Input, Output, Insight: Inference from Black Boxes – Contextuality, Bell Inequalities, and Beyond

871. WE-Heraeus-Seminar

14 Oct - 17 Oct 2026
at the Physikzentrum Bad Honnef, Germany

WILHELM UND ELSE
HERAEUS-STIFTUNG

Introduction

The Wilhelm und Else Heraeus-Stiftung is a private foundation that supports research and education in science with an emphasis on physics. It is recognized as Germany's most important private institution funding physics. Some of the activities of the foundation are carried out in close cooperation with the German Physical Society (Deutsche Physikalische Gesellschaft). For detailed information see https://www.we-heraeus-stiftung.de

Aims and scope of the 871. WE-Heraeus-Seminar:

System-agnostic black box methods in quantum information include contextuality, communication matrices, device-independent cryptography, and any other approach to quantum information where quantum devices are described as uncharacterized black boxes with inputs and outputs. Some of these approaches, such as contextuality, were developed to address problems in foundations of quantum theory and they are currently finding their way towards applications in quantum information. Others were already developed with applications in mind.

This seminar will bring together the experts in various flavors of system-agnostic methods from both academia and industry, together with early-carreer researchers and PhD students. The goal is to discuss and compare the various methods, and to encourage cross-pollination of ideas, as well as to discuss recent theoretical progress and applications of these methods in quantum computing, quantum key distribution, and others.

Scientific Organizers:

Dr. Martin Plávala — Leibniz Universität Hannover
E-Mail: martin.plavala@itp.uni-hannover.de

Dr. Rene Schwonnek — Leibniz Universität Hannover
E-Mail: rene.schwonnek@itp.uni-hannover.de

Introduction

Administrative Organization:

Dr. Stefan Jorda
Martina Albert

Wilhelm und Else Heraeus-Stiftung
Kurt-Blaum-Platz 1
63450 Hanau, Germany

Phone +49 6181 92325-14
Fax +49 6181 92325-15
E-mail albert@we-heraeus-stiftung.de
Internet: www.we-heraeus-stiftung.de

Venue:

Physikzentrum
Hauptstrasse 5
53604 Bad Honnef, Germany

Conference Phone +49 2224 9010-120

Phone +49 2224 9010-113 or -114 or -117
Fax +49 2224 9010-130
E-mail gomer@pbh.de
Internetwww.pbh.de

Taxi Phone +49 2224 2222

Registration:

Martina Albert (WE Heraeus Foundation)
at the Physikzentrum, reception office
Wednesday (16:00 h – 20:00 h) and Thursday morning

Program

Program

Wednesday, 14 October 2026

16:00 – 20:00	Registration	
18:00 – 19:45	*BUFFET SUPPER*	
19:45 – 20:00	Organizers	**Opening remarks**
20:00 – 21:00	Adán Cabello	**Understanding Quantum Theory through Non-locality and Contextuality**

Thursday, 15 October 2026

08:00	*BREAKFAST*	
09:00 – 10:00	Péter Frenkel	**Classical simulations of quantum channels**
10:00 – 10:30	Jan-Åke Larsson	**Oracles, Contextuality, and the advantage of Quantum Computation**
10:30 – 11:00	*COFFEE BREAK*	
11:00 – 12:00	Mariami Gachechiladze	**Quantum Bell Inequalities from Physical Principles**
12:00 – 12:30	Flavien Hirsch	**Bell nonlocality without labels**
12:30 – 12:40	**Conference Photo**	
12:40 – 14:00	*LUNCH*	

Program

Thursday, 15 October 2026

14:00 – 14:30	Oskari Kerppo	**Minimizing entanglement entropy for enhanced quantum state preparation**
14:30 – 15:00	Leevi Leppäjärvi	**Communication matrices: overview and applications**
15:00 – 15:30	Teiko Heinosaari	**Minimal communication tests revealing quantum benefit**
15:30 – 16:00	*COFFEE BREAK*	
16:00 – 18:00	**Discussions**	
18:00 – 19:00	***HERAEUS DINNER***	
	(social event with cold & warm buffet and complimentary drinks)	
19:00 – 19:30	**Poster Flash I**	
19:30 – 21:00	**Poster Session I**	

Program

Friday, 16 October 2026

08:00	*BREAKFAST*	
09:00 – 10:00	Zhen Peng Xu	**Optimal strategies for shadow tomography with limited resources**
10:00 – 10:30	Markus Frembs	**Generalised contextuality in the n-qubit Pauli group**
10:30 – 11:00	*COFFEE BREAK*	
11:00 – 12:00	Markus Müller	**How can probabilities of events depend on spatial rotations in any physical theory?**
12:00 – 12:30	Mehdi Mhalla	**Interrupting the link between correlations and probabilities**
12:30 – 14:00	*LUNCH*	
14:00 – 14:30	Mirjam Weilenmann	**Timed demolition measurements**
14:30 – 15:00	Miguel Navascues	**Causality and realizability of local operations in quantum field theory**
15:00 – 15:30	Fatemeh Moradi Kalarde	**Fermions are fundamentally more non local than Bosons.**
15:30 – 16:00	*COFFEE BREAK*	
16:00 – 16:15	Video	**About the WE-Heraeus Foundation**
16:15 – 18:00	**Discussions**	

Program

Friday, 16 October 2026

18:00 – 19:00	*DINNER*	
19:00 – 19:30	**Poster Flash II**	
19:30 – 21:00	**Poster Session II**	

Saturday, 17 October 2026

08:00	*BREAKFAST*	
09:00 – 10:00	Stefano Pironio	**An EPR principle for quantum correlations**
10:00 – 10:30	Lidya Law	**Family of Bell inequalities suited for the (robust) self-testing of n-qubit W states alongside trine measurements**
10:30 – 11:00	*COFFEE BREAK*	
11:00 – 12:00	Sixia Yu	**TBA**
12:00 – 12:30	Monika Mothsara	**Robust One-Sided Device-Independent Quantum Key Distribution via High-Dimensional Steering**
12:30 – 12:45	Organizers	**Closing Remarks**
12:45 – 14:00	*LUNCH*	

End of the seminar and departure

Posters

Posters I

Ieline Ahmed	**Multipartite Bell inequalities with interferometric multiports**
Patrick Andriolo	**Witnessing nonstabilizerness with Bell inequalities**
Alexander Bernal	**Absolute CHSH-locality and maximally CHSH-nonlocal states**
Some Sankar Bhattacharya	**Quantum Advantage in Multi-Party Conflict-of-Interest Bayesian Games & Interferometric Optical Routing**
Enrico Bozzetto	**Warring contextualities - Provably classical vs provably nonclassical**
Lorenzo Catani	**Bell's Go theorem: regaining local causality with a new notion of realism**
Raman Choudhary	**Exploring Bell Nonlocality with Extremal Non-Signaling Boxes**
Ozgur Cildiroglu	**Geometric Control of Bell Correlations**
Lorenzo Coccia	**Systematic derivation of Tsirelson bounds in arbitrary dimensions**
Juan Diego Diaz Martinez	**Modal Logic and No-Go Theorems in GHZ-Frauchiger–Renner Scenarios**
Hippolyte Dourdent	**Paradox-free classical non-causality and unambiguous non-locality without entanglement are equivalent**
Reyhan Durucu Hamzaogullari	**Necessity of fine-tuning in classical causal models reproducing KCBS inequality violations**
Ricardo Faleiro	**Bell nonlocality does not imply violation of nonlocal games**

Posters I

Tomás Fernández Martos	**Deterministic randomness extraction for quantum random number generation with partial trust**
Denis Freudenheim Moraes	**Communication-based operational principles bounding nonlocal correlations**
Subhendu Bikash Ghosh	**Strong Inequivalence of Quantum Nonlocal Resources**
Tamal Guha	**Optimal Unlocking of Encoding Strength: Assistance from Environment**
Joel Huber	**Consistent Dynamics in Phase Space: Quantum States Require Quantum Time Evolution**
Kartik Kakade	**Maximum Entropy Principle for Quantum Channels**

Posters II

Robin Krebs	**Polynomial optimization of the parallel repetition of classical nonlocal games**
Luca Mariani	**Quantum Key Distribution over Complex Networks**
Nikolai Miklin	**Universal method for optimized robustness in self-testing of quantum resources**
Aurora Mugnai	**Certifying randomness in a semi-device-independent scenario via Probability Estimation**
Bita Olamaei	**Genuine linear-optical test of quantum contextuality with sequential measurements**
Lucas Porto	**CABIPARA.jl: A user-friendly Julia package for two-qubit steering and Bell nonlocality**
Samgeeth Puliyil	**Predictive and retrodictive power of operational theories**
Maria Eduarda Reichmann Filippetto	**tba**
Martin J. Renner	**All pure entangled states can lead to fully nonlocal correlations**
Albert Rico	**Robust certification of high-dimensional quantum devices**
Abhyoudai Sajeevkumar Shaleena	**Communication complexity games and Continuous variable Bell inequalities**
Oxana Shaya	**Certifying measurement incompatibility under bounded classical communication**
Ritesh Kumar Singh	**Multipartite Device-Independent Quantum Key Distribution using Genuinely nonlocal correlations**

Posters II

Shawn Skelton	**On the relationship between quantum adiabatic evolution and quantum signal processing**
Adrian Solymos	**No-local-broadcasting theorem for nonsignaling behaviors and assemblages**
Carlos Vieira	**Non-signaling assistance in prepare-and-measure scenarios with classical communication**
Kannan Vijayadharan	**Towards rigorous tests of Bell nonlocality with time-bin entanglement**
Sujan Vijayaraj	**Improving device-independent quantum key distribution protocols through multiple routed Bell tests**
Kläre Wienecke	**Field Test of Entanglement Assisted Classical Communication**

Abstracts of Lectures

(in alphabetical order)

Understanding Quantum Theory through Non-locality and Contextuality

Adán Cabello

Departamento de Física Aplicada II,
Universidad de Sevilla, E-41012 Sevilla,
Spain
Instituto Carlos I de Física Teórica y Computacional,
Universidad de Sevilla, E-41012 Sevilla,
Spain

(Dated: July 6, 2026)

By establishing a connection between three foundational programs—the search for the principle that shapes the sets of quantum correlations in Bell scenarios, the reconstruction of quantum theory within general probabilistic theories, and Einstein-Podolsky-Rosen's program for a complete physical theory beyond quantum mechanics—, we obtain a simple answer to the question of what is the principle that singles out quantum theory.

Generalised contextuality in the n-qubit Pauli group

Markus Frembs, Leibniz University Hannover

The n-qubit Pauli group is an essential ingredient to most quantum applications, from computing and error correction to benchmarking and simulation. Despite comprising merely a discrete set of operators, it exhibits many quintessential features of quantum theory, including contextuality, which has been identified as a key resource to quantum advantage in a variety of different flavours. Here, we extend this analysis, using the notion of `noncontextual property' whose nonexistence proves the Kochen-Specker theorem, similarly to and generalising common arguments based on the nonexistence of valuations. The usual argument based on valuations arises as a special case.

