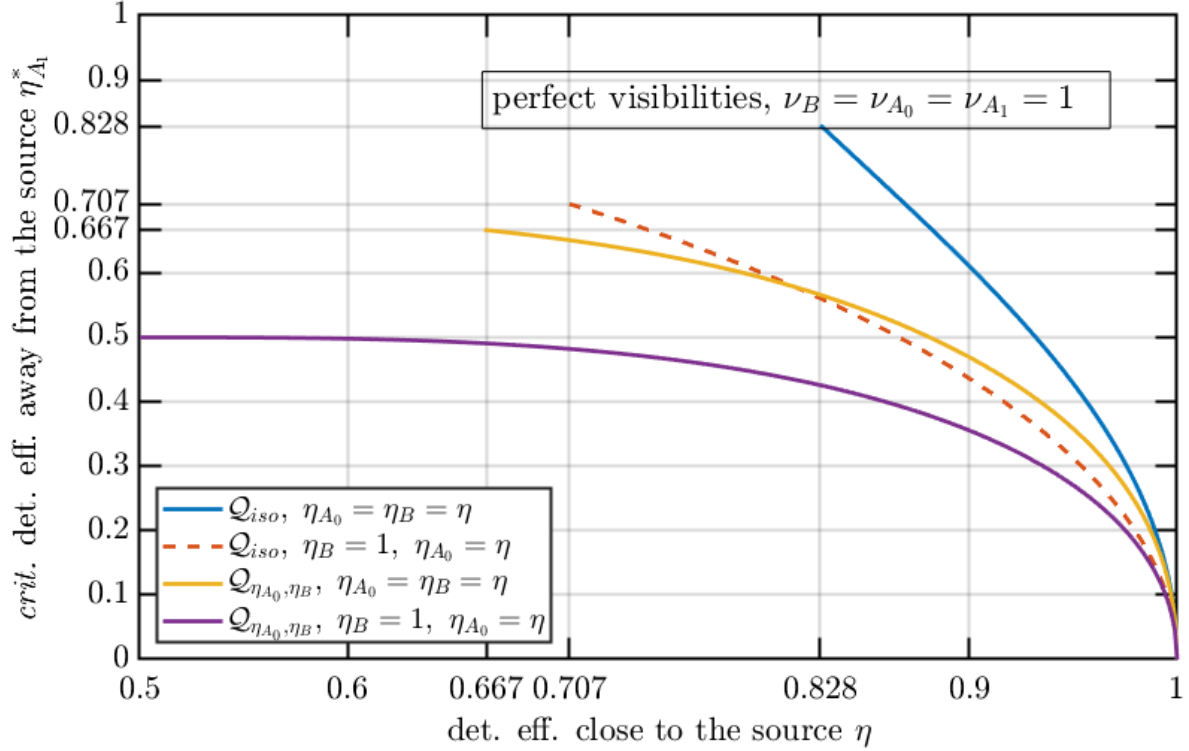


Figure 3.3: The critical detection efficiency, $\eta_{A_1}^*$, of Alice’s measurement device placed away from the source, A_1 , versus the effective detection efficiency, η , close to the source, obtained with the analytical trade-off (2.18), when the party’s employ the isotropic strategy, Q_{iso} , for the symmetric case, $\eta_{A_0}=\eta_B=1$ (top solid blue curve), and for the asymmetric case, $\eta_{A_0}=\eta, \eta_B=1$ (dashed orange curve), and when the party’s employ the tilted strategies, $Q_{\eta_{A_0},\eta_B}$, for the symmetric case (middle solid yellow curve), and for the asymmetric case (bottom solid purple curve), with perfect visibilities, $\nu_B=\nu_{A_0}=\nu_{A_1}=1$. The critical detection efficiency starts declining after η exceeds the respective threshold values: $\eta=\frac{2}{1+\sqrt{2}}\approx 0.828$, $\eta=\frac{1}{\sqrt{2}}\approx 0.707$, for the symmetric, and the asymmetric cases, respectively, when the parties employ the isotropic strategy, Q_{iso} , and $\eta=\frac{2}{3}\approx 0.67$, $\eta=\frac{1}{2}$, for the symmetric, and the asymmetric cases, when the parties use the tilted strategies, $Q_{\eta_{A_0},\eta_B}$, respectively. In both symmetric and asymmetric cases, the tilted strategies, $Q_{\eta_{A_0},\eta_B}$, perform better than the isotropic strategy, Q_{iso} , at minimizing the critical detection efficiency, $\eta_{A_1}^*$.

In the second article, through the introduction of the routed Bell experiment, we showed that when agents positioned close to the source of quantum states exhibit correlations that maximise the violation of the CHSH inequality, then it is possible to measure non-local behaviour even for agents positioned arbitrarily far from the source (1). Considering instead the case in which agents positioned close to the source have imperfect devices at their disposal, we have demonstrated a trade-off between violation of the CHSH inequality exhibited by agents

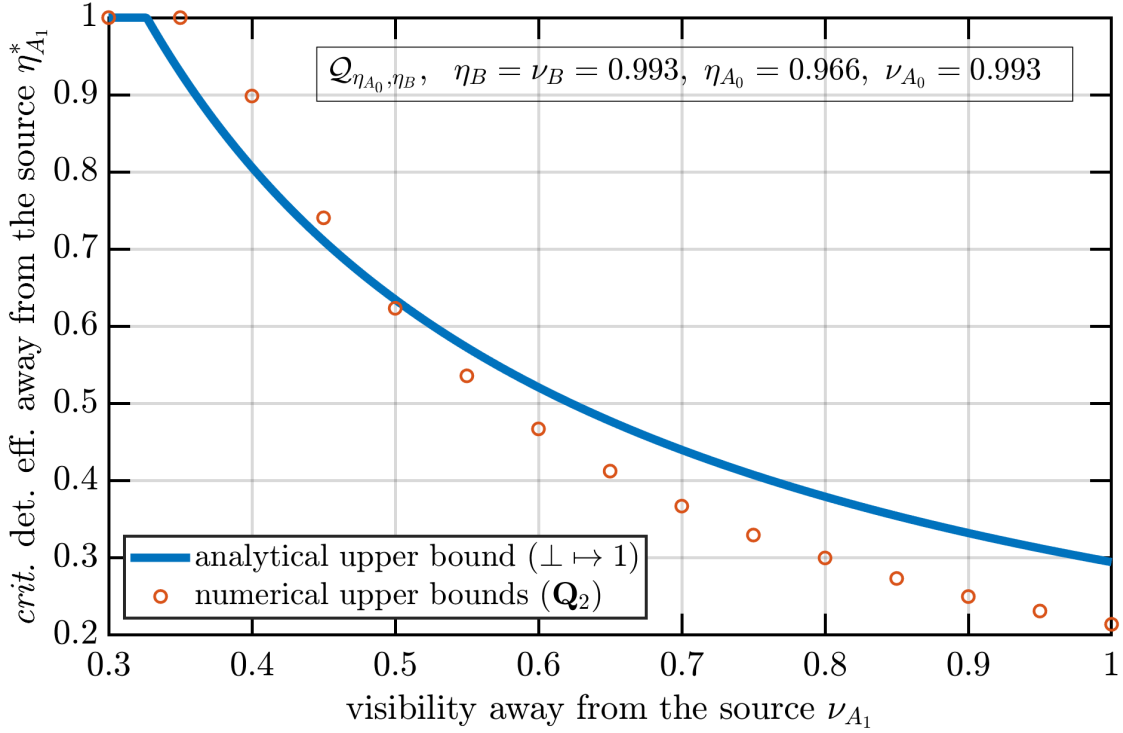


Figure 3.4: Upper bounds on the critical detection efficiency, $\eta_{A_1}^*$, of Alice’s measurement device placed away from the source, versus the effective visibility between (A_1, B) , ν_{A_1} , calculated analytically using (2.18), when the parties use the tilted strategy, $Q_{\eta_{A_0}, \eta_B}$, where $\eta_B = \nu_B = 0.993$, $\eta_{A_0} = 0.966$, $\nu_{A_0} = 0.993$, and the assignment strategy, $\perp \mapsto +1$ (solid blue curve), and numerically using certifiable randomness as a measure for the nonlocal behavior of A_1 , and the second level (\mathbf{Q}_2) of Nieto-Silleras hierarchy of semi-definite programs, while keeping the “no-click” event as an additional outcome, $\tilde{a}, \tilde{b} \in \{\pm 1, \perp\}$ (orange circles). The curves demonstrate the advantage of keeping the “no-click” as an additional outcome, $\tilde{a}, \tilde{b} \in \{\pm 1, \perp\}$ over the post-processing strategy of assigning a valid outcome to the “no-click” event, $\perp \mapsto +1$.

positioned close to the source and thresholds on detector efficiency and visibility that the detectors of agents positioned far from the source must respect in order to exhibit nonlocal behaviour (2).

In Fig. (3.3) we have shown the advantage of using tilted strategies $Q_{\eta_{A_0}, \eta_B}$, i.e. the strategies which attain maximum quantum violation of the tilted CHSH (2.19), over the isotropic strategy when the detection efficiency of devices positioned close to the source are not perfect.

Additionally, through Fig. (3.4) we demonstrated the advantage of using the numerical technique, which allowed us to consider the entire outcome statistics, thus considering the no-click event as an additional outcome, compared to the exclusive use of the theoretical results obtained through the application of Eq. (2.18) for which only two outcomes are considered.

Table 3.1: Results associated with the single-step rendezvous task, two agents case, when the agents can start from any position.

Name	Random	Classical	NPA	Adv. [%]
tetrahedron Fig. 2.7(b)	$\frac{1}{4}$	$\frac{5}{8}$	0.64506*	5
square curly, Fig. 2.7(c)	$\frac{1}{4}$	$\frac{5}{8}$	0.64506*	5
pentagon curly, Fig. 2.7(d)	$\frac{1}{5}$	$\frac{13}{25}$	0.53009*	3
arrow Fig. 2.7(g)	0.20667	$\frac{13}{25}$	0.52051*	0.1
clamp Fig. 2.7(i)	0.18827	$\frac{7}{18}$	0.40063*	6
hat Fig. 2.7(j)	0.17207	$\frac{5}{9}$	$0.58333 \approx \frac{7}{12}$	7
house Fig. 2.7(k)	0.18210	$\frac{5}{9}$	$0.58333 \approx \frac{7}{12}$	7
caltrop Fig. 2.7(m)	0.20833	$\frac{5}{9}$	$0.58333 \approx \frac{7}{12}$	8
cube Fig. 2.7(n)	$\frac{1}{8}$	$\frac{5}{16}$	0.32253*	5
triangle 3-gon	$\frac{1}{3}$	$\frac{5}{9}$	$0.58333 \approx \frac{7}{12}$	13
pentagon 5-gon	$\frac{1}{5}$	$\frac{9}{25}$	0.38090	13
hexagon 6-gon	$\frac{1}{6}$	$\frac{5}{18}$	0.29167	13
heptagon 7-gon	$\frac{1}{7}$	$\frac{13}{49}$	0.27864	11
ennagon 9-gon	$\frac{1}{9}$	$\frac{17}{81}$	0.21887	9
decagon 10-gon	$\frac{1}{10}$	$\frac{9}{50}$	0.19045	13
11-gon	$\frac{1}{11}$	$\frac{21}{121}$	0.17998	8
13-gon	$\frac{1}{13}$	$\frac{25}{169}$	0.15273	7
3-line curly	$\frac{1}{3}$	$\frac{5}{9}$	$0.58333 \approx \frac{7}{12}$	13
5-line curly	$\frac{1}{5}$	$\frac{9}{25}$	0.38090	13
7-line curly	$\frac{1}{7}$	$\frac{13}{49}$	0.27864	11

In the third article by means of convex optimisation, it emerged that a quantum advantage can be obtained for many scenarios connected with communications tasks involving agents distributed on a graph. In particular we studied the rendezvous and graph domination tasks.

In the following tables the column "Random" contains the values of the score that the agents obtain when they select the destination node in a random uniform way, the column "Classical"

(C) contains the value which the agents can achieve using classical strategies and the column "NPA" (Q) contains the values which can be achieved when the agents share a quantum state. The values which appear without "*" are calculated with NPA level 1+ ab , an intermediate level between NPA level 1 and 2, otherwise they are calculated with NPA level 2. The column "Adv." contains the quantum advantages expressed in percents, calculated according to the following expression:

$$(3.1) \quad \frac{Q - R}{C - R} - 1.$$

In Tab. 3.1 we listed the cases for which we found an advantage when the two agents, performing the single-step rendezvous task, share a quantum state, while in Tab. 3.2 is considered the further constraint that the agents can't start from the same positions, and in Tab. 3.3 the agents are also constrained to adopt only symmetric strategies.

In Tab. 3.4 we listed the cases for which we found an advantage when the two agents, performing the single-step domination task, share a quantum state, while in Tab. 3.5 is considered the further constraint that the agents can't start from the same positions.

Table 3.2: Results associated with the single-step rendezvous task, two agents case, when the agents can't start in the same positions.

Name	Random	Classical	NPA	Adv. [%]
tetrahedron Fig. 2.7(b)	$\frac{2}{9}$	$\frac{1}{2}$	$0.53333^* \approx \frac{8}{15}$	12
square curly, Fig. 2.7(c)	$\frac{2}{9}$	$\frac{1}{2}$	$0.53333^* \approx \frac{8}{15}$	12
pentagon curly, Fig. 2.7(d)	$\frac{1}{6}$	$\frac{2}{5}$	0.41316^*	6
arrow Fig. 2.7(g)	0.16667	$\frac{2}{5}$	0.40490^*	2
clamp Fig. 2.7(i)	0.13704	$\frac{4}{15}$	0.28229^*	12
hat Fig. 2.7(j)	0.15093	$\frac{7}{15}$	$0.50000 \approx \frac{1}{2}$	11
house Fig. 2.7(k)	0.15463	$\frac{7}{15}$	$0.50000 \approx \frac{1}{2}$	11
caltrop Fig. 2.7(m)	$\frac{7}{40}$	$\frac{7}{15}$	$0.50000 \approx \frac{1}{2}$	11
cube Fig. 2.7(n)	$\frac{2}{21}$	$\frac{3}{14}$	0.22857^*	12

In other cases we proved that quantum resources do not bring any advantage, while in the remaining cases treated, the computing resources we exploited were not sufficient to conclude whether quantum resources can bring any advantage. In particular, no case was found for which

Table 3.3: Results associated with the single-step rendezvous task, two agents case, when the agents can't start in the same positions and they are constrained to adopt only symmetric strategies. Note that the first nine cases has identical values as those in Tab. 3.2.

Name	Random	Classical	NPA	Adv. [%]
tetrahedron Fig. 2.7(b)	$\frac{2}{9}$	$\frac{1}{2}$	$0.53333^* \approx \frac{8}{15}$	12
square curly, Fig. 2.7(c)	$\frac{2}{9}$	$\frac{1}{2}$	$0.53333^* \approx \frac{8}{15}$	12
pentagon curly, Fig. 2.7(d)	$\frac{1}{6}$	$\frac{2}{5}$	0.41316^*	6
arrow Fig. 2.7(g)	$\frac{1}{6}$	$\frac{2}{5}$	0.40490^*	2
clamp Fig. 2.7(i)	0.13704	$\frac{4}{15}$	0.28229^*	12
hat Fig. 2.7(j)	0.15093	$\frac{7}{15}$	$0.50000 \approx \frac{1}{2}$	11
house Fig. 2.7(k)	0.15463	$\frac{7}{15}$	$0.50000 \approx \frac{1}{2}$	11
caltrop Fig. 2.7(m)	$\frac{7}{40}$	$\frac{7}{15}$	$0.50000 \approx \frac{1}{2}$	11
cube Fig. 2.7(n)	$\frac{2}{21}$	$\frac{3}{14}$	0.22857^*	12
triangle 3-gon	$\frac{1}{4}$	$\frac{1}{3}$	$0.50000 \approx \frac{1}{2}$	200
pentagon 5-gon	$\frac{1}{8}$	$\frac{1}{5}$	$0.25000 \approx \frac{1}{4}$	67
hexagon 6-gon	$\frac{1}{10}$	$\frac{2}{15}$	$0.20000 \approx \frac{1}{5}$	200
heptagon 7-gon	$\frac{1}{12}$	$\frac{1}{7}$	$0.16667 \approx \frac{1}{6}$	40
ennagon 9-gon	$\frac{1}{16}$	$\frac{1}{9}$	$0.12500 \approx \frac{1}{8}$	29
decagon 10-gon	$\frac{1}{18}$	$\frac{4}{45}$	$0.11111 \approx \frac{1}{9}$	67
11-gon	$\frac{1}{20}$	$\frac{1}{11}$	$0.10000 \approx \frac{1}{10}$	22
13-gon	$\frac{1}{24}$	$\frac{1}{13}$	$0.08333 \approx \frac{1}{12}$	18
3-line curly	$\frac{1}{4}$	$\frac{1}{3}$	$0.50000 \approx \frac{1}{2}$	200
5-line curly	$\frac{1}{8}$	$\frac{1}{5}$	$0.25000 \approx \frac{1}{4}$	67
7-line curly	$\frac{1}{12}$	$\frac{1}{7}$	$0.16667 \approx \frac{1}{6}$	40

quantum resources bring an advantage in cases where the number of agents involved in the studied tasks is three.

Table 3.4: Results associated with the single-step domination task, two agents case, when the agents can start from any position.

Name	Random	Classical	NPA	Adv. [%]
pentagon curly, Fig. 2.7(d)	4.2	4.64	4.67361*	8
caltrop Fig. 2.7(m)	5.458333	5.88889	5.916667	6
spike Fig. 2.7(e)	4.51333	4.92	4.93	2
clamp Fig. 2.7(i)	4.94907	5.44444	5.45453	2
pentagon	4.2	4.6	4.67361	18
hexagon	4.50000	4.95000	5.0000	13
heptagon	4.71428	5.08163	5.15517	20
octagon	4.875	5.1875	5.23928	17
9-gon	5	5.24691	5.29434	19
10-gon	5.1	5.3	5.33680	18
11-gon	5.18182	5.39669	5.43395	17
12-gon	5.25	5.47222	5.5	13
13-gon	5.30769	5.50888	5.54543	18
6-line curly	4.11111	4.44445	4.44895	1

Table 3.5: Results associated with the single-step domination task, two agents case, when the agents cant start in the same positions.

Name	Random	Classical	NPA	Adv. [%]
pentagon curly, Fig. 2.7(d)	4,27778	4.7	4.73987	9
clamp Fig. 2.7(i)	5.01482	5.4	5.41210*	3
caltrop Fig. 2.7(m)	5.48750	5.86667	5.9	9
spike Fig. 2.7(e)	4.56944	4.9	4.9125	4
pentagon	4.25	4.5	4.59201	37
hexagon	4.60000	4.93333	5.00000	20
heptagon	4.83333	5.09524	5.18103	33
octagon	5	5.21429	5.27346	28
9-gon	5.125	5.27778	5.33113	35
10-gon	5.22222	5.34444	5.37423	24
11-gon	5.3	5.43636	5.47735	30
12-gon	5.36364	5.51515	5.54545	20
13-gon	5.41667	5.51515	5.59088	29

Bibliography

- [1] A. K. Ekert, “Quantum cryptography based on Bell’s theorem,” *Phys. Rev. Lett.*, vol. 67, pp. 661–663, Aug 1991.
- [2] D. Mayers and A. Yao, “Quantum cryptography with imperfect apparatus,” in *Proceedings 39th Annual Symposium on Foundations of Computer Science*, (Los Alamitos, CA), p. 503, IEEE, 1998.
- [3] J. Barrett, L. Hardy, and A. Kent, “No signaling and quantum key distribution,” *Phys. Rev. Lett.*, vol. 95, p. 010503, Jun 2005.
- [4] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, “Device-independent security of quantum cryptography against collective attacks,” *Phys. Rev. Lett.*, vol. 98, p. 230501, Jun 2007.
- [5] U. Vazirani and T. Vidick, “Fully device-independent quantum key distribution,” *Phys. Rev. Lett.*, vol. 113, p. 140501, Sep 2014.
- [6] I. W. Primaatmaja, K. T. Goh, E. Y.-Z. Tan, J. T.-F. Khoo, S. Ghorai, and C. C.-W. Lim, “Security of device-independent quantum key distribution protocols: a review,” *Quantum*, vol. 7, p. 932, Mar. 2023.
- [7] R. Colbeck, *Quantum and relativistic protocols for secure multi-party computation*. PhD thesis, University of Cambridge, 2009.
- [8] S. Pironio, A. Acín, S. Massar, A. B. de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, “Random numbers certified by Bell’s theorem,” *Nature*, vol. 464, pp. 1021–1024, Apr 2010.
- [9] W.-Z. Liu, M.-H. Li, S. Ragy, S.-R. Zhao, B. Bai, Y. Liu, P. J. Brown, J. Zhang, R. Colbeck, J. Fan, Q. Zhang, and J.-W. Pan, “Device-independent randomness expansion against quantum side information,” *Nat. Phys.*, Feb 2021.
- [10] L. K. Shalm, Y. Zhang, J. C. Bienfang, C. Schlager, M. J. Stevens, M. D. Mazurek, C. Abellán, W. Amaya, M. W. Mitchell, M. A. Alhejji, H. Fu, J. Ornstein, R. P. Mirin, S. W. Nam, and E. Knill, “Device-independent randomness expansion with entangled photons,” *Nat. Phys.*, Jan 2021.

BIBLIOGRAPHY

- [11] J. S. Bell, “On the Einstein Podolsky Rosen paradox,” *Phys. Phys. Fiz.*, vol. 1, pp. 195–200, Nov 1964.
- [12] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, “Proposed experiment to test local hidden-variable theories,” *Phys. Rev. Lett.*, vol. 23, no. 15, pp. 880–884, 1969.
- [13] P. Skrzypczyk and D. Cavalcanti, *Semidefinite Programming in Quantum Information Science*. 2053-2563, IOP Publishing, 2023.
- [14] P. Mironowicz, “Semi-definite programming and quantum information,” *Journal of Physics A: Mathematical and Theoretical*, 2024.
- [15] A. Tavakoli, A. Pozas-Kerstjens, P. Brown, and M. Araújo, “Semidefinite programming relaxations for quantum correlations,” *arXiv:2307.02551*, 2023.
- [16] M. Navascués, S. Pironio, and A. Acín, “Bounding the set of quantum correlations,” *Physical Review Letters*, vol. 98, no. 1, p. 010401, 2007.
- [17] M. Navascués, S. Pironio, and A. Acín, “A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations,” *New Journal of Physics*, vol. 10, no. 7, p. 073013, 2008.
- [18] K. F. Pál and T. Vértesi, “Maximal violation of a bipartite three-setting, two-outcome Bell inequality using infinite-dimensional quantum systems,” *Physical Review A*, vol. 82, no. 2, p. 022116, 2010.
- [19] M. Czechlewski and M. Pawłowski, “Influence of the choice of postprocessing method on Bell inequalities,” *Physical Review A*, vol. 97, no. 6, p. 062123, 2018.
- [20] S. Alpern, “The rendezvous search problem,” *SIAM Journal on Control and Optimization*, vol. 33, no. 3, pp. 673–683, 1995.
- [21] T. W. Haynes, S. Hedetniemi, and P. Slater, *Fundamentals of domination in graphs*. CRC press, 2013.
- [22] T. W. Haynes, S. T. Hedetniemi, and M. A. Henning, *Domination in graphs: Core concepts*. Springer, 2023.
- [23] P. Mironowicz, *Applications of semi-definite optimization in quantum information protocols*. PhD thesis, Gdańsk University of Technology, 2015.
- [24] J. Uffink, “Quadratic bell inequalities as tests for multipartite entanglement,” *Phys. Rev. Lett.*, vol. 88, p. 230406, May 2002.

-
- [25] L. Vandenberghe and S. Boyd, “Semidefinite programming,” *SIAM review*, vol. 38, no. 1, pp. 49–95, 1996.
- [26] F. A. Potra and S. J. Wright, “Interior-point methods,” *Journal of computational and applied mathematics*, vol. 124, no. 1-2, pp. 281–302, 2000.
- [27] E. D. Andersen and K. D. Andersen, “The MOSEK interior point optimizer for linear programming: an implementation of the homogeneous algorithm,” in *High performance optimization*, pp. 197–232, Springer, 2000.
- [28] V. Scarani, “The device-independent outlook on quantum physics,” *Acta Physica Slovaca*, vol. 62, pp. 1–60, 03 2013.
- [29] “Optical fiber loss and attenuation.” <https://www.fiberoptics4sale.com/blogs/archive-posts/95048006-optical-fiber-loss-and-attenuation>. Accessed: 2022-11-25.
- [30] M. Giustina, M. A. M. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phe-lan, F. Steinlechner, J. Kofler, J.-Å. Larsson, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, J. Beyer, T. Gerrits, A. E. Lita, L. K. Shalm, S. W. Nam, T. Scheidl, R. Ursin, B. Wittmann, and A. Zeilinger, “Significant-loophole-free test of Bell’s theorem with entangled photons,” *Phys. Rev. Lett.*, vol. 115, p. 250401, Dec 2015.
- [31] J.-D. Bancal, L. Sheridan, and V. Scarani, “More randomness from the same data,” *New Journal of Physics*, vol. 16, p. 033011, mar 2014.
- [32] O. Nieto-Silleras, S. Pironio, and J. Silman, “Using complete measurement statistics for optimal device-independent randomness evaluation,” *New Journal of Physics*, vol. 16, p. 013035, jan 2014.
- [33] E. J. Anderson and S. Essegaiier, “Rendezvous search on the line with indistinguishable players,” *SIAM Journal on Control and Optimization*, vol. 33, no. 6, pp. 1637–1642, 1995.
- [34] X. Yu and M. Yung, “Agent rendezvous: A dynamic symmetry-breaking problem,” in *International Colloquium on Automata, Languages, and Programming*, pp. 610–621, Springer, 1996.
- [35] S. Alpern and W. S. Lim, “The symmetric rendezvous-evasion game,” *SIAM Journal on Control and Optimization*, vol. 36, no. 3, pp. 948–959, 1998.
- [36] Q. Han, D. Du, J. Vera, and L. F. Zuluaga, “Improved bounds for the symmetric rendezvous value on the line,” *Operations Research*, vol. 56, no. 3, pp. 772–782, 2008.

BIBLIOGRAPHY

- [37] S. Massar, S. Pironio, J. Roland, and B. Gisin, “Bell inequalities resistant to detector inefficiency,” *Physical Review A*, vol. 66, no. 5, p. 052112, 2002.

PAPER • OPEN ACCESS

Entanglement witnessing with untrusted detectors

To cite this article: Giuseppe Viola *et al* 2023 *J. Phys. A: Math. Theor.* **56** 425301

View the [article online](#) for updates and enhancements.

You may also like

- [Heralded mapping of photonic entanglement into single atoms in free space: proposal for a loophole-free Bell test](#)
Nicolas Sangouard, Jean-Daniel Bancal, Philipp Müller et al.
- [An instrument-free demonstration of quantum key distribution for high-school students](#)
María José Carreño, Jonathan Sepúlveda, Silvia Tecpan et al.
- [Minimum detection efficiency for testing a multi-particle Bell inequality](#)
Wenchao Ma, Peng Chen and Xiaosong Ma

Entanglement witnessing with untrusted detectors

Giuseppe Viola¹, Nikolai Miklin^{1,2,*} ,
Mariami Gachechiladze^{3,4} and Marcin Pawłowski¹

¹ International Centre for Theory of Quantum Technologies (ICTQT), University of Gdansk, 80-309 Gdańsk, Poland

² Heinrich Heine University Düsseldorf, Universitätsstraße 1, 40225 Düsseldorf, Germany

³ Institute for Theoretical Physics, University of Cologne, Cologne, Germany

⁴ Department of Computer Science, Technical University of Darmstadt, Darmstadt 64289, Germany

E-mail: nikolai.miklin@tuhh.de

Received 16 March 2023; revised 23 August 2023

Accepted for publication 21 September 2023

Published 3 October 2023



CrossMark

Abstract

We consider the problem of entanglement detection in the presence of faulty, potentially malicious detectors. A common—and, as of yet, the only—approach to this problem is to perform a Bell test in order to identify non-locality of the measured entangled state. However, there are two significant drawbacks in this approach: the requirement to exceed a critical, and often high, detection efficiency, and much lower noise tolerance. In this paper, we propose an alternative approach to this problem, which is resilient to the detection loophole and is based on the standard tool of entanglement witness. We discuss how the two main techniques to detection losses, namely the discard and assignment strategies, apply to entanglement witnessing. We demonstrate using the example of a two-qubit Bell state that the critical detection efficiency can be significantly reduced compared to the Bell test approach.

Keywords: entanglement witness, detection loophole, semi-device-independent

(Some figures may appear in colour only in the online journal)

* Author to whom any correspondence should be addressed.



Original Content from this work may be used under the terms of the [Creative Commons Attribution 4.0 licence](https://creativecommons.org/licenses/by/4.0/). Any further distribution of this work must maintain attribution to the author(s) and the title of the work, journal citation and DOI.

1. Introduction

Entanglement of quantum states is one of the most cited and studied quantum phenomena [1]. This fact is largely explained by the simplicity of its formulation and a promising technological advancement that it offers, primary to the field of quantum cryptography [2, 3]. At the same time, a variety of theoretical, experimental, and technological challenges are yet to be overcome before entanglement can find its real-world applications [4].