We show that the Pauli group for two qubits does admit noncontextual properties, despite admitting no valuations. We then establish this as the only such case, by proving that any Boolean-valued frame function on stabiliser states is constant for more than two qubits. We also perform a similar analysis for the symplectic theory underlying the n-qubit Pauli group, for which nonconstant Boolean-valued frame functions exist for all n, yet only in a very restricted form. By comparison, this shows that contextuality in the n-qubit Pauli group is not only a consequence of the projective character of the Pauli group as a representation of its underlying symplectic vector space, but in larger part of the geometry of symplectic polar spaces itself.

CLASSICAL SIMULATIONS OF QUANTUM CHANNELS

PÉTER E. FRENKEL

A communication protocol with l possible inputs and k possible outputs can be described by a *transition matrix* $A = (a_{ij}) \in [0,1]^{k\times l}$, where a_{ij} is the conditional probability of output i if the input is j. A *communication channel* can be described by the set of transition matrices that it affords. Channel Q *can be simulated* by channel C if all transition matrices afforded by Q are convex combinations of transition matrices afforded by C. Such convex combinations occur naturally in information theory; they correspond to the sender and receiver having access to (unlimited) shared randomness.

The *classical channel with n states* affords column-stochastic 0-1 matrices with at most n nonzero rows. The *quantum channel of level n* affords matrices of the form $(\operatorname{tr} E_i\rho_j)$, where $\rho_1,\dots,\rho_l \in M_n(\mathbb{C})$ are *density matrices*, and $E_1,\dots,E_k \in M_n(\mathbb{C})$ is a *positive operator valued measure*. It is easy to see that the classical channel with n states can be simulated by the quantum channel of level n. By [1], the converse also holds. I will sketch the proof of this theorem and its generalization to noisy quantum channels, where the mathematical model of noise, rather than the usual CPTP map framework, is the following.

In quantum communication, information is encoded by quantum states. Mathematically, a quantum state is described by a density operator on a Hilbert space which, for us, will have a fixed finite dimension n. Communication is most efficient if we use pure states. To model noise, however, we consider a quantum channel where each state used for the encoding is mixed "to at least a certain extent". If shared randomness is available to the sender and the receiver, then any such channel can be simulated by an n-state classical channel using classical states that are "at least as mixed" as the corresponding quantum states [2].

References

[1] P. E. Frenkel and M. Weiner: Classical information storage in an n-level quantum system, Communications in Mathematical Physics 340 (2015), 563–574.

[2] P. E. Frenkel: Classical simulations of communication channels. Quantum 6, 751 (2022).

Email address: peter.e.frenkel@gmail.com

Eötvös Loránd University, Pázmány Péter sétány 1/C, Budapest, 1117 Hungary

N. Minklin[1], P. Jain[1], C. Smaczny[1], C. Budroni[2], M. Gachechiladze[1]

[1]TU Garmstadt, Darmstadt, Germany, [2]University of Pisa, Pisa, Italy

Information Causality was introduced as a physical principle for constraining nonlocal correlations. We present a series of developments that broaden its scope beyond the standard random access code setting. Allowing correlations among Alice's inputs connects the principle to general one-way communication complexity and yields tighter constraints, in some cases recovering parts of the quantum boundary. We also extend the method to more general Bell scenarios and derive new bounds for entanglement-assisted communication tasks. Finally, we discuss a new multi-copy activation phenomenon, in which correlations satisfying all relevant single-copy constraints violate Information Causality when two copies are combined through an adaptive local wiring. This suggests a hierarchy of increasingly strong Information Causality constraints.

References

[1] P Jain, N Miklin, M Gachechiladze, arXiv:2606.02416 (2026)

[2] N Miklin, P Jain, M Gachechiladze, arXiv:2602.10206 (2026)

[3] P Jain, M Gachechiladze, N Miklin, Physical Review Letters 133 (16), 160201(2024)

[4] M Gachechiladze, B Bąk, M Pawłowski, N Miklin, Quantum 6, 717 (2022)

[5] N Miklin, M Pawłowski, Physical Review Letters 126 (22), 220403 (2021)

[6] M Pawłowski, T Paterek, D Kaszlikowski, V Scarani, A Winter, M Żukowski, Nature 461, 1101–1104 (2009)

Minimal communication tests revealing quantum benefit

Teiko Heinosaari

A black-box test is characterized by an analysis based solely on input –output statistics. Communication tests form a particular subclass of such tests, in which the sender is allowed to transmit a physical system to the receiver in addition to the shared inputs. Quantum random access coding provides a paradigmatic example of this setting. In this contribution, I present a classification of a certain class of simple communication tests. These tests are divided into three groups according to the resources they reveal: those compatible with no communication, those requiring classical bit communication, and those requiring qubit communication. The two qubit-based tests identified in this framework are minimal in the sense that they involve the smallest possible input structure for the communicating parties.

Bell nonlocality without labels

Flavien Hirsch and Ricardo Faleiro and Emmanuel Zambrini Cruzeiro

Instituto de Telecomunicações, Lisbon

Instituto Superior Técnico - Torre Norte - Piso 10 Av. Rovisco Pais, 1 1049 - 001 Lisboa

We consider a minimal Bell scenario, where Alice and Bob cannot reliably assign labels to their outcomes. Instead, in each round, they only receive a single global bit of information.

In this minimal scenario, we show that one can still certify Bell nonlocality, without any further assumptions than the usual ones of Bell's theorem. That is, minimal received information can be enough to violate locality, without knowing anything about the underlying "real" outcomes, or even assuming anything about the outcome structure.

We construct Bell-like inequalities for these minimal scenarios, and display several examples of quantum violations. We also apply these inequalities to a scenario where the outcomes are themselves quantum states - a case where they are thus inherently "unlabelizable".

We also show how these new families of inequalities are relevant and useful in and of themselves, and how our scenario can naturally appear in realistic experiments where outcomes are hard to label.

Minimizing entanglement entropy for enhanced quantum state preparation

Oskari Kerppo[1], William Steadman[2], Ossi Niemimäki[3], and Valtteri Lahtinen[4]
[1,2,3,4]Quanscient Oy, Peltokatu 34, 33100 Tampere, Finland
[4]School of Engineering Science, Lappeenranta–Lahti University of Technology, P.O. Box 20, 53851, Lappeenranta, Finland

State preparation is a crucial component of modern quantum algorithms. To process classical data on a quantum device, it must first be encoded into a quantum state. While bit and angle encodings are straightforward to implement, amplitude encoding offers exponential memory savings by mapping 2^n classical data points into n qubits. However, preparing an arbitrary amplitude-encoded state generally requires exponential circuit complexity. To overcome this computational bottleneck, approximate state preparation techniques using variational methods and Matrix Product States (MPS) have become vital.

In this presentation, I will discuss quantum state preparation in the context of designing quantum algorithms at an industrially meaningful scale. Drawing on results from our recent work [1], I will examine why state preparation is challenging in general and present possible pathways toward preparing states on larger numbers of qubits. Specifically, I will show how the entanglement entropy of a quantum state directly dictates its MPS representation and the resulting algorithmic preparation cost. This analysis demonstrates how minimizing entanglement entropy can enable enhanced quantum state preparation with high output fidelity at a low gate cost.

References

[1] O. Kerppo, W. Steadman, O. Niemimäki, V. Lahtinen, arXiv:2507.22562 (2026).

Oracles, Contextuality, and the advantage of Quantum Computation

Jan-Åke Larsson

Linköping University, Linköping, Sweden

The usual explanation of the quantum computing speedup is parallel calculation, inserting a superposition of all possible input values to be processed in parallel, perhaps in multiple parallell worlds, and then combined by interference to obtain the desired answer. Unfortunately, this does not give any guidance on how to identify new mathematical problems that could be solved. This presentation will introduce an alternative approach: tracing the calculation in phase space. We will see that a function oracle with phase space inputs and outputs that realizes the phase space map promised by quantum mechanics, will reproduce the quantum advantage. This happens even if the constituent information-bearing systems are classical, but have a (discrete) phase space structure. This indicates that the quantum speedup is a consequence of the phase space structure of the information-bearing systems, and not a consequence of the quantum nature of the systems themselves, nor of quantum parallelism. It rather is a consequence of limitations to the amount of information that can be extracted from the output of a black-box classical oracle, a limitation that is not present if the outputs have the richer structure of a (discrete) phase space. It may therefore be useful to avoid the oracle paradigm. This presentation will therefore also introduce a positive-distribution phase space description of a restriction of quantum mechanics, that still reproduces the contextual behavior of quantum systems, and exhibits nonlocality. The description is Einstein-complete, but distinct from Bohmian mechanics. We will briefly see how this can be used describe one particular quantum algorithm, the Shallow Circuit Algorithm, proven to give a non-oracular advantage. In conclusion, the phase space approach to quantum algorithms together with new phase space descriptions of the kind presented here will provide a better understanding of the origin of the quantum speedup.

Family of Bell inequalities suited for the (robust) self-testing of n-qubit W states alongside trine measurements

Lidya Law[1], **Ranendu Adhikary**[1,*], **and Yeong-Cherng Liang**[1,†]

[1] *Department of Physics and Center for Quantum Frontiers of Research & Technology (QFort), National Cheng Kung University, Tainan 701, Taiwan*

In device-independent quantum information, self-testing [1] provides the strongest form of certification, allowing quantum states and measurements to be identified solely from observed correlations, without assumptions about the internal workings of the devices. Extending this approach to multipartite systems is particularly challenging because multipartite entanglement exhibits a much richer structure than the bipartite [2]. Among multipartite states, the N-qubit W state, $|W_N\rangle$, is particularly interesting because its entanglement can survive particle losses [3]. Nevertheless, Bell inequalities capable of self-testing multipartite states for an arbitrary number of parties remain scarce, and no Bell-inequality construction was previously known to self-test the N-qubit W state beyond $N \leq 3$.

We introduce a family of Bell inequalities, defined for every $N \geq 3$, whose maximal quantum violations self-test $|W_N\rangle$ together with a set of *trine* measurements for each party. These measurements correspond to three equally spaced observables in the real ZX-plane of the Bloch sphere. Since an exact maximal violation cannot be attained in a realistic experiment, we further investigate the robustness. For the three-qubit case, we derive an explicit robustness bound showing that any observed near-maximal violation certifies a physical realization whose extracted state and measurements are $O(\sqrt{\varepsilon})$-close to the ideal realizations. Further experimental imperfections are examined under white-noise and detector-inefficiency models. The white-noise tolerance is evaluated as a function of the number of parties. On the other hand, the detector-loss analysis demonstrates improved robustness over previous constructions with a comparable number of measurement settings. Finally, the proposed inequalities also certifies genuine multipartite entanglement from small Bell violations.

Our results thus provide a scalable family of Bell-inequalities for self-testing N-qubit W state with experimental robustness and certification of genuine multipartite entanglement via an appropriate amount of quantum violation.

References

[1] I. Šupić and J. Bowles, Quantum **4**, 337 (2020).
[2] A. Acín, D. Bruß, M. Lewenstein, and A. Sanpera, Phys. Rev. Lett. **87**, 040401 (2001).
[3] T. J. Barnea *et al.*, Phys. Rev. A **91**, 032108 (2015).