Among these challenges, perhaps the most crucial one is distribution of entangled particles among two or more laboratories that are far away from each other. It is rather clear that photons are the most natural, and essentially the only, candidates for such tasks. Entangled states of photons are easy to prepare (the first experiments date back to 1960s [5, 6]), and, moreover, photons can be sent easily through optical fibers or simply the atmosphere [7]. However, there are major downsides in using photons as carriers of entanglement, namely high losses during transmission in channels and a low efficiency of single-photon detectors [8].

The detection efficiency problem is most often discussed in the context of quantum cryptography or Bell experiments [2, 9], where making the *fair sampling assumption* can be unjustified. There, either an eavesdropper or a local hidden variable can gain control over the measurement devices, leading to insecure communication protocol or false nonlocality claims. However, it is often unjustified to assume the independence of detector's efficiency on the choice of measurement setting, which also affects simpler experiments such as entanglement detection.

If the fair sampling is not assumed, non-detection events must be accounted for. Surprisingly, it is still possible to achieve unconditionally secure cryptography or a loophole-free Bell test demonstration for non-perfect detectors [10, 11]. However, such demonstrations are only possible for detection efficiencies above certain threshold values, which are often higher than the typical values of photodetectors used in today's experiments.

Studying and lowering critical detection efficiency for quantum key distribution (QKD) and Bell tests has been the subject of extensive research [12–16]. At the same time, the problem of untrusted detectors in entanglement detection remains mostly unexplored [17]. As of yet the only approach to this problem is to perform a Bell test, in which the detection loophole is closed [18, 19]. Apart from requiring high threshold detection efficiency, this approach can also be inapplicable to noisy entangled states that do not violate any of the known Bell inequalities. Note, that if one can trust the detector of one of the two parties, then the steering framework is appropriate [20].

In this work, we take a different approach to the problem of entanglement detection with untrusted detectors. Instead of uplifting to a fully device-independent framework, we consider a scenario in which only the detection part of the measurement process, i.e. photon counting, is untrusted. More precisely, we assume that the measuring device can be divided physically or hypothetically into two parts, the part responsible for setting the measurement basis and the part responsible for particle counting. This is especially well-motivated for photonic experiments, where photon counting is performed by a separate device, the photodetector, which cannot be easily analyzed or monitored, whereas the measurement basis can be easily adjusted by a waveplate for which an adversary has relatively limited attack vectors.

Skwara *et al* [17] was the first to point out the importance of studying the detection loophole in entanglement witnessing experiments. It also suggested removing trust from the detectors while maintaining some trust in the parts of the measurement devices that tune the measurement basis. However, the authors of [17] follow a more cross-grain approach, in which the no-click events can contribute arbitrarily to the value of the witness. In the current paper, we

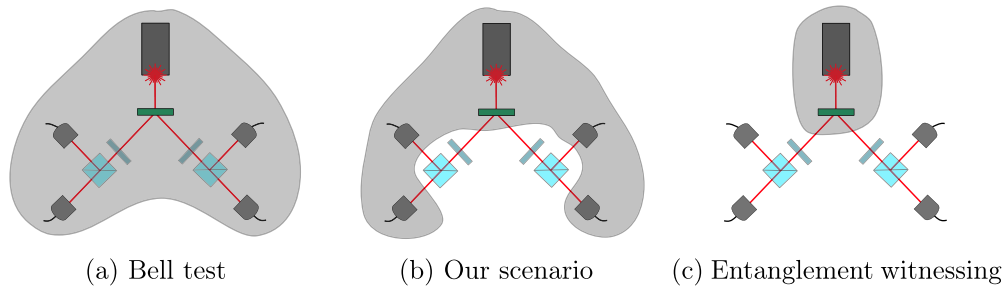


Figure 1. A schematic representation of a two-photon experiment with polarization qubits. Parts of the experimental apparatus covered in grey are assumed to be untrusted. (a) The Bell test. (b) Scenario considered in this work; the detection part of the measurement devices and the entanglement source are assumed to be untrusted. (c) The entanglement witnessing scenario.

make a more nuanced analysis and use the structure of entanglement witnesses while accounting for both, the click and no-click events, which leads to better estimates of required detection efficiencies, compared to [17].

It is important to point out that the source of entanglement and transmission channels do not need to be trusted, just in case of the standard entanglement witnessing scenario. At the same time, we need to assume the independence of distributed states across different runs of the experiment. Figure 1 further clarifies the set of assumptions that we make in this work, and compares it to the set of assumptions in the Bell test and the standard entanglement witnessing experiment. Such scenarios in which only a part of the experimental apparatus is assumed to be characterized and trusted are often called *semi-device-independent* [21].

For entanglement detection, we consider the common tool of entanglement witnessing [22]. This method is universal, because for every entangled state, including mixed states, one can find an entanglement witness that detects it, and efficient, because it does not require performing the state tomography [1]. As the main technical contribution of this work, we discuss and analyze the discard and assignment strategies in entanglement witnessing with untrusted detectors. We show that both of these approaches to dealing with imperfect detectors can be analyzed using semi-definite programming [23]. As an example, we apply our methods to two-qubit entanglement witnesses. Our results suggest that the critical detection efficiency of entanglement detection with untrusted detectors in the proposed semi-device-independent paradigm is significantly lower than that for Bell test experiments.

2. Preliminaries

We start by establishing notation and providing a few definitions required to present the results in the next sections. In this paper, we consider entanglement in bipartite systems, for which there is only one notion of separability and entanglement. Additionally, in our analysis, we consider qubit-qubit systems for the sake of simplicity. However, the results are directly generalizable to higher-dimensional systems, and we provide comments about this generalization whenever necessary. Finally, in this paper, we take all the observed efficiencies of all detectors to be the same and denote it by η .

We take the standard definition of *entanglement witness* as a linear Hermitian operator W , such that $\langle W \rangle_{\rho_s} := \text{Tr}[W\rho_s] \geq 0$ for all separable states ρ_s and $\langle W \rangle_{\rho} < 0$ for the entangled

state ρ under investigation. In the presence of inefficient detectors, it also becomes important how the witness W is measured in the experiment, the fact that was also pointed out in [17]. Typically, a witness W is decomposed as a sum of tensor products of local observables. In this work, we focus on two-qubit states for which the typical observables are the Pauli operators, i.e. we consider witnesses W of the form

$$W = w_{0,0} \mathbb{1} \otimes \mathbb{1} + \sum_{i=1}^3 w_{i,0} \sigma_i \otimes \mathbb{1} + \sum_{j=1}^3 w_{0,j} \mathbb{1} \otimes \sigma_j + \sum_{i,j=1}^3 w_{i,j} \sigma_i \otimes \sigma_j, \quad (1)$$

with $w_{i,j} \in \mathbb{R}$ being coefficients of the decomposition, and $\{\sigma_1, \sigma_2, \sigma_3\} = \{\sigma_x, \sigma_y, \sigma_z\}$ being the set of Pauli operators. For qudit systems, a possible set of observables are the Heisenberg–Weyl operators [24].

To evaluate the expectation value $\langle W \rangle_\rho$ in equation (1), we need to estimate each of the terms $\langle \sigma_i \otimes \sigma_j \rangle_\rho$ for which $w_{i,j} \neq 0$ for all $i, j \in \{1, 2, 3\}$, as well as the marginal terms $\langle \sigma_i \otimes \mathbb{1} \rangle_\rho$ for $i \in \{1, 2, 3\}$ and $\langle \mathbb{1} \otimes \sigma_j \rangle_\rho$ for $j \in \{1, 2, 3\}$. Let us denote the outcomes of the parties' measurements as '+' and '-', in which case the expectation values are calculated as

$$\langle \sigma_i \otimes \sigma_j \rangle_\rho = p(+, +|i, j) + p(-, -|i, j) - p(+, -|i, j) - p(-, +|i, j), \quad (2)$$

for $i, j \in \{1, 2, 3\}$, and

$$\begin{aligned} \langle \mathbb{1} \otimes \sigma_j \rangle_\rho &= p^B(+|j) - p^B(-|j), \\ \langle \sigma_i \otimes \mathbb{1} \rangle_\rho &= p^A(+|i) - p^A(-|i), \end{aligned} \quad (3)$$

otherwise. In the above, we used the superscript A and B to denote the marginal probabilities. The expectation values in equations (2), (3) are estimated from the respective frequencies of detectors' clicks. The key problem that we investigate in this work is how the no-click events affect the expectation value of W and, consequently, entanglement detection.

The literature that addresses the detection inefficiency problem, primarily in the context of the Bell test, describes two primary methods for handling no-click events [25]. In the first approach, referred to as the *discard strategy*, one simply ignores all the events where at least one of the detectors did not click (for estimation of joint probabilities). Mathematically, it means that the joint probabilities as well as marginal probabilities in equations (2), (3) are replaced by the probabilities, conditioned on the click events:

$$p(+, +|i, j) \mapsto p(+, +|i, j, c^A, c^B), \quad (4)$$

for all $i, j \in \{1, 2, 3\}$ and similarly for other outcomes. In the above, c^A and c^B denote the *events* of Alice's and Bob's detectors clicking. The marginal probabilities are mapped as

$$\begin{aligned} p^A(+|i) &\mapsto p^A(+|i, c^A), \\ p^B(+|j) &\mapsto p^B(+|j, c^B), \end{aligned} \quad (5)$$

for all $i, j \in \{1, 2, 3\}$. The above marginal probabilities depend only on the clicks events of single party's detector, because in this work we consider the situation in which expectation values in equation (3) are estimated in different runs of the experiment than the joint expectation values in equation (2). In other words, we treat each marginal term in equation (3)

as a separate measurement setting, just like the correlation terms in equation (2) for different i and j .

The same mapping of probabilities is performed when one assumes the fair sampling. However, in case of the discard strategy (in Bell tests) one takes into account the effect of losses by increasing the local bound of a Bell inequality [25, 26]. As we show in the next section, this also applies to entanglement witnessing: for imperfect detectors, the expectation value of a witness with respect to separable states can take negative values. However, there is still a range of values of η for which entanglement detection is possible. A similar observation has been made in [17], which was the first to consider the problem of detection loophole in entanglement witnessing.

The second common approach of dealing with detection inefficiencies in Bell tests is the *assignment strategy* method, sometimes also called binning. There, for every no-click event, one assigns one of the outcomes, in our case ‘+’ or ‘-’, either randomly or deterministically. Mathematically, it means that the evaluated probabilities are mapped as

$$p(+, +|i, j) \mapsto \eta^2 p(+, +|i, j, c^A, c^B) + \eta(1 - \eta)p(+, +|i, j, c^A, \neg c^B) + (1 - \eta)\eta p(+, +|i, j, \neg c^A, c^B) + (1 - \eta)^2 p(+, +|i, j, \neg c^A, \neg c^B), \quad (6)$$

for all $i, j \in \{1, 2, 3\}$, and similarly for the other outcomes. In the above, $\neg c^A, \neg c^B$ denote the no-click events. The marginal probabilities are mapped as

$$\begin{aligned} p^A(+|i) &\mapsto \eta p^A(+|i, c^A) + (1 - \eta)p^A(+|i, \neg c^A), \\ p^B(+|j) &\mapsto \eta p^B(+|j, c^B) + (1 - \eta)p^B(+|j, \neg c^B), \end{aligned} \quad (7)$$

for all $i, j \in \{1, 2, 3\}$.

A particular assignment is determined by the form of the probabilities, conditioned on the events $\neg c^A$ and $\neg c^B$. For instance, if Alice chooses to always output ‘+’ if her detector does not click, then we have that $p(+, +|i, j, \neg c^A, c^B) = p^B(+|j, c^B)$ and $p(-, +|i, j, \neg c^A, c^B) = 0$, etc. Since for an entanglement witness of the form in equation (1) we need to estimate the expectation values rather than probabilities, it is more convenient to define an assignment as follows

$$\begin{aligned} a_i &:= p^A(+|i, \neg c^A) - p^A(-|i, \neg c^A), \\ b_j &:= p^B(+|j, \neg c^B) - p^B(-|j, \neg c^B), \end{aligned} \quad (8)$$

for $i, j \in \{1, 2, 3\}$.

In Bell tests, the assignment strategy leads to lowering the maximally achievable quantum value of the Bell inequality, but does not increase the local bound [25]. As we show in the next section, this is not true in general for entanglement witnessing, and some local assignments can lead to negative values.

We demonstrate our findings on the example of pure entangled two-qubit states, for which we use a notation

$$|\Psi_\theta\rangle := \sin(\theta)|0, 0\rangle + \cos(\theta)|1, 1\rangle, \quad (9)$$

with $\theta \in (0, \frac{\pi}{4}]$. The corresponding witness for $|\Psi_\theta\rangle$ reads

$$W_\theta := \cos(\theta)^2 \mathbb{1} \otimes \mathbb{1} - |\Psi_\theta\rangle\langle\Psi_\theta|. \quad (10)$$

The non-zero coefficients of the decomposition of W_θ into Pauli observables are $w_{0,0} = \frac{1}{2} \cos(2\theta) + \frac{1}{4}$, $w_{0,3} = w_{3,0} = \frac{1}{4} \cos(2\theta)$, $w_{1,1} = -w_{2,2} = -\frac{1}{4} \sin(2\theta)$, and $w_{3,3} = -\frac{1}{4}$. We refer to $|\Psi_{\frac{\pi}{4}}\rangle$ and $W_{\frac{\pi}{4}}$ as the Bell state and the Bell witness, respectively.

3. Results

We start with a general formulation of the detection efficiency problem in entanglement witnessing. Similarly to the situation in Bell tests, we cannot rule out the possibility that a *hidden variable* λ gains control over the detectors and correlates their efficiencies with the source of quantum states. Mathematically, it means that the observed joint probability distribution, e.g. for the outcome $+, +$, decomposes as

$$\begin{aligned} p(+, + | i, j, c^A, c^B) &= \sum_{\lambda \in \Lambda} p(+, +, \lambda | i, j, c^A, c^B) = \sum_{\lambda \in \Lambda} \frac{p(+, +, \lambda, c^A, c^B | i, j)}{p(c^A | i) p(c^B | j)} \\ &= \frac{1}{\eta^2} \sum_{\lambda \in \Lambda} p(+, +, c^A, c^B | i, j, \lambda) p(\lambda) \\ &= \frac{1}{\eta^2} \sum_{\lambda \in \Lambda} p(+, + | i, j, c^A, c^B, \lambda) p(c^A | i, \lambda) p(c^B | j, \lambda) p(\lambda), \end{aligned} \quad (11)$$

where we used the fact that the click events can be correlated only due to the hidden variable λ . The key observation here is that the response functions of click events, $p(c^A | i, \lambda)$ and $p(c^B | j, \lambda)$, may depend on the measurement settings i and j . At the same time, since the entanglement source may also be controlled by the hidden variable λ , the states ρ_λ , with respect to which the outcome probabilities $p(+, + | i, j, c^A, c^B, \lambda)$ are calculated, may also vary with λ . In what follows, we show how to account for such situations in both, the discard and the assignment strategies.

In this work, we focus on the situation in which the detection events are uncorrelated and independent of the measurement choices with respect to the observed probability distribution, i.e. $p(c^A, c^B | i, j) = p(c^A | i) p(c^B | j) = \eta^2$, which can be verified experimentally. We find this case particularly interesting because one could mistakenly believe that the click events of the parties' detectors are uncorrelated and thus invoke the fair sampling assumption. At the same time, our approach can be easily modified to accommodate the other case $p(c^A, c^B | i, j) \neq p(c^A | i) p(c^B | j)$. In particular, one simply needs to substitute every term η^2 in the formulations that follow with a corresponding joint probability $p(c^A, c^B | i, j)$. To avoid overly complicated mathematical statements, we avoid describing this general case in the current paper.

3.1. Discard strategy

In this section, we discuss two main questions regarding the discard strategy: given an entanglement witness, what is the minimal value that it can take for separable states for a given detection efficiency η , and what is the critical detection efficiency η_{crit} for which no entanglement detection is possible? We show below how to formulate these questions as optimization problems, which can be cast as semidefinite programming problems (SDPs) [23].

Looking at the expansion of the observed probabilities in equation (11), we can realize that the probabilities of click events, $p(c^A | i, \lambda)$ and $p(c^B | j, \lambda)$, without loss of generality can

be taken to be deterministic, i.e. 0 or 1, by considering a sufficiently large set Λ . This is a standard technique in the literature on hidden variables [27, 28]. As a next step, we define sets Λ_i^A and Λ_j^B as

$$\Lambda_i^A = \left\{ \lambda \in \Lambda \mid p(c^A|i, \lambda) = 1 \right\}, \quad \Lambda_j^B = \left\{ \lambda \in \Lambda \mid p(c^B|j, \lambda) = 1 \right\}, \quad (12)$$

for $i, j \in \{1, 2, 3\}$. We also consider unnormalized density operators ρ_λ , such that $\text{Tr}[\rho_\lambda] = p(\lambda)$, and $\frac{\rho_\lambda}{p(\lambda)}$ is the state in which the particles are prepared for the value λ of the hidden variable. This allows us to write the mapped expectation values $\langle \sigma_i \otimes \sigma_j \rangle$ simply as

$$\langle \sigma_i \otimes \sigma_j \rangle \mapsto \frac{1}{\eta^2} \sum_{\lambda \in \Lambda_i^A \cap \Lambda_j^B} \langle \sigma_i \otimes \sigma_j \rangle_{\rho_\lambda}, \quad (13)$$

and the marginal expectation values as

$$\begin{aligned} \langle \mathbb{1} \otimes \sigma_j \rangle &\mapsto \frac{1}{\eta} \sum_{\lambda \in \Lambda_j^B} \langle \mathbb{1} \otimes \sigma_j \rangle_{\rho_\lambda}, \\ \langle \sigma_i \otimes \mathbb{1} \rangle &\mapsto \frac{1}{\eta} \sum_{\lambda \in \Lambda_i^A} \langle \sigma_i \otimes \mathbb{1} \rangle_{\rho_\lambda}, \end{aligned} \quad (14)$$

for $i, j \in \{1, 2, 3\}$. We can now formulate the problem of finding the minimal value of W as the following SDP,

$$\begin{aligned} \min_{\rho_\lambda} \quad & w_{0,0} + \frac{1}{\eta} \sum_{i=1}^3 w_{i,0} \sum_{\lambda \in \Lambda_i^A} \langle \sigma_i \otimes \mathbb{1} \rangle_{\rho_\lambda} + \frac{1}{\eta} \sum_{j=1}^3 w_{0,j} \sum_{\lambda \in \Lambda_j^B} \langle \mathbb{1} \otimes \sigma_j \rangle_{\rho_\lambda} \\ & + \frac{1}{\eta^2} \sum_{i,j=1}^3 w_{i,j} \sum_{\lambda \in \Lambda_i^A \cap \Lambda_j^B} \langle \sigma_i \otimes \sigma_j \rangle_{\rho_\lambda}, \\ \text{s.t.} \quad & \sum_{\lambda \in \Lambda_i^A} \text{Tr}[\rho_\lambda] = \sum_{\lambda \in \Lambda_j^B} \text{Tr}[\rho_\lambda] = \eta, \quad \sum_{\lambda \in \Lambda_i^A \cap \Lambda_j^B} \text{Tr}[\rho_\lambda] = \eta^2, \quad \forall i, j \in \{1, 2, 3\}, \end{aligned} \quad (15a)$$

$$\rho_\lambda \geq 0, \quad \rho_\lambda^{\text{T}^A} \geq 0, \quad \forall \lambda \in \Lambda, \quad (15b)$$

$$\rho_{\text{observed}} \geq 0, \quad \sum_{\lambda \in \Lambda} \text{Tr}[\rho_\lambda] = 1. \quad (15c)$$

In the above SDP, we have introduced an operator ρ_{observed} , which corresponds to the physically observed state, and is defined as

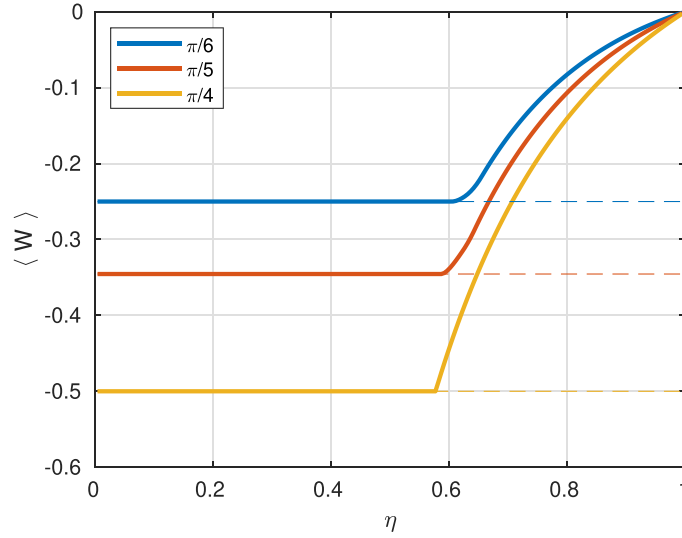


Figure 2. Minimal values that the witness $\langle W_\theta \rangle$ can take in the discard strategy as a function of detection efficiency η (solid lines), and the corresponding values of the witness $\langle W_\theta \rangle$ for the entangled state $|\Psi_\theta\rangle$ (dashed lines).

$$\begin{aligned} \rho_{\text{observed}} := & \frac{\mathbb{1} \otimes \mathbb{1}}{4} + \frac{1}{\eta} \sum_{i=1}^3 \left(\sum_{\lambda \in \Lambda_i^A} \langle \sigma_i \otimes \mathbb{1} \rangle_{\rho_\lambda} \right) \frac{\sigma_i \otimes \mathbb{1}}{4} + \frac{1}{\eta} \sum_{j=1}^3 \left(\sum_{\lambda \in \Lambda_j^B} \langle \mathbb{1} \otimes \sigma_j \rangle_{\rho_\lambda} \right) \frac{\mathbb{1} \otimes \sigma_j}{4} \\ & + \frac{1}{\eta^2} \sum_{i,j=1}^3 \left(\sum_{\lambda \in \Lambda_i^A \cap \Lambda_j^B} \langle \sigma_i \otimes \sigma_j \rangle_{\rho_\lambda} \right) \frac{\sigma_i \otimes \sigma_j}{4}. \end{aligned} \quad (16)$$

The condition $\rho_{\text{observed}} \geq 0$ in equation (15c) requests that the observed statistics corresponds to some physical state, which otherwise could lead to the parties realizing that the behavior of their detectors is malicious. Note that the same holds for qudit system if the Pauli observables in equation (16) are replaced by their higher-dimensional generalizations, e.g. Heisenberg-Weyl observables [24]. Although the objective function of the SDP in equation (15) could also be written as $\langle W \rangle_{\rho_{\text{observed}}}$, we found that it is more instructive to give a full expansion of the witness in equation (15). Alternatively to defining the state ρ_{observed} in equation (16), one can request an existence of some density operator, such that the experimentally observed expectation values can be explained by this state. This can be easier to implement, e.g. in the situation when the decomposition of the witness in equation (1) features non-orthogonal observables.

The conditions in equation (15a) ensure that the events of photons being detected by Alice’s and Bob’s devices appear to be uncorrelated and occur with the same probability η for all the measurement settings. The conditions in equation (15b) ensure that the operators ρ_λ are positive semidefinite and separable, due to the positive-partial-transpose (PPT) criterion [1]. For the higher-dimensional case, the separability condition can be enforced by a hierarchy of SDP relaxations [29].

In figure 2 we demonstrate the solution of the SDP in equation (15) for the witness W_θ in equation (10) for $\theta \in \{\frac{\pi}{6}, \frac{\pi}{5}, \frac{\pi}{4}\}$. The values of η for which $\langle W_\theta \rangle$ reaches its minimal value, shown by the dashed lines in figure 2, is the critical detection efficiency. In appendix A, we give an explicit solution for the Bell witness, and show that in this case the critical detection

efficiency is $\frac{1}{\sqrt{3}}$. This value is significantly smaller than $\sqrt{\frac{2}{3}}$, which is the critical detection efficiency of detecting the Bell state device-independently in a Bell experiment [30].

3.2. Assignment strategy

In this section, we discuss the assignment strategy to entanglement witnessing with untrusted detectors. As stated in the introduction, in Bell tests, the assignment strategy reduces the maximal possible violation of a Bell inequality while preserving the local hidden variable bound [26]. Additionally, there is no restriction on the particular choice of the assignment as long as it is performed locally by the parties. This, however, does not translate to the case of entanglement witnessing, as we show below.

Let (a_1, a_2, a_3) and (b_1, b_2, b_3) , as defined by equation (8), be assignments chosen by the parties. Let us first assume that the behavior of the detectors is *honest*, i.e. whenever the detectors click, the probabilities of outcomes, e.g. $p(+, +|i, j, c^A, c^B)$, correspond to a single state ρ which is not in the control of the hidden variable. In that case, it is easy to observe that the transformation of probabilities due to the assignment strategy in equation (6) can be equivalently captured by the following transformation of state ρ ,

$$\rho \mapsto \eta^2 \rho + \eta(1 - \eta) \rho^A \otimes \beta + (1 - \eta) \eta \alpha \otimes \rho^B + (1 - \eta)^2 \alpha \otimes \beta, \tag{17}$$

where ρ^A and ρ^B are the reduced states of Alice's and Bob's subsystems, and we have introduced the notation

$$\alpha := \frac{\mathbb{1}}{2} + \frac{1}{2} \sum_{i=1}^3 a_i \sigma_i, \quad \beta := \frac{\mathbb{1}}{2} + \frac{1}{2} \sum_{i=1}^3 b_i \sigma_i. \tag{18}$$

From the form of the state in equation (17), it is clear that as long as the initial state ρ is separable and the operators α and β in equation (18) are positive semidefinite, the transformed state operator is also positive semidefinite and separable. Thus, we obtain a sufficient condition on the assignments for which no false detection of entanglement occurs:

$$\sum_{i=1}^3 a_i^2 \leq 1, \quad \sum_{i=1}^3 b_i^2 \leq 1. \tag{19}$$

Note that, a common deterministic assignment $p(+|i, -c^A) = 1$ for Bell tests, i.e. $a_i = 1 \forall i \in \{1, 2, 3\}$, does not satisfy the above constraint and can lead to a false detection of entanglement. In appendix B, we show that if the detection efficiencies of Alice's and Bob's detectors can be different, then there are values of them for which the above condition is also necessary.

As an example of a good assignment, let us consider the Bell witness $W_{\frac{\pi}{4}}$ and the Bell state $\rho_{\frac{\pi}{4}} = |\Psi_{\frac{\pi}{4}}\rangle\langle\Psi_{\frac{\pi}{4}}|$. From the transformation in equation (17), we find that the expectation value of the witness equals to

$$\langle W_{\frac{\pi}{4}} \rangle_{\rho_{\frac{\pi}{4}}} = \frac{1}{2} \left(1 - \eta^2 - \eta - (1 - \eta)^2 \text{Tr}[\alpha^\top \beta] \right). \tag{20}$$

It is clear, that a good assignment corresponds to taking α and β rank-1 and satisfying $\alpha^\top = \beta$. This can be achieved, e.g. by $(a_1, a_2, a_3) = (b_1, b_2, b_3) = (1, 0, 0)$. One can also see from the above that entanglement of ρ can be detected for $\eta > \frac{1}{2}$.