*ronjumath@gmail.com

†ycliang@mail.ncku.edu.tw

Communication matrices: overview and applications

Leevi Leppäjärvi

Faculty of Information Technology, University of Jyväskylä, Jyväskylä, Finland

Communication scenarios between two parties can be implemented in prepare-and-measure set-ups by first encoding messages into some states of a physical system which acts as the physical medium of communication and then decoding the messages by measuring the state of the system (see Fig. 1.). These types of scenarios can be described by collecting the measurement outcome probabilities for the different states into a row-stochastic matrix called the communication matrix. By looking at the properties of the communication matrices, we can say a lot not only about the specific communication tasks that they describe but also about the underlying physical system which was used to implement the communication. In this talk I will review some of the recent results on communication matrices including how can we show an unbounded quantum advantage over classical communication [1] and how we can use communication matrices for semi-device-independent identification of quantum channels/gates [2].

References:

[1] T. Heinosaari, O. Kerppo, L. Leppäjärvi, M. Plávala, Phys. Rev. A 109, 032627 (2024).

[2] S. Puliyil, L. Leppäjärvi, M. Ziman, arXiv:2511.14273 (2025).

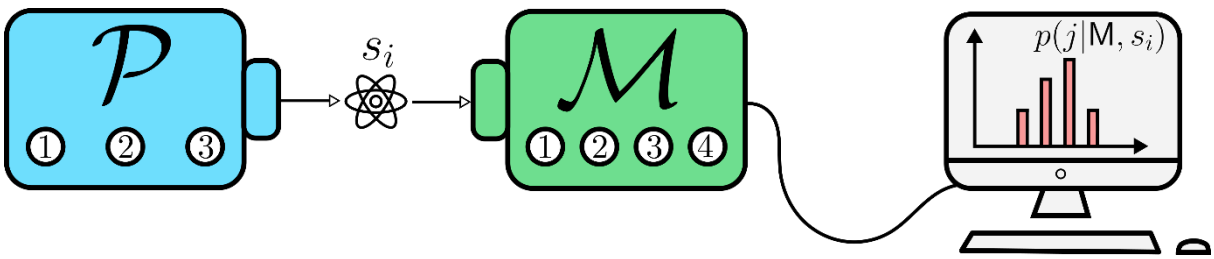


Fig. 1. Basic one-way communication setup between two parties. On each round of communication the sender receives a random variable and prepares a state from their state ensemble. The receiver performs a measurement and receives and registers an outcome. Communication matrix represents the measurement outcome probabilities for all states in the state ensemble.

Interrupting the Link between Correlations and Probabilities: Contextuality from Open Dynamical Processes

M. Mhalla[1] and L. Triouleyre[2]

[1,2] Université -Grenoble Alpes, Grenoble INP, CNRS LIG Grenoble

Recent advances in the study of contextuality have provided increasingly refined quantitative characterizations of non-classical correlations. In particular, our work on the multipartiteness width of contextuality naturally raises a more fundamental question: what should count as a "part" in a physical or informational process? More generally, within an explanatory framework, what are the minimal representational structures that the theory does not exclude *a priori* and that may therefore be considered, at the meta-language level, as observers, subsystems, or simply parts?

Motivated by this question, we initiated, through Louis Triouleyre's Master's project, a study of contextuality from a dynamical perspective. Instead of taking measurement scenarios as primitive, we study contextual behaviours generated by interacting open automata, whose observable behaviours emerge through their interactions. The underlying idea is that a probabilistic description of observed correlations need not be the primitive level of description: it may arise by forgetting part of the dynamical structure that produces the observations.

The ongoing work, *Contextuality as Automata: Open Generators and the Dynamics of Quantum Phenomena* [1], develops a process-oriented interpretation of contextuality. We show how the contextual fraction can be recovered when lifting the description from observed states to execution paths generated by open automata. In this sense, the dynamical description provides an intermediate level between the processes that generate observations and the probabilistic correlations extracted from them.

Finally, I will briefly discuss the broader research program suggested by this perspective. Rather than taking observers, subsystems, and representations as primitive notions, we aim to investigate how they may emerge collectively as localized perspectives within interruptible interaction processes. This suggests a longer-term framework in which contextuality, distributed computation, and information processing can be viewed as different aspects of a common dynamics of representation.

References

[1] `https://membres-lig.imag.fr/mhalla/understanding/Rapport_de_stage_M2-Louis.pdf`

Fermions are fundamentally more nonlocal than Bosons

Fatemeh Moradi Kalarde[1†], Sadra Boreiri[2], Xiangling Xu[1], Lucas Tendick[1], Salman Beigi[3], Paolo Perinotti[4,5], Tommaso Guaita[6], Marc-Olivier Renou[1]

[1]Inria, CPHT, LIX, CNRS, Ecole polytechnique, Institut Polytechnique de Paris, Palaiseau, France
[2]Department of Applied Physics, University of Geneva, Geneva, Switzerland
[3]School of Mathematics, Institute for Research in Fundamental Sciences (IPM), P.O. Box 19395-5746, Tehran, Iran
[4]Dipartimento di Fisica dell'Università di Pavia, via Bassi 6, 27100 Pavia
[5]Istituto Nazionale di Fisica Nucleare, Gruppo IV, via Bassi 6, 27100 Pavia
[6]Dahlem Center for Complex Quantum Systems, Freie Universität Berlin, Arnimallee 14, 14195 Berlin, Germany

[†]fatemeh.moradi-kalarde@inria.fr

Abstract

Bell's theorem shows that entangled quantum particles can exhibit correlations that classical particles cannot reproduce without an additional nonlocal resource, such as communication. In this sense, quantum particles are fundamentally more nonlocal than classical ones, and entanglement becomes unavoidable in physics. Here we prove the analogous result within quantum theory itself: indistinguishable fermions transmitted through a quantum network can generate correlations that distinguishable particles or indistinguishable bosons cannot reproduce without additional communication. In the same sense, fermions are fundamentally more nonlocal than bosons or distinguishable particles, motivating fermionic anticommutation and indistinguishability as unavoidable operational resources. Our result further implies that fermions can strictly surpass all qubit-based protocols for certain distributed computing tasks, demonstrating that a complete understanding of information processing requires going beyond qubits to fermionic information carriers—*febits*.

Robust One-Sided Device-Independent Quantum Key Distribution via High-Dimensional Steering

Monika Mothsara[1], Suraj Goel[2], Bohnishikha Ghosh[2], Vatshal Srivastav[2], Will McCutcheon[2], Mehul Malik[2], Gláucia Murta[1]

[1]TU Wien, Atominstitut, Stadionallee 2, 1020 Vienna, Austria

[2]Institute of Photonics and Quantum Sciences, Heriot-Watt University, Edinburgh, UK

Abstract

Quantum key distribution (QKD) brings the promise of communication with information-theoretic security but is limited in practice due to its susceptibility to noise, losses, and device imperfections. To address these challenges, we propose a robust high-dimensional (HD) *one-sided* device-independent QKD (1sDI-QKD) protocol and present a proof-of-principle experimental implementation using photons entangled in the transverse-spatial degree-of-freedom. We develop a systematic security analysis of HD 1sDI-QKD protocols, leveraging quantum steering to certify security, and evaluate achievable secret key rates for different measurement configurations and system dimensions using reverse reconciliation. Our analysis shows that increasing the dimension enhances robustness against both noise and loss. We then demonstrate the key experimental building blocks required for implementing the protocol: (a) a high-quality source of high-dimensional photonic entanglement, and (b) a fully programmable, high-dimensional multi-outcome measurement device operating in up to dimension 11. Using these components, we obtain positive key rates for all investigated dimensions under the fair-sampling assumption, with the highest key rates achieved for dimension $d = 7$. Finally, we discuss the steps required for a practical, loophole-free implementation of 1sDI-QKD in realistic regimes of loss and noise.

Causality and realizability of local operations in quantum field theory

Jan Mandrysch, Robin Simmons and Miguel Navascués

Institute of Quantum Optics and Quantum Information (IQOQI) Vienna

As noted by Sorkin, identifying the operations accessible within some spacetime region with quantum instruments whose Kraus operators are localizable therein leads to superluminal communication. This so-called Sorkin paradox can be resolved by further constraining the set of allowed local operations in quantum field theory (QFT). In this spirit, Fewster and Verch proposed a framework for local QFT operations that generalizes non-relativistic quantum measurement theory and does not lead to Sorkin-like paradoxes. Shortly afterwards, Jubb (and later Oeckl) identified the minimal conditions that QFT instruments must satisfy to be compatible with Einstein's causality. In this work, we study both approaches in the quantum field theory of the free scalar field. First, we prove that a very wide class of causal instruments is FV-realizable: namely, those whose measurement channels are random displacements of the field operators. As we show, those allow implementing arbitrary instruments in a heralded, probabilistic way, as well as non-demolition measurements deterministically. Second, we construct examples of causal channels that do not admit an approximate FV realization. Some of such causal, not FV-realizable channels violate basic physical principles, so they should not be part of any future measurement theory for QFT. Third, we investigate the difficulty of characterizing the set of QFT channels that can be generated through the composition of several FV schemes. In this regard, we find a countable family of QFT channels for which no Turing machine can discriminate between channels within or far away from the implementable set.

An EPR principle for quantum correlations

Stefano Pironio,
Jef Pauwels, Lidya Law and Yeong-Cherng Liang
Université libre de Bruxelles, Belgium

Einstein, Podolsky and Rosen argued that a quantity which can be predicted with certainty, without disturbing a system, must have a definite value. Bell showed that such pre-existing local values cannot reproduce quantum correlations. We show that EPR's intuition nevertheless survives once the predicting system is discarded: all reliably predictable measurements on a system have a joint probability distribution, which reproduces their statistics and their correlations with every other system except the one used for the prediction. Quantum theory satisfies this property, and we propose it as a physical principle, the EPR principle, for theories beyond quantum mechanics.

The EPR principle forbids bound randomness: a single external system cannot perfectly predict both outcomes of a nonlocal Bell experiment for every pair of measurement choices. We construct explicit tripartite correlations showing that the almost quantum set, which satisfies nearly every previously proposed principle, permits precisely this phenomenon of bound randomness and hence violates the principle. The construction extends to every finite level of the Navascués–Pironio–Acín hierarchy. The EPR principle also implies both standard and generalized information causality, using information measures only for classical data, and with them every limit on correlations known to follow from these conditions. Finally, it excludes the tripartite time-ordered bilocal correlations of Gallego et al., which satisfy every bipartite information principle compatible with classical correlations. The principle thus passes two tests that have resisted previous proposals.

Timed demolition measurements

Konstantinos Manos and Miguel Navascués
Institute for Quantum Optics and Quantum Information (IQOQI) Vienna, Austrian Academy of Sciences, Boltzmanngasse 3, Wien 1090, Austria

Mirjam Weilenmann
Inria Saclay, Télécom Paris – LTCI, Institut Polytechnique de Paris, 19 Place Marguerite Perey, 91120 Palaiseau, France

Imagine an experimental scenario where a closed quantum system, evolving through a time-independent Hamiltonian, is subject to a demolition measurement at a chosen time. The Hamiltonian, the measured observables, the initial state of the physical system and even its Hilbert space dimension are unknown; we nonetheless assume a promise or constraint on the energy distribution of the state. What can we infer about the underlying system from measurement data collected at few different times?