Now, we look at the general case of potentially malicious behavior of the detectors. This, in particular, means that the observed probabilities of outcomes, conditioned on click events, are given by equation (11). We start with the same argument that by considering a large enough set

Λ , the probabilities of click events can be taken to be either 0 or 1. For the assignment strategy we would need to introduce an extra notation for subsets of Λ ,

$$\bar{\Lambda}_i^A = \left\{ \lambda \in \Lambda \mid p(c^A|i, \lambda) = 0 \right\}, \quad \bar{\Lambda}_j^B = \left\{ \lambda \in \Lambda \mid p(c^B|j, \lambda) = 0 \right\}, \quad (21)$$

which are just the complements of the sets Λ_i^A and Λ_j^B . Using this notation, we can write the observed expectation values as

$$\begin{aligned} \langle \sigma_i \otimes \sigma_j \rangle &\mapsto \sum_{\lambda \in \Lambda_i^A \cap \Lambda_j^B} \langle \sigma_i \otimes \sigma_j \rangle_{\rho_\lambda} + \sum_{\lambda \in \Lambda_i^A \cap \bar{\Lambda}_j^B} \langle \sigma_i \otimes \mathbb{1} \rangle_{\rho_\lambda} b_j \\ &+ \sum_{\lambda \in \bar{\Lambda}_i^A \cap \Lambda_j^B} \langle \mathbb{1} \otimes \sigma_j \rangle_{\rho_\lambda} a_i + \sum_{\lambda \in \bar{\Lambda}_i^A \cap \bar{\Lambda}_j^B} \text{Tr}[\rho_\lambda] a_i b_j, \end{aligned} \quad (22)$$

for all pairs of $i, j \in \{1, 2, 3\}$. The marginal expectation values are mapped as follows

$$\begin{aligned} \langle \sigma_i \otimes \mathbb{1} \rangle &\mapsto \sum_{\lambda \in \Lambda_i^A} \langle \sigma_i \otimes \mathbb{1} \rangle_{\rho_\lambda} + \sum_{\lambda \in \bar{\Lambda}_i^A} \text{Tr}[\rho_\lambda] a_i, \\ \langle \mathbb{1} \otimes \sigma_j \rangle &\mapsto \sum_{\lambda \in \Lambda_j^B} \langle \mathbb{1} \otimes \sigma_j \rangle_{\rho_\lambda} + \sum_{\lambda \in \bar{\Lambda}_j^B} \text{Tr}[\rho_\lambda] b_j. \end{aligned} \quad (23)$$

We now formulate an SDP that determines the minimal value of a witness for separable states given assignments (a_1, a_2, a_3) and (b_1, b_2, b_3) and detection efficiency η .

$$\begin{aligned} \min_{\rho_\lambda} \quad & w_{0,0} + \sum_{i=1}^3 w_{i,0} \left(\sum_{\lambda \in \Lambda_i^A} \langle \sigma_i \otimes \mathbb{1} \rangle_{\rho_\lambda} + \sum_{\lambda \in \bar{\Lambda}_i^A} \text{Tr}[\rho_\lambda] a_i \right) + \sum_{j=1}^3 w_{0,j} \left(\sum_{\lambda \in \Lambda_j^B} \langle \mathbb{1} \otimes \sigma_j \rangle_{\rho_\lambda} \right. \\ & \left. + \sum_{\lambda \in \bar{\Lambda}_j^B} \text{Tr}[\rho_\lambda] b_j \right) + \sum_{i,j=1}^3 w_{i,j} \left(\sum_{\lambda \in \Lambda_i^A \cap \Lambda_j^B} \langle \sigma_i \otimes \sigma_j \rangle_{\rho_\lambda} + \sum_{\lambda \in \Lambda_i^A \cap \bar{\Lambda}_j^B} \langle \sigma_i \otimes \mathbb{1} \rangle_{\rho_\lambda} b_j \right. \\ & \left. + \sum_{\lambda \in \bar{\Lambda}_i^A \cap \Lambda_j^B} \langle \mathbb{1} \otimes \sigma_j \rangle_{\rho_\lambda} a_i + \sum_{\lambda \in \bar{\Lambda}_i^A \cap \bar{\Lambda}_j^B} \text{Tr}[\rho_\lambda] a_i b_j \right) \\ \text{s.t.} \quad & \sum_{\lambda \in \Lambda_i^A} \text{Tr}[\rho_\lambda] = \sum_{\lambda \in \Lambda_j^B} \text{Tr}[\rho_\lambda] = \eta, \quad \sum_{\lambda \in \Lambda_i^A \cap \Lambda_j^B} \text{Tr}[\rho_\lambda] = \eta^2, \quad \forall i, j \in \{1, 2, 3\}, \end{aligned} \quad (24a)$$

$$\rho_\lambda \geq 0, \quad \rho_\lambda^{\text{T}^A} \geq 0, \quad \forall \lambda \in \Lambda, \quad (24b)$$

$$\rho_{\text{observed}} \geq 0, \quad \sum_{\lambda \in \Lambda} \text{Tr}[\rho_\lambda] = 1, \quad (24c)$$

$$\begin{aligned} \sum_{\lambda \in \Lambda_i^A \cap \bar{\Lambda}_j^B} \langle \sigma_i \otimes \mathbb{1} \rangle_{\rho_\lambda} &= (1 - \eta) \sum_{\lambda \in \Lambda_i^A} \langle \sigma_i \otimes \mathbb{1} \rangle_{\rho_\lambda}, \\ \sum_{\lambda \in \bar{\Lambda}_i^A \cap \Lambda_j^B} \langle \mathbb{1} \otimes \sigma_j \rangle_{\rho_\lambda} &= (1 - \eta) \sum_{\lambda \in \Lambda_j^B} \langle \mathbb{1} \otimes \sigma_j \rangle_{\rho_\lambda} \quad \forall i, j \in \{1, 2, 3\}. \end{aligned} \quad (24d)$$

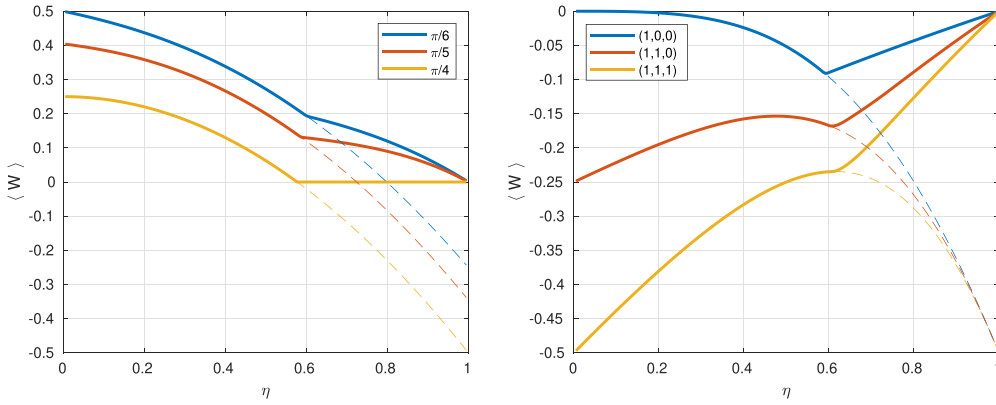


Figure 3. Left: Minimal values of the witness $\langle W_\theta \rangle$ in the assignment strategy with $a_i = 0$ and $b_j = 0, \forall i, j, \in \{1, 2, 3\}$ as a function of detection efficiency η (solid lines) and the corresponding values of the witness for the entangled state $|\Psi_\theta\rangle$ (dashed lines). Right: Minimal values of the Bell witness for the assignments $(a_1, a_2, a_3) \in \{(1, 0, 0), (1, 1, 0), (1, 1, 1)\}$ and $b_i = (-1)^{i+1} a_i \forall i$ (solid lines), and the corresponding minimal values of the witness over entangled states (dashed lines).

where ρ_{observed} is defined in equation (16). As in the case of the SDP for the discard strategy, the constraints in equation (24a) guarantee that the observed probabilities of click events are uncorrelated for Alice and Bob and are independent of their measurement settings. The conditions on ρ_λ in equation (24b) and on ρ_{observed} in equation (24c) are also motivated analogously to the discard strategy case. Finally, the constraints in equation (24d) guarantee that the observed marginal state of Alice is independent of whether Bob detectors click or not, and analogously that Bob’s marginal is independent of the behavior of Alice’s detector.

In figure 3(left) we demonstrate the solution to the SDP in equation (24) for the witness W_θ and the assignment $(a_1, a_2, a_3) = (b_1, b_2, b_3) = (0, 0, 0)$. This particular assignment preserves the property $\langle W \rangle_{\rho_s} \geq 0$ for all separable states. In figure 3(left) by the dashed lines we depict values of the witness W_θ with respect to the corresponding state $|\Psi_\theta\rangle$. These values increase as η decreases due to the assignment strategy. The points where the dashed lines intersect the solid lines are the critical detection efficiencies for the chosen assignment.

In figure 3(right) we also compare different assignments for the Bell witness. One can see that the property of $\langle W \rangle_{\rho_s} \geq 0$ is not preserved for any of the selected assignments. At the same time, one can still detect entanglement if the expectation value with respect to an entangled state is lower than the calculated bound on $\langle W_{\frac{\pi}{4}} \rangle_{\rho_s}$ due to untrusted detectors, as we demonstrate in figure 3. Notably, the minimal expectation values that the witnesses can take with respect to entangled states (dashed lines) do not correspond to the Bell state.

The critical detection efficiency for the Bell witness in this calculation is again $\eta = \frac{1}{\sqrt{3}}$ as for the discard strategy. In appendix C we give an explicit solution to the SDP in equation (24) for the Bell witness. The value of $\langle W_{\frac{\pi}{4}} \rangle_{\rho_{\frac{\pi}{4}}}$ with respect to the Bell state can be calculated from equation (20) by taking $\alpha = \beta = \frac{1}{2}$, and is equal to $\frac{1}{4} - \frac{3}{4}\eta^2$.

3.3. Visibility analysis

When discussing detection efficiency, one is often focused on the critical values that must be exceeded in order to observe a violation of a Bell inequality, or in our case an entanglement

witness. At the same time, these theoretical limits must be adjusted in experiments due to inevitable noise. The relevant figure of merit in this discussion is the visibility, which we define here for a witness W as follows

$$v_\rho = \min \left[v \left| v \langle W \rangle_\rho + (1 - v) \langle W \rangle_{\frac{\mathbb{1} \otimes \mathbb{1}}{4}} \leq \langle W \rangle_\lambda \right. \right], \quad (25)$$

where $\langle W \rangle_{\frac{\mathbb{1} \otimes \mathbb{1}}{4}}$ is the value of the witness W with respect to the maximally mixed state $\frac{\mathbb{1} \otimes \mathbb{1}}{4}$, and $\langle W \rangle_\lambda$ is the minimal value attainable by malicious strategies, in which the detectors can be controlled by a hidden variable λ . Visibility, as defined by equation (25), is directly connected to white noise robustness, but has the opposite interpretation. Namely, values of visibility close to 1 mean that little amount of noise can be tolerated in the experiment.

The definition in equation (25) is applicable to both, the discard and the assignment strategy. For the former, $\langle W \rangle_\rho$ is independent of η and $\langle W \rangle_\lambda$ gets more negative as η decreases, as shown in figure 2. For the latter, $\langle W \rangle_\rho$ increases as η decreases, while $\langle W \rangle_\lambda$ remains zero for η above the critical value, as shown in figure 3. In both situations, for the critical value of η , the visibility v_ρ is equal to 1 for the state ρ giving the minimal value of the witness W . For η above critical, some amount of white noise can be tolerated, resulting in the required visibility values going below 1. Equivalently, one can say that for η above critical, one can observe loophole-free witnessing of some mixed states, e.g. Werner states [31]. Visibility analysis also shows that in the regime of high detection efficiencies when one is able to perform loophole-free Bell test, there is still an advantage of using our approach if one is willing to put trust in some parts of the measurement devices.

4. Conclusions and discussions

In this paper, we discuss the problem of untrusted detectors in photonic experiments of entanglement detection. Even though the role of untrusted detectors is much more crucial for cryptographic applications and Bell tests, in this work we argue that malicious, or non-ideal, behavior of photodetectors can lead to false positive claims in simpler experiments of entanglement witnessing. We then analyze in detail the two main approaches to detection losses, namely the discard and the assignment strategies, and show that this analysis for a given entanglement witness can in both cases be cast as a semidefinite programming optimization problem. As an example, we analyze critical detection efficiencies for entanglement witnesses of pure two-qubit states. In particular, we show that the critical detection efficiency corresponding to the Bell state is $\frac{1}{\sqrt{3}}$ for the discard strategy. For the assignment strategy we could show that the same value of $\frac{1}{\sqrt{3}}$ can be attained, but the question whether this value can be reduced further by a suitable choice of an assignment is open.

Throughout the paper, we commented on generalization of our approach to higher-dimensional systems. The only non-trivial generalization is the replacement of the PPT criterion by the hierarchy of SDP conditions of [29] in both optimization problems in equations (15), (24). Of course, in practice, one can impose the conditions only up to a certain level of the SDP hierarchy. The resulting SDPs in equations (15), (24) in that case produce lower bounds on the value that a witness can obtain due to malicious behavior of the detectors. In turn, one obtains upper bounds on the critical detection efficiency, which means that our approach can still guarantee that the detection loophole is closed if those values are exceeded in the experiment.

It is worth to point out a related study on ‘squashing operations’ in QKD and entanglement detection [32–34]. In our paper, we concentrate on the analysis of measurement data post-processing and how this post-processing can influence the conclusions drawn about entanglement of the measured state. In this manner, our approach is agnostic to the specific physical process of registering click and no-click events. On the other hand, when studying ‘squashing operations,’ one examines how photon counting is translated into a measurement of the desired degree of freedom, such as polarization.

On a more fundamental level, our work introduces a new type of semi-device-independent paradigm, the one in which only the detection part of measurement process is untrusted, while the measurement setting, e.g. the measurement basis, is assumed to be characterized. This is particularly relevant for the standard entanglement-based QKD, where the detectors are usually assumed to be fair. This assumption is difficult to justify because the most widely documented attacks against practical QKD are the detector blinding attacks, which boil down to gaining control of the detectors in the parties’ devices [35]. Additionally, dopant-level hardware Trojan attacks were demonstrated, which allow the manufacturer to place a malware in electronics, such as detector controllers, in a way that is very difficult to detect by the user [36, 37]. We therefore believe that it is interesting to analyze security of QKD scheme in the introduced paradigm of untrusted detectors. As an additional motivation for this further work, one can notice that requirement on the detection efficiency reported in the current work is significantly lower than that in Bell test for the case of the Bell state.

Data availability statement

No new data were created or analysed in this study.

Acknowledgment

We thank Dagmar Bruß for interesting discussions and Otfried Gühne for providing comments on the first version of the paper. This research was made possible by funding from QuantERA, an ERA-Net cofund in Quantum Technologies (www.quantera.eu) under project eDICT. We acknowledge the support by the Foundation for Polish Science (IRAP project, ICTQT, Contract No. MAB/2018/5, co-financed by EU within Smart Growth Operational Programme). This research was funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation, Project Nos. 441423094 and 236615297 - SFB 1119), and under Germany’s Excellence Strategy—Cluster of Excellence Matter and Light for Quantum Computing (ML4Q) EXC 2004/1–390534769.

Appendix A. Discard strategy for the Bell witness

Here we provide an explicit solution to the SDP in equation (15) for the Bell witness $W_{\frac{\pi}{4}}$. This solution, more precisely the minimal value that $\langle W_{\frac{\pi}{4}} \rangle$ can take for a given η , is shown in figure 2.

To describe the solution, i.e. to specify the operators ρ_{λ} for each value of η , we need to introduce a few notations. Let Λ be the set of all binary strings of length 6. Each value of λ , specified by a string, specifies the probabilities of detectors’ clicks with the first three bits corresponding to the measurement settings of Alice, and the second three bits corresponding to the measurement settings of Bob. For example, for $\lambda = (1, 0, 0, 0, 1, 0)$, we have that

$p(c^A|1, \lambda) = 1$ and $p(c^B|2, \lambda) = 1$, while the other probabilities are zero. Clearly, this choice of the alphabet of λ is sufficient for the problem in case of three measurement settings per party.

Let us define the following states

$$\begin{aligned} \rho_{x,x} &:= \frac{1}{2} (|+, +\rangle\langle +, +| + |-, -\rangle\langle -, -|), \\ \rho_{y,y} &:= \frac{1}{2} (|+i, -i\rangle\langle +i, -i| + |-i, +i\rangle\langle -i, +i|), \\ \rho_{z,z} &:= \frac{1}{2} (|0, 0\rangle\langle 0, 0| + |1, 1\rangle\langle 1, 1|), \end{aligned} \tag{A.1}$$

which are separable states with the property that $\langle \sigma_1 \otimes \sigma_1 \rangle_{\rho_{x,x}} = \langle \sigma_3 \otimes \sigma_3 \rangle_{\rho_{z,z}} = 1$, and $\langle \sigma_1 \otimes \sigma_1 \rangle_{\rho_{y,y}} = -1$. Here, we used the notation $|+i\rangle$ and $|-i\rangle$ to denote the $+1$ and -1 eigenstates of σ_2 . In terms of these states, the operators ρ_λ in our solution are specified to be the following

$$\begin{aligned} \rho_{(0,0,0,0,0)} &= p_0 \frac{\mathbb{1} \otimes \mathbb{1}}{4}, \quad \rho_{(1,1,1,1,1)} = p_1 \frac{1}{3} (\rho_{x,x} + \rho_{y,y} + \rho_{z,z}), \\ \rho_{(1,0,0,1,0,0)} &= \rho_{(1,0,1,1,0,0)} = \rho_{(1,1,0,1,0,1)} = p_2 \rho_{x,x}, \quad \rho_{(1,0,0,1,1,1)} = \rho_{(1,1,1,1,0,0)} = p_3 \rho_{x,x}, \\ \rho_{(0,1,0,0,1,0)} &= \rho_{(0,1,1,1,1,0)} = \rho_{(1,1,0,0,1,1)} = p_2 \rho_{y,y}, \quad \rho_{(0,1,0,1,1,1)} = \rho_{(1,1,1,0,1,0)} = p_3 \rho_{y,y}, \\ \rho_{(0,0,1,0,0,1)} &= \rho_{(0,1,1,1,0,1)} = \rho_{(1,0,1,0,1,1)} = p_2 \rho_{z,z}, \quad \rho_{(0,0,1,1,1,1)} = \rho_{(1,1,1,0,0,1)} = p_3 \rho_{z,z}, \\ \rho_{(0,0,0,0,0,1)} &= \rho_{(0,0,0,0,1,0)} = \rho_{(0,0,0,1,0,0)} = \rho_{(0,0,1,0,0,0)} = \rho_{(0,1,0,0,0,0)} = \rho_{(1,0,0,0,0,0)} \\ &= p_4 \frac{\mathbb{1} \otimes \mathbb{1}}{4}, \end{aligned} \tag{A.2}$$

where the parameters $p_i \in \mathbb{R}$, $i \in \{0, 1, 2, 3, 4\}$ will be specified later. The rest of the operators ρ_λ are taken to be zero-trace.

The objective function of the SDP in equation (15) can be calculated to be

$$\begin{aligned} &\frac{1}{4} - \frac{1}{4\eta^2} \left(\sum_{\lambda \in \Lambda_1^A \cap \Lambda_1^B} \langle \sigma_1 \otimes \sigma_1 \rangle_{\rho_\lambda} - \sum_{\lambda \in \Lambda_2^A \cap \Lambda_2^B} \langle \sigma_2 \otimes \sigma_2 \rangle_{\rho_\lambda} + \sum_{\lambda \in \Lambda_3^A \cap \Lambda_3^B} \langle \sigma_3 \otimes \sigma_3 \rangle_{\rho_\lambda} \right) \\ &= \frac{1}{4} - \frac{1}{4\eta^2} (p_1 + 9p_2 + 6p_3), \end{aligned} \tag{A.3}$$

while the constraints in equation (15) correspond to

$$\begin{aligned} p_1 + 5p_2 + 4p_3 + p_4 &= \eta, \\ p_1 + 3p_2 + 2p_3 &= \eta^2, \\ p_0 + p_1 + 9p_2 + 6p_3 + 6p_4 &= 1. \end{aligned} \tag{A.4}$$

The observed state in equation (16) can be easily found to be

$$\begin{aligned} \rho_{\text{observed}} &= \frac{\mathbb{1} \otimes \mathbb{1}}{4} + \frac{1}{4\eta^2} \left(\frac{p_1}{3} + 3p_2 + 2p_3 \right) (\sigma_1 \otimes \sigma_1 - \sigma_2 \otimes \sigma_2 + \sigma_3 \otimes \sigma_3) \\ &= \frac{\mathbb{1} \otimes \mathbb{1}}{4} \left(1 - \frac{p_1}{3} + 3p_2 + 2p_3 \right) + \frac{1}{\eta^2} \left(\frac{p_1}{3} + 3p_2 + 2p_3 \right) |\Psi_{\frac{\pi}{4}}\rangle\langle\Psi_{\frac{\pi}{4}}|. \end{aligned} \tag{A.5}$$

From the above expression, it is clear that as long as $0 \leq \frac{p_1}{3} + 3p_2 + 2p_3 \leq \eta^2$, the above density operator is positive semidefinite, and since this constraint is implied by equation (A.4), these are the only constraints associated with the SDP.

Now, we can specify our solution to the original optimization problem in terms of the coefficients $\{p_i\}_{i=0}^4$. For the case of $\eta > \frac{1}{\sqrt{3}}$, the minimal value which can be attained is $\frac{1}{4} - \frac{1}{4\eta^2}$, which is also clear from the expression in equation (A.3). This is achieved for the following values of the parameters,

$$p_0 = p_4 = 0, p_1 = \frac{3\eta^2 - 1}{2}, p_2 = \frac{(1 - \eta)^2}{2}, p_3 = \frac{(1 - \eta)(2\eta - 1)}{2}. \quad (\text{A.6})$$

For the case of $\eta \leq \frac{1}{\sqrt{3}}$, the minimal value $-\frac{1}{2}$ can be reached. The corresponding values of the parameters are $p_1 = 0$ and

$$\begin{aligned} p_0 &= (1 - 3\eta)^2, p_2 = 0, p_3 = \frac{\eta^2}{2}, p_4 = \eta - 2\eta^2, \quad \text{for } \eta \leq \frac{1}{3}, \\ p_0 &= 0, p_2 = \frac{(1 - 3\eta)^2}{6}, p_3 = \frac{6\eta - 1 - 7\eta^2}{4}, p_4 = \frac{1 - 3\eta^2}{6}, \quad \text{for } \eta \in \left(\frac{1}{3}, \frac{1}{\sqrt{3}}\right]. \end{aligned} \quad (\text{A.7})$$

Appendix B. Necessity of the condition in equation (19) for the assignment strategy in case of different detectors' efficiencies

Here, we show that if the detection efficiencies can be different for Alice and Bob, then the condition in equation (19) is also necessary. More precisely, there are values of the detection efficiencies η^A and η^B for which this condition is necessary.

First, consider the case of $\eta^A = 0$ and $\eta^B = 1$. For any separable state ρ_s and a witness W , the following must hold true, $\text{Tr}(W\alpha \otimes \rho_s^B) \geq 0$, where $\rho_s^B = \text{Tr}_A[\rho_s]$. If we take the Bell state witness $W_{\frac{\pi}{4}}$, the condition further simplifies to $\text{Tr}[\alpha^T \rho_s^B] \leq 1$ for all states ρ_s^B . Inserting in the latter a particular state of the form,

$$\rho_s^B = \frac{\mathbb{1}}{2} + \frac{1}{2} \sum_{i=1}^3 \frac{a_i}{\sqrt{\sum_{j=1}^3 a_j^2}} \sigma_i, \quad (\text{B.1})$$

directly results into the condition $\sum_{i=1}^3 a_i^2 \leq 1$. The same way, we can prove the necessity of the constraint on b_i 's for the situation when $\eta^A = 1$ and $\eta^B = 0$.

Appendix C. Assignment strategy for the Bell witness

The solution to the SDP in equation (24) for the assignment strategy can be taken in the same form as in the case of the discard strategy, as described in appendix A. In particular, one can take the states ρ_λ as in equation (A.2), which leads to the constraints of the SDP to take the form in equation (A.4). The particular solution in terms of the parameters p_0, p_1, p_2, p_3 and p_4 is also the same as in equation (A.6) for $\eta > \frac{1}{\sqrt{3}}$ and as in equation (A.7) for $\eta \leq \frac{1}{\sqrt{3}}$. The only difference with the case of the discard strategy is the optimal value of the objective function, which is equal to 0 for $\eta > \frac{1}{\sqrt{3}}$ and $\frac{1}{4} - \frac{3}{4}\eta^2$ for $\eta \leq \frac{1}{\sqrt{3}}$.

ORCID iD

Nikolai Miklin  <https://orcid.org/0000-0001-8046-382X>

References

- [1] Horodecki R, Horodecki P, Horodecki M and Horodecki K 2009 Quantum entanglement *Rev. Mod. Phys.* **81** 865
- [2] Bennett C H and Brassard G 1984 Quantum cryptography: public-key distribution and coin tossing *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing* (IEEE Press) pp 175–9
- [3] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 Quantum cryptography *Rev. Mod. Phys.* **74** 145
- [4] Liao S-K *et al* 2017 Satellite-to-ground quantum key distribution *Nature* **549** 43–47
- [5] Kocher C A and Commins E D 1967 Polarization correlation of photons emitted in an atomic cascade *Phys. Rev. Lett.* **18** 575
- [6] Aspect A, Grangier P and Roger G 1982 Experimental realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: a new violation of Bell's inequalities *Phys. Rev. Lett.* **49** 91
- [7] Ursin R *et al* 2007 Entanglement-based quantum communication over 144 km *Nat. Phys.* **3** 481–6
- [8] Bedington R, Arrazola J M and Ling A 2017 Progress in satellite quantum key distribution *npj Quantum Inf.* **3** 1–13
- [9] Bell J S 1964 On the Einstein-Podolsky-Rosen paradox *Phys. Phys. Fiz.* **1** 195
- [10] Pironio S, Acín A, Brunner N, Gisin N, Massar S and Scarani V 2009 Device-independent quantum key distribution secure against collective attacks *New J. Phys.* **11** 045021
- [11] Eberhard P H 1993 Background level and counter efficiencies required for a loophole-free Einstein-Podolsky-Rosen experiment *Phys. Rev. A* **47** R747
- [12] Brunner N, Gisin N, Scarani V and Simon C 2007 Detection loophole in asymmetric Bell experiments *Phys. Rev. Lett.* **98** 220403
- [13] Vértesi T, Pironio S and Brunner N 2010 Closing the detection loophole in Bell experiments using qudits *Phys. Rev. Lett.* **104** 060401
- [14] Brown P, Fawzi H and Fawzi O 2021 Device-independent lower bounds on the conditional von Neumann entropy (arXiv:2106.13692)
- [15] Miklin N, Chaturvedi A, Bourennane M, Pawłowski M and Cabello A 2022 Exponentially decreasing critical detection efficiency for any Bell inequality *Phys. Rev. Lett.* **129** 230403
- [16] Łukanowski K, Balanzó-Juandó M, Farkas M, Acín A and Kołodyński J 2022 Upper bounds on key rates in device-independent quantum key distribution based on convex-combination attacks (arXiv:2206.06245)
- [17] Skwara P, Kampermann H, Kleinmann M and Bruß D 2007 Entanglement witnesses and a loophole problem *Phys. Rev. A* **76** 012312
- [18] Shalm L K *et al* 2015 Strong loophole-free test of local realism *Phys. Rev. Lett.* **115** 250402
- [19] Giustina M *et al* 2015 Significant-loophole-free test of Bell's theorem with entangled photons *Phys. Rev. Lett.* **115** 250401
- [20] Uola R, Costa A C S, Nguyen H C and Gühne O 2020 Quantum steering *Rev. Mod. Phys.* **92** 015001
- [21] Pawłowski M and Brunner N 2011 Semi-device-independent security of one-way quantum key distribution *Phys. Rev. A* **84** 010302
- [22] Terhal B M 2001 A family of indecomposable positive linear maps based on entangled quantum states *Linear Algebr. Appl.* **323** 61–73
- [23] Vandenberghe L and Boyd S 1996 Semidefinite programming *SIAM Rev.* **38** 49–95
- [24] Asadian A, Erker P, Huber M and Klöckl C 2016 Heisenberg-Weyl observables: Bloch vectors in phase space *Phys. Rev. A* **94** 010301
- [25] Czechlewski M and Pawłowski M 2018 Influence of the choice of postprocessing method on Bell inequalities *Phys. Rev. A* **97** 062123
- [26] Branciard C 2011 Detection loophole in Bell experiments: how postselection modifies the requirements to observe nonlocality *Phys. Rev. A* **83** 032123
- [27] Brunner N, Cavalcanti D, Pironio S, Scarani V and Wehner S 2014 Bell nonlocality *Rev. Mod. Phys.* **86** 419
- [28] Fine A 1982 Hidden variables, joint probability and the bell inequalities *Phys. Rev. Lett.* **48** 291
- [29] Doherty A C, Parrilo P A and Spedalieri F M 2004 Complete family of separability criteria *Phys. Rev. A* **69** 022308
- [30] Massar S, Pironio S, Roland J'emie and Gisin B 2002 Bell inequalities resistant to detector inefficiency *Phys. Rev. A* **66** 052112
- [31] Werner R F 1989 Quantum states with einstein-Podolsky-Rosen correlations admitting a hidden-variable model *Phys. Rev. A* **40** 4277

- [32] Beaudry N J, Moroder T and Lütkenhaus N 2008 Squashing models for optical measurements in quantum communication *Phys. Rev. Lett.* **101** 093601
- [33] Moroder T, Gühne O, Beaudry N, Piani M and Lütkenhaus N 2010 Entanglement verification with realistic measurement devices via squashing operations *Phys. Rev. A* **81** 052342
- [34] Gittsovich O, Beaudry N J, Narasimhachar V, Alvarez R R, Moroder T and Lütkenhaus N 2014 Squashing model for detectors and applications to quantum-key-distribution protocols *Phys. Rev. A* **89** 012325
- [35] Makarov V 2009 Controlling passively quenched single photon detectors by bright light *New J. Phys.* **11** 065003
- [36] Becker G T, Regazzoni F, Paar C and Burleson W P 2013 Stealthy dopant-level hardware trojans *Cryptographic Hardware and Embedded Systems-CHES 2013: 15th Int. Workshop, Proc. 15 (Santa Barbara, CA, USA, August 20–23 2013)* (Springer) pp 197–214
- [37] Ghandali S, Holcomb D and Paar C 2019 Temperature-based hardware trojan for ring-oscillator-based trngs (arXiv:1910.00735)

ARTICLE OPEN



Extending loophole-free nonlocal correlations to arbitrarily large distances

Anubhav Chaturvedi^{1,2}, Giuseppe Viola² and Marcin Pawłowski²

Quantum theory allows spatially separated observers to share nonlocal correlations, which enable them to accomplish classically inconceivable information processing and cryptographic feats. However, the distances over which nonlocal correlations can be realized remain severely limited due to their high fragility to noise and high threshold detection efficiencies. To enable loophole-free nonlocality across large distances, we introduce Bell experiments wherein the spatially separated parties randomly choose the location of their measurement devices. We demonstrate that when devices close to the source are perfect and witness extremal nonlocal correlations, such correlations can be extended to devices placed arbitrarily far from the source. To accommodate imperfections close to the source, we demonstrate an analytic trade-off: the higher the loophole-free nonlocality close to the source, the lower the threshold requirements away from the source. We utilize this trade-off and formulate numerical methods to estimate the critical requirements of individual measurement devices in such experiments.

npj Quantum Information (2024)10:7; <https://doi.org/10.1038/s41534-023-00799-1>

INTRODUCTION

Spatially separated observers cannot communicate faster than the speed of light, à la relativity. However, they can share quantum correlations born of local measurements performed on entangled particles which resist local hidden variable (classical) explanations. This phenomenon is called Bell nonlocality^{1,2}. The nonlocal correlations enable the observers to accomplish classically inconceivable information processing and cryptographic feats such as unconditionally secure device-independent (DI) quantum key distribution^{3–8} and randomness expansion^{9–12}. The efficacy of these applications necessitates loophole-free certification of nonlocality. The most challenging loophole impeding practical long-distance DI cryptography is the detection loophole¹³, exploiting which a malicious adversary can fake nonlocal correlations if a sufficient fraction of the entangled particles remains undetected.