We find that, for many natural energy constraints, the set of feasible time series or datasets can be characterized efficiently. Furthermore, under the assumption of a bounded energy spectrum, we prove that there exist "self-testing" datasets, whose approximate realization singles out specific states and Hamiltonians and measurement operators on their support. Investigating to what extent the extrapolation of past measurement data is possible in this framework, we identify energy-constrained physical systems for which a non-trivial prediction at time τ requires a precision in the measurement data superexponential in τ . We also discover two extrapolation phenomena: "aha! datasets", which drastically increase the predictability of the future statistics of an unrelated measurement; and "fog banks": fairly simple datasets that exhibit complete unpredictability at some future time τ, but full predictability at a later time $\tau' > \tau$. Besides their relevance for quantum foundations, our results have applications in semi-device independent quantum communication, the simulation of complex quantum systems, and the design of optimal atomic clocks.

Optimal strategies for shadow tomography with limited resources

Z.-P. Xu[1], Q. Ye[2], J. Wang[3], G. Koßmann[4], A. Winter[5,6,7,8] and R. Schwonnek[9]

[1]School of Physics, Anhui University, Hefei 230601, China
[2]Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing 100084, China
[3]State Key Laboratory of Mathematical Sciences, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing, China
[4]Institute for Quantum Information, RWTH Aachen University, 52074 Aachen, Germany
[5]Department Mathematik/Informatik—Abteilung Informatik, Universität zu Köln, Albertus-Magnus-Platz, 50923 Köln, Germany
[6]ICREA—Institució Catalana de Recerca i Estudis Avançats, Pg. Lluis Companys, 23, 08010 Barcelona, Spain
[7]ICREA & Grup d'Informació Quàntica, Departament de Física, Universitat Autònoma de Barcelona, 08193 Bellaterra (Barcelona), Spain
[8]Institute for Advanced Study, Technische Universität München, Lichtenbergstraße 2a, 85748 Garching, Germany
[9]Institut für Theoretische Physik, Leibniz Universität Hannover, 30167 Hannover, Germany

Shadow tomography addresses the task of efficiently predicting many expectation values of an unknown quantum state from randomized measurements on comparatively few copies. Existing analyses promise large scaling advantages, but the optimal strategies realizing these guarantees are not always known, and the required measurements are potentially challenging to implement on current hardware. We address this gap for Pauli observables by computing optimal sample-complexity parameters and constructing optimal measurement strategies under realistic resource constraints. We focus on memoryless protocols, where each copy is measured only once, and on measurements with bounded interaction range. Our approach reduces the problem to the analysis of graph parameters of the frustration graph encoding the Pauli anticommutation relations. We provide efficient numerical methods for the general case and analytically prove that Clifford measurements are optimal in many situations. This includes all perfect graphs, all single-qubit, all two-qubit measurement scenarios, and more. Applied to Hamiltonian energy estimation, our framework yields constructive strategies and improved variance bounds.

References

[1] Z.-P. Xu, Q. Ye, J. Wang, G. Koßmann, A. Winter and R. Schwonnek, arXiv: 2608.08429 (2026)

Abstracts of Posters

(in alphabetical order)

Multipartite Bell inequalities with interferometric multiports

Ieline Ahmed[1], Seyed Arash Ghoreishi[1], and Giovanni Scala[2]

[1] Institute of Physics, Slovak Academy of Sciences, Dúbravská Cesta 9, 84511 Bratislava, Slovakia

[2] Dipartimento Interateneo di Fisica, Politecnico di Bari, 70126 Bari, Italy

Bell inequalities are difficult to construct systematically when the number of parties, measurement settings, or outcomes becomes large. In this work, we use a characteristic-function representation to describe such Bell scenarios in a compact way. We encode *d*-valued outcomes as roots of unity, so that Bell functionals can be written as linear combinations of Fourier-type correlators. This representation is especially natural for interferometric multiport measurements, where local settings are implemented by phase shifts followed by a fixed Fourier multiport. We first show that well-known inequalities such as CHSH, CGLMP, and MABK can be recovered within this formalism by choosing suitable functionals, a.k.a. probes, in the space of characteristic correlators. We then study a fixed family of Fourier-generated probes for more general *N* players, *m* settings with *d* outcomes (*N*, *m*, *d*) scenarios. By optimizing over the shared quantum state and the local multiport phases, we find several numerical violations, including cases involving non-maximally entangled states. These results should be understood as structured, multiport-compatible Bell tests rather than globally optimal or facet-defining inequalities. The framework provides a practical route for exploring Bell inequalities adapted to interferometric implementations and suggests a natural path toward future optimized-probe constructions.

References

[1] R. F. Werner and M. M. Wolf, All-multipartite Bell-correlation inequalities for two dichotomic observables per site, *Physical Review A* **64**, 032112 (2001).

[2] M. Zukowski and C. Brukner, Bell's theorem for general *n*-qubit states, *Physical Review Letters* **88**, 210401 (2002).

[3] M. Karczewski, G. Scala, A. Mandarino, A. B. Sainz, and M. Zukowski, Avenues to generalising Bell inequalities, *Journal of Physics A: Mathematical and Theoretical* **55**, 384011 (2022).

Witnessing Non-stabilizerness with Bell Inequalities

R. A. Macêdo[1,2], Patrick Andriolo[2,3,4], S. Zamora[1,2], D. Poderini[2,5], R. Chaves[3,6]

[1]Departamento de Física Teórica e Experimental, Universidade Federal do Rio Grande do Norte, 59078-970 Natal-RN, Brazil; [2]International Institute of Physics, Federal University of Rio Grande do Norte, 59078-970 Natal, Brazil; [3]Physics Institute, University of São Paulo, Rua do Matão 1371, São Paulo, Brazil; [4]Atominstitut, Technische Universität Wien, Stadionallee 2, 1020 Vienna, Austria; [5]Università degli Studi di Pavia, Dipartimento di Fisica, QUIT Group, via Bassi 6, 27100 Pavia, Italy; [6]School of Science and Technology, Federal University of Rio Grande do Norte, 59078-970 Natal, Brazil

Non-stabilizerness is a fundamental resource for quantum computation, enabling quantum algorithms to surpass classical capabilities. Despite its importance, characterizing this resource remains challenging due to the intricate geometry of stabilizer polytopes and the difficulty of simulating non-stabilizer states. In this work, through device-independent considerations, we reveal an unexpected connection between non-stabilizerness and Bell inequalities. Although certain stabilizer states can already achieve maximal violations of specific Bell inequalities, we demonstrate that appropriately constructed Bell inequalities can nevertheless serve as witnesses of non-stabilizerness, revealing when a state lies beyond the stabilizer set. This result bridges two key quantum resources, uncovering a novel relationship between the device-independent framework and resource-theoretic properties of quantum computation.

References

[1] Macedo, R. A., Andriolo, P., Zamora, S., Poderini, D., Chaves, R. (2025). Witnessing nonstabilizerness with Bell inequalities. Physical Review A, 112(5), L050401.

Absolute CHSH-locality and maximally CHSH-nonlocal states

Alexander Bernal[1], J. Alberto Casas[2], Jesús M. Moreno[2]

[1]*Physics Department and NanoLund, Lund University, Box 118, 22100 Lund, Sweden.*
[2]*Instituto de Física Teórica, IFT-UAM/CSIC, Universidad Autónoma de Madrid, Cantoblanco, 28049 Madrid, Spain*

Abstract

In this poster, we consider the problem of determining, for a fixed spectrum of a density matrix, the largest attainable CHSH violation. We give a complete characterization for the qubit-qudit and qutrit-qudit case and provide the explicit form of a maximizing state for arbitrary local dimensions (d_A, d_B). In addition, motivated by the general problem, we introduce the notion of absolutely CHSH-local states, i.e., states that are unable to violate the CHSH inequality after arbitrary unitary transformations. Using this definition together with the qubit-qudit criterion, we characterize all (2,d)-dimensional states that are entangled in some basis (i.e., are not absolutely separable) but nevertheless cannot exhibit a CHSH-Bell violation under any unitary transformation. Finally, we analyze the infinite-dimensional asymptotic behavior as well as we explore some further multipartite scenarios.

Quantum Advantage in Multi-Party Conflict-of-Interest Bayesian Games & Interferometric Optical Routing

Kornikar Sen[1], Some Sankar Bhattacharya[2]

[1]Departamento de Física Teórica, Universidad Complutense de Madrid, Plaza de las Ciencias 1. Ciudad Universitaria, Madrid, 28040, Madrid, Spain

[2]Física Teòrica: Informació i Fenòmens Quàntics, Universitat Autònoma de Barcelona, 08193 Bellaterra, Spain

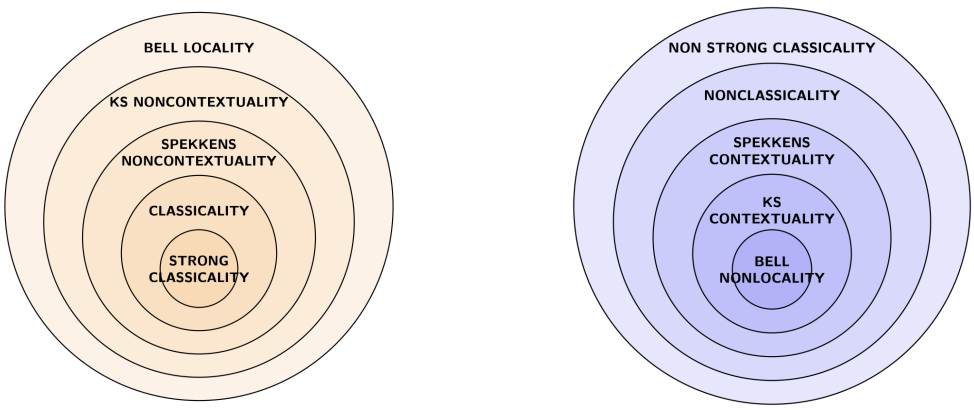
We formalize a multi-party conflict-of-interest Bayesian game framework to investigate quantum advantage in non-cooperative strategic scenarios under incomplete information. Under classical local realistic constraints, spatially separated agents face a fundamental trade-off between individual payoff optimization and global social efficiency, forcing the system into inefficient, asymmetric Nash equilibria where socially optimal outcomes are structurally unstable. By equipping players with a shared Greenberger-Horne-Zeilinger (GHZ) state and local Pauli measurements, we demonstrate that genuine multipartite nonlocality resolves strategic friction, establishing a symmetric quantum equilibrium that strictly Pareto-dominates all classical correlated Nash equilibria. We also prove that this quantum advantage is structurally universal across a generalized utility space, resilient against isotropic state depolarization up to 27.2% noise, and scales to arbitrary n-player setting where classical coordination decays exponentially. As a physical application, we map this strategic framework onto a highly constrained instance of a multi-port optical interferometric network, where nonlocal phase alignment deterministically eliminates modal crosstalk penalties without inter-node communication.