A measurement device's detection efficiency, η , is the probability with which the device detects an incoming system emitted by the source. In Bell tests, closing the detection loophole amounts to having a detection efficiency above a characteristic threshold value, η^* , often referred to as the critical detection efficiency, below which local hidden variable models can simulate the considered nonlocal correlation. In symmetric Bell tests, wherein all detectors are equally inefficient, η^* is a characteristic property of the target nonlocal correlation. For instance, in the simplest bipartite symmetric Bell scenario, quantum correlations that maximally violate the Clauser-Horne-Shimony-Holt (CHSH) Bell inequality¹⁴ have a critical detection efficiency, $\eta^* \approx 0.828$ ¹⁵. However, the effective detection efficiency, η , depends not only on the properties of the measurement device but also on the losses incurred during transmission. In photonic Bell experiments, the effective detection efficiency decays exponentially with the length of the optical fiber, l , such that $\eta = \eta_0 10^{-\frac{\alpha l}{10}}$, where η_0 is the detection efficiency of the measuring apparatus due to the use of imperfect detectors, and α is the attenuation coefficient typically ≈ 0.2 dB/km at a wavelength of 1550 nm (third telecom window)¹⁶. Therefore, the lower the critical detection efficiency of a nonlocal

correlation, the further away the measurement devices can be from the source while retaining loophole-free nonlocal behavior. Consequently, the detection loophole is practically unavoidable in photonic Bell experiments and DIQKD systems when using optical fibers of about 5 km¹⁷ and 3.5 km¹⁸ in length, respectively. Another crucial quantity for long-distance loophole-free Bell tests is the visibility, v , of the entangled quantum systems, which quantifies the amount of noise added during transmission and due to imperfections in the source. Analogously to the critical detection efficiency, each nonlocal quantum strategy has a characteristic threshold value of visibility, v^* , below which the consequent correlations cease to be nonlocal.

Over the years, several proposals have identified nonlocal quantum correlations with lower critical detection efficiencies. For instance, in the symmetric CHSH scenario, one can reduce it down to $\eta^* = 2/3$ by using a pair of almost-product partially entangled qubits¹⁹. However, this lower critical detection efficiency comes at the cost of very high susceptibility to noise with $v^* \approx 1$. The other proposals fall into one of the two categories, (i) the ones which increase the complexity of the quantum set-up by either utilizing entangled quantum systems of higher local dimension^{20–23}, or by increasing the number of spatially separated parties^{24–26}, and (ii) the ones which invoke theoretical idealizations such as perfect detectors for a measuring party^{27–31}. While the latter are clearly of little practical significance, the former necessitates more intricate state preparation procedures, which invariably lead to a higher susceptibility to noise and experimental fragility.

Consequently, long-distance loophole-free nonlocal correlations remain elusive, even in the near-term future. This is reflected in the current state-of-the-art combinations of (η, v) reported in photonic Bell experiments over distances ≤ 400 m, $(0.774, 0.99)$ ³², $(0.763, 0.99)$ ¹², and $(0.8411, 0.9875)$ ¹¹. On the other hand, if DI cryptography is to become a near-term commonplace technology, operationally certifiable robust nonlocal correlations must be sustained over distances orders of magnitude larger ($\gg 100$ km). Due to the sheer enormity of this gap, the traditional approach of

¹Faculty of Applied Physics and Mathematics, Gdańsk University of Technology, Gabriela Narutowicza 11/12, 80-233 Gdańsk, Poland. ²International Centre for Theory of Quantum Technologies (ICTQT), University of Gdańsk, 80-308 Gdańsk, Poland. ✉email: anubhav.chaturvedi@phdstud.ug.edu.pl

looking for nonlocal quantum correlations with marginally lower critical detection efficiency seems futile. Instead, in this work, we exploit the properties of strong nonlocal correlations, which can be readily attained today, albeit at short distances, to extend them to arbitrarily large distances.

Specifically, we consider a generalization to the standard Bell experiments, wherein each round, the measuring parties randomly choose the location (distance from the source) of their measurement devices in addition to their measurement settings. It then follows from relativity, and specifically from the so-called non-signaling condition, that the behavior of any particular measurement device remains unaffected by the changes in the location of spatially separated measurement devices. Based exclusively on this relativistic fact and the operational validity of quantum mechanics, we demonstrate that nonlocal correlations can be operationally certified arbitrarily far away from the source, which is to say, with arbitrarily inefficient measurement devices, when devices close to the source operate flawlessly and witness extremal nonlocal correlations. We then proceed to derive an analytic trade-off specific to the CHSH scenario: the higher loophole-free nonlocality close to the source, as measured by the violation of the CHSH inequality, the lower the threshold value for local hidden variable explanations away from the source. We utilize this trade-off to estimate the critical detection efficiency and visibility of the measurement device placed away from the source when the devices close are imperfect, thereby demonstrating the robustness of the effect. Moreover, utilizing certifiable randomness as a measure of the nonlocal behavior of a device, we present a versatile numerical technique based on the Nieto-Silleras hierarchy of semi-definite programs^{33,34}, to estimate the critical requirements of individual measurement devices in generic network scenarios with several spatially separated measurement devices. Finally, we discuss experimental setups utilizing relay switches to demonstrate this effect, more complex network scenarios entailing multiple measurement devices, the possibility of DI cryptography schemes fueled by this effect, and the key challenges that lay on the way.

RESULTS

Preliminaries

Let us consider the simplest bipartite Bell scenario entailing a source, \mathcal{S} , distributing entangled quantum systems, ideally in a two-qubit pure state, $|\psi\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$, to two spatially separated

parties, Alice and Bob. The parties have measurement devices with binary inputs, $x, y \in \{0, 1\}$, specifying the measurement settings, and produce binary outcomes, $a, b \in \{+1, -1\}$, respectively. In ideal circumstances, the measurement devices perform measurements corresponding to binary outcome projective observables, $\hat{a}_x \in B(\mathbb{C}^2), \hat{b}_y \in B(\mathbb{C}^2)$. The three tuple, $\mathcal{Q} \equiv (|\psi\rangle, \{\hat{a}_x\}_x, \{\hat{b}_y\}_y)$, constitutes a quantum strategy (entailing operational instructions) which ideally results in the experimental behavior, $\mathbf{p} \equiv \{p(a, b|x, y) = \frac{1}{4} \langle \psi | (\mathbb{I} + a\hat{a}_x) \otimes (\mathbb{I} + b\hat{b}_y) | \psi \rangle\} \in \mathbb{R}_+^{16}$. In general, up to local relabeling, a given behavior, \mathbf{p} , is said to be nonlocal if and only if it violates the CHSH inequality,

$$C(\mathbf{p}) \equiv \sum_{x,y} (-1)^{xy} \langle \hat{a}_x \hat{b}_y \rangle_{\mathcal{L}} \leq 2, \quad (1)$$

where $\langle \hat{a}_x \hat{b}_y \rangle = \sum_{a,b} abp(a, b|x, y)$. The inequality (1) holds for all behaviors, $\mathbf{p} \in \mathbb{R}_+^{16}$, which admit local hidden variable explanations (\mathcal{L}), such that, $p(a, b|x, y) = \sum_{\lambda \in \Lambda} p(\lambda) p_{\lambda}^A(a|x) p_{\lambda}^B(b|y)$, where λ is the local hidden variable, Λ is a measurable hidden variable state space, $p(\lambda)$ specifies the probability of the system occupying the state corresponding to λ , and for a specific λ , the conditional probability distributions, $\{p_{\lambda}^A(a|x)\}$ and $\{p_{\lambda}^B(b|y)\}$, represent stochastic response schemes specifying the outcome probabilities for Alice and Bob, respectively.

However, the actual measurement devices may be imperfect and sometimes fail to detect the incoming quantum system, an event referred to as the “no-click” event, and the effective probability with which a measurement device, D , “clicks”, is referred to as its detection efficiency, $\eta_D \in [0, 1]$, where, $\eta_D = 1$ signifies perfect detectors. We consider a generalization of the simplest Bell experiment, depicted in Fig. 1, wherein Bob’s measurement device, B , is at a fixed distance from the source throughout the experiment and has an unvarying effective detection efficiency, η_B . Alice, on the other hand, randomly chooses the spatial location of her device based on an additional input bit, $i \in \{0, 1\}$. When $i = 0$, she places her measurement device, A_0 , close to the source achieving an effective detection efficiency, η_{A_0} , whereas when $i = 1$, she places her device, A_1 , further away from the source, attaining a lower effective detection efficiency, $\eta_{A_1} \leq \eta_{A_0}$. Additionally, to account for imperfections in the source and noise added during transmission from the source, we associate effective visibilities, $v_B, v_{A_i} \in [0, 1]$ to each measurement device, such that the quantum state shared between the

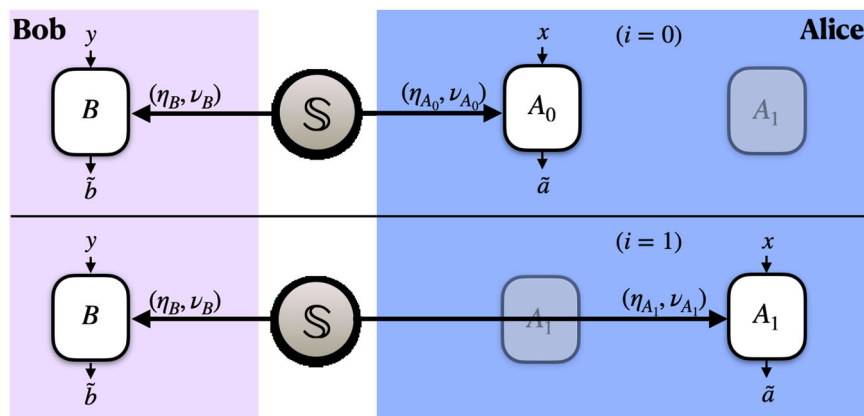


Fig. 1 Topology. The graphic is a schematic depiction of the generalized or routed Bell CHSH experiment introduced in this work. In each round of the experiment, just as in the standard case, the parties choose their respective measurement settings, $x, y \in \{0, 1\}$ and obtain outcomes, $\tilde{a}, \tilde{b} \in \{+1, -1, \perp\}$, where the outcome, \perp , signifies the “no-click” event. While Bob’s measurement device, B , is at a fixed distance from the source throughout the experiment with an unvarying effective detection efficiency and visibility, (η_B, v_B) , the location of Alice’s measurement device, A_i , depends on a randomly chosen input bit, $i \in \{0, 1\}$. When $i = 0$, Alice places her measurement device, A_0 , close to the source with an effective detection efficiency and visibility, (η_{A_0}, v_{A_0}) , whereas when $i = 1$, she places her measurement device, A_1 , further away from the source, with a lower detection efficiency and visibility, (η_{A_1}, v_{A_1}) , such that, $\eta_{A_1} < \eta_{A_0}, v_{A_1} < v_{A_0}$.

measurement devices, (A_i, B) , is,

$$\begin{aligned} \rho(v_i) = & v_{A_i} v_B |\psi\rangle\langle\psi| + v_{A_i} (1 - v_B) (\rho_B \otimes \frac{\mathbb{I}}{2}) \\ & + (1 - v_{A_i}) v_B (\frac{\mathbb{I}}{2} \otimes \rho_A) + (1 - v_{A_i}) (1 - v_B) \frac{\mathbb{I}_4}{4}, \end{aligned} \quad (2)$$

where $\rho_A = \text{Tr}_B(|\psi\rangle\langle\psi|)$, $\rho_B = \text{Tr}_A(|\psi\rangle\langle\psi|)$, \mathbb{I} is the two-dimensional identity operator, and $\mathbb{I}_4 = \mathbb{I} \otimes \mathbb{I}$. Analogously to the detection efficiencies, the effective visibility of Alice's measurement device decreases with the distance from the source, such that $v_{A_i} \leq v_{A_0}$.

Treating the no-click event as an additional outcome, \perp , the parties observe the experimental behavior in the form of conditional probability distributions, $\mathbf{p}_{(exp)} \equiv \{p(\tilde{a}, \tilde{b}|(x, i), y)\} \in \mathbb{R}_+^{22}$, where $\tilde{a}, \tilde{b} \in \{+1, -1, \perp\}$. A convenient way to post-process the experimental behavior, $\mathbf{p}_{(exp)}$, which avoids considering additional outcomes and as well as the fair-sampling assumption, is to assign a valid outcome, say $+1$, to each no-click event, such that, the effective distribution reduces to $\mathbf{p}_{(exp)}^{(\perp \rightarrow 1)} \equiv \{p(a, b|(x, i), y)\} \in \mathbb{R}_+^{32,35}$. One of the benefits of such a post-processing is the applicability of well-studied, reliable means of quantifying loophole-free nonlocal correlations such as the observed value of the CHSH expression,

$$C_{A_i, B}(\mathbf{p}_{(exp)}^{(\perp \rightarrow 1)}) \equiv \sum_{x, y} (-1)^{x \cdot y} \langle \hat{a}_{(x, i)} \hat{b}_y \rangle \quad (3)$$

where $\langle \hat{a}_{(x, i)} \hat{b}_y \rangle = \sum_{a, b} a b p(a, b|(x, i), y)$.

The measurement devices (A_i, B) are said to share loophole-free nonlocal correlations if the behavior $\mathbf{p}_{(exp)}^{(\perp \rightarrow 1)}$ does not allow for a local hidden variable explanation of the form,

$$p(a, b|(x, i), y) = \sum_{\lambda \in \Lambda} p(\lambda) p_\lambda^A(a|x, i) p_\lambda^B(b|y), \quad (4)$$

for all $a, b \in \{+1, -1\}$ and $x, y \in \{0, 1\}$, where λ is a local hidden variable, Λ is a measurable hidden variable state space, $p(\lambda)$ specifies the probability of the shared system occupying the state corresponding to λ , and for a specific λ , the conditional probability distributions, $\{p_\lambda^A(a|x, i)\}$ and $\{p_\lambda^B(b|y)\}$, represent stochastic response schemes specifying the outcome probabilities for Alice and Bob, respectively. As assigning a local pre-determined outcome to the "no-click" event cannot increase the local hidden variable bound, 2, of the CHSH expression, the experimental violation of the CHSH inequality (1), $C_{A_i, B}(\mathbf{p}_{(exp)}^{(\perp \rightarrow 1)}) > 2$, constitutes a sufficient operational condition for certifying loophole-free nonlocal correlations between the spatially separated measurement devices, (A_i, B) . However, as we demonstrate below, this threshold requirement for the certification of loophole-free nonlocal correlations between (A_1, B) reduces drastically when (A_0, B) witness loophole-free violation of the CHSH inequality (1). Specifically, let us suppose that the measurement devices close to the source (A_0, B) witness a loophole-free violation of the CHSH inequality $C_{A_0, B}(\mathbf{p}_{(exp)}^{(\perp \rightarrow 1)}) > 2$, this implies that their behavior must spring from an underlying quantum set-up, i.e., from quantum measurements $\{M_a^{(x, i=0), \lambda} \in B_+(\mathcal{H}_A), M_b^{y, \lambda} \in B_+(\mathcal{H}_B)\}$ on shared entangled states $\{\rho_\lambda \in B_+(\mathcal{H}_A \otimes \mathcal{H}_B)\}$, where $\mathcal{H}_A, \mathcal{H}_B$ are arbitrary underlying Hilbert spaces, such that, for all $a, b \in \{+1, -1\}$ and $x, y \in \{0, 1\}$,

$$p(a, b|(x, i=0), y) = \sum_{\lambda \in \Lambda} p(\lambda) \text{Tr}(\rho_\lambda M_a^{(x, i=0), \lambda} \otimes M_b^{y, \lambda}). \quad (5)$$

In particular, this implies that Bob's outcome must spring from genuine quantum measurements $\{M_b^{y, \lambda} \in B_+(\mathcal{H}_B)\}$ on his part of entangled states $\{\rho_\lambda^{(B)} = \text{Tr}_A(\rho_\lambda)\}$ shared with A_0 , such that, $p_\lambda^B(b|y) = \text{Tr}(\rho_\lambda^{(B)} M_b^{y, \lambda})$.

As the source as well as the the internal workings of Bob's measurement device, B , remain unaffected by the changes in the location of Alice's measurement device, i.e., by the choice i , if the

behavior Alice's other device were possess a local hidden variable explanation of the form (4), i.e., it obtains its measurement outcomes from the post-processing of a shared local hidden variable λ , then,

$$p(a, b|(x, i=1), y) = \sum_{\lambda \in \Lambda} p(\lambda) p_\lambda^A(a|x, i=1) \text{Tr}(\rho_\lambda^{(B)} M_b^{y, \lambda}). \quad (6)$$

Notice, in the local hidden variable models invoked here, the local hidden variable λ is implicitly assumed to be independent of the location of Alice's measurement device, i.e., $p(\lambda, i) = p(\lambda)p(i)$. As we treat $i \in \{0, 1\}$ as an additional Alice's input, this assumption follows from the so-called "measurement independence" or "free-choice" assumption invoked while describing local hidden variable models in standard Bell experiments. In particular, this assumption has interesting cryptographic consequences, which are deferred to the discussion section, towards the end of the manuscript. Now, we are prepared to present our central result.

Perfect devices close to the source

Let us first consider the ideal case wherein the measurement devices located close to the source, (A_0, B) , are effectively perfect, i.e., $\eta_B = \eta_{A_0} = v_B = v_{A_0} = 1$. Then, via the following the Theorem, we demonstrate that extremal loophole-free nonlocal correlations witnessed close to source can be extended to a measurement device placed arbitrarily far away from the source,

Theorem 1. (Nonlocality at arbitrary distance). If the measurement devices close to the source, (A_0, B) , are perfect, i.e., $\eta_B = \eta_{A_0} = v_B = v_{A_0} = 1$, and witness maximally nonlocal correlations, such that, $C_{A_0, B}(\mathbf{p}_{(exp)}^{(\perp \rightarrow 1)}) = 2\sqrt{2}$, then such nonlocal correlations may be operationally extended to Alice's other measurement device placed arbitrarily far away from the source, i.e., loophole-free nonlocal correlations between (A_1, B) can be operationally certified for any non-zero values of (η_{A_1}, v_{A_1}) .

Proof. Let the parties employ the maximally nonlocal isotropic two-qubit strategy, $\mathcal{Q}_{iso} \equiv (|\phi^+\rangle, \{\sigma_z, \sigma_x\}, \{\frac{1}{\sqrt{2}}(\sigma_z \pm \sigma_x)\})$, where $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Consequently, the measurement devices witness the maximum quantum violation of the CHSH inequality (1), such that $C_{A_0, B}(\mathbf{p}_{(exp)}^{(\perp \rightarrow 1)}) = 2\sqrt{2}$.

The loophole-free observation of such extremal nonlocal quantum correlations not only discards local hidden variable explanations of the form (4) for the measurement devices (A_1, B) , but also uniquely identifies the effective underlying shared quantum states $\{\rho_\lambda\}$ and the local measurements $\{M_a^{(x, i=0), \lambda}\}, \{M_b^{y, \lambda}\}$ to be equivalent to the ones in \mathcal{Q}_{iso} , respectively, up to auxiliary degrees of freedom and local isometries for all λ , a phenomenon referred to as DI self-testing³⁶. In particular, this implies that the effective states $\{\rho_\lambda^{(B)}\}$ of Bob's local subsystem on which the anticommuting observables act non-trivially are equivalent to the maximally mixed qubit state, $\frac{\mathbb{I}}{2}$, such that Bob's measurement outcomes must be intrinsically random, i.e., $\langle \hat{b}_y \rangle = 0$ for all $y \in \{0, 1\}$. As the internal workings of Bob's measurement device, B , remain unaffected by the changes in the location of Alice's measurement device, her effective subsystem and observables remain unaffected by Alice's choice of i .

Now, if Alice's other device, A_1 , were to be classical, i.e., it obtains its measurement outcomes from the post-processing of a shared local hidden variable, λ , such that, the behavior witness by the measurement devices (A_1, B) allows for a local hidden variable explanation of the form (6), then the outcomes of A_1 cannot be correlated to that of Bob, which results in,

$$\begin{aligned} C_{A_1, B}(\mathbf{p}_{(exp)}^{(\perp \rightarrow 1)}) &= \sum_{\lambda \in \Lambda} p(\lambda) \sum_{x, y} (-1)^{x \cdot y} \langle \hat{a}_{(x, 1)} \rangle_\lambda \langle \hat{b}_y \rangle_\lambda \\ &= 0, \end{aligned} \quad (7)$$

where $\langle \hat{a}_{(x,1)} \rangle_\lambda = \sum_a a p_\lambda^A(a|x, 1)$, $\langle \hat{b}_y \rangle_\lambda = \sum_b b p_\lambda^B(b|y)$, and the second equality follows from the fact that the maximal quantum violation of the CHSH inequality, $C_{A_0B}(\mathbf{p}_{(exp)}^{(\perp \rightarrow \perp)}) = 2\sqrt{2}$, self-tests, and hence, can only be attained by a unique quantum behavior, which in-turn implies that, $\forall \lambda : \langle \hat{b}_y \rangle_\lambda = \langle \hat{b}_y \rangle = 0$.

Now, if A_1 were to behave honestly with the strategy, \mathcal{Q}_{iso} , but imperfectly, i.e., with detection efficiency η_{A_1} , visibility v_{A_1} , they observe,

$$C_{A_1B}(\mathbf{p}_{(\perp \rightarrow \perp)}) = 2\sqrt{2}\eta_{A_1}v_{A_1}, \quad (8)$$

which violates (7), and certifies loophole-free nonlocal correlations between (A_1, B) , for any non-zero values of (η_{A_1}, v_{A_1}) . \square

Theorem 1 brings forth the principal effect we employ to extend ideal loophole-free nonlocal correlations. However, as perfect measurement devices close to the source are but a theoretical idealization, i.e., the pre-requisites of Theorem 1, namely, $\eta_{A_0} = \eta_B = v_0 = 1$, cannot be achieved in the actual experiments, we now consider cases wherein the devices close to source although better than the one placed further way, are not perfect.

Imperfect devices close to the source

To account for such realistic cases and the estimation of the critical requirements, $(\eta_{A_1}^*, v_{A_1}^*)$, of Alice's other measurement device, A_1 , we present a trade-off specific to the CHSH inequality (1) via the following Theorem, namely, the higher the loophole-free nonlocality witnessed close to source, the lower the threshold requirements of the measurement device placed away from the source.

Theorem 2. (A specific analytical trade-off). If the measurement devices close to the source, (A_0, B) , witness loophole-free nonlocal correlations such that, $C_{A_0B}(\mathbf{p}_{(exp)}^{(\perp \rightarrow \perp)}) > 2$, then loophole-free nonlocal correlations between (A_1, B) can be certified whenever the following inequality is violated,

$$C_{A_1B}(\mathbf{p}_{(exp)}^{(\perp \rightarrow \perp)}) \leq_{\mathcal{L}(A_1)} \sqrt{8 - (C_{A_0B}(\mathbf{p}_{(exp)}^{(\perp \rightarrow \perp)}))^2}. \quad (9)$$

Proof. Let us assume that the parties share an arbitrary behavior, $\mathbf{p} \in \mathbb{R}_+^{32}$. We now recall that if the measurement devices, (A_0, B) , witness the violation the CHSH inequality, $C_{A_0B}(\mathbf{p}) > 2$, then the outcomes of B must be intrinsically random, which is to say, that they cannot be predicted perfectly³⁷, specifically,

$$\forall y \in \{0, 1\} : |\langle \hat{b}_y \rangle| \leq \frac{1}{2} \sqrt{8 - (C_{A_0B}(\mathbf{p}))^2}. \quad (10)$$

Now, if Alice's other device, A_1 , were to be classical, i.e., it obtains its measurement outcomes from the post-processing of a shared local hidden variable, λ , such that, the behavior witnessed by the measurement devices (A_1, B) allows for a local hidden variable explanation of the form (6), then the value of the CHSH expression can be bounded from above in the following way,

$$\begin{aligned} C_{A_1B}(\mathbf{p}) &=_{\mathcal{L}(A_1)} \sum_{\lambda \in \Lambda} p(\lambda) \sum_{x,y} (-1)^{xy} \langle \hat{a}_{(x,1)} \rangle_\lambda \langle \hat{b}_y \rangle_\lambda, \\ &= \sum_{\lambda \in \Lambda} p(\lambda) \sum_x \langle \hat{a}_{(x,1)} \rangle_\lambda (\langle \hat{b}_0 \rangle_\lambda + (-1)^x \langle \hat{b}_1 \rangle_\lambda), \\ &\leq \sum_{\lambda \in \Lambda} p(\lambda) (|\langle \hat{b}_0 \rangle_\lambda + \langle \hat{b}_1 \rangle_\lambda| + |\langle \hat{b}_0 \rangle_\lambda - \langle \hat{b}_1 \rangle_\lambda|), \\ &= 2 \sum_{\lambda \in \Lambda} p(\lambda) \max_{y \in \{0,1\}} |\langle \hat{b}_y \rangle_\lambda| \end{aligned} \quad (11)$$

where the first inequality follows from the observation that $|\langle \hat{a}_{(x,1)} \rangle_\lambda| \leq 1$, for all x and $\lambda \in \Lambda$.

Let us now split the hidden variable state space, Λ , into the following four disjoint subspaces,

$$\begin{aligned} \Lambda_0 &\equiv \left\{ \lambda \in \Lambda \mid \max_{y \in \{0,1\}} |\langle \hat{b}_y \rangle_\lambda| = \langle \hat{b}_0 \rangle_\lambda \right\}, \\ \Lambda_1 &\equiv \left\{ \lambda \in \Lambda \mid \max_{y \in \{0,1\}} |\langle \hat{b}_y \rangle_\lambda| = -\langle \hat{b}_0 \rangle_\lambda \right\}, \\ \Lambda_2 &\equiv \left\{ \lambda \in \Lambda \mid \max_{y \in \{0,1\}} |\langle \hat{b}_y \rangle_\lambda| = \langle \hat{b}_1 \rangle_\lambda \right\}, \\ \Lambda_3 &\equiv \left\{ \lambda \in \Lambda \mid \max_{y \in \{0,1\}} |\langle \hat{b}_y \rangle_\lambda| = -\langle \hat{b}_1 \rangle_\lambda \right\}. \end{aligned} \quad (12)$$

This allows us expand the RHS of (11) such that,

$$\begin{aligned} C_{A_1B}(\mathbf{p}) &\leq_{\mathcal{L}(A_1)} 2 \left(\sum_{\lambda \in \Lambda_0} p(\lambda) \langle \hat{b}_0 \rangle_\lambda - \sum_{\lambda \in \Lambda_1} p(\lambda) \langle \hat{b}_0 \rangle_\lambda \right. \\ &\quad \left. + \sum_{\lambda \in \Lambda_2} p(\lambda) \langle \hat{b}_1 \rangle_\lambda - \sum_{\lambda \in \Lambda_3} p(\lambda) \langle \hat{b}_1 \rangle_\lambda \right) \\ &= 2 \left(p(\Lambda_0) |\langle \hat{b}_0 \rangle_{\Lambda_0}| + p(\Lambda_1) |\langle \hat{b}_0 \rangle_{\Lambda_1}| \right. \\ &\quad \left. + p(\Lambda_2) |\langle \hat{b}_1 \rangle_{\Lambda_2}| + p(\Lambda_3) |\langle \hat{b}_1 \rangle_{\Lambda_3}| \right), \end{aligned} \quad (13)$$

where $p(\Lambda_j) = \sum_{\lambda \in \Lambda_j} p(\lambda)$, and $\langle \hat{b}_k \rangle_{\Lambda_j} = \frac{1}{p(\Lambda_j)} \sum_{\lambda \in \Lambda_j} p(\lambda) \langle \hat{b}_k \rangle_\lambda$ for all $j \in \{0, 1, 2, 3\}$ and $k \in \{0, 1\}$. Now, we can use (10) to further upper bound (13), such that,

$$\begin{aligned} C_{A_1B}(\mathbf{p}) &\leq_{\mathcal{L}(A_1)} \sum_{j \in \{0,1,2,3\}} p(\Lambda_j) \sqrt{8 - (C_{A_0B}(\mathbf{p}_{\Lambda_j}))^2}, \\ &\leq \sqrt{8 - \left(\sum_{j \in \{0,1,2,3\}} p(\Lambda_j) C_{A_0B}(\mathbf{p}_{\Lambda_j}) \right)^2}, \\ &= \sqrt{8 - (C_{A_0B}(\mathbf{p}))^2}. \end{aligned} \quad (14)$$

where $\mathbf{p}_{\Lambda_j} = \frac{1}{p(\Lambda_j)} \sum_{\lambda \in \Lambda_j} p(\lambda) \mathbf{p}_\lambda$, and $\mathbf{p}_\lambda \in \mathbb{R}_+^{32}$ is the joint behavior for a specific λ , the second inequality follows from the fact that the function, $\sqrt{8 - (C_{A_0B}(\mathbf{p}_{\Lambda_j}))^2}$, is concave in its argument, $C_{A_0B}(\mathbf{p}_{\Lambda_j})$, and the final equality follows from the operational requirement that averaging \mathbf{p}_{Λ_j} over our ignorance of the hidden variable λ reproduces the observed behavior, \mathbf{p} , i.e., $\mathbf{p} = \sum_j p(\Lambda_j) \mathbf{p}_{\Lambda_j}$, and $C_{A_0B}(\mathbf{p}) = \sum_j p(\Lambda_j) C_{A_0B}(\mathbf{p}_{\Lambda_j})$.