Warring Contextualities - Provably Classical vs Provably Nonclassical

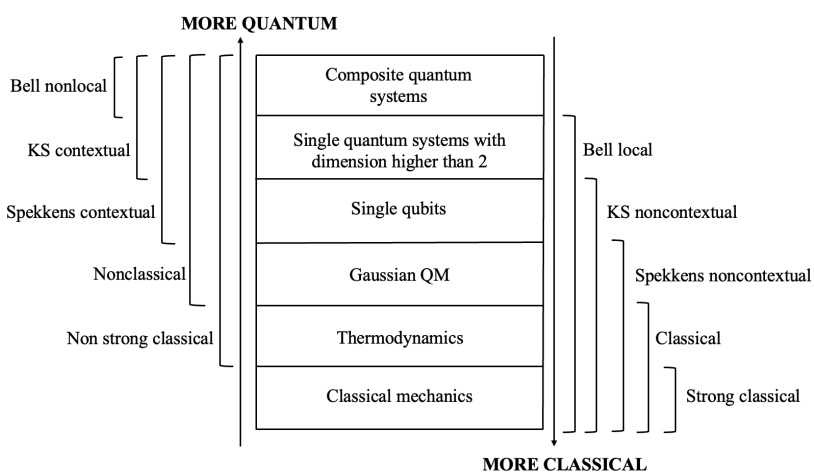
Enrico Bozzetto[1,2] and Jonte R. Hance[2,*]

[1] *DET, Politecnico di Torino, Corso Duca degli Abruzzi, 24, 10129 Torino, Italy*
[2] *Quantum Group, School of Computing, Newcastle University, 1 Science Square, Newcastle upon Tyne, NE4 5TG, UK*

In the literature, there are two differing definitions of contextuality: Kochen and Specker's, and Spekkens' (or "generalised"). However, researchers using one of these definitions rarely consider the other, meaning comparative analysis of these two notions is rare. In this paper, we advance the idea that Kochen-Specker contextuality provides a generalisation of the idea of system being fundamentally *nonclassical*, while Spekkens' noncontextuality provides a generalisation of the idea of a system being *classical*. This allows us to reconcile the two approaches, as different stages in a hierarchy of classicality/nonclassicality.



(a) (b)



* jonte.hance@newcastle.ac.uk

Bell's *go* theorem: regaining local causality with a new notion of realism

Lorenzo Catani,[1,*] Nesta Van Der Schaaf,[2] and Rui Soares Barbosa[3]

[1] *INESC TEC, Rua da Universidade, 4710-057 Braga, Portugal*
[2] *Université Paris-Saclay, CNRS, CentraleSupélec, ENS Paris-Saclay, Inria, Laboratoire Méthodes Formelles, 91190, Gif-sur-Yvette, France*
[3] *International Iberian Nanotechnology Laboratory, Av. Mestre José Veiga s/n, 4715-330 Braga, Portugal*

Bell's theorem is popularly stated as the inconsistency of quantum theory with local realism. More precisely, realism here is mathematically described by the ontological models framework, where the elements of reality are represented by points in a measurable space, and probabilities obey the Kolmogorov axioms. In the Bell scenario, such models amount to a common cause supporting a global valuation—a joint assignment of outcomes to all measurements at once, across mutually incompatible contexts. Within this notion of realism, Bell's theorem implies that any realist explanation of the quantum predictions must be conspiratorial: any underlying mechanism, whether superluminal, superdeterministic, or retrocausal, must be finely tuned so as never to manifest at the operational level. In this work, we redefine realism by developing a new ontological framework that generalizes the standard one and takes the incompatibility of measurement contexts seriously. The elements of reality are no longer points but regions of a point-free topological space (sublocales of a locale). These regions are primitive and inherently relational: they act as records that establish the sameness of a measurement across two incompatible contexts, without these pairwise identities composing into a global assignment across all of them. The common cause becomes a network of such records rather than a global valuation. Within this framework, Bell's no-go theorem becomes a go theorem: local causality is no longer at odds with the statistics of quantum theory. This is possible because, with no global valuation to preserve, the underlying probability theory generalizes Kolmogorov's, modularity being no longer required across incompatible contexts. We exhibit an explicit family of models in the new framework, reproducing several quantum strategies, including the optimal CHSH violation. More broadly, locally causal models of this kind attain every Bell–CHSH value up to the algebraic maximum. [a]

* lorenzo.catani4@gmail.com

[a] A preprint will be posted on arXiv prior to the conference.

Exploring Bell Nonlocality with Extremal Non-Signaling Boxes

Emmanuel Zambrini Cruzeiro[1,2], Junior R. Gonzales-Ureta[3], Raman Choudhary[4,5], Hugo Abreu[6], Adán Cabello[7,8], and Sébastien Designolle[6,9]

[1]Quantum Information and Quantum Optics Laboratory, Instituto Superior Técnico, Lisboa, Portugal
[2]Quantum Physics of Information Group, Instituto de Telecomunicações, Lisboa, Portugal
[3]Q*Bird BV, Delftechpark 1, 2628 XJ Delft, The Netherlands
[4]INL – International Iberian Nanotechnology Laboratory, Braga, Portugal
[5]Sorbonne Université, CNRS, LIP6, F-75005 Paris, France
[6]Zuse Institute Berlin, Takustraße 7, 14195 Berlin, Germany
[7]Departamento de Física Aplicada II, Universidad de Sevilla, E-41012 Sevilla, Spain
[8]Instituto Carlos I de Física Teórica y Computacional, Universidad de Sevilla, E-41012 Sevilla, Spain
[9]Inria, ENS de Lyon, UCBL, LIP, 69342 Lyon Cedex 07, France

Extremal non-signaling (ENS) boxes are the vertices of the non-signaling polytope and generalize the Popescu-Rohrlich box to arbitrary Bell scenarios. Although nonlocal ENS boxes are excluded by quantum theory and by theories of ideal measurements, they provide natural extremal resources for probing the boundary between quantum and post-quantum correlations. We develop a systematic approach to ENS boxes in bipartite Bell scenarios by combining explicit constructions with computational polytope methods. This yields complete and partial classifications in several previously unexplored scenarios, including vertices beyond PR-box-based constructions. We then use these boxes to address three foundational questions. First, we show that the magic-square correlation admits a minimal decomposition into exactly two ENS boxes. Second, every nonlocal ENS box found in the scenarios analyzed violates local orthogonality at the two-copy level, supporting the conjecture that this is a generic property of bipartite nonlocal ENS boxes. Third, we quantify their one-way classical-communication simulation cost and identify examples requiring messages ranging from one bit up to a five-level message; the largest cost found occurs in the (6,4,2,2) scenario. These results show that ENS boxes beyond the PR-box paradigm form a useful resource-theoretic toolkit for turning qualitative questions about Bell nonlocality into concrete problems involving decomposition, physical principles, and simulation cost.

Geometric Control of Bell Correlations

H.O. Cildiroglu

Ankara University, Physics Department, Ankara, Turkey

Here, we analyze spatially correlated two-quanton systems within single and double beam splitter Mach-Zehnder configurations. By evaluating these pure spatial correlations, we identify a critical particle production angle of 24.97 degrees. This specific angle fundamentally serves as the geometric analog of Bell inequalities. Building upon this foundational geometry, we then introduce adiabatic cyclic evolution into the system. This reveals that geometric and topological phases act as additional independent degrees of freedom to actively tune Bell correlations. Finally, we present a comprehensive fidelity analysis across these interferometric architectures to capture the dynamics of entanglement under phase manipulations. Our findings demonstrate that while single beam splitter configurations exhibit a decrease in fidelity with increasing concurrence, the double beam splitter setup robustly maintains maximum fidelity for maximally entangled states through precise retarder phase tuning.

References

[1] H.O. Cildiroglu, Annals of Physics, **489**, 170442 (2026)
[2] H.O. Cildiroglu, Physical Review A, **112**, 6, 062231 (2025)

Systematic derivation of Tsirelson bounds in arbitrary dimensions

Lorenzo Coccia[1], Matteo Padovan[1], and Giuseppe Vallone[1,2]

[1]*Dipartimento di Ingegneria dell'Informazione, Università degli Studi di Padova, via Gradenigo 6B, IT-35131 Padova, Italy*

[2]*Padua Quantum Technologies Research Center, Università degli Studi di Padova, via Gradenigo 6B, IT-35131 Padova, Italy*

The study of Bell nonlocality and the bounds of quantum correlations, the so-called Tsirelson bounds, is fundamental to quantum information science and the exploration of the limits of quantum theory. While quantum bounds for qubit systems have been extensively characterized, determining tight quantum bounds for correlations attainable with high-dimensional quantum states and measurements remains a significant challenge. In this work, we propose a systematic derivation of bipartite Tsirelson and local bounds written in terms of sum-of-squares decompositions. Using this method, we discover novel bounds and recover established results for maximally entangled states of qubits and qudits.

References

[1] Coccia, Padovan, Vallone, arXiv:2606.21626

Modal Logic and No-Go Theorems in GHZ-Frauchiger–Renner Scenarios

J.D. Díaz-Martínez[1] , Howard M. Wiseman[2], and Eric G. Cavalcanti[3]
[1,2,3]*Queensland Quantum and Advanced Technologies Research Institute (QUATRI), Griffith University, Brisbane, Australia*

Quantum foundations has advanced from Bell's theorem to the Local-Friendliness (LF) no-go theorem [1], which adopts weaker assumptions by treating observers themselves as quantum systems. Extensions of this kind lead to the Frauchiger–Renner (FR) paradox [2] and raise further questions related to the measurement problem. Underlying these arguments is contextuality: combining Born-rule predictions across different measurement contexts effectively imposes a non-contextuality assumption.

We examine a recent GHZ-based refinement of FR-type paradoxes by Walleghem et al [3]. By formalising its assumptions in modal logic, we show that the claimed paradox does not follow from the assumptions stated. We then formulate further no-go theorems within the same scenario. These recover an inconsistency between modal interpretations and Lorentz invariance, establish a new relational no-go theorem for theories allowing second-order absolute facts and composite observers, and identify the missing assumption needed to obtain a genuine GHZ-FR paradox, yielding a contradiction within a single experimental run.

Our framework makes explicit which inferences an agent is physically licensed to perform given the information accessible to them, distinguishing such inferences from those that implicitly rely on inaccessible knowledge. More speculatively, this provides a way to characterise the physical limits of reasoning for agents described quantum mechanically, potentially informing future implementations of Wigner's-friend scenarios with quantum computers and AI agents on quantum hardware.

These results clarify the logical structure, physical motivation, and consequences of the assumptions underlying FR-type and related quantum no-go arguments.

References

[1] K.-W. Bong et al., Nat. Phys. 16, 1199 (2020).
[2] D. Frauchiger and R. Renner, Nat. Commun. 9, 3711 (2018).
[3] N. Walleghem et al., Quantum 10, 2116 (2026), arXiv:2409.05491.

Paradox-free classical non-causality and unambiguous non-locality without entanglement are equivalent

Hippolyte Dourdent[1,2], Kyrylo Simonov[3], Andreas Leitherer[1], Emanuel-Cristian Boghiu[3], Ravi Kunjwal[4, 5], Saronath Halder[6,7], Remigiusz Augusiak[6] and Antonio Acín[1,8]

1 ICFO-Institut de Ciencies Fotoniques, The Barcelona Institute of Science and Technology, 08860 Castelldefels, Barcelona, Spain
2 Department for Quantum Technology, Universität Münster, Heisenbergstraße 11, 48149 Münster, Germany
3 Fakultät für Mathematik, Universität Wien, Oskar-Morgenstern-Platz 1, 1090 Vienna, Austria
4 Université libre de Bruxelles, QuIC, Brussels, Belgium
5 Aix-Marseille University, CNRS, LIS, Marseille, France
6 Center for Theoretical Physics, Polish Academy of Sciences, Aleja Lotnikow 32/46, 02-668 Warsaw, Poland
7 Department of Physics, School of Advanced Sciences, VIT-AP University, Amaravati 522241, Andhra Pradesh, India
8 ICREA, Passeig Lluis Companys 23, 08010 Barcelona, Spain

Closed timelike curves (CTCs) challenge our conception of causality by allowing information to loop back into its own past. Any consistent description of such scenarios must avoid time-travel paradoxes while respecting the no-new-physics principle, which requires that the set of operations available within any local spacetime region remain unchanged, irrespective of whether CTCs exist elsewhere. Within an information-theoretic framework, this leads to process functions: deterministic classical communication structures that remain logically consistent under arbitrary local operations, yet can exhibit correlations incompatible with any definite causal order - a phenomenon known as non-causality. In this work, we establish a correspondence between process functions and unambiguous complete product bases, i.e. product bases in which every local state belongs to a unique local basis. This equivalence implies that non-causality of process functions is exactly mirrored by quantum nonlocality without entanglement (QNLWE) - the impossibility of perfectly distinguishing separable states using local operations and causal classical communication - for such bases. Our results generalize previous special cases to arbitrary local dimensions and any number of parties, enable systematic constructions of non-causal process functions and unambiguous QNLWE bases, and implies, inter alia, that bipartite unambiguous QNLWE bases do not exist. Finally, this work reveals an unexpected connection between causal and non-signaling inequalities: every process function both maximally violates an associated causal inequality and yields a corresponding Bell inequality that admits no violation.

Paper: arXiv:2512.23599

NECESSITY OF FINE-TUNING IN CLASSICAL CAUSAL MODELS REPRODUCING KCBS INEQUALITY VIOLATIONS

Reyhan Durucu Hamzaoğulları[1]

[1]Sabancı University, İstanbul, Türkiye

Quantum contextuality demonstrates that the predictions of quantum mechanics cannot, in general, be reproduced by noncontextual hidden-variable models. From the perspective of classical causal modelling, this raises a further question: whether contextual quantum correlations can be explained by introducing additional causal relations while preserving the principle of no fine-tuning. This thesis investigates this question in the Klyachko–Can–Binicioğlu–Shumovsky (KCBS) scenario, a state-dependent test of contextuality in a local spin-1 system. After reviewing Bell inequalities, contextuality, noncontextual ontological models, and the causal-model framework, the KCBS inequalities and their quantum violations are derived. The KCBS scenario is then formulated as a causal model in terms of two measurement settings and their corresponding outcomes. Five physically motivated extensions of this causal structure are examined to explain the quantum correlations: causal influence between the outcomes, cross-setting influence on an outcome, outcome-dependent selection of a measurement setting, hidden-variable influence of a measurement setting, and dependence of the hidden variable on a measurement setting. Although these additional causal relations can provide mechanisms for correlations beyond the noncontextual bound, their parameters are shown to be fine-tuned, violating faithfulness. Thus, this work demonstrates the general result that classical causal models reproducing Bell–Kochen–Specker inequality violations in no-disturbance phenomena cannot do so faithfully.

Bell nonlocality does not imply violation of nonlocal games

Ricardo Faleiro1, Flavien Hirsch1, Lucas Porto2 and Marco Túlio Quintino2

1-Instituto de Telecomunicações, Av. Rovisco Pais n1, Lisboa

2- Sorbonne Université, CNRS, LIP6, F-75005 Paris, France

Nonlocal games provide a clear operational language to talk about Bell inequalities, framed as win-or-lose games mediated by an impartial Referee [1]. However, we show that without allowing for probabilistic-predicate games, this language is inadequate for detecting all possible nonlocal quantum behaviors. In a fixed Bell scenario, let L be the local polytope and Q the quantum set [2]. Furthermore, define G to be the set of nonsignaling behaviours that provide no advantage over the optimal classical strategy in any deterministic-predicate nonlocal game. We prove that G is a polytope, where each of its facets admits a game representation, strictly containing L. We then exhibit quantum-violated facets of the local polytope that admit no such representation. It follows geometrically that $Q \cap (G \setminus L)$ is nonempty. In words, there are Bell nonlocal quantum behaviours that give no advantage in any deterministic-predicate, in a fixed scenario. Thus, the existence of such points proves the inequivalence between proper Bell inequalities and nonlocal games as witnesses for nonlocality. This inequivalence occurs already in (4,4,2,2) and, through lifting-stable facets, in every bipartite scenario (X, Y, A, B) with X, Y ≥ 2 and A, B ≥ 4.

[1] - R. Cleve et al, Consequences and limits of nonlocal strategies, Proceedings of the 19th IEEE Annual Conference on Computational Complexity, Amherst, (IEEE, Piscataway, 2004), pp. 236–249.

[2]- Brunner, N. et al., Rev. Mod. Phys. 86, 419--478 (2014).

Deterministic randomness extraction for quantum random number generation with partial trust

Pablo Tikas Pueyo[1,2], Tomás Fernández Martos[1,3], and Gabriel Senno[1,3]
[1] *Quside Technologies S.L., 08860 Castelldefels, Barcelona, Spain*
[2] *Universitat de Barcelona, 08028 Barcelona, Spain*
[3] *ICFO-Institut de Ciències Fotòniques, 08860 Castelldefels, Barcelona, Spain*

The basic structure of a quantum random number generator consists of two main building blocks: an *entropy source* and a *randomness extractor*. The entropy source produces raw bit strings containing some amount of private randomness, usually quantified by the conditional min-entropy [1]. The randomness extractor then converts the raw string into a shorter one that is ε-close to perfectly random, i.e., uniform and independent of any eavesdropper's side information.

It is widely known that no deterministic procedure can extract randomness from the class of all entropy sources with a given min-entropy lower bound, instead requiring a seed or the combination of several weak sources [2]. Santha and Vazirani famously showed that this impossibility persists even for a restricted but natural class of sources with arbitrarily high min-entropy [3]. In a remarkable result [4], the first quantum random number generation protocol with deterministic extraction was constructed. Focusing on a device-independent (DI) setting, the authors prove that the violation of a Bell inequality can replace a min-entropy lower bound as the extractor's promise.

In this work, we extend the framework from [4] to multiple prepare-and-measure settings with *partial trust*, either in the state generation or in the measurement. In our main result, we show that the role played by a Bell functional in the DI construction can be played by a solution to the dual of the guessing probability in any of these partial trust settings. This generalization is of relevance since most current commercial devices operate in a device-dependent setting, with the technology slowly shifting towards semi-DI protocols, while fully DI randomness expansion has not yet proven to be practical beyond laboratory settings [5-7].

In the finite-size regime, we observe that positive key rates can be achieved with multi-bit extraction for as low as 7×10^3 rounds. Furthermore, in the asymptotic limit of infinitely many rounds, we find that successful extraction can be achieved using the single-bit XOR extractor from arbitrarily close to deterministic behaviors and a vanishing fraction of estimating rounds.

References

[1] R. König et al., IEEE Trans. Inf. Theory **55**, 4337 (2009).
[2] R. Arnon-Friedman et al., in TQC 2016, LIPIcs Vol. 61, pp. 2:1–2:34 (2016).
[3] M. Santha et al., in 25th Symp. Found. Comput. Sci., pp. 434–440 (1984).
[4] C. Foreman et al., Quantum **9**, 1654 (2025).
[5] L. K. Shalm et al., Nature Physics **17**, 452 (2021).
[6] W.-Z. Liu et al., Nature Physics **17**, 448 (2021).
[7] A. Kulikov et al., Nature **653**, 1033-1038 (2026).

Communication-based operational principles bounding nonlocal correlations

Lucas Pollyceno[1], Denis Moraes[2,3], José Nogueira[3], Anubhav Chaturvedi[4], Rafael Rabelo[3] and Marcin Pawłowski[1]

[1] International Centre for Theory of Quantum Technologies, University of Gdańsk, 80-308 Gdańsk, Poland
[2] Department for Quantum Technology, Universität Münster, Heisenbergstraße 11, 48149 Münster, Germany
[3] Instituto de Física Gleb Wataghin, Universidade Estadual de Campinas, 13083-859, Campinas, Brazil
[4] Division of Quantum Optics and Information, Institute of Theoretical Physics and Astrophysics, Faculty of Mathematics, Physics and Informatics, University of Gdańsk, 80-308 Gdańsk, Poland

The principle of *nonsignaling* (NS) is insufficient to single out the set of quantum correlations in Bell scenarios [1]. Further communication-based principles, such as *information causality* (IC) [2], exclude part of nonsignaling correlations beyond quantum theory. These principles, however, rely on arbitrary classical protocols to transform Bell correlations into behaviors of specific communication tasks. In this work, we extend the communication-based approach by introducing the framework of *general communication (GC) scenarios* [3]. We systematically identify novel classes of communication tasks exhibiting quantum-NS separations not captured by existing IC formulations, and overcome protocol-dependance by considering correlation sets directly embedded in the communication scenario. By adapting the geometric information-theoretic framework [4] to GC scenarios, we derive operational constraints that rule out stronger-than-quantum performances missed by previous formulations.

References

[1] Popescu, S. and Rohrlich, D., *Found Phys* **24**, 379–385 (1994).
[2] Pawłowski, M., Paterek, T., Kaszlikowski, D., Scarani, V., Winter, A. and Żukowski, M., *Nature* **461**, 1101–1104 (2009).
[3] Pollyceno, L., Moraes, D., Nogueira, J., Chaturvedi, A., Rabelo, R. and Pawłowski, M., arXiv:2603.08610 [quant-ph] (2026).
[4] Chaves, R., Majenz, C. and Gross, D., *Nat Commun* **6**, 5766 (2015).

Strong Inequivalence of Quantum Nonlocal Resources

S. B. Ghosh[1], S. Roy Chowdhury[2], G. Kar[2], A. Roy[3], T. Guha[4] and M. Banik[1]

[1]S. N. Bose National Centre for Basic Sciences, Kolkata, India
[2]Indian Statistical Institute, Kolkata, , India
[3]Hooghly Mohsin College, Chinsurah, India
[4]Mathematical Institute, Slovak Academy of Sciences, Bratislava, Slovakia

In this work[1] we present instances of quantum nonlocal correlations that are incomparable in the strongest sense. Specifically, when starting with an arbitrary many copies of one nonlocal correlation, it becomes impossible to obtain even a single copy of the other correlation, and this incomparability holds in both directions. Such incomparable quantum correlations can be obtained even in the simplest Bell scenario, which involves two parties, each having two dichotomic measurements setups. Notably, there exist an uncountable number of such incomparable correlations. Our result challenges the notion of a 'unique gold coin', often referred to as the 'maximally resourceful state', within the framework of the resource theory of quantum nonlocality. To this end, we provide examples of isotropic quantum correlations that cannot be distilled up-to Tsirelson point,and thus partially answer a long standing open question in nonlocality distillation.