Finally, plugging the precondition that the parties observe the post-processed experimental behavior, $\mathbf{p} \equiv \mathbf{p}_{(exp)}^{(\perp \rightarrow \perp)}$, into (14) yields (9). \square

As $\sqrt{8 - (C_{A_0B}(\mathbf{p}_{(exp)}^{(\perp \rightarrow \perp)}))^2}$ is a monotonically decreasing function of $C_{A_0B}(\mathbf{p}_{(exp)}^{(\perp \rightarrow \perp)}) \in (2, 2\sqrt{2}]$, the inequality (9) implies that any amount of loophole-free violation of the CHSH inequality (1) witnessed by (A_0, B) , reduces the threshold value of the CHSH expression for (A_1, B) . Specifically, when (A_0, B) witness maximally nonlocal correlations, $C_{A_0B}(\mathbf{p}_{(exp)}^{(\perp \rightarrow \perp)}) = 2\sqrt{2}$, the threshold value reduces to zero (7), whereas when (A_0, B) fail to violate the CHSH inequality, (A_1, B) must violate the CHSH inequality (1) on their own, to certify loophole-free nonlocal correlations.

In what follows, we use Theorem 2, as a convenient tool to estimate the critical parameters, $(\eta_{A_1}^*, v_{A_1}^*)$, for the loophole-free certification of nonlocal correlations between (A_1, B) .

Analytical estimation of critical parameters

Given a quantum strategy, \mathcal{Q} , and the tuple of experimental parameters, $(\eta_B, \eta_{A_0}, v_B, v_{A_0})$, we retrieve the experimental

behavior, $\mathbf{p}_{(exp)}^{(\perp \rightarrow 1)}$, as a function of (η_{A_1}, ν_{A_1}) . Now, the critical parameters, $(\eta_{A_1}^*, \nu_{A_1}^*)$, are simply the ones for which the inequality (9) is saturated.

To demonstrate our methodology, we first consider the asymmetric case wherein, B is placed extremely close to a perfect source, such that $\eta_B = 1$, $\eta_{A_0} = \eta$, and all devices have perfect visibility, $\nu_B = \nu_{A_0} = \nu_{A_1} = 1$. The parties employ the maximally nonlocal isotropic strategy, \mathcal{Q}_{iso} , such that, $C_{A_0B}(\mathbf{p}_{(exp)}^{(\perp \rightarrow 1)}) = 2\sqrt{2}\eta$, where (A_0, B) observe a loophole-hole violation for $\eta \in (\frac{1}{\sqrt{2}}, 1]$, and $C_{A_1B}(\mathbf{p}_{(exp)}^{(\perp \rightarrow 1)}) = 2\sqrt{2}\eta_{A_1}$, which when plugged into (9) yields, $\eta_{A_1}^* = \sqrt{1 - \eta^2}$. This relation is plotted in Fig. 2, serves to bring up the central insight that the closer to the source A_0 is placed, the higher will be its effective detection efficiency, η_{A_0} , and consequently, the lower will be the critical detection efficiency of A_1 , $\eta_{A_1}^*$, i.e., the further away A_1 can be placed from the source, whilst retaining loophole-free nonlocal correlations with B .

For the symmetric case, wherein (A_0, B) are equidistant from the source, such that, $\eta_B = \eta_{A_0} = \eta$, and all devices have perfect visibility, $\nu_B = \nu_{A_0} = \nu_{A_1} = 1$, if the parties employ the isotropic strategy, \mathcal{Q}_{iso} , then $C_{A_0B}(\mathbf{p}_{(exp)}^{(\perp \rightarrow 1)}) = 2\sqrt{2}\eta^2 + 2(1 - \eta)^2$, where (A_0, B) observe a loophole-hole violation for $\eta \in (\frac{2}{1+\sqrt{2}}, 1]$ and $C_{A_1B}(\mathbf{p}_{(exp)}^{(\perp \rightarrow 1)}) = 2\sqrt{2}\eta_{A_1}\eta + 2(1 - \eta_{A_1})(1 - \eta)$. We plot the values of $\eta_{A_1}^*$, which saturate (9) against the effective detection efficiency η in Fig. 2.

Up till this point, we have relied exclusively on the isotropic strategy, \mathcal{Q}_{iso} . Next, we address whether we can further lower the critical requirements of A_1 by employing better quantum strategies.

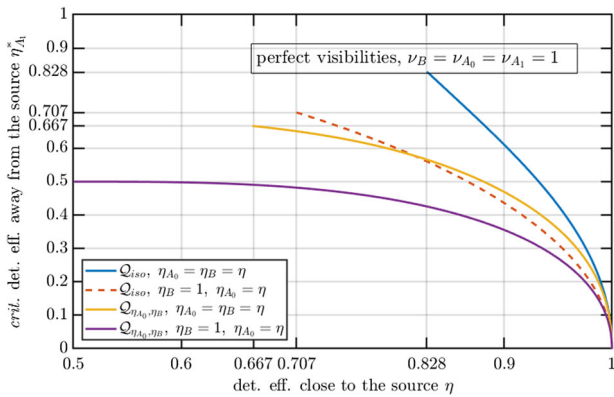


Fig. 2 Isotropic versus tilted strategies. The critical detection efficiency, $\eta_{A_1}^*$, of Alice's measurement device placed away from the source, A_1 , versus the effective detection efficiency, η , close to the source, obtained with the analytical trade-off (9), when the party's employ the isotropic strategy, \mathcal{Q}_{iso} , for the symmetric case, $\eta_{A_0} = \eta_B = 1$ (top solid blue curve), and for the asymmetric case, $\eta_{A_0} = \eta$, $\eta_B = 1$ (dashed orange curve), and when the party's employ the tilted strategies, $\mathcal{Q}_{\eta_{A_0}, \eta_B}$, for the symmetric case (middle solid yellow curve), and for the asymmetric case (bottom solid purple curve), with perfect visibilities, $\nu_B = \nu_{A_0} = \nu_{A_1} = 1$. The critical detection efficiency starts declining after η exceeds the respective threshold values: $\eta = \frac{2}{1+\sqrt{2}} \approx 0.828$, $\eta = \frac{1}{\sqrt{2}} \approx 0.707$, for the symmetric, and the asymmetric cases, respectively, when the parties employ the isotropic strategy, \mathcal{Q}_{iso} , and $\eta = \frac{2}{3} \approx 0.67$, $\eta = \frac{1}{2}$ for the symmetric, and the asymmetric cases, when the parties use the tilted strategies, $\mathcal{Q}_{\eta_{A_0}, \eta_B}$, respectively. In both symmetric and asymmetric cases, the tilted strategies, $\mathcal{Q}_{\eta_{A_0}, \eta_B}$, perform better than the isotropic strategy, \mathcal{Q}_{iso} , at minimizing the critical detection efficiency, $\eta_{A_1}^*$.

Optimal quantum strategies

Given the effective detection efficiencies of the measurement devices close to the source, (η_{A_0}, η_B) , the parties now use the tilted strategies, $\mathcal{Q}_{\eta_{A_0}, \eta_B}$, which attain maximum quantum violation of the following tilted CHSH inequality,

$$\begin{aligned} C_{A_0B}^{\eta_{A_0}, \eta_B}(\mathbf{p}) &\equiv \eta_{A_0}\eta_B C_{A_0B}(\mathbf{p}) + 2(1 - \eta_B)\eta_{A_0}\langle \hat{a}_{(0,0)} \rangle \\ &\quad + 2(1 - \eta_{A_0})\eta_B\langle \hat{b}_0 \rangle + 2(1 - \eta_{A_0})(1 - \eta_B) \\ &\leq 2. \end{aligned} \quad (15)$$

Notice that, given the detection efficiencies, (η_{A_0}, η_B) , the strategy, $\mathcal{Q}_{\eta_{A_0}, \eta_B}$, attains the maximum loophole-free violation of the CHSH inequality (1) for (A_0, B) , as $C_{A_0B}(\mathbf{p}_{(exp)}^{(\perp \rightarrow 1)}) = C_{A_0B}^{\eta_{A_0}, \eta_B}(\mathbf{p}_{\eta_{A_0}, \eta_B})$, where $\mathbf{p}_{\eta_{A_0}, \eta_B} \in \mathbb{R}_+^{32}$ is the ideal experimental behavior corresponding to the quantum strategy, $\mathcal{Q}_{\eta_{A_0}, \eta_B}$. As the threshold value for loophole-free certification of the nonlocal behavior of A_1 ,

$\sqrt{8 - (C_{A_0B}(\mathbf{p}_{(exp)}^{(\perp \rightarrow 1)}))^2}$ (9), is a monotonically decreasing function of $C_{A_0B}(\mathbf{p}_{(exp)}^{(\perp \rightarrow 1)})$, the tilted strategies, $\mathcal{Q}_{\eta_{A_0}, \eta_B}$, minimize it, and hence, are optimal for lowering the critical requirements of A_1 . In general, one can use the heuristic see-saw semi-definite programming method to numerically find these strategies. In an upcoming work, we describe a much more precise method for obtaining these strategies based on self-testing of the tilted CHSH inequalities (15). In Fig. 2 we plot the resultant curves for $\eta_{A_1}^*$ against the effective detection efficiency, η , for the asymmetric case, $(\eta_{A_0} = \eta, \eta_B = 1)$, as well as for the symmetric case, $\eta_{A_0} = \eta_B = \eta$, demonstrating the advantage of the tilted strategies, $\mathcal{Q}_{\eta_{A_0}, \eta_B}$, over the isotropic strategy, \mathcal{Q}_{iso} .

While Theorem 2 unitizes the value of the CHSH expression as a measure of nonlocal correlations shared between (A_1, B) , and provides a convenient method for the estimation of critical parameters of A_1 , its applicability is limited to the simplest Bell scenario, as well as to the choice of the post-processing strategy, specifically, assigning a pre-determined valid outcome whenever the measurement device fails to detect the incoming quantum system (the "no-click" event). We now describe a much more broadly applicable numerical method for the estimation of the critical parameters of individual measurement devices in generic network Bell scenarios.

A versatile numerical tool for estimation of critical parameters

For generic Bell scenarios, a more versatile measure of the nonlocal behavior of an individual measurement device, for instance, A_1 , which takes into the raw three-outcome experimental behavior, $\mathbf{p}_{(exp)}$, is the amount of certifiable randomness, $H_{min}(G_x(\mathbf{p}_{(exp)}))$, where $H_{min}(\cdot)$ is the min-entropy, and $G_x(\mathbf{p}_{(exp)})$ is maximum guessing probability³⁴,

$$\begin{aligned} G_x(\mathbf{p}_{(exp)}) &= \max_{\mathbf{p}_a} \sum_{\tilde{a} \in \{\pm 1, \perp\}} p_a(\tilde{a}|x, 1) \\ \text{s.t.} \quad &\sum_{\tilde{a} \in \{\pm 1, \perp\}} \mathbf{p}_a = \mathbf{p}_{(exp)} \\ &\forall \tilde{a} \in \{\pm 1, \perp\} : \mathbf{p}_a \in \mathbf{Q}, \end{aligned} \quad (16)$$

where $p_a(\tilde{a}|x, 1) = \sum_{\tilde{b} \in \{\pm 1, \perp\}} p_a(\tilde{a}, \tilde{b}|(x, 1), y)$, $\{\mathbf{p}_a \in \mathbb{R}_+^{72}\}$ are convex decompositions of the raw experimental behavior $\mathbf{p}_{(exp)} \in \mathbb{R}_+^{72}$, wherein we have absorbed the convex coefficients into the respective decompositions, and \mathbf{Q} is the convex set of quantum behaviors, $\mathbf{p} \equiv \{p(\tilde{a}, \tilde{b}|(x, i), y)\} \in \mathbb{R}_+^{72}$.

Observe that, for any behavior possessing a local hidden variable explanation for A_1 of the form (6), we can, without loss of generality, take the response schemes to be deterministic, i.e.,

$p_\lambda^A(a|x, i=1) \in \{0, 1\}$. This observation in-turn implies that for an experimental behavior $\mathbf{p}_{(exp)}$ possessing a local hidden variable explanation for Alice's device A_1 similar to (6), the outcomes of A_1 can always be perfectly guessed if one has access to the local hidden variable λ , such that $G_x(\mathbf{p}_{(exp)}) = 1$. On the contrary, if the outcomes of A_1 cannot be guessed perfectly (prior to the specific round of the experiment), i.e., the guessing probability optimization yields $G_x(\mathbf{p}_{(exp)}) < 1$, no local hidden variable explanation for the experimental behavior, similar to (6), exists. Consequently, the critical parameters for witnessing loophole-free nonlocality, $(\eta_{A_1}^*, \nu_{A_1}^*)$, correspond to the threshold values of (η_{A_1}, ν_{A_1}) , for which, $G_x(\mathbf{p}_{(exp)}) < 1$.

This measure is particularly well-suited for generic network Bell scenarios entailing many spatially separated parties, wherein we are interested in the certification of the nonlocal behavior of individual measurement devices when other measurement devices may or may not be already witnessing loophole-free nonlocality. Moreover, apart from the direct relevance to DI randomness certification, $H_{min}(G_x(\mathbf{p}_{(exp)}))$, constitutes a crucial ingredient in the security proofs of more complex DI cryptography protocols.

The optimization problem (16) is extremely arduous to solve because of the constraint $\mathbf{p}_{\tilde{a}} \in \mathbf{Q}$. Instead, to retrieve progressively tightening upper-bounds on the maximum guessing probability, $G_x(\mathbf{p}_{(exp)})$, and the estimation of the critical parameters $(\eta_{A_1}^*, \nu_{A_1}^*)$, we employ the Nieto-Silleras hierarchy of semi-definite programs^{33,34}, which relaxes the constraint $\mathbf{p}_{\tilde{a}} \in \mathbf{Q}$, to $\mathbf{p}_{\tilde{a}} \in \mathbf{Q}_L$, where \mathbf{Q}_L are the convex relaxations of the quantum set, \mathbf{Q} , corresponding to Navascués–Pironio–Acín hierarchy, $L \in \mathbb{N}_+$ denotes the level of the relaxation, such that, $\mathbf{Q} \subset \mathbf{Q}_{L+1} \subset \mathbf{Q}_L$ for all $L \in \mathbb{N}_+$, and $\lim_{L \rightarrow \infty} \mathbf{Q}_L = \mathbf{Q}$ ³⁸. In Fig. 3 we plot the critical detection efficiency of A_1 , $\eta_{A_1}^*$, versus its visibility ν_{A_1} , for an experimentally relevant case, while keeping the “no-click” as an additional outcome, $\tilde{a}, \tilde{b} \in \{\pm 1, \perp\}$, and using the second level of the Nieto-Silleras hierarchy, i.e., with the relaxed constraint $\mathbf{p}_{\tilde{a}} \in \mathbf{Q}_2$. In Fig. 3, we also plot the corresponding curve retrieved analytically using (9) and the assignment strategy, $\perp \mapsto +1$. The plot serves to

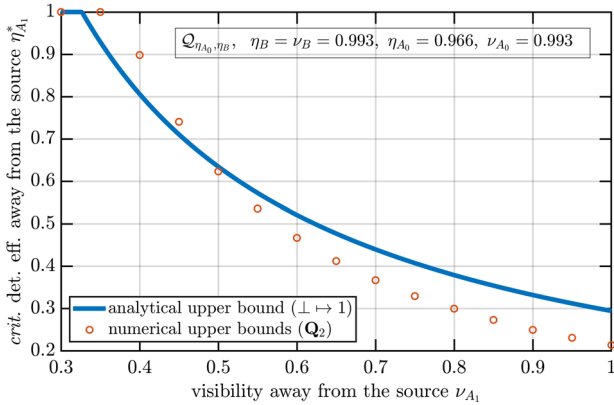


Fig. 3 Analytical versus numerical estimation. Upper bounds on the critical detection efficiency, $\eta_{A_1}^*$, of Alice's measurement device placed away from the source, versus the effective visibility between (A_1, B) , ν_{A_1} , calculated analytically using (9), when the parties use the tilted strategy, $\mathbf{Q}_{\eta_{A_0}, \nu_B}$, where $\eta_B = \nu_B = 0.993$, $\eta_{A_0} = 0.966$, $\nu_{A_0} = 0.993$, and the assignment strategy, $\perp \mapsto +1$ (solid blue curve), and numerically using certifiable randomness as a measure for the nonlocal behavior of A_1 , and the second level (\mathbf{Q}_2) of Nieto-Silleras hierarchy of semi-definite programs, while keeping the “no-click” event as an additional outcome, $\tilde{a}, \tilde{b} \in \{\pm 1, \perp\}$ (orange circles). The curves demonstrate the advantage of keeping the “no-click” as an additional outcome, $\tilde{a}, \tilde{b} \in \{\pm 1, \perp\}$ over the post-processing strategy of assigning a valid outcome to the “no-click” event, $\perp \mapsto +1$.

demonstrate the advantage of the numerical technique, and in particular, of keeping the entire raw experimental behavior over the analytical technique and the post-processing strategy of assigning a valid outcome to the “no-click” event.

DISCUSSION

In this work, we introduced a scheme to overcome the most significant impediment in realizing long-distance loophole-free nonlocal correlations, namely, the detection loophole. Our scheme exploits the properties of short-distance loophole-free nonlocal correlations, which can be readily attained in present-day Bell experiments to extend them to longer distances. Specifically, we considered Bell experiments wherein the involved parties randomly choose the location of their measurement devices in each round. To demonstrate the considered effect, we stuck to the most straightforward generalization of the Bell-CHSH experiment, wherein only Alice randomly chooses the location of her measurement devices based on an input $i \in \{0, 1\}$. However, our approach can be applied to more complex scenarios as well. For instance, consider the case wherein, along with Alice, Bob randomly chooses the location of his measurement device, B_j , based on an input $j \in \{0, 1\}$, in each round of the experiment (Fig. 4). When $i = j = 0$, both parties place their devices close to the source and witness strong loophole-free nonlocal correlations. Consequently, in the rounds when a party places their measurement device close to the source while the other places their device away from the source, i.e., when either $i = 0, j = 1$ or $i = 1, j = 0$, loophole-free nonlocal correlations can be certified at arbitrarily low detection efficiency and visibility. This observation, in turn, enables the certification of loophole-free nonlocal correlations between measurement devices placed arbitrarily far away from the source and each other when $i = j = 1$.

Physically moving the measurement device during the experiment is arduous and impractical. Therefore, experiments aimed at showcasing the considered effect could employ relay-switches, which alter the path of the quantum system transmitted from the source actively, which is to say, based on inputs from the involved parties, in each round of the experiment. We call such Bell experiments “routed” Bell experiments, specifically for the simple case depicted in Fig. 1, such a relay switch can be placed between the source and the measurement device A_1 . In each round of the experiment, Alice transmits her choice of $i \in \{0, 1\}$ to the relay switch, which then transmits the quantum system from the source to either the measurement device, A_0 , placed close to the source or A_1 , placed further away, based on the input from Alice, i .

The generalized or routed Bell experiments introduced in this work are closely related to the EPR steering scenarios³⁹; however, the “trust structure” is different. Specifically, in bipartite steering scenarios, the measurement device of one of the spatially separated parties, referred to as the “steering party”, is completely characterized or “trusted.” On the other hand, our treatment of the generalized or routed Bell experiments is completely DI, i.e., all devices along with the source remain completely uncharacterized or “untrusted”. We use the fact that the devices close to the source witness nonlocal correlations, specifically, a violation of CHSH inequality, to characterize Bob measurement device B subsequently. We then use this characterization of Bob's measurement device to derive operational consequences of local hidden variable models for A_1 , such as (9). Finally, we demonstrate the operational quantum violation of these consequences.

Besides increasing the distance over which loophole-free nonlocal correlations can be sustained, our scheme enables the certification of nonlocal behavior of off-the-shelf measurement devices. Finally, it follows from the proof of Theorem 1 that the parties can extend extremal loophole-free nonlocal correlations to an arbitrarily large number of additional measurement devices placed away from the source. These observations together enable

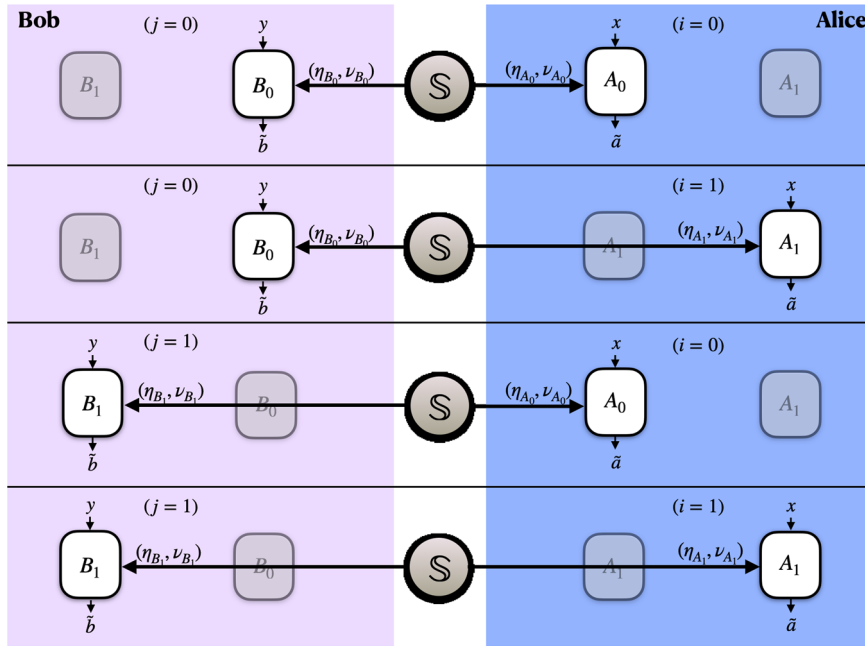


Fig. 4 Symmetric generalization. The graphic is a schematic depiction of the next generalization to the generalized or routed Bell experiment depicted in Fig. 1. Along with Alice, in each round of the experiment, Bob chooses the location of his measurement device, B_j , based on a randomly chosen input bit, $j \in \{0, 1\}$. When $j = 0$, Bob places his measurement device, B_0 , close to the source with an effective detection efficiency and visibility, (η_{B_0}, ν_{B_0}) . When $j = 1$, he places her measurement device, B_1 , further away from the source, with a lower detection efficiency and visibility, (η_{B_1}, ν_{B_1}) , such that $\eta_{B_1} < \eta_{B_0}, \nu_{B_1} < \nu_{B_0}$. Our results imply that in rounds with $i = j = 1$, loophole-free nonlocal correlations can be certified between the measurement devices, (A_1, B_1) , placed arbitrarily far away from each other.

applications such as a central hub equipped with expensive state-of-the-art measurement apparatus witnessing strong loophole-free nonlocal correlations and distributing them to an arbitrary number of remotely located commercial off-the-shelf measurement devices, making loophole-free nonlocality much more broadly accessible. To summarize, we anticipate our findings to significantly accelerate the advent of DI information processing as a near-term commonplace technology.

Apart from the direct application of the routed Bell experiments introduced here to Device Independent Randomness Certification with very inefficient detectors, the fact that local hidden variable explanations of the form (4) and (6) are isomorphic to quantum explanations entailing local measurements on separable states implies that the violation of their operational consequences, such as the violation of the trade-off (9), in routed Bell experiments can enable Device Independent Entanglement Certification and Quantification⁴⁰ at arbitrarily large distances. Moreover, the scheme proposed in this work can implement DIQKD protocols, enabling remote measurement devices to share a secret key. Although naive DIQKD protocols based on this scheme are secure against passive source-based attacks and eavesdroppers placed between the source and Alice's closest measurement device A_0 , they are susceptible to active device-controlling attacks by eavesdroppers placed between Alice's measurement devices (A_0, A_1). Specifically, in the Supplementary Note, we demonstrate that for a measurement device with N inputs and N' outputs, there exist two distinct active attacks which render any DIQKD protocol insecure whenever the detection efficiency of such a measurement device is below $\min\{\frac{1}{N}, \frac{1}{N'}\}$. In our set-up this translates to a minimum detection efficiency of $\frac{1}{2}$ for all measurement devices for completely secure DIQKD. Therefore, a crucial open question remains whether the generalized or routed Bell experiments introduced in this work can be used to implement improved DIQKD protocols with lower critical detection efficiency and visibility requirements than standard DIQKD protocols.

Furthermore, while the bipartite quantum strategies considered here are well suited to the routed Bell experiments, tripartite no-signaling quantum strategies are an interesting alternative natural generalization to the local hidden variable models described in (6). Specifically, probability distributions explainable via such local hidden variable models can be interpreted as those stemming from local measurements performed on a shared tripartite classical-quantum-quantum state. It then follows that the most obvious modeling of the fully quantum case is promoting the classical register of Alice's distant device to a quantum register such that the devices measure a tripartite quantum-quantum-quantum state. However, such tripartite quantum strategies have an additional implicit no-signaling constraint between Alice's devices compared to the bipartite quantum strategies considered in the article. Consequently, even the most straightforward experimentally implementable quantum strategy for the generalized or routed Bell experiments wherein the source shares (potentially noisy) maximally entangled states to the devices cannot be accounted for by such tripartite quantum strategies, nor could such strategies violate the trade-off (9). Nevertheless, it is interesting to explore in more detail the role of tripartite quantum strategies, especially strategies involving genuine tripartite entanglement in routed Bell experiments. Finally, it would be interesting to replace the guessing probability maximization (16) with the minimization of conditional von Neumann entropies⁴¹ and investigate the behavior in the context of the generalized or routed Bell experiments introduced in this work.

Note Added: After completion and communication of the first version of our manuscript we were informed of an independent work⁴² which resolves the open question of enabling DIQKD protocols based on the routed Bell experiments introduced in this article with lower critical requirements than standard DIQKD schemes. In particular, the scheme employs jointly-measurable measurements for Alice's device A_1 as classical models, instead of the local hidden variable models invoked here.