References

[1] S. B. Ghosh et al., *Phys. Rev. Lett.* **132**, 250205 (2024).

Optimal Unlocking of Encoding Strength: Assistance from Environment

S. R. Chowdhury 1, S. Saha 2, S. B. Ghosh 3, R. Adhikary 4 and Tamal Guha 5
1 *Indian Statistical Institute, Kolkata, India*
2 *Institute of Mathematical Sciences, Chennai, India*
3 *S. N. Bose National Center for Basic Sciences, Kolkata, India*
4 *National Cheng Kung University, Tainan, Taiwan*
5 *Slovak Academy of Sciences, Bratislava, Slovakia*

Noise in quantum transmission lines typically prevents a quantum channel from achieving its maximal classical information encoding strength, i.e., the full dimension of its input system. While auxiliary resources such as pre-shared correlations or environmental access can mitigate noise, standard communication models fail to capture their full operational potential. Here, we introduce the notion of *unlocking encoding strength*, providing a framework that extends beyond the conventional characterization of classical communication through quantum channels [1]. In particular, we investigate how limited access to the environment can unlock otherwise inaccessible encoding strength and reveal operational features that remain hidden within standard paradigms. Remarkably, channels known to exhibit a strict gap between their conventional environment-assisted classical capacity and optimal communication strength [2,3] can nevertheless achieve full optimality under the proposed framework. Moreover, minimal assistance from the environment strictly outperforms the assistance provided by sharing the strongest 2-2-2 nonlocal boxes. These results demonstrate that encoding strength captures a broader operational potential of quantum channels and offers a unified perspective on how auxiliary resources unlock their information-processing capabilities.

References

[1] S. R. Chowdhury *et. al.* *arXiv 2509.09340 [quant-ph]*

[2] J. Watrous, *Phys. Rev. Lett., 95, 080505*

[3] R. Duan *et. al.*, *IEEE Trans. Info. Theo., 55, 1320*

Consistent Dynamics in Phase Space: Quantum States Require Quantum Time Evolution

JOEL D. HUBER, MATTHIAS KLEINMANN

Departement für Quantentechnologie, Universität Münster, Münster, Germany
Naturwissenschaftlich-Technische Fakultät, Universität Siegen, Siegen, Germany

Within the Hilbert space formulation of quantum mechanics, reversible dynamics is described by unitary time evolution. We investigate whether and how reversible quantum dynamics can be modified while still yielding a consistent theory. For this, we use a phase-space formulation of quantum mechanics, in which time evolution is governed by the Moyal bracket. To study deviations from quantum dynamics, we consider time evolutions that allow for linear phase-space transformations, which essentially enable phase-space state tomography. This can also be regarded as equipping generalized probabilistic theories (GPTs) with an additional phase-space structure that introduces a notion of dynamics. We find that dynamics in phase space is strongly operationally constrained, and that knowledge of just a few states of a theory can be used to make statements about its time evolution. Notably, the mere existence of the first excited state of the harmonic oscillator necessitates quantum time evolution. We demonstrate this to leading order in $\hbar^2$ by showing that time evolution in a cubic potential results in negative probabilities of observable quantities if it differs from quantum dynamics. This motivates high-precision Wigner tomography of mechanical systems to substantiate our finding in experiments.

Maximum Entropy Principle for Quantum Channels

Kartik Kakade[1], Fereshte Shahbeigi[1], Mário Ziman[1]

1 Slovak Academy of Sciences, Dubravska cesta 9, 845 11 Bratislava, Slovakia

Many quantum information tasks rely on characterizing quantum devices from incomplete operational data, motivating inference methods that remain as unbiased as possible while respecting the available observations. This is the goal of the maximum entropy (MaxEnt) principle developed by Jaynes [1], justified by the information-theoretic uniqueness of the Shannon entropy [2, 3] and later extended to quantum state estimation [4, 5]. Extending MaxEnt to quantum *processes*, however, is not straightforward: unlike states, quantum channels lack an intrinsic notion of entropy.

Here we study a channel entropy defined via the Choi–Jamiołkowski isomorphism, taking the von Neumann entropy of the associated Choi state as the channel's entropy [6, 7]. We then ask: given partial knowledge of a channel, expressed as expectation values from projective measurements on input and output states, which channel has maximal entropy consistent with these observations? This is the process-level analogue of the least-biased state in tomography; our approach differs from the recently proposed microcanonical formulation of channel entropy [8].

We report three preliminary results for qubit channels. First, for input and output states aligned along a common axis, the maximum-entropy channel consistent with a single input–output pair has a diagonal Choi matrix, and we derive the algebraic condition on the channel parameters characterizing this optimum. Second, for arbitrary states on the Bloch sphere, the maximum-entropy channel follows by rotating input and output to a common axis, applying this extremal channel, and rotating back, giving a closed-form expression for its Bloch-vector action. Third, entropy increases as the input approaches the pure state on a fixed line segment mapped to a given output, and, dually, as the output approaches the maximally mixed state for a fixed input. Together, these results show that the maximum-entropy channels compatible with partial input–output data are precisely those whose image on the Bloch ball collapses onto a line segment.

These results give an information-theoretic notion of channel entropy and a MaxEnt inference procedure for quantum processes, identifying the least-committal device description compatible with limited data, and point toward a systematic MaxEnt theory of channels beyond the qubit case.

References

[1] E. T. Jaynes, *Probability Theory: The Logic of Science* (Cambridge University Press, 2003).

[2] C. E. Shannon, Bell Syst. Tech. J. **27**, 379–423, 623–656 (1948).

[3] E. T. Jaynes, in *Statistical Physics*, ed. K. Ford (Benjamin, New York, 1963), p. 181.

[4] R. Blankenbecler and M. H. Partovi, Phys. Rev. Lett. **54**, 373 (1985).

[5] V. Bužek, G. Drobný, G. Adam, R. Derka, and P. L. Knight, J. Mod. Opt. **44**, 2607 (1997).

[6] K. Życzkowski and I. Bengtsson, Open Syst. Inf. Dyn. **11**, 3–42 (2004).

[7] W. Roga, M. Fannes, and K. Życzkowski, J. Phys. A **41**, 035305 (2008).

[8] P. Faist and S. Khatri, "Maximum channel entropy principle and microcanonical channels," arXiv:2508.03994 (2025).

Polynomial optimization of the parallel repetition of classical nonlocal games

Robin Krebs,* Lucas Vieira,* Nikolai Miklin,† and Mariami Gachechiladze*

Motivation Bipartite XOR games are a crucial tool in device-independent quantum applications such as Bell nonlocality and quantum cryptography. In these settings, it is particularly attractive that the quantum value of XOR games is determined by a simple SDP corresponding to the lowest level of the NPA hierarchy, which immediately allows constructing optimal quantum strategies, which can be self-tested. In these games, a verifier poses questions $x, y \in \mathcal{X} \times \mathcal{Y}$ drawn from a probability distribution $p(x, y)$ to two parties, Alice and Bob, respectively. The players proceed to output one bit each, $a(x)$ and $b(y)$, which they proceed to send to the verifier. The verifier compares the value $a \oplus b$ to a pre-agreed winning condition $f(x, y)$, deciding if the game is won.

While the quantum value can be computed efficiently here, no such simplification occurs in the classical case, which is NP-hard [1] to compute for general XOR games, with few analytical methods. This disparity is explained by the fact that every quantum XOR game can be associated to a non-commutative sum-of-squares (SOS) polynomial. In the analogue classical case, we are forced to rely on SOS hierarchies, applicable to any polynomial optimization problem. We discuss the simplification of mapping XOR games to bilinear polynomials $\sum_{xy} B_{xy} s_x t_y$ on the hypercube defined by the equations $s_x^2 = 1$ $(\forall x)$, $t_y^2 = 1$ $(\forall y)$. We analyze the SOS decomposition of an XOR game by considering its SOS matrix as equivalent to an enlarged symmetric XOR game, which satisfies a simple geometric condition from [2]. This condition ensures that no quantum advantage exists in the enlarged game. Reintroducing communication constraints to the larger game simplifies it to the original game. Additionally, we discuss methods of splitting the set of questions into subsets, which can be jointly played optimally, permitting further simplification of problems.

We discuss a possible connection between these observations and the values of games under parallel repetition. Furthermore, we present group-theoretical methods for XOR games of the form $B = B_0^{\otimes n}$, simultaneously utilizing symmetries of a single copy, and the overall permutation symmetry between copies, discussed here on the example of the CHSH game. We hope to discuss whether similar methods are either known or useful in other areas of the wide field of device independent quantum theory:

---

[1] J. Håstad. *JACM*, 48(4):798–859, 2001.

[2] R. Ramanathan et.al. *PRL*, 113(24):240401, 2014.

---

* Department of Computer Science, Technical University of Darmstadt, Germany

† Department of Physics, Technical University of Darmstadt, Germany

Quantum Key Distribution over Complex Networks

L. Mariani[1,2,3], R. Yehia[3], C. Pascual-García[3], F. Centrone[3,4], J. van der Kolk[5,6,7], M. Á. Serrano[5,6,8], A. Acín[3,8]

[1] ICAR-CNR, Institute for High Performance Computing and Networking, via Pietro Bucci, Rende, Italy
[2] Department of Physics "E. R. Caianiello", University of Salerno, via Giovanni Paolo II 132, Fisciano, Italy
[3] ICFO – Institut de Ciències Fotòniques, The Barcelona Institute of Science and Technology, Castelldefels, Spain
[4] Instituto de Física de Buenos Aires (IFIBA), Universidad de Buenos Aires, Ciudad Universitaria, 1428 Buenos Aires, Argentina
[5] Universitat de Barcelona Institute of Complex Systems (UBICS), E-08028 Barcelona, Spain
[6] Department of Condensed Matter Physics, Universitat de Barcelona, Martí i Franquès 1, E-08028 Barcelona, Spain
[7] Department of Network and Data Science, Central European University, Vienna 1100, Austria
[8] ICREA – Institució Catalana de Recerca i Estudis Avançats, 08010 Barcelona, Spain

There exist several initiatives worldwide to deploy quantum key distribution (QKD) over existing fibre networks and achieve quantum-safe security at large scales. To understand the overall QKD network performance, it is required to transition from the analysis of individual links, as done so far, to the characterization of the network as a whole. In this work, we undertake this study by embedding QKD protocols on complex networks, which correctly model the existing fibre networks. We focus on networks with trusted nodes and on continuous-variable (CV) schemes, which have much higher key rates than their discrete-variable (DV) counterparts. In the effective CV network, however, many of the unique properties of complex networks, such as small-worldness and the presence of hubs, are lost due to the fast decay of the key rate with physical distance for CV systems. These properties can be restored when considering a hybrid network consisting of both CV and DV protocols, achieving at the same time high average rate and inter-connectivity. Our work opens the path to the study of QKD complex networks in existing infrastructures [1].

References

[1] L. Mariani, R. Yehia, C. Pascual-García, F. Centrone, J. van der Kolk, M. Á. Serrano, and A. Acín, *Quantum Key Distribution over Complex Networks*, arXiv:2504.02372 (2025)

Universal method for optimized robustness in self-testing of quantum resources

S.-L. Chen[1,2,3] and N. Miklin[4]

[1] Department of Physics, National Chung Hsing University, Taichung, Taiwan
[2]Physics Division, National Center for Theoretical Sciences, Taipei, Taiwan
[3]Center for Quantum Frontiers of Research & Technology (QFort), National Cheng Kung University, Tainan, Taiwan
[4]Technische Universität Darmstadt, Darmstadt, Germany

Self-testing is a phenomenon where the use of specific quantum states or measurements can be inferred solely from the correlations they generate [1]. We introduce a universal method for conducting robustness analysis in the self-testing of various quantum resources. Unlike previous numerical approaches, which rely on selecting specific isometries, our method optimizes over equivalence transformations, thereby leading to tighter robustness bounds. This optimization employs the well-established technique of semidefinite programming relaxations for non-commuting polynomial optimization [2]. Our method can be universally applied to diverse self-testing settings, including steerable assemblages in the Bell scenario, constellations of quantum states in the prepare-and-measure scenario, and entangled states in the steering scenario. We demonstrate the method's capability to surpass previously reported robustness bounds across a range of concrete examples.

References

[1] I. Šupić, and J. Bowles, Quantum **4,** 337 (2020)

[2] S. Pironio, M. Navascués, and A. Antonio, SIAM Journal on Optimization **20.5**, 2157-2180 (2010)

Certifying randomness in a semi-device-independent scenario via Probability Estimation

Aurora Mugnai[1], Raffaele D'Avino[1], Gabriel Senno[2,1] and Antonio Acín[1,3]

[1]ICFO – Institut de Ciències Fotòniques, The Barcelona Institute of Science and Technology, Av. Carl Friedrich Gauss 3, 08860 Castelldefels (Barcelona), Spain [2]Quside Technologies S.L., C/Esteve Terradas 1, 08860 Castelldefels (Barcelona), Spain [3]ICREA – Institució Catalana de Recerca i Estudis Avançats, 08010 Barcelona, Spain

We study randomness certification in the semi-device-independent *overlap scenario* of [1], in which the measurement device is uncharacterised and untrusted, while the source is constrained only by a lower bound δ on the overlap (fidelity) between the states it may emit. In this setting, the Entropy Accumulation Theorem (EAT) was shown to certify positive smooth min-entropy only after approximately 7×10^4 rounds for a security parameter $\varepsilon = 10^{-10}$ [2].

We show that probability estimation (PE) [3] can substantially improve finite-size performance. By adapting recent polytope-approximation techniques [4], we construct computable outer approximations to the set of behaviours compatible with the overlap constraint, allowing the entropy generated over multiple rounds to be efficiently optimised and certified using PE. Our current PE analysis certifies positive smooth min-entropy after approximately 8×10^2 rounds at the same ε.

This certificate assumes classical side information, whereas the EAT result is secure against quantum side information, and we are therefore extending the construction to the quantum case following [5]. In the scenario studied in [6], the rates certified against quantum side information matched those obtained under the classical assumption, so that nothing was lost in passing to quantum adversaries. Should the same hold here, our construction would improve on the EAT threshold by nearly two orders of magnitude while retaining security against quantum side information.

References

[1] J. B. Brask, A. Martin, W. Esposito, R. Houlmann, J. Bowles, H. Zbinden and N. Brunner, Phys. Rev. Applied 7, 054018 (2017)

[2] B. Mir, T. Fernández Martos, M. Rudé, G. Senno and D. Tulli, Measurement-device-independent QRNG based on mode-competition in a gain-switched VCSEL, in preparation (2025)

[3] E. Knill, Y. Zhang and P. Bierhorst, Phys. Rev. Research 2, 033465 (2020)

[4] H. H. Jee, F. J. Curchod and M. L. Almeida, Quantum 10, 2019 (2026)

[5] Y. Zhang, H. Fu and E. Knill, Phys. Rev. Research 2, 013016 (2020)

[6] Y. Zhang, L. K. Shalm, J. C. Bienfang, M. J. Stevens, M. D. Mazurek, S. W. Nam, C. Abellán, W. Amaya, M. W. Mitchell, H. Fu, C. A. Miller, A. Mink and E. Knill, Phys. Rev. Lett. 124, 010505 (2020)

Genuine linear-optical test of quantum contextuality with sequential measurements

Jiaqi Liu[1], Bita Olamaei[2,3], Lijian Zhang[1], Ali Asadian[4], Saleh Rahimi-Keshari[5,6]

[1] *National Laboratory of Solid State Microstructures, Key Laboratory of Intelligent Optical Sensing and Manipulation, College of Engineering and Applied Sciences and School of Physics, Collaborative Innovation Center of Advanced Microstructures, Nanjing University, Nanjing, 210093, China*

[2] *Atominstitut, Technische Universität Wien, Stadionallee 2, 1020 Vienna, Austria*

[3] *Vienna Center for Quantum Science and Technology, Technische Universität Wien, 1020 Vienna, Austria*

[4] *Physics Department, Institute for Advanced Studies in Basic Sciences (IASBS), Gava Zang, P.O. Box 45137-66731, Zanjan, Iran*

[5] *School of Quantum Physics and Matter, Institute for Research in Fundamental Sciences (IPM), P.O. Box 19395-5531, Tehran, Iran*

[6] *Wallenberg Centre for Quantum Technology, Department of Microtechnology and Nanoscience, Chalmers University of Technology, SE-412 96 Gothenburg, Sweden*

Abstract

Quantum contextuality provides a fundamental signature of nonclassical behavior that cannot be explained by noncontextual hidden-variable models. We propose and experimentally implement a linear-optical setup for demonstrating Kochen–Specker contextuality via a violation of the KCBS inequality using single photons. Our scheme employs sequential measurements realized with linear-optical networks and on–off photodetectors. The construction ensures that each co-measured observable is implemented by the same physical operation across different contexts. Our experimental results demonstrate a clear violation of the KCBS inequality and robustness against photon loss. Beyond fundamental investigations, the proposed setup provides a practical tool for probing non-classicality and photon-number statistics of quantum states, which in turn enables the verification of single-photon sources.

[1] A. A. Klyachko, M. A. Can, S. Binicioğlu, and A. S. Shumovsky, Phys. Rev. Lett. 101, 020403 (2008).

[2] R. Lapkiewicz, P. Li, C. Schaeff, N. K. Langford, S. Ramelow, M. Wieśniak, and A. Zeilinger, Nature 474, 490 (2011).

[3] A. Cabello, Phys. Rev. A 93, 032102 (2016)

[4] A. Zhang, H. Xu, J. Xie, H. Zhang, B. J. Smith, M. S. Kim, and L. Zhang, Phys. Rev. Lett. 122, 080401 (2019).

CABIPARA.jl: A user-friendly Julia package for two-qubit steering and Bell nonlocality

Lucas E. A. Porto[1] , Sébastien Designolle[2], Marco Túlio Quintino[1]

[1]Sorbonne Université, CNRS, LIP6, Paris, France
[2] Inria, ENS de Lyon, UCBL, LIP, 69342, Lyon Cedex 07, France

Entanglement, steering, and Bell nonlocality are distinct forms of quantum correlations that underpin our current understanding of quantum theory. A central problem is to characterise and identify the quantum states capable of exhibiting these correlations, which is in general a very difficult task. Even for the simplest case of two qubits, while entanglement is easily characterised by partial transposition, deciding whether a given two-qubit state can manifest Bell nonlocality or steering is considerably more challenging. In this work, we gather, refine, and implement in a user-friendly way the current best computational methods that either certify the existence of local hidden-state (LHS) and local hidden-variable (LHV) models or demonstrate violations of steering and Bell inequalities for two-qubit states under projective measurements. Our code is freely available as a Julia package called CAPIBARA.jl. We apply these methods to estimate, with respect to the Hilbert-Schmidt measure, the relative volumes of two-qubit states that are unsteerable, one-way steerable, and Bell local, values we contrast with the volume of separable qubit pairs. Moreover, we obtain new LHV models for several classes of states, improving the bounds previously known in the literature.

References

[1] F. Hirsch *et al.*, Phys. Rev. Lett. 117, 190402 (2016)
[2] D. Cavalcanti *et al.,* Phys. Rev. Lett. 117, 190401 (2016)
[3] H. C. Nguyen *et al.*, Phys. Rev. Lett. 122, 240401 (2019)

PREDICTIVE AND RETRODICTIVE POWER OF OPERATIONAL THEORIES

TIM ACHENBACH, HANWOOL LEE, LEEVI LEPPÄJÄRVI, AND SAMGEETH PULIYIL

We study prepare-and-measure tasks from two perspectives: the forward picture, where the statistics are given by the output probabilities conditioned on the input probabilities; and the reverse picture, where the statistics are given by the input probabilities conditioned on the output probabilities. The forward picture is connected to the information storability of the setup, related to minimum error discrimination tasks and an indicator of the predictive power of a theory; while the reverse picture is connected to the total confidence of the setup, related to maximum confidence discrimination and an indicator of the retrodictive power of a theory. Although the predictive and retrodictive powers are equal in quantum and classical theories, we show that this is generally not the case. There exist theories in which the maximum total confidence is strictly greater than the information storability of the theory. We also show that the total confidence of a theory is bounded above by the linear dimension of the theory. Together with the bounds on information storability, this indicates that the reverse picture can outperform the forward picture depending on the theory one chooses to work with.

Email address, Tim Achenbach: `tim.n.achenbach@jyu.fi`

(Tim Achenbach) Faculty of Information Technology, University of Jyväskylä, 40100 Jyväskylä, Finland

Email address, Hanwool Lee: `hanwool.h.lee@jyu.fi`

(Hanwool Lee) Faculty of Information Technology, University of Jyväskylä, 40100 Jyväskylä, Finland

Email address, Leevi Leppäjärvi: `leevi.i.leppajarvi@jyu.fi`

(Leevi Leppäjärvi) Faculty of Information Technology, University of Jyväskylä, 40100 Jyväskylä, Finland

Email address, Samgeeth Puliyil: `samgeethmohanan@gmail.com`

(Samgeeth Puliyil) RCQI, Institute of Physics, Slovak Academy of Sciences, Dúbravská cesta 9, 84511 Bratislava, Slovakia

All pure entangled states can lead to fully nonlocal correlations

Martin J. Renner*

ICFO - Institut de Ciencies Fotoniques, The Barcelona Institute of Science and Technology, Castelldefels, Spain

Edwin Peter Lobo*

Laboratoire d'Information Quantique, Université libre de Bruxelles (ULB), Belgium

Arturo Konderak and Remigiusz Augusiak

Center for Theoretical Physics, Polish Academy of Science, al. Lotników 32/46, 02-668 Warsaw, Poland

Antonio Acín

ICFO - Institut de Ciencies Fotoniques, The Barcelona Institute of Science and Technology, Castelldefels, Spain and ICREA-Institucío Catalana de Recerca i Estudis Avancats, Llúıs Companys 23, 08010 Barcelona, Spain

It is a well-established fact that some quantum correlations