Received: 25 July 2023; Accepted: 14 December 2023;
Published online: 11 January 2024

REFERENCES

- Bell, J. S. On the Einstein Podolsky Rosen paradox. *Phys. Phys. Fiz.* **1**, 195–200 (1964).
- Brunner, N., Cavalcanti, D., Pironio, S., Scarani, V. & Wehner, S. Bell nonlocality. *Rev. Mod. Phys.* **86**, 419–478 (2014).
- Ekert, A. K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **67**, 661–663 (1991).
- Mayers, D. & Yao, A. Quantum cryptography with imperfect apparatus. In *Proceedings 39th Annual Symposium on Foundations of Computer Science*, 503 (IEEE, Los Alamitos, CA, 1998).
- Barrett, J., Hardy, L. & Kent, A. No signaling and quantum key distribution. *Phys. Rev. Lett.* **95**, 010503 (2005).
- Acín, A. et al. Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.* **98**, 230501 (2007).
- Vazirani, U. & Vidick, T. Fully device-independent quantum key distribution. *Phys. Rev. Lett.* **113**, 140501 (2014).
- Primaatmaja, I. W. et al. Security of device-independent quantum key distribution protocols: a review. *Quantum* **7**, 932 (2023).
- Colbeck, R. *Quantum and relativistic protocols for secure multi-party computation*. Ph.D. thesis, University of Cambridge (2009). <https://arxiv.org/abs/0911.3814>.
- Pironio, S. et al. Random numbers certified by Bell's theorem. *Nature* **464**, 1021–1024 (2010).
- Liu, W.-Z. et al. Device-independent randomness expansion against quantum side information. *Nat. Phys.* <https://doi.org/10.1038/s41567-020-01147-2> (2021).
- Shalm, L. K. et al. Device-independent randomness expansion with entangled photons. *Nat. Phys.* <https://doi.org/10.1038/s41567-020-01153-4> (2021).
- Pearle, P. M. Hidden-variable example based upon data rejection. *Phys. Rev. D* **2**, 1418–1425 (1970).
- Clauser, J. F., Horne, M. A., Shimony, A. & Holt, R. A. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.* **23**, 880–884 (1969).
- Garg, A. & Mermin, N. D. Detector inefficiencies in the Einstein-Podolsky-Rosen experiment. *Phys. Rev. D* **35**, 3831–3835 (1987).
- Optical fiber loss and attenuation. <https://www.fiberoptics4sale.com/blogs/archive-posts/95048006-optical-fiber-loss-and-attenuation>. Accessed: 2022-11-25.
- Gerhardt, I. et al. Experimentally faking the violation of Bell's inequalities. *Phys. Rev. Lett.* **107**, 170404 (2011).
- Zapatero, V. et al. Advances in device-independent quantum key distribution. *npj Quantum Inf.* **9**, 10 (2023).
- Eberhard, P. H. Background level and counter efficiencies required for a loophole-free Einstein-Podolsky-Rosen experiment. *Phys. Rev. A* **47**, R747–R750 (1993).
- Massar, S. Nonlocality, closing the detection loophole, and communication complexity. *Phys. Rev. A* **65**, 032121 (2002).
- Vértesi, T., Pironio, S. & Brunner, N. Closing the detection loophole in Bell experiments using qudits. *Phys. Rev. Lett.* **104**, 060401 (2010).
- Miklin, N., Chaturvedi, A., Bourennane, M., Pawłowski, M. & Cabello, A. Exponentially decreasing critical detection efficiency for any Bell inequality. *Phys. Rev. Lett.* **129**, 230403 (2022).
- Xu, Z.-P. et al. Graph-theoretic approach to Bell experiments with low detection efficiency. *Quantum* **7**, 922 (2023).
- Larsson, J.-Å. & Semitecolos, J. Strict detector-efficiency bounds for n-site Clauser-Horne inequalities. *Phys. Rev. A* **63**, 022117 (2001).
- Cabello, A., Rodríguez, D. & Villanueva, I. Necessary and sufficient detection efficiency for the Mermin inequalities. *Phys. Rev. Lett.* **101**, 120402 (2008).
- Pál, K. F., Vértesi, T. & Brunner, N. Closing the detection loophole in multipartite Bell tests using Greenberger-Horne-Zeilinger states. *Phys. Rev. A* **86**, 062111 (2012).
- Cabello, A. & Larsson, J.-Å. Minimum detection efficiency for a loophole-free atom-photon Bell experiment. *Phys. Rev. Lett.* **98**, 220402 (2007).
- Brunner, N., Gisin, N., Scarani, V. & Simon, C. Detection loophole in asymmetric Bell experiments. *Phys. Rev. Lett.* **98**, 220403 (2007).
- Garbarino, G. Minimum detection efficiencies for a loophole-free observable-asymmetric Bell-type test. *Phys. Rev. A* **81**, 032106 (2010).
- Araújo, M. et al. Tests of Bell inequality with arbitrarily low photodetection efficiency and homodyne measurements. *Phys. Rev. A* **86**, 030101 (2012).
- Lim, C. C. W., Portmann, C., Tomamichel, M., Renner, R. & Gisin, N. Device-independent quantum key distribution with local Bell test. *Phys. Rev. X* **3**, 031006 (2013).
- Giustina, M. et al. Significant-loophole-free test of Bell's theorem with entangled photons. *Phys. Rev. Lett.* **115**, 250401 (2015).
- Nieto-Silleras, O., Pironio, S. & Silman, J. Using complete measurement statistics for optimal device-independent randomness evaluation. *New J. Phys.* **16**, 013035 (2014).
- Bancal, J.-D., Sheridan, L. & Scarani, V. More randomness from the same data. *New J. Phys.* **16**, 033011 (2014).
- Czechlewski, M. & Pawłowski, M. Influence of the choice of postprocessing method on Bell inequalities. *Phys. Rev. A* **97**, 062123 (2018).
- Šupić, I. & Bowles, J. Self-testing of quantum systems: a review. *Quantum* **4**, 337 (2020).
- Acín, A., Massar, S. & Pironio, S. Randomness versus nonlocality and entanglement. *Phys. Rev. Lett.* **108**, 100402 (2012).
- Navascués, M., Pironio, S. & Acín, A. A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. *New Journal of Physics* **10**, 073013 (2008).
- Xiang, Y., Cheng, S., Gong, Q., Ficek, Z. & He, Q. Quantum steering: Practical challenges and future directions. *PRX Quantum* **3**, 030102 (2022).
- Moroder, T., Bancal, J.-D., Liang, Y.-C., Hofmann, M. & Gühne, O. Device-independent entanglement quantification and related applications. *Phys. Rev. Lett.* **111**, 030501 (2013).
- Brown, P., Fawzi, H. & Fawzi, O. Computing conditional entropies for quantum correlations. *Nat. Commun.* **12**, 575 (2021).
- Lobo, E. P., Pauwels, J. & Pironio, S. Certifying long-range quantum correlations through routed Bell tests (2023). 2310.07484.
- Wittek, P. Algorithm 950: Ncpol2sdpa—sparse semidefinite programming relaxations for polynomial optimization problems of noncommuting variables. *ACM Trans. Math. Softw. (TOMS)* **41**, 1–12 (2015).
- Löfberg, J. Yalmip: A toolbox for modeling and optimization in Matlab. In *Proc. ACSD Conference* (Taipei, Taiwan, 2004).
- ApS, M. *The MOSEK optimization toolbox for MATLAB manual. Version 9.0*. <http://docs.mosek.com/9.0/toolbox/index.html> (2019).

ACKNOWLEDGEMENTS

We are grateful to Ekta Panwar, Nicolás Gigena, and Piotr Mironowicz, Jef Pauwels, Tamás Vértesi, Renato Renner, Stefano Pironio & Marek Żukowski for enlightening discussions. This work was partially supported by the Foundation for Polish Science (IRAP project, ICTQT, contract No. MAB/218/5, co-financed by EU within the Smart Growth Operational Programme) and partially supported by the Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korean government (MSIT) (No.2022-0-00463, Development of a quantum repeater in optical fiber networks for quantum internet). MP also acknowledges financial support from QuantERA, an ERA-Net co-fund in Quantum Technologies (www.quantera.eu), under project eDICT (contract No. Quantera/2/2020). The numerical optimization was carried out using [Ncpol2sdpa](https://github.com/ncpol2sdpa)⁴³, [YALMIP](https://github.com/yalmip)⁴⁴, and [MOSEK](https://github.com/mosek)⁴⁵.

AUTHOR CONTRIBUTIONS

All authors contributed equally to this manuscript.

COMPETING INTERESTS

The authors declare no competing interests.

ADDITIONAL INFORMATION

Supplementary information The online version contains supplementary material available at <https://doi.org/10.1038/s41534-023-00799-1>.

Correspondence and requests for materials should be addressed to Anubhav Chaturvedi.


Reprints and permission information is available at <http://www.nature.com/reprints>

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this license, visit <http://creativecommons.org/licenses/by/4.0/>.

© The Author(s) 2024

Quantum strategies for rendezvous and domination tasks on graphs with mobile agentsGiuseppe Viola ^{1,*} and Piotr Mironowicz ^{1,2,3,†}¹*International Centre for Theory of Quantum Technologies, University of Gdańsk, Wita Stwosza 63, 80-308 Gdańsk, Poland*²*Department of Physics, Stockholm University, S-10691 Stockholm, Sweden*³*Department of Algorithms and System Modeling, Faculty of Electronics, Telecommunications and Informatics, Gdańsk University of Technology, 80-308 Gdańsk, Poland* (Received 22 November 2023; revised 28 February 2024; accepted 4 March 2024; published 4 April 2024)

This paper explores the application of quantum nonlocality, a renowned and unique phenomenon acknowledged as a valuable resource. Focusing on an alternative application, we demonstrate its quantum advantage for mobile agents engaged in specific distributed tasks without communication. The research addresses the significant challenge of rendezvous on graphs and introduces a distributed task for mobile agents grounded in the graph domination problem. Through an investigation across various graph scenarios, we showcase the quantum advantage. Additionally, we scrutinize deterministic strategies, highlighting their comparatively lower efficiency compared to quantum strategies. The paper concludes with a numerical analysis, providing further insights into our findings.

DOI: [10.1103/PhysRevA.109.042201](https://doi.org/10.1103/PhysRevA.109.042201)**I. INTRODUCTION**

Quantum information has emerged as a valuable asset in a multitude of tasks inherent to information and communication technologies. Remarkably, quantum cryptography stands out as an example, where the harnessing of quantum entanglement has paved the way for innovative protocols ensuring secure key exchange and robust randomness certification [1]. Despite these achievements, the phenomena of Bell inequalities and nonlocality, which defy the boundaries of correlations allowed in classical physics [2,3], have remained largely unexplored for other pragmatic endeavors. In particular, their potential for distributed tasks in facilitating the coordination of actions among distributed agents with a shared goal, even in situations with limited or no communication, remains almost untapped [4], with preliminary trials in [5,6].

In the realm of quantum information, the accomplishments have been particularly pronounced in quantum cryptography [1], where the manipulation of quantum entanglement has enabled the creation of novel protocols guaranteeing the confidentiality and integrity of exchanged keys, as well as certifying the security of random data [7]. The potential of quantum phenomena achieved with the aid of entanglement has been illustrated by multiple examples of so-called nonlocal games [8–10]. A prominent example of them are the exclusive alternative (XOR) games [11], and generalizations thereof [12–15]. However, amidst these striking achievements, the captivating domains of Bell inequalities and nonlocality [16], which intrinsically challenge the limitations imposed by classical physics on correlations, have not been widely applied to other practical tasks. A notable area that

remains unexplored is their potential application in orchestrating the collaboration of distributed agents striving towards a collective objective, even in scenarios where communication is restricted or absent, like the rendezvous task [17].

This paper delves into the realm of quantum entanglement and its application in coordinating distributed tasks on graphs. The groundwork is laid with two fundamental problems of graph theory: rendezvous and graph domination [18]. These problems serve as the foundation for exploring the potential benefits of quantum entanglement in achieving coordinated actions among distributed agents striving to achieve a common goal on graphs. We continue and extend the investigations initiated in [6] where it was shown how to exploit quantum resources for the rendezvous task.

To tackle this topic, we use semidefinite programming (SDP) [19–21], in particular two prominent methods: the Navascués-Pironio-Acín method (NPA) [22,23] and the seesaw method [24]. These techniques offer valuable insights into the quantum nonlocality, which challenges the boundaries set by classical physics. We explore how quantum entanglement enables distributed agents to achieve rendezvous with no communication, surpassing classical constraints. Then, the paper introduces the domination distributed task for agents. We are in this way laying out the framework for incorporating quantum entanglement as a resource for enhanced coordination. To demonstrate the practical implications of the findings, the paper presents a series of numerical calculations and examples involving various graph structures. These numerical simulations showcase the effectiveness of quantum entanglement in scenarios of distributed actions of agents, illustrating the potential advantages of using quantum strategies over classical ones.

The organization of this paper is the following. In Sec. II we discuss the two relevant problems of graph theory, viz., the task of rendezvous of mobile agents, and the problem

*giuseppe.viola.res@gmail.com

†piotr.mironowicz@gmail.com

of domination number in graphs. We show how to turn the latter problem into a task for mobile agents. Then we discuss multipartite probability distributions in classical and quantum physics and show how to express distributed tasks as so-called Bell, or nonlocal, games investigated in quantum theory. In Sec. III we briefly describe the numerical methods used in this paper based on SDP. Next, in Sec. IV we provide analytical results about deterministic strategies that can be used by the agents for the tasks. The results showing the quantum advantage of the tasks are presented in Sec. V. We discuss the obtained results in Sec. VI and conclude in Sec. VII.

II. DISTRIBUTED TASKS FOR AGENTS

We will now describe the tasks for mobile agents investigated in this paper. The rendezvous task is discussed in Sec. II A. In Sec. II B we cover the domination number of graphs and then propose a distributed task inspired by it. The examples of graphs considered in this paper are given in Sec. II C together with definitions of selected terms used in describing mobile agents. In Sec. II D we introduce classical and quantum probability distributions and Bell games. Finally, in Sec. II E we show how to relate distributed tasks with Bell games.

A. Rendezvous on graphs

The rendezvous problem, as formulated by Alpern [17], is a mathematical problem that deals with the challenge of two or more mobile agents trying to meet at a specific location without any form of communication. In its simplest form, the rendezvous problem involves two mobile agents, referred to as players or parties, that are initially located in different positions within a known environment. The objective is for both players to reach a common meeting point simultaneously. The key constraint is that the players cannot communicate with each other and have no knowledge of each other's current position.

To elucidate the concept of the rendezvous problem we refer to the following two motivating examples. The first one is named the telephone problem and is formulated as follows: "In each of two rooms, there are n telephones randomly strewn about. They are connected in a pairwise fashion by n wires. At discrete times $t = 0, 1, 2, \dots$ players in each room pick up a phone and say 'hello.' They wish to minimize the time t when they first pick up paired phones and can communicate" [25]. This problem is the spatial rendezvous on a complete graph, i.e., a graph where an edge exists between every pair of vertices.

The second motivating problem is the Mozart Café rendezvous problem: "Two friends agree to meet for lunch at the Mozart Café in Vienna on the first of January, 2000. However, on arriving at Vienna airport, they are told there are three (or n) cafés with that name, no two close enough to visit on the same day. So each day each can go to one of them, hoping to find his friend there" [26].

One variant of the rendezvous problem is the "symmetric rendezvous" where both players have equal capabilities and constraints or are following the same strategy [27–30]. In this case, the goal is to find a strategy that ensures both players meet at some vertex, regardless of their initial posi-

tions. Another variant is the "asymmetric rendezvous," where the players have different capabilities or constraints and are following the same strategy [31–34]. For example, one player may have limited mobility or restricted vision compared to the other player. In this case, the objective is to find a strategy that maximizes the probability of meeting at the rendezvous point while taking into account the differences in capabilities.

The importance of studying the rendezvous problem lies in its relevance to various real-world applications. For instance, in search and rescue missions, autonomous robots or drones may need to coordinate their movements to cover a large area efficiently and meet at a specific location to exchange information or resources. Similarly, in autonomous vehicle systems, vehicles may need to coordinate their routes and timing to avoid collisions and efficiently utilize shared resources like charging stations [35].

By understanding and solving the rendezvous problem, researchers can develop efficient strategies for coordinating multiple agents without relying on direct communication. This can lead to improved efficiency, resource utilization, and safety in various domains. More generally, the problem is about coordinating action when the communication is prohibited or severely limited; see, e.g., [36] for an overview.

For this paper, we will use the following definition.

Definition 1. Given a graph, and a number $h \geq 1$, the *rendezvous task* is defined as the task in which $r \geq 2$ agents, placed uniformly randomly among the vertices of the graph, move along edges of the graph h times. They are successful if, after crossing the edges h times, they are all positioned in the same vertex. They can establish a strategy before being placed on the graph, but they are not allowed to communicate before each of the agents has completed their move.

If $h = 1$ then the rendezvous task is called *single-step*.

Note that, for the single-step task, to allow strategies for which the agents can end their movement on the same vertex in which they started, each of the vertices of the graph must be connected with itself.

B. Domination on graphs

The domination number is a fundamental concept in graph theory [37,38]. It quantifies the minimum number of vertices needed to control, or dominate, all other vertices in a graph. In essence, it identifies the smallest set of vertices where each vertex either belongs to the set or is adjacent to at least one member of the set. Formally, consider a graph $G = (N, E)$ with a vertex set N and an edge set E . A dominating set D is a subset of N such that every vertex in N is either part of D or adjacent to a vertex in D . The domination number, denoted as $\gamma(G)$, is defined as the minimum cardinality of any dominating set D .

Various variants of the domination number exist, each imposing specific conditions on dominating sets. Common variants include the following.

(1) Total domination number [39,40]: This requires that every vertex in the graph is adjacent to at least one vertex in the dominating set, ensuring direct control over each vertex.

(2) Independent domination number [41–43]: In this variant, the dominating set must also be an independent set, meaning no two vertices in the set are adjacent. This variant seeks dominating sets without redundant control.

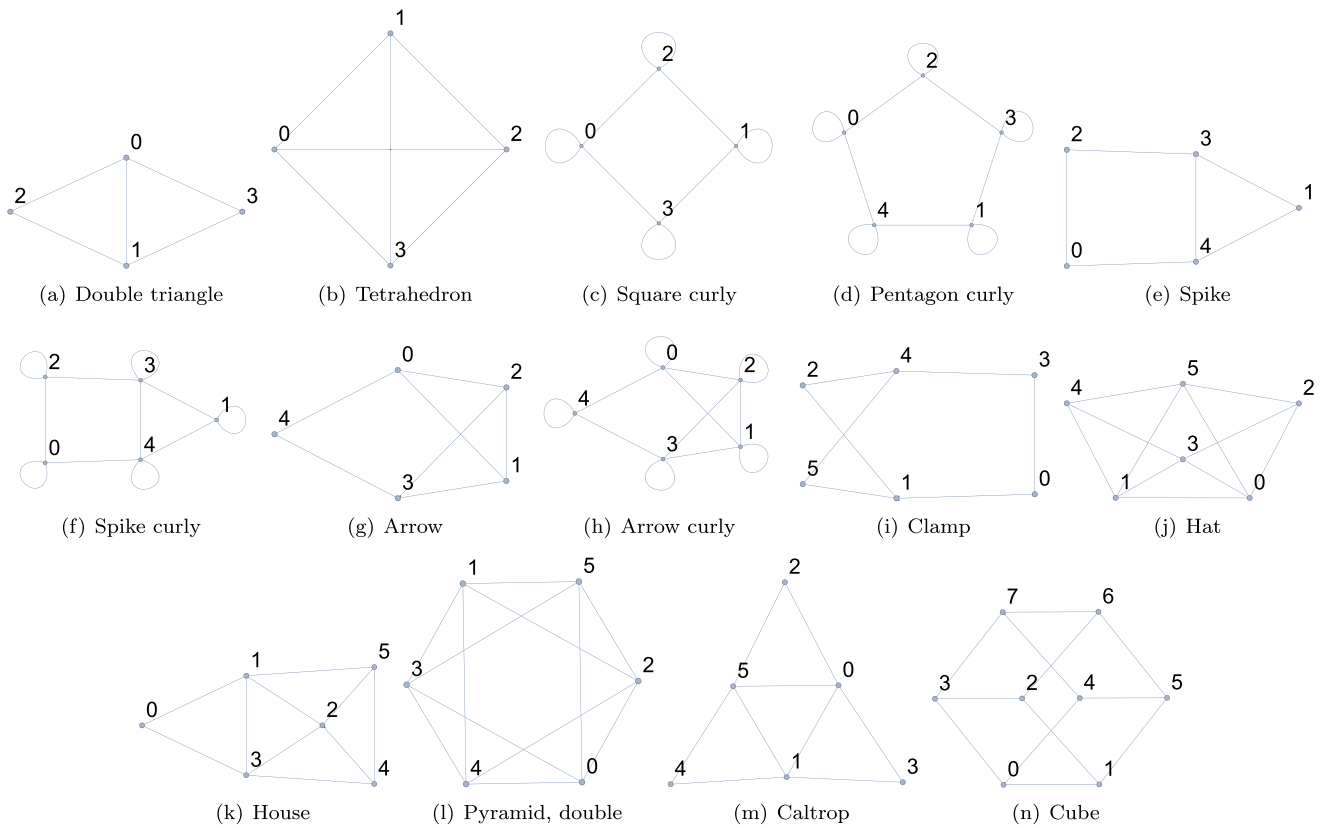


FIG. 1. Some of the graphs analyzed in this paper.

(3) Connected domination number [44]: Here, the dominating set must induce a connected subgraph, ensuring an efficient path between any two vertices in the set for comprehensive control over the entire graph.

The domination number and its variants have various applications and usefulness in different domains. For network design, the domination number can be used to optimize network design problems, such as determining the minimum number of sensors or routers required to monitor or control a network effectively. By finding an optimal dominating set, resources can be allocated efficiently while maintaining network connectivity. In the area of facility location, this quantity can help in determining the optimal location of facilities, such as hospitals, fire stations, or surveillance cameras, to ensure maximum coverage and control over a given area. By minimizing the domination number, the cost and resources required for facility placement can be reduced. The domination number can be also applied in social network analysis to identify influential individuals or groups. By finding dominating sets in social networks, it is possible to identify key players who have control or influence over a large portion of the network.

The domination problem until now has been investigated only from the static global point of view, where the entity was deciding which vertices can be used to dominate the graph. In our paper, we propose a distributed approach to the problem and treat it as a dynamic task of a group of mobile agents who start at not known in advance locations, and want to organize themselves without communication so that they dominate as

large part of a graph as possible. To be more specific, in this paper, we use the following definition.

Definition 2. Given a graph, and a number $h \geq 1$, the *domination task* is defined as the task in which $r \geq 2$ agents, placed uniformly randomly among the vertices of the graph, move along edges of the graph h times. They try to dominate as many vertices as they can, counting the dominated points only after all the agents completed their moves.

A vertex is said to be dominated when an agent occupies it or it is connected with an edge to a vertex where there is an agent.

The agents can establish a strategy before being placed on the graph, but they are not allowed to communicate before each of the agents has completed their move.

If $h = 1$ then the domination task is called *single-step*.

Note that, for the single-step task, to allow strategies for which the agents can end their movement on the same vertex in which they started, each vertex of the graph must be connected with itself.

C. Considered scenarios and definitions

In Fig. 1 we present some of the graph scenarios with which we dealt. With the name “ n -gon” we refer to the graphs described by a polygon with n vertices, with the name “ n -line” we refer to the graphs described by a line connecting n vertices, while with the name “ n -line curly” we refer to a n -line graph where the extrema are connected with themselves.

With the exception of the n -line curly graphs, for which we provided a specific definition, for all the graphs we included

the word “curly” in their name when each of their vertices is connected with itself.

Let r denote the number of agents performing a given distributed task, let N be the set of all the nodes of the considered graph, and let n be the number of nodes, $n = |N|$. Let us introduce the following notation.

(1) $p_i(a|x)$ denotes the probability that the i th agent will go to the node $a \in N$ when starting from the node $x \in N$.

(2) $S_i := \{p_i(a|x)\}_{a,x \in N}$ is the classical strategy for the i th agent.

(3) $p_i(a) := \frac{1}{n} \sum_{x \in N} p_i(a|x)$ is the probability to find the i th agent in the node $a \in N$.

(4) $\tilde{S}_i := \{p_i(a)\}_{a \in N}$.

Note that \tilde{S}_i is uniquely determined by the set S_i . A strategy is called deterministic (for all the agents) if and only if all the elements of S_i , $\forall i \in \{1, \dots, r\}$, are either zeros or ones. Given the set of strategies adopted by the agents $\{S_i\}_{i \in \{1, \dots, r\}}$, the strategies S_i 's are called *symmetric* if they are all equal among each other.

D. Classical and quantum probabilities and Bell games

The classical joint probability distribution $P(a, b|x, y)$ for obtaining outcomes a and b in response to inputs x and y is expressed as a sum over a hidden variable λ , viz.,

$$P(a, b|x, y) = \sum_{\lambda} P(\lambda) P_{A|x, \Lambda}(a|x, \lambda) P_{B|y, \Lambda}(b|y, \lambda). \quad (1)$$

Each term in the sum corresponds to a specific hidden state λ and is weighted by the probability $P(\lambda)$ of observing that hidden state. The conditional probabilities $P_{A|x, \Lambda}(a|x, \lambda)$ and $P_{B|y, \Lambda}(b|y, \lambda)$ represent the likelihood of obtaining outcomes a and b for Alice and Bob, respectively, given their inputs x and y and the hidden state λ . The probability distribution $P_{\Lambda}(\lambda)$ characterizes the likelihood of different hidden internal states. The normalization condition $\sum_{\lambda \in \Lambda} P_{\Lambda}(\lambda) = 1$ ensures that the probabilities are properly scaled. This formulation captures the classical statistical description of the behavior of the devices and is often called a local hidden variables (LHV) model, which assumes that the measurement outcomes are determined by preexisting properties of the system that are independent of the measurement settings.

A bipartite quantum probability distribution of joint measurement results refers to the statistical distribution of outcomes obtained from a joint measurement performed on a bipartite quantum system. The bipartite system is described by a density operator ρ . The joint measurement performed by Alice and Bob is typically represented by a set of positive operator-valued measures (POVMs), denoted as $M(a, x)$ [$N(b, y)$], where a (b) and x (y) represent the measurement outcomes and settings of Alice (Bob). These POVMs satisfy the completeness relation $\sum_a M(a, x) = \mathbb{1}$ [$\sum_b N(b, y) = \mathbb{1}$], where $\mathbb{1}$ is the identity operator [45].

The bipartite quantum probability distribution $P(a, b|x, y)$ gives the probability of obtaining measurement outcomes a and b when Alice and Bob use measurement settings x and y , respectively. It is calculated using the Born rule, which states that the probability is given by

$$P(a, b|x, y) = \text{Tr}[\rho M(a, x) \otimes N(b, y)]. \quad (2)$$

Here, $\text{Tr}[\rho M(a, x) \otimes N(b, y)]$ represents the trace of the product of the density operator ρ and the corresponding POVM elements $M(a, x)$ and $N(b, y)$. The bipartite quantum probability distribution captures the correlations between Alice's and Bob's measurement outcomes. These correlations can exhibit various phenomena such as entanglement, nonlocality, or classical correlations depending on the quantum state ρ . We denote the set of all possible quantum bipartite probability distributions by \mathcal{Q} .

A bipartite game is a linear functional over probability distribution of the form

$$\mathcal{B}[P(a, b|x, y)] = \sum_{a, b, x, y} \beta_{a, b, x, y} P(a, b|x, y) \quad (3)$$

for some coefficients $\{\beta_{a, b, x, y}\}$. Equation (3) can be easily generalized to more parties.

It is worth noting that in some cases, the bipartite quantum probability distribution may be incompatible with classical theories. This means that it cannot be explained solely by LHV models. If this is the case for a given game, then such a game is called a Bell game or nonlocal game [2,3]. Its maximal value over classical distributions is called the classical bound and denoted C , and its maximal value over quantum distributions is called the Tsirelson bound and denoted by Q [8], $Q > C$.

In the case in which the agents participating in the domination or rendezvous tasks have access to quantum resources, they share a chosen quantum state before being placed on the graph. Once on the graph, they can measure their own state depending on the node they are at and choose which node to move to based on the outcome of their local measurement.

E. Distributed tasks as Bell games

The success probability of a distributed task involving two agents, Alice and Bob, can be expressed as a linear functional of joint probabilities $P(a, b|x, y)$, where successes are assigned a coefficient of 1 and failures are assigned a coefficient of 0. This approach allows us to quantify the likelihood of success based on the joint probabilities of the agents' actions and observations.

To understand this concept better, let us break down the notation used. In this point of view the probabilities $P(a, b|x, y)$ as defined in Sec. IID represent the joint probability distribution of Alice's action a , Bob's action b , Alice's observation x , and Bob's observation y . Thus, it captures the probabilistic relationship between the actions and observations of both agents. We note that the observation is performed depending on the agent's local situation, like information about its position in a graph, and the action depends on the measurement result.

Indeed, in a distributed task, Alice and Bob may need to coordinate their actions or make decisions based on their individual observations. The success of the task depends on how well they align their actions and observations to achieve the desired outcome. By considering the joint probabilities $P(a, b|x, y)$, we can analyze the likelihood of success in different scenarios. To express the success probability as a linear functional, we assign coefficients to each possible outcome (success or failure) based on its desirability. In this case,

successes are assigned a coefficient of 1, indicating their importance in determining overall success. Failures, on the other hand, are assigned a coefficient of zero since they do not contribute to the success of the task. Let $S(a, b, x, y)$ be a relevant scoring function of a distributed task. Using the coefficients for all possible outcomes and their corresponding joint probabilities, we obtain a linear combination that represents the score as

$$\sum_{a,b,x,y} S(a, b, x, y) \times P(a, b|x, y), \quad (4)$$

which is in the form of a bipartite game. This approach allows us to quantify the likelihood of success in distributed tasks by considering the joint probabilities and assigning appropriate coefficients to different outcomes. By manipulating these coefficients, we can prioritize certain outcomes or adjust the importance of different actions and observations in determining success or normalize events to interpret the score as a success probability of a task.

This approach allows us to analyze the likelihood of success based on the agents' actions and observations and compare the capabilities possible in classical and quantum probability distributions. We say that we have a quantum advantage for a given task if the score is a Bell game with $Q > C$.

III. NUMERICAL OPTIMIZATION METHODS

In this section, we describe the SDP method in Sec. III A. This optimization technique is used to formulate two tools allowing for calculations of the success measure in distributed tasks, viz., NPA and see-saw. The former, discussed in Sec. III B, provides upper, and the latter, discussed in Sec. III C, lower bounds on successes, respectively.

A. Semidefinite programming

SDP is a mathematical optimization technique that extends the concepts of linear programming to handle matrices and, in particular, positive semidefinite matrices. It addresses problems where the goal is to optimize a linear objective function subject to linear equality and semidefinite inequality constraints. SDP finds applications in diverse fields [46], including quantum information [19–21]. Advancements in algorithmic design and improvements in computational power have significantly enhanced the efficiency of SDP solvers. Modern interior-point methods [47] have proven to be effective in solving large-scale SDP, making them a versatile tool for addressing complex optimization problems [48]. For $m, n \in \mathbb{N}_+$ the primal optimization task of SDP is

$$\text{minimize } c^T x \text{ subject to } F(x) \geq 0, \quad (5)$$

where $c \in \mathbb{R}^m$, $F(x) := F_0 + \sum_{i=1}^m x_i F_i$, $F_i \in \mathbb{R}^{n \times n}$, and $x \in \mathbb{R}^m$ is the variable. The so-called dual of this problem with a symmetric matrix variable $Z \in \mathbb{R}^{n \times n}$ is

$$\begin{aligned} \text{maximize } & -\text{Tr}[F_0 Z] \text{ subject to } \text{Tr}[F_i Z] = c_i, \\ & \text{for } i = 1, \dots, m, Z \geq 0. \end{aligned} \quad (6)$$

B. Navascués-Pironio-Acín method

The NPA method, introduced by Navascués *et al.* in 2007 [22], is a mathematical framework used to study quantum correlations and entanglement in quantum information theory. It provides a systematic approach to analyze the behavior of quantum systems and their correlations. Recall that in quantum mechanics, entanglement refers to the phenomenon where two or more particles become correlated in such a way that their states cannot be described independently. These correlations are stronger than any classical (or local) correlations and play a crucial role in various quantum information processing tasks.

This technique aims to quantify and characterize these quantum correlations by constructing a hierarchy of SDPs. The hierarchy is defined by introducing a sequence of operators that capture the correlations between systems under consideration and are associated with different levels of the hierarchy. Moving up the hierarchy, at each level, new sequences of operators are introduced that constrain or restrict additional correlations beyond those captured at lower levels. The NPA method provides a systematic way to compute these moment operators at each level and study the properties of quantum correlations rigorously. In this paper, we employ the so-called almost quantum [49] level $1 + ab$, and more precise, but also more computationally demanding, level 2.

Let us now explain NPA in more detail. As we mentioned, quantum probability distributions $P(a, b|x, y)$ [see Eq. (2)] are challenging to characterize due to their inherent complexity. Recall that they belong to the set \mathcal{Q} if certain conditions are met, namely, if there exists a Hilbert space \mathcal{H} , a state (vector) $|\psi\rangle$, and a set of operators (measurements) $\{E_x^a, E_y^b\}_{a,b,x,y}$ satisfying specific criteria. These criteria include Hermitian properties of operators, orthogonality of different measurement outcomes, normalization conditions, and commutativity of measurements between Alice and Bob. The probability distribution is then expressed as an inner product involving measurements of the quantum states. However, characterizing \mathcal{Q} without quantum formalism poses a challenge. The NPA method provides a solution by defining a hierarchy $\{\mathcal{Q}_k\}_{k=1}^\infty$ of SDP problems. This hierarchy offers increasingly accurate approximations of \mathcal{Q} , with higher levels yielding more precise solutions, albeit at the expense of increased computational complexity. Ultimately, the hierarchy converges to the quantum set \mathcal{Q} [23], reflecting the effectiveness of the NPA method in characterizing quantum correlations.

A sequence of operators is formed by concatenating projective measurement operators. For instance, $E_2^1 E_2^3 F_1^2 E_1^1$ represents a sequence of four operators. Exploiting the commutativity of Alice's operators E_x^a with Bob's operators F_y^b , we can rearrange the sequence as $E_2^1 E_2^3 E_1^1 F_1^2$. Given that $E_x^a E_x^{a'} = 0$ and $F_y^b F_y^{b'} = 0$ for $a \neq a'$ and $b \neq b'$, and leveraging the commutation property, we obtain, for instance, $E_1^2 F_3^3 E_1^1 = E_1^2 E_1^1 F_3^3 = 0$ since E_1^2 and E_1^1 are orthogonal. Moreover, as E_x^a are projectors, $(E_x^a)^k = E_x^a$ for any $k \geq 1$, and similarly for F_y^b [20,50].

The length of a sequence of operators S denotes the minimal number of projectors required to express it. The null sequence corresponds to the identity operator, denoted by $\mathbb{1}$, with its length defined as zero. Consider an

n -element set \mathcal{S} of sequences of operators, such as $\mathcal{S}_{1+ab} = \{\mathbb{1}, E_x^a, F_y^b, E_x^a F_y^b\}_{a \in A, b \in B}$. By employing the NPA method, one constructs a hierarchy of relaxations using different choices of the set of sequences \mathcal{S} . Specifically, a set \mathcal{S}_k is composed of all sequences of operators $\{E_x^a, F_y^b\}$ with a length at most k . It follows that $\mathcal{S}_{1+ab} = \mathcal{S}_1 \cup \{E_x^a F_y^b\}$, where \mathcal{S}_{1+ab} is defined accordingly.

The NPA method aims to characterize a given bipartite probability distribution as quantum, implying the existence of a realization with a state $|\psi\rangle$ and projective measurements $\{E_x^a, F_y^b\}$. This realization satisfies, for all settings $x \in X$ and $y \in Y$ and outcomes $a \in A$ and $b \in B$, the equation $P(a, b|x, y) = \langle \psi | E_x^a F_y^b | \psi \rangle$. Considering operators O_i and O_j in the set \mathcal{S} , let Γ_{O_i, O_j} be defined as $\langle \psi | O_i^\dagger O_j | \psi \rangle$. Consequently, $\Gamma_{E_x^a, E_y^b} = P(a, b|x, y)$ and $\Gamma_{\mathbb{1}, \mathbb{1}} = 1$. This equation defines an $n \times n$ matrix, where rows and columns are indexed by elements of \mathcal{S} , forming the so-called moment matrix Γ .

The elements of Γ satisfy linear constraints: $\Gamma_{i,j} = \Gamma_{k,l}$ if and only if $O_i^\dagger O_j = O_k^\dagger O_l$, and $O_i^\dagger O_j = 0$ implies $\Gamma_{i,j} = 0$. For $v \in \mathbb{C}^n$ and $V = \sum_j v_j O_j$, it follows that $v^\dagger \Gamma v = \sum_{i,j} v_i^* \Gamma_{i,j} v_j = \sum_{i,j} v_i^* \langle \psi | O_i^\dagger O_j | \psi \rangle v_j = \langle \psi | V^\dagger V | \psi \rangle = |\langle V | \psi \rangle|^2 \geq 0$, thereby ensuring $\Gamma \geq 0$. We obtain the relaxation by requiring the existence of such Γ instead of the existence of states and operators realizing $P(a, b|x, y)$. This method is particularly useful for analyzing complex quantum systems and can provide valuable insights into the nature of quantum correlations and phenomena. The results obtained from NPA, as it constitutes a relaxation, provide an upper bound on the exact solution of the quantum optimization problem.

C. See-saw method

An alternative approach to optimization over quantum distributions \mathcal{Q} , when we have certain restrictions on the dimensions of operators included in the setup, is the so-called see-saw [24] method. Again, we consider bipartite quantum probabilities given by expressions of the form of Eq. (2). It is easy to see that expressions that are linear combinations of probabilities given by formulas of the form of Eq. (3), such as Bell-type operators, are linear in each term, viz., the quantum state, Alice's measurement operators, and Bob's measurement operators. However, since the optimization must be done over all these groups of variables, the whole expression is nonlinear.

The key idea of the see-saw method is the alternating use of a series of optimizations for which two of the expressions constituting Eq. (2) are treated as constants, and the third of them is a variable subjected to optimization by SDP methods with the objective function being the considered Bell operator. For this purpose, in the first iteration, two of the terms take fixed, often randomly chosen, values.

To be more specific, see-saw allows us to maximize a given Bell expression, which serves as a score function in the considered bipartite games. This Bell expression, denoted as $\mathcal{B}[P(a, b|x, y)]$, quantifies the correlations between measurement outcomes a and b for settings x and y . It is computed

as a weighted sum of bipartite probabilities $P(a, b|x, y)$, as defined in Eq. (2), where the coefficients $\beta_{a,b,x,y}$ weight the contributions of each outcome to the overall score.

At each iteration of the see-saw method, the quantum state and measurements of both Alice and Bob are optimized to maximize the Bell expression. This involves three main optimization steps: first, the state ρ is optimized while holding the measurements of Alice and Bob constant; next, all Alice's measurements $M(a, x)$ are optimized while keeping the state and Bob's measurements fixed; finally, Bob's measurements $N(b, y)$ are optimized while the state and Alice's measurements are held constant.

During each iteration, the value of the Bell expression is computed using the updated quantum state and measurements. If the improvement in the Bell expression value falls below a predefined threshold or the maximum number of iterations is reached, the optimization process terminates. Through this iterative procedure, the see-saw method efficiently explores the space of possible quantum correlations, even though it is not guaranteed to be converging towards the optimal solution that globally maximizes the Bell expression. Nonetheless, by providing explicit quantum state and measurements, it sheds light on the quantum nature of the underlying system. Indeed, note that while the NPA method provides an approximation of the quantum set of probabilities from its exterior, meaning a relaxation, the see-saw method finds direct representations of the quantum state and measurements implementing the found distribution. Thus, any solution obtained by the see-saw method is a lower bound on the exact solution of the quantum optimization problem, complementing the results from NPA.

IV. PROPERTIES OF SYMMETRIC DETERMINISTIC STRATEGIES FOR DISTRIBUTED TASKS

In Sec. IV A we prove lemmas showing that deterministic symmetric strategies are sufficient for consideration of LHV models for the rendezvous task, and then in Sec. IV B we prove an analogous result for the domination task.

A. Symmetric deterministic strategies for rendezvous on graphs

Given any set of strategies $\{\mathcal{S}_i\}_{i \in \{1, \dots, r\}}$ we have the success probability $W(\{\mathcal{S}_i\}_{i \in \{1, \dots, r\}})$ given by

$$W(\{\mathcal{S}_i\}_{i \in \{1, \dots, r\}}) = \sum_{a \in N} \prod_{i=1}^r p_i(a) = \tilde{W}(\{\tilde{\mathcal{S}}_i\}_{i \in \{1, \dots, r\}}) \quad (7)$$

so the success probability is completely determined by the set $\{\tilde{\mathcal{S}}_i\}_{i \in \{1, \dots, r\}}$.

Lemma 1. Symmetric strategies for the rendezvous task are at least as good as nonsymmetric strategies.

Proof. We have that

$$\begin{aligned} \tilde{W}(\{\tilde{\mathcal{S}}_i\}_{i \in \{1, \dots, r\}}) &= \sum_{a \in N} \prod_{i=1}^r p_i(a) \leq \prod_{i=1}^r \sqrt{\sum_{a \in N} p_i(a)^r} \\ &\leq \max_{i \in \{1, \dots, r\}} \sum_{a \in N} p_i(a)^r = \tilde{W}(\{\tilde{\mathcal{S}}_i^*, \dots, \tilde{\mathcal{S}}_i^*\}), \end{aligned} \quad (8)$$

where i^* is the value of i for which the maximum is reached. Here for the first estimation we used the Hölder inequality for sums [51].

So, given any set of strategies adopted by the r agents, the winning probability is upper bounded by the success probability of the symmetric strategy which employs a suitable strategy chosen among the set of the given strategies. ■

Lemma 2. Symmetric deterministic strategies for the rendezvous task are at least as good as symmetric nondeterministic strategies.

Proof. Given any nondeterministic strategy $S = \{p(a|x)\}_{a,x \in N}$, repeated for each of the agents, and the associated set $\tilde{S} = \{p(a)\}_{a \in N}$, we have that it is always possible to build a deterministic strategy, repeated for each of the agents, which has a greater success probability. In fact, if S_1 is not deterministic, there is at least one input node x_0 for which there are at least two nodes a_1 and a_2 for which $p(a_1|x_0), p(a_2|x_0) > 0$.

Without loss of generality, we consider the case in which $p(a_1) \geq p(a_2)$. A better strategy $S' = \{p'(a|x)\}_{a,x \in N}$, repeated for each of the agents, is built by assigning to the node x_0 a probability $p'(a_1|x_0) = p(a_1|x_0) + p(a_2|x_0)$ and $p'(a_2|x_0) = 0$, and the same probabilities in all the other cases. This is true because, for any $b, c \in N, r \geq 2$ with $p(b) \geq p(c)$ and $0 < \epsilon \leq p(c)$, we have that

$$p(b)^r + p(c)^r < (p(b) + \epsilon)^r + [p(c) - \epsilon]^r. \quad (9)$$

Then, it is possible to repeat this procedure until you obtain a deterministic strategy.

So any nondeterministic symmetric strategy has a lower success probability of at least one symmetric deterministic strategy. ■

Putting together the previous two results from Lemmas 1 and 2 we get the Corollary 1.

Corollary 1. It is possible to find the optimal strategy for the rendezvous problem by investigating only deterministic symmetric strategies.

Note that these results may not be applicable in other variants of the rendezvous task, such as when agents cannot be placed in the same initial nodes, in which case it is still possible to find the optimal solution by investigating only deterministic strategies, because the success probability remains a linear function of the probabilities, which are subject to linear constraints.

B. Deterministic strategies for domination on graphs

Let us now consider the graph domination task.

Lemma 3. Deterministic strategies for the domination task are at least as good as nondeterministic strategies.

Proof. Let us consider $K(\{S_j\}_{j \in \{1, \dots, r\}})$ the score, i.e., the average number of dominated points, of a given strategy $\{S_j\}_{j \in \{1, \dots, r\}}$. A set of strategies that provides a score at least as high as $K(\{S_j\}_{j \in \{1, \dots, r\}})$ can be obtained by replacing the strategy of the first agent with the following deterministic strategy.

Knowing the strategies $\{S_j\}_{j \in \{2, \dots, r\}}$, for any fixed input $x \in N$ for the first agent the best move would be to go to the accessible node which would provide the highest increment in the score, knowing what is the probability that any node is

going to be dominated by any of the other agents. Assigning this deterministic strategy to the first agent the score is greater or equal to the case in which they were using any other strategy.

Then, repeating the procedure for each of the agents and updating the strategies employed by them, we obtain the thesis. ■

V. RESULTS

The content of this section includes the results of rendezvous with quantum entanglement in Sec. V A, domination with quantum entanglement in Sec. V B, and a detailed analysis of selected cases in Sec. V C.

In the following will be presented the scenarios where we applied this technique and the tables that contain the results obtained.

In tables the columns ‘‘Classical’’ denote the maximum values which can be achieved by classical strategies. The columns ‘‘Random’’ denote the value obtained when the parties choose in a random uniform way which node to reach from the starting position. The values associated with the column ‘‘NPA’’ are calculated for the level $1 + ab$ when they appear without an asterisk; otherwise, they are calculated for level 2. The column ‘‘Adv.’’ contains the gain obtained by using quantum resources compared to the optimal classical strategy. The quantity is expressed in percents, and is calculated according to the following expression:

$$\frac{Q - R}{C - R} - 1 = \frac{Q - C}{C - R}, \quad (10)$$

where C denotes the classical value, i.e., the highest value that can be achieved when the parties can use only classical strategies. R denotes the average success probability for the rendezvous task and the average number of dominated nodes for the domination task, when the agents choose in a random uniform way which node to reach from the starting position, selecting the node to reach among the nodes that can be reached while respecting the rules of the given task. Q denotes the value achieved when the agents employ the strategy found with the see-saw technique.

When, for a given scenario, within at least 100 runs of the see-saw algorithm we did not find an average success probability greater than the one obtainable employing classical strategies and which does not match the upper bound found with level 2 of the NPA hierarchy, we say that the results are inconclusive.

Inconclusive results can happen because the level of the NPA hierarchy investigated, or the number of runs of the see-saw algorithm, or the dimension of the investigated quantum states, or the rank of the projectors generated with see-saw was too low.

Applying the see-saw algorithm we investigated only projectors of rank 1 for all the cases of three agents and up to rank 2 for the cases involving two agents. For the dimension of the generated quantum states, we have always chosen the lowest one determined by the rank of the generated projectors.

Note that in the case of the rendezvous task, due to Lemma 2, to find the best classical value it is sufficient to investigate only all the symmetric deterministic strategies. In the case of

TABLE I. Results associated with the single-step rendezvous task, two agents case, when the agents can start from any position.

Name	Random	Classical	NPA	Adv. (%)
tetrahedron Fig. 1(b)	$\frac{1}{4}$	$\frac{5}{8}$	0.64506*	5
square curly, Fig. 1(c)	$\frac{1}{4}$	$\frac{5}{8}$	0.64506*	5
pentagon curly, Fig. 1(d)	$\frac{1}{5}$	$\frac{13}{25}$	0.53009*	3
arrow Fig. 1(g)	0.20667	$\frac{13}{25}$	0.52051*	0.1
clamp Fig. 1(i)	0.18827	$\frac{7}{18}$	0.40063*	6
hat Fig. 1(j)	0.17207	$\frac{5}{9}$	$0.58333 \approx \frac{7}{12}$	7
house Fig. 1(k)	0.18210	$\frac{5}{9}$	$0.58333 \approx \frac{7}{12}$	7
caltrop Fig. 1(m)	0.20833	$\frac{5}{9}$	$0.58333 \approx \frac{7}{12}$	8
cube Fig. 1(n)	$\frac{1}{8}$	$\frac{5}{16}$	0.32253*	5
triangle 3-gon	$\frac{1}{3}$	$\frac{5}{9}$	$0.58333 \approx \frac{7}{12}$	13
pentagon 5-gon	$\frac{1}{5}$	$\frac{9}{25}$	0.38090	13
hexagon 6-gon	$\frac{1}{6}$	$\frac{5}{18}$	0.29167	13
heptagon 7-gon	$\frac{1}{7}$	$\frac{13}{49}$	0.27864	11
ennagon 9-gon	$\frac{1}{9}$	$\frac{17}{81}$	0.21887	9
decagon 10-gon	$\frac{1}{10}$	$\frac{9}{50}$	0.19045	13
11-gon	$\frac{1}{11}$	$\frac{21}{121}$	0.17998	8
13-gon	$\frac{1}{13}$	$\frac{25}{169}$	0.15273	7
Three-line curly	$\frac{1}{3}$	$\frac{5}{9}$	$0.58333 \approx \frac{7}{12}$	13
Five-line curly	$\frac{1}{5}$	$\frac{9}{25}$	0.38090	13
Seven-line curly	$\frac{1}{7}$	$\frac{13}{49}$	0.27864	11

the domination task, due to Lemma 3, to find the best classical value it is sufficient to investigate only all the deterministic strategies.

Both for the domination task and rendezvous task, with the additional constraint that the agents cannot start from the same positions, to find the classical value it is sufficient to study only deterministic strategies. This is true because the average success probability for the rendezvous task and the average number of dominated points for the domination task are still linear functions of probabilities which are subject to linear constraints.

When dealing with quantum strategies constrained to be symmetric, we considered only strategies for which all the agents can perform only the same set of measurements on the state, which to them is associated with the same marginal probability distribution, adjusting accordingly the constraints when performing the see-saw technique.

A. Rendezvous with quantum entanglement

We will now present the results obtained when the agents are dealing with the single-step rendezvous task.

Table I illustrates the scenarios where a quantum advantage is observed for two agents undertaking the rendezvous task, with the freedom to commence from any location, including the same initial position for both parties.

In contrast, Table II delineates situations where this advantage occurs when agents are refrained from initiating from identical positions. This dichotomy underscores the robustness of quantum strategies across diverse starting conditions, offering a notable advantage over classical counterparts.

Expanding on this comparison, Table III delves into the case where agents cannot start in the same positions, and they are allowed to use only symmetric strategies. Here, the introduction of symmetric strategies sheds light on the intricate interplay between quantum and classical approaches.

Remarkably, classical strategies exhibit limitations in maximizing success probabilities under symmetric conditions unless, as shown in Sec. IV A, any starting position is allowed. On the other hand, quantum strategies continue to demonstrate a clear advantage in both cases, as we elucidate further in Sec. V C 1.

The juxtaposition of these findings underscores the nuanced dynamics at play in the rendezvous task, emphasizing the pivotal role of starting conditions and strategy symmetry. While classical strategies attain their peak when any starting position is permissible, quantum strategies transcend these limitations, showcasing their adaptability and efficacy even under symmetric constraints. This nuanced understanding is pivotal for harnessing the full potential of quantum strategies in real-world applications of multiagent coordination.

When dealing with the rendezvous task with three agents we have found no advantage when they can exploit quantum resources, when they can start in any position, when they cannot start in the same position, with and without the restriction of using symmetric strategies for the following graphs: square curly [Fig. 1(c)], double triangle [Fig. 1(a)], cube [Fig. 1(n)], tetrahedron [Fig. 1(b)], arrow curly [Fig. 1(h)], clamp [Fig. 1(i)], hat [Fig. 1(j)], and house [Fig. 1(k)]. It is not conclusive for pentagon curly [Fig. 1(d)] and arrow [Fig. 1(g)] when the agents cannot start in the same positions. We found no advantage for any case for the graphs n -lines and n -lines curly for $4 \leq n \leq 8$.

TABLE II. Results associated with the single-step rendezvous task, two agents case, when the agents cannot start in the same positions.

Name	Random	Classical	NPA	Adv. (%)
tetrahedron Fig. 1(b)	$\frac{2}{9}$	$\frac{1}{2}$	$0.53333^* \approx \frac{8}{15}$	12
square curly, Fig. 1(c)	$\frac{2}{9}$	$\frac{1}{2}$	$0.53333^* \approx \frac{8}{15}$	12
pentagon curly, Fig. 1(d)	$\frac{1}{6}$	$\frac{2}{5}$	0.41316^*	6
arrow Fig. 1(g)	0.16667	$\frac{2}{5}$	0.40490^*	2
clamp Fig. 1(i)	0.13704	$\frac{4}{15}$	0.28229^*	12
hat Fig. 1(j)	0.15093	$\frac{7}{15}$	$0.50000 \approx \frac{1}{2}$	11
house Fig. 1(k)	0.15463	$\frac{7}{15}$	$0.50000 \approx \frac{1}{2}$	11
caltrop Fig. 1(m)	$\frac{7}{40}$	$\frac{7}{15}$	$0.50000 \approx \frac{1}{2}$	11
cube Fig. 1(n)	$\frac{2}{21}$	$\frac{3}{14}$	0.22857^*	12

We have no reason to exclude that, in the three agent case, an advantage could be found by using more computational resources, when dealing with the inconclusive cases, or increasing the number of nodes of the graphs studied.

Let us denote the considered cases given in Tables I, II, and III by \mathcal{A} , \mathcal{B} , and \mathcal{C} , respectively. Recall that they refer to cases when any starting position is allowed (\mathcal{A}), when the agents cannot start in the same positions, also with nonsymmetric strategies (\mathcal{B}), and when the agents cannot start in the same positions and they use symmetric strategies (\mathcal{C}).

We observe that if for a given graph $1 + ab$ is enough to determine its exact Tsirelson bound for one of the cases (\mathcal{A} , \mathcal{B} , or \mathcal{C}) then it is enough for all cases (\mathcal{A} , \mathcal{B} , and \mathcal{C}). What is more, for cycles in all cases the NPA level $1 + ab$ is enough.

All the cases in \mathcal{C} that do not appear in \mathcal{B} are cases for which we found that there is no advantage when the agents share a quantum state, so they are cases for which the quantum correlations are exploited to break the symmetry between the agents, as will be described more in detail in Sec. VC 1. Additionally, all the cases in \mathcal{B} present the same average success probabilities both for the classical and the quantum case as the ones that they present in \mathcal{C} , and so they are cases for which the classical value can be reached by symmetric strategies.

The graphs triangle, three-line curly, hat, house, and caltrop have always the same value of classical and quantum for a given case \mathcal{A} or \mathcal{C} . Except for triangle and three-line curly, this holds also for case \mathcal{B} .

TABLE III. Results associated with the single-step rendezvous task, two agents case, when the agents cannot start in the same positions and they are constrained to adopt only symmetric strategies. Note that the first nine cases have identical values as those in Table II.

Name	Random	Classical	NPA	Adv. (%)
tetrahedron Fig. 1(b)	$\frac{2}{9}$	$\frac{1}{2}$	$0.53333^* \approx \frac{8}{15}$	12
square curly, Fig. 1(c)	$\frac{2}{9}$	$\frac{1}{2}$	$0.53333^* \approx \frac{8}{15}$	12
pentagon curly, Fig. 1(d)	$\frac{1}{6}$	$\frac{2}{5}$	0.41316^*	6
arrow Fig. 1(g)	$\frac{1}{6}$	$\frac{2}{5}$	0.40490^*	2
clamp Fig. 1(i)	0.13704	$\frac{4}{15}$	0.28229^*	12
hat Fig. 1(j)	0.15093	$\frac{7}{15}$	$0.50000 \approx \frac{1}{2}$	11
house Fig. 1(k)	0.15463	$\frac{7}{15}$	$0.50000 \approx \frac{1}{2}$	11
caltrop Fig. 1(m)	$\frac{7}{40}$	$\frac{7}{15}$	$0.50000 \approx \frac{1}{2}$	11
cube Fig. 1(n)	$\frac{2}{21}$	$\frac{3}{14}$	0.22857^*	12
triangle 3-gon	$\frac{1}{4}$	$\frac{1}{3}$	$0.50000 \approx \frac{1}{2}$	200
pentagon 5-gon	$\frac{1}{8}$	$\frac{1}{5}$	$0.25000 \approx \frac{1}{4}$	67
hexagon 6-gon	$\frac{1}{10}$	$\frac{2}{15}$	$0.20000 \approx \frac{1}{5}$	200
heptagon 7-gon	$\frac{1}{12}$	$\frac{1}{7}$	$0.16667 \approx \frac{1}{6}$	40
ennagon 9-gon	$\frac{1}{16}$	$\frac{1}{9}$	$0.12500 \approx \frac{1}{8}$	29
decagon 10-gon	$\frac{1}{18}$	$\frac{4}{45}$	$0.11111 \approx \frac{1}{9}$	67
11-gon	$\frac{1}{20}$	$\frac{1}{11}$	$0.10000 \approx \frac{1}{10}$	22
13-gon	$\frac{1}{24}$	$\frac{1}{13}$	$0.08333 \approx \frac{1}{12}$	18
Three-line curly	$\frac{1}{4}$	$\frac{1}{3}$	$0.50000 \approx \frac{1}{2}$	200
Five-line curly	$\frac{1}{8}$	$\frac{1}{5}$	$0.25000 \approx \frac{1}{4}$	67
Seven-line curly	$\frac{1}{12}$	$\frac{1}{7}$	$0.16667 \approx \frac{1}{6}$	40

TABLE IV. Results associated with the single-step domination task, two agents case, when the agents can start from any position.

Name	Random	Classical	NPA	Adv. (%)
pentagon curly, Fig. 1(d)	4.2	4.64	4.67361*	8
caltrop Fig. 1(m)	5.458333	5.88889	5.916667	6
spike Fig. 1(e)	4.51333	4.92	4.93	2
clamp Fig. 1(i)	4.94907	5.44444	5.45453	2
pentagon	4.2	4.6	4.67361	18
hexagon	4.50000	4.95000	5.0000	13
heptagon	4.71428	5.08163	5.15517	20
octagon	4.875	5.1875	5.23928	17
9-gon	5	5.24691	5.29434	19
10-gon	5.1	5.3	5.33680	18
11-gon	5.18182	5.39669	5.43395	17
12-gon	5.25	5.47222	5.5	13
13-gon	5.30769	5.50888	5.54543	18
Six-line curly	4.11111	4.44445	4.44895	1

It is worth noting that, at least for the cases analyzed, if for a cycle the number of vertices is divisible by 4 then there is no advantage in any case \mathcal{A} , \mathcal{B} , or \mathcal{C} .

B. Domination with quantum entanglement

In Tables IV and V we present the results obtained when the agents deal with the graph domination task when they can exploit quantum resources.

For the two agents case we found that there is not an advantage for any case associated with the following graphs: double triangle [Fig. 1(a)], tetrahedron [Fig. 1(b)], square curly [Fig. 1(c)], arrow [Fig. 1(g)], arrow curly [Fig. 1(h)], pyramid double [Fig. 1(l)], hat [Fig. 1(j)], cube [Fig. 1(n)], three-line curly, and four-line curly.

In the case of spike curly [Fig. 1(f)], we found that there is no advantage in using quantum resources when the agents can start from any position, while we found an advantage of +0.224% when they cannot start in the same position, although with see-saw we did not obtain the value found with level 2 of the NPA hierarchy.

When the agents cannot start in the same positions we did not find any advantage for all n -line curly with $4 \leq n \leq 8$.

When dealing with the three agents cases we found no advantage when the agents cannot start in the same positions for all n -line and n -line curly with $4 \leq n \leq 8$ and, when they can start in any position not conclusive for n -line and n -line curly with $4 \leq n \leq 7$ and for $n = 8$ we found no advantage. In the case of n -gon, when the agents can start in the same positions, we found no advantage for $5 \leq n \leq 8$, while, for the same graphs, when the agents can start in any positions, the results are inconclusive.

We have no reason to exclude that, in the three agent case, an advantage could be found by using more computational resources, when dealing with the inconclusive cases, or increasing the number of nodes of the graphs to study.

C. Detailed analysis of selected cases

We will now consider several examples of strategies for the rendezvous and domination tasks to illustrate their working. In Sec. VC 1 we discuss one of the cases from Table III with particularly high advantage and discuss the role of quantum resources in this particular case. Next, in Sec. VC 2, we discuss the quantum nature of the advantage for the rendezvous task with agents that are not symmetric. Finally, in Sec. VC 3

TABLE V. Results associated with the single-step domination task, two agents case, when the agents cannot start in the same positions.

Name	Random	Classical	NPA	Adv. (%)
pentagon curly, Fig. 1(d)	4.27778	4.7	4.73987	9
clamp Fig. 1(i)	5.01482	5.4	5.41210*	3
caltrop Fig. 1(m)	5.48750	5.86667	5.9	9
spike Fig. 1(e)	4.56944	4.9	4.9125	4
pentagon	4.25	4.5	4.59201	37
hexagon	4.60000	4.93333	5.00000	20
heptagon	4.83333	5.09524	5.18103	33
octagon	5	5.21429	5.27346	28
9-gon	5.125	5.27778	5.33113	35
10-gon	5.22222	5.34444	5.37423	24
11-gon	5.3	5.43636	5.47735	30
12-gon	5.36364	5.51515	5.54545	20
13-gon	5.41667	5.51515	5.59088	29



FIG. 2. Graph with a three-line curly structure.

we explicitly illustrate a particular case of quantum advantage for the domination task.

1. Three-line curly graph with symmetric strategies for rendezvous

Considering the case of the single-step rendezvous task with two agents, when the agents cannot start in the same positions and they are constrained to adopt only symmetric strategies, we now focus on the particular case of the graph *three-line curly*, as reported in Table III. We have that in this case the best classical strategy achieves the average success probability $C = \frac{1}{3}$, while, when the players choose randomly the node to reach, they have an average success probability $R = \frac{1}{4}$. The quantum success probability is $Q = \frac{1}{2}$.

For the three-line curly graph, shown in Fig. 2, if one of the parties starts in node 0 and the other in node 1, they win only if the former decides to stay in node 0, and the other moves to node 0, and this happens with probability $\frac{1}{4} = \frac{1}{2} \times \frac{1}{2}$. If one of the parties starts in node 0 and the other in node 2, they win only if both decide to move to node 1, with probability $\frac{1}{4}$. Finally, if one of the parties starts in node 1 and the other in node 2 they win only if the former moves to node 2, and the latter decides to stay in node 2, which happens, for the random strategy, again with probability $\frac{1}{4}$. Thus the average winning probability with random strategy is $\frac{1}{4}$.

The optimal symmetric deterministic strategy is the following: if the party is in node 0 or 1, then it should move to the possible node with the smaller label, i.e., 0; if the party is in node 2 it should move to the possible node with the largest label, i.e., 2.

Stating this more explicitly, for the three-line curly graph, when using the optimal deterministic strategy, if one of the parties starts in node 0 and the other in node 1, the former stays in node 0, and the latter moves to node 0, and they win. If one of the parties starts in node 0 and the other in node 2, then the former stays in node 0, and the other stays in node 2, and they fail. If one of the parties starts in node 1 and the other in node 2, the former moves to node 0, and the latter stays in node 2, and they fail. Thus, the winning probability is $\frac{1}{3}$.

In the quantum case, the strategy is found applying see-saw, finding the quantum state ρ shared by the agents and the measurements performed by them, viz., $\{M(a, x)\}_{x \in \{0,1,2\}, a \in \{0,1\}}$ and $\{N(b, y)\}_{y \in \{0,1,2\}, b \in \{0,1\}}$, with x and y denoting the input node and a and b denoting the output of the measurement. It is sufficient to consider only measurements to which there are associated two outcomes because in this graph each vertex is attached to at most two edges. In this example the joint probability distribution of the measurement results $\{P(a, b|x, y)\}_{a, b \in \{0,1\}, x, y \in \{0,1,2\}}$ can be transformed to a strategy $\{\tilde{P}(\tilde{a}, \tilde{b}|x, y)\}_{\tilde{a}, \tilde{b} \in \{0,1\}, x, y \in \{0,1,2\}}$ where \tilde{a} and \tilde{b} denote the output nodes, for example, if the agent is starting in the vertex $x \in \{0, 1, 2\}$, associating to the output $a = 0$ the vertex labeled by the smallest number among the ones which can be reached starting from the input node x and

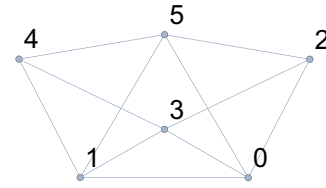


FIG. 3. Graph with the ‘‘hat’’ structure.

associating to the output $a = 1$ the vertex labeled by the largest number among the ones which can be reached starting from the input node x . We have the following quantum strategy $\{P(a, b|x, y)\}_{a, b \in \{0,1\}, x, y \in \{0,1,2\}}$:

$$\begin{aligned} P(1, 0|0, 0) &= P(0, 1|0, 0) = P(0, 0|1, 0) = P(1, 1|1, 0) \\ &= P(1, 0|2, 0) = P(0, 1|2, 0) = P(0, 0|0, 1) \\ &= P(1, 1|0, 1) = P(1, 0|1, 1) = P(0, 1|1, 1) \\ &= P(0, 0|2, 1) = P(1, 1|2, 1) = P(1, 0|0, 2) \\ &= P(0, 1|0, 2) = P(0, 0|1, 2) = P(1, 1|1, 2) \\ &= P(1, 0|2, 2) = P(0, 1|2, 2) = 0.5, \end{aligned} \quad (11)$$

and zero otherwise.

So, considering only the cases for which $x \neq y$, we have that the average success probability provided by this strategy is

$$\begin{aligned} Q &= \frac{P(0, 0|1, 0) + P(0, 1|2, 0) + P(0, 0|0, 1)}{6} \\ &+ \frac{P(1, 1|2, 1) + P(1, 0|0, 2) + P(1, 1|1, 2)}{6} = 0.5 \end{aligned} \quad (12)$$

where 6 is the number of possible inputs for the agents for which they are not starting in the same node. So, applying Eq. (10), we obtain that the advantage is 200%.

2. Hat graph with nonsymmetric strategies for rendezvous

We will now discuss the hat graph shown in Fig. 1(j), and repeated here in Fig. 3 for convenience.

In the case in which Alice and Bob cannot start in the same position and without the symmetric strategy constraint, the optimal deterministic strategy, leading to the result stated in Table II, is the following: Alice starting from nodes 0 or 3 or 4 or 5 goes to node 1; from node 1 and 2 she goes to node 3. The same strategy holds for Bob. This covers 12 possible initial positions. Since we consider the case in which the agents start at different positions, we have 30 possible initial locations. The parties win when Alice starts from nodes $\{0, 3, 4, 5\}$ and Bob starts from nodes $\{0, 3, 4, 5\}$, as then they meet at node 1. This covers 12 possible initial positions. The other winning possibilities are when they meet at node 3, which happens in two cases when Alice starts from node 1 and Bob starts from node 2 and vice versa. The average success probability in this case is $\frac{14}{30} = \frac{7}{15}$.

One of the quantum strategies giving the optimal value 0.5 uses the entangled state $\frac{1}{\sqrt{2}}(|00\rangle + |33\rangle)$ on Hilbert space

$\mathbb{C}^4 \otimes \mathbb{C}^4$. For $x = 0$ the measurements of Alice are the following:

$$M(0, 0) = |0\rangle\langle 0| + 0.25|1\rangle\langle 1| + 0.25|2\rangle\langle 2|, \quad (13a)$$

$$M(1, 0) = M(3, 0) = 0.25(|1\rangle\langle 1| + |2\rangle\langle 2|), \quad (13b)$$

$$M(2, 0) = 0.25(|1\rangle\langle 1| + |2\rangle\langle 2|) + |3\rangle\langle 3|. \quad (13c)$$

For $x = 1$ the measurements are

$$M(0, 1) = 0.75|0\rangle\langle 0| + 0.25(|1\rangle\langle 1| + |2\rangle\langle 2| + |3\rangle\langle 3|) + \alpha(|0\rangle\langle 3| + |3\rangle\langle 0|), \quad (14a)$$

$$M(1, 1) = 0.25(|0\rangle\langle 0| + |1\rangle\langle 1| + |2\rangle\langle 2|) + 0.75|3\rangle\langle 3| - \alpha(|0\rangle\langle 3| + |3\rangle\langle 0|), \quad (14b)$$

and

$$M(2, 1) = M(3, 1) = M(1, 0). \quad (14c)$$

Then, for $x = 2$ Alice uses the measurements

$$M(0, 2) = 0.75|0\rangle\langle 0| + \frac{1}{3}(|1\rangle\langle 1| + |2\rangle\langle 2|) + 0.25|3\rangle\langle 3| \times |3\rangle\langle 3| + \alpha(|0\rangle\langle 3| + |3\rangle\langle 0|), \quad (15a)$$

$$M(1, 2) = 0.25|0\rangle\langle 0| + \frac{1}{3}(|1\rangle\langle 1| + |2\rangle\langle 2|) + 0.75|3\rangle\langle 3| \times |3\rangle\langle 3| - \alpha(|0\rangle\langle 3| + |3\rangle\langle 0|), \quad (15b)$$

$$M(2, 2) = \frac{1}{3}(|1\rangle\langle 1| + |2\rangle\langle 2|), \quad (15c)$$

and $M(3, 2) = 0$. The measurements for $x = 3$ and 5 are

$$M(0, 3) = M(0, 5) = 0.25(|0\rangle\langle 0| + |1\rangle\langle 1| + |2\rangle\langle 2|) + 0.75|3\rangle\langle 3| + \alpha(|0\rangle\langle 3| + |3\rangle\langle 0|), \quad (16a)$$

$$M(1, 3) = M(1, 5) = 0.75|0\rangle\langle 0| + 0.25(|1\rangle\langle 1| + |2\rangle\langle 2| + |3\rangle\langle 3|) - \alpha(|0\rangle\langle 3| + |3\rangle\langle 0|), \quad (16b)$$

and

$$M(2, 3) = M(3, 3) = M(2, 5) = M(3, 5) = M(1, 0). \quad (16c)$$

Finally, for $x = 4$ the measurement is given by

$$M(0, 4) = |0\rangle\langle 0| + \frac{1}{3}(|1\rangle\langle 1| + |2\rangle\langle 2|), \quad (17a)$$

$$M(1, 4) = M(2, 4) = \frac{1}{3}(|1\rangle\langle 1| + |2\rangle\langle 2|) + |3\rangle\langle 3|, \quad (17b)$$

and $M(3, 4) = 0$.

The measurements of Bob are the same, and thus the quantum strategy is symmetric.

Let us now discuss some of the probabilities which occur in this case. For instance, let Alice start at node 0 and Bob at node 1. With probability 0.5 Alice goes to node 1 or 3, and Bob with probability 0.5 goes to node 0 or 3, but due to quantum steering [53–56], which is an effect of the entanglement, the probability of both parties arriving at node 3 is $\frac{3}{8} > \frac{1}{2} \times \frac{1}{2}$. A similar situation happens for all other 23 pairs of possible settings, excluding the six discussed below.

A different type of movement occurs in the following six cases. The first two cases are when one of the parties starts at

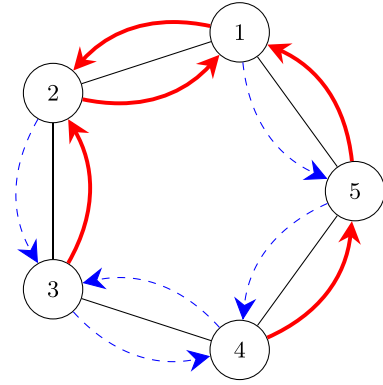


FIG. 4. Pentagon with optimal classical strategies of Alice and Bob for domination. Red arrows denote moves of one of the parties, and blue arrows denote moves of the other party.

node 0 and the other at node 4. Then with probability 0.5, they both move to node 1, and with probability 0.5 they both move to node 3, so they win with probability 1. Analogous action is performed when parties are at nodes 1 and 2 and the parties meet either at node 0 or at node 3. Similarly for starting at a pair of nodes 3 and 5 the parties meet either at 0 or at 1 with certainty.

The total winning probability is thus $\frac{3}{8} \times \frac{24}{30} + 1 \times \frac{6}{30} = 0.5$.

3. Domination task on a pentagon

Now, we consider the other cooperation tasks, viz., the domination.

In the case in which the agents can start from any position, the optimal classical strategy is shown in Fig. 4. It can be noticed that the strategy can be summarized as trying to concentrate on one of the parties, as Alice, near nodes 1 and 2, and the other party near nodes 3 and 4. It can be calculated that the parties on average will dominate 4.6 nodes.

One of the quantum strategies achieving the optimal value has the following properties.

First, consider the case in which Alice and Bob start in the same position, which happens in 5 out of 25 cases. In this case, we have that half of the times Alice moves in the “clockwise” direction [17,25,36,52], while Bob moves “counterclockwise,” and in the other half of the times Alice moves counterclockwise while Bob moves clockwise, dominating in both cases the five nodes.

Now let us consider the case when the starting nodes of Alice and Bob are neighboring. This happens in 10 out of 25 possible initial position pairs. In this case, with a probability about $p_1 \approx 0.3273$, they are moving in opposite directions, so that after their movement they will be separated by one node. Thus they will dominate all five nodes; in Fig. 5 it is represented with green ultr-thin arrows.

With the same probability p_1 , they will move towards each other, effectively exchanging their positions. They will dominate four nodes; in Fig. 5 this move is represented with blue ultrathick arrows. With smaller probability $0.5 - p_1 \approx 0.1727$ both will move either clockwise or counterclockwise, and dominate four nodes.

The remaining possible case is when the starting nodes of Alice and Bob are not neighboring. This happens in 10

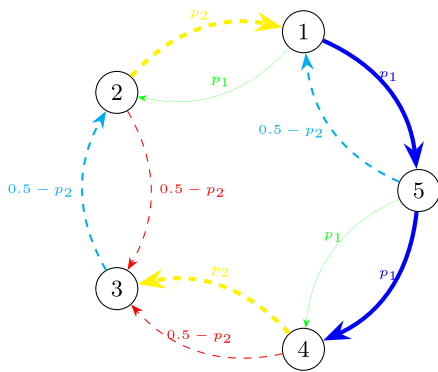


FIG. 5. Pentagon with optimal quantum strategies of Alice and Bob for domination. Arrows denote the moves of the parties in different cases, and the labels refer to probabilities of the movement; see the text in Sec. VC3 for the description.

out of 25 possible initial positions. The quantum strategy implies that with probability $p_2 \approx 0.45224$, both parties move clockwise, and with the same probability they both move counterclockwise, and thus after the movement they are still not neighboring. In that case, they dominate all five nodes. In Fig. 5 this move is represented with yellow dashed ultrathick arrows.

With smaller probability $0.5 - p_2 \approx 0.04773$, the first of the parties is moving clockwise, and the second counterclockwise; with the same probability the first is moving counterclockwise and the second clockwise. Depending on the exact starting node locations, the former situation will lead either to the moving of both parties to the same node, dominating three nodes, or to the moving to two neighboring nodes, dominating four nodes; both situations happen with equal probability. In Fig. 5 this move is represented with red dashed and cyan dashed thick arrows.

Summarizing, the average number of dominated nodes is

$$\begin{aligned} & \frac{5}{25} \times 5 + \frac{10}{25} \times [p_1 \times 5 + (1 - p_1) \times 4] \\ & + \frac{10}{25} \times [2p_2 \times 5 + (0.5 - p_2) \times 4 + (0.5 - p_2) \times 3] \\ & \approx 4.6736. \end{aligned} \quad (18)$$

VI. DISCUSSION

The two problems under scrutiny in this paper, namely, rendezvous on graphs and the introduced domination on graphs task for mobile agents, represent specific instances of a broader concept known as pattern formation [57–60]. Among the array of challenges in pattern formation research, the most akin task is dispersion on graphs [61], wherein the agents' objective is to efficiently spread throughout a defined territory, or graph exploration [62]. These problems are particularly significant as they find applications across a range of fields, encompassing robotics, networking, and distributed systems, and they grapple with fundamental issues pertaining to effective coordination and information exchange among mobile agents operating within a graph-based framework.

In the seminal paper preceding our current research [6], the focus was primarily on cubic graphs and cycles. Our present

paper extends this investigation to explore the broader applicability of the conclusions drawn from the advantage quantum entanglement offers in the context of rendezvous tasks for mobile agents. This paper aims to establish the extent to which these findings can be generalized and the ubiquity of situations where quantum entanglement provides a strategic edge.

On the other hand, it is both surprising and somewhat disappointing that, on graphs where a quantum advantage was observed for two parties, we could not identify any gain for three agents. Consequently, investigating whether such an advantage is feasible, at least in certain scenarios, for more than two agents becomes a crucial avenue for further exploration. Uncovering such examples appears to be a nontrivial task. If it turns out to be unattainable, it would be valuable to discern and understand the underlying reasons for this limitation.

VII. CONCLUSIONS

In our paper, we introduced a distributed task for mobile agents, specifically the domination task, drawing inspiration from a classical concept in graph theory. Our exploration encompassed various scenarios across different types of graphs for both the domination task and another crucial multiagent task, namely, rendezvous. After obtaining some results about classical strategies, we examined cases involving two and three agents. Intriguingly, we consistently observed a quantum advantage for scenarios involving two parties, while no such advantage was found for three parties. This highlights the potential efficacy of the proposed method for tasks involving two agents and prompts further investigation into why it proves challenging to identify examples for three agents. This, along with the quest for general analytical formulas for various families of graphs, remains an open question for future explorations.

It is important to note that this approach offers the possibility to search for Bell inequalities associated with tasks with an arbitrary number of inputs and number of outputs associated with each input by building one of the suitable graphs and, after selecting a communication task, looking for gaps between the maximum success probabilities associated with classical and quantum strategies.

ACKNOWLEDGMENTS

We acknowledge partial financial support by the Foundation for Polish Science (IRAP project, ICTQT, Contract No. 2018/MAB/5, cofinanced by the European Union within the Smart Growth Operational Programme), from the Knut and Alice Wallenberg Foundation through the Wallenberg Centre for Quantum Technology, and from the National Centre for Research and Development (NCBiR) QUANTERA/2/2020—an ERA-Net cofund in Quantum Technologies under project eDICT. We thank the National Science Center, CHIST-ERA Call 2022 (Modern Device Independent Cryptography project, ChistEra-2023/05/Y/ST2/00005) for the financial support. The numerical calculation was conducted using NCPOL2SDPA [63,64] and MOSEK [48]. P.M. acknowledges discussions with Jorge Quintanilla Tizon, Paul Strange, and Joshua Tucker from University of Kent.

- [1] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. Shamsul Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, Advances in quantum cryptography, *Adv. Opt. Photon.* **12**, 1012 (2020).
- [2] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Quantum entanglement, *Rev. Mod. Phys.* **81**, 865 (2009).
- [3] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Bell nonlocality, *Rev. Mod. Phys.* **86**, 419 (2014).
- [4] Y. Cao, W. Yu, W. Ren, and G. Chen, An overview of recent progress in the study of distributed multi-agent coordination, *IEEE Trans. Indust. Inf.* **9**, 427 (2012).
- [5] S. Muhammad, A. Tavakoli, M. Kurant, M. Pawłowski, M. Żukowski, and M. Bourennane, Quantum bidding in bridge, *Phys. Rev. X* **4**, 021047 (2014).
- [6] P. Mironowicz, Entangled rendezvous: A possible application of Bell non-locality for mobile agents on networks, *New J. Phys.* **25**, 013023 (2023).
- [7] S. Pironio, A. Acín, S. Massar, A. B. de La Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, and T. A. Manning, Random numbers certified by Bell's theorem, *Nature (London)* **464**, 1021 (2010).
- [8] B. S. Cirel'son, Quantum generalizations of Bell's inequality, *Lett. Math. Phys.* **4**, 93 (1980).
- [9] R. Cleve, P. Hoyer, B. Toner, and J. Watrous, Consequences and limits of nonlocal strategies, in *Proceedings of the 19th IEEE Annual Conference on Computational Complexity* (IEEE, New York, 2004), pp. 236–249.
- [10] V. Russo, Extended nonlocal games, Ph.D. thesis, University of Waterloo, 2017.
- [11] O. Regev and T. Vidick, Quantum XOR games, *ACM Trans. Comput. Theory (ToCT)* **7**, 1 (2015).
- [12] R. Ramanathan, R. Augusiak, and G. Murta, Generalized XOR games with d outcomes and the task of nonlocal computation, *Phys. Rev. A* **93**, 022333 (2016).
- [13] V. Russo and J. Watrous, Extended nonlocal games from quantum-classical games, [arXiv:1709.01837](https://arxiv.org/abs/1709.01837).
- [14] M.-X. Luo, Nonlocality of all quantum networks, *Phys. Rev. A* **98**, 042317 (2018).
- [15] M.-X. Luo, A nonlocal game for witnessing quantum networks, *npj Quantum Inf.* **5**, 91 (2019).
- [16] J. S. Bell, On the Einstein Podolsky Rosen paradox, *Physics* **1**, 195 (1964).
- [17] S. Alpern, The Rendezvous search problem, *SIAM J. Control Optim.* **33**, 673 (1995).
- [18] R. B. Allan and R. Laskar, On domination and independent domination numbers of a graph, *Discr. Math.* **23**, 73 (1978).
- [19] P. Skrzypczyk and D. Cavalcanti, *Semidefinite Programming in Quantum Information Science* (University of Reading, Berkshire, 2023), pp. 2053–2563.
- [20] P. Mironowicz, Semi-definite programming and quantum information, *J. Phys. A: Math. Theor.* (2024), doi:[10.1088/1751-8121/ad2b85](https://doi.org/10.1088/1751-8121/ad2b85).
- [21] A. Tavakoli, A. Pozas-Kerstjens, P. Brown, and M. Araújo, Semidefinite programming relaxations for quantum correlations, [arXiv:2307.02551](https://arxiv.org/abs/2307.02551).
- [22] M. Navascués, S. Pironio, and A. Acín, Bounding the set of quantum correlations, *Phys. Rev. Lett.* **98**, 010401 (2007).
- [23] M. Navascués, S. Pironio, and A. Acín, A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations, *New J. Phys.* **10**, 073013 (2008).
- [24] K. F. Pál and T. Vértesi, Maximal violation of a bipartite three-setting, two-outcome Bell inequality using infinite-dimensional quantum systems, *Phys. Rev. A* **82**, 022116 (2010).
- [25] S. Alpern, Rendezvous search: A personal perspective, *Oper. Res.* **50**, 772 (2002).
- [26] S. Alpern, Rendezvous games (non-antagonistic search games), in *Wiley Encyclopedia of Operations Research and Management Science*, edited by J. J. Cochran (John Wiley & Sons, Hoboken, NJ, 2010), p. 30.
- [27] E. J. Anderson and S. Essegai, Rendezvous search on the line with indistinguishable players, *SIAM J. Control Optim.* **33**, 1637 (1995).
- [28] X. Yu and M. Yung, Agent rendezvous: A dynamic symmetry-breaking problem, in *International Colloquium on Automata, Languages, and Programming* (Springer, New York, 1996), pp. 610–621.
- [29] S. Alpern and W. S. Lim, The symmetric Rendezvous-Evasion game, *SIAM J. Control Optim.* **36**, 948 (1998).
- [30] Q. Han, D. Du, J. Vera, and L. F. Zuluaga, Improved bounds for the symmetric rendezvous value on the line, *Oper. Res.* **56**, 772 (2008).
- [31] E. J. Anderson and S. P. Fekete, Asymmetric rendezvous on the plane, in *Proceedings of the Fourteenth Annual Symposium on Computational Geometry* (ACM Press, New York, 1998), pp. 365–373.
- [32] S. Alpern and A. Beck, Asymmetric rendezvous on the line is a double linear search problem, *Math. Oper. Res.* **24**, 604 (1999).
- [33] S. Alpern, Asymmetric rendezvous search on the circle, *Dyn. Control* **10**, 33 (2000).
- [34] S. Alpern and A. Beck, Pure strategy asymmetric rendezvous on the line with an unknown initial distance, *Oper. Res.* **48**, 498 (2000).
- [35] P. G. F. Dias, M. C. Silva, G. P. Rocha Filho, P. A. Vargas, L. P. Cota, and G. Pessin, Swarm robotics: A perspective on the latest reviewed concepts and applications, *Sensors* **21**, 2062 (2021).
- [36] A. Pelc, Deterministic rendezvous in networks: A comprehensive survey, *Networks* **59**, 331 (2012).
- [37] T. W. Haynes, S. Hedetniemi, and P. Slater, *Fundamentals of Domination in Graphs* (CRC Press, Boca Raton, FL, 2013).
- [38] T. W. Haynes, S. T. Hedetniemi, and M. A. Henning, *Domination in Graphs: Core Concepts* (Springer, New York, 2023).
- [39] E. J. Cockayne, R. M. Dawes, and S. T. Hedetniemi, Total domination in graphs, *Networks* **10**, 211 (1980).
- [40] M. A. Henning and A. Yeo, *Total Domination in Graphs* (Springer, New York, 2013).
- [41] C. Berge, *The Theory of Graphs and its Applications* (Methuen, New York, 1962).
- [42] O. Ore, Theory of graphs, in *Colloquium Publications*, American Mathematical Society Translations Series 2 (American Mathematical Society, Providence, 1962).
- [43] W. Goddard and M. A. Henning, Independent domination in graphs: A survey and recent results, *Disc. Math.* **313**, 839 (2013).

- [44] E. Sampathkumar and H. B. Walikar, The connected domination number of a graph, *J. Math. Phys. Sci.* **13**, 607 (1979).
- [45] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, New York, 2010).
- [46] L. Vandenberghe and S. Boyd, Semidefinite programming, *SIAM Rev.* **38**, 49 (1996).
- [47] F. A. Potra and S. J. Wright, Interior-point methods, *J. Comput. Appl. Math.* **124**, 281 (2000).
- [48] E. D. Andersen and K. D. Andersen, The MOSEK interior point optimizer for linear programming: An implementation of the homogeneous algorithm, in *High Performance Optimization* (Springer, New York, 2000), pp. 197–232.
- [49] M. Navascués, Y. Guryanova, M. J. Hoban, and A. Acín, Almost quantum correlations, *Nat. Commun.* **6**, 6288 (2015).
- [50] P. Mironowicz, Applications of semi-definite optimization in quantum information protocols, Ph.D. thesis, Gdańsk University of Technology, 2015.
- [51] O. Holder, Über einen Mittelwertsatz. *Nachr. Ges. Wiss. Göttingen, Göttingen*, pp. 38–47 (1889).
- [52] P. Flocchini, B. Mans, and N. Santoro, Sense of direction: Definitions, properties, and classes, *Networks: An Intl. J.* **32**, 165 (1998).
- [53] E. Schrödinger, Discussion of probability relations between separated systems, in *Mathematical Proceedings of the Cambridge Philosophical Society* (Cambridge University Press, Cambridge, 1935), Vol. 31, pp. 555–563.
- [54] H. M. Wiseman, S. J. Jones, and A. C. Doherty, Steering, entanglement, nonlocality, and the Einstein-Podolsky-Rosen paradox, *Phys. Rev. Lett.* **98**, 140402 (2007).
- [55] R. Ramanathan, D. Goyeneche, S. Muhammad, P. Mironowicz, M. Grünfeld, M. Bourennane, and P. Horodecki, Steering is an essential feature of non-locality in quantum theory, *Nat. Commun.* **9**, 4244 (2018).
- [56] R. Uola, A. C. S. Costa, H. C. Nguyen, and O. Gühne, Quantum steering, *Rev. Mod. Phys.* **92**, 015001 (2020).
- [57] K. Sugihara and I. Suzuki, Distributed algorithms for formation of geometric patterns with many mobile robots, *J. Robotic Syst.* **13**, 127 (1996).
- [58] I. Suzuki and M. Yamashita, Distributed anonymous mobile robots: Formation of geometric patterns, *SIAM J. Comput.* **28**, 1347 (1999).
- [59] A. Aggarwal, C. P. Rangan, P. Flocchini, G. Prencipe, N. Santoro, and P. Widmayer, Hard tasks for weak robots: The role of common knowledge in pattern formation by autonomous mobile robots, in *Proceedings of the 10th International Symposium on Algorithms and Computation, ISAAC'99* (Springer, New York, 1999), pp. 93–102.
- [60] G. Prencipe, Achievable patterns by an even number of autonomous mobile robots Technical Report, del Dipartimento di Informatica (Università di Pisa, Pisa, IT, 2000).
- [61] A. D. Kshemkalyani and F. Ali, Efficient dispersion of mobile robots on graphs, in *Proceedings of the 20th International Conference on Distributed Computing and Networking* (ACM Press, New York, 2019), pp. 218–227.
- [62] D. Dereniowski, Y. Disser, A. Kosowski, D. Pająk, and P. Uznański, Fast collaborative graph exploration, *Inf. Comput.* **243**, 37 (2015).
- [63] P. Wittek, Algorithm 950: Ncpol2sdpa—Sparse semidefinite programming relaxations for polynomial optimization problems of noncommuting variables, *ACM Trans. Math. Softw.* **41**, 1 (2015).
- [64] P. Wittek and P. J. Brown, Updating ncpol2sdpa after Peter Wittek, <https://github.com/peterjbrown519/ncpol2sdpa>.

width=!,height=!,page=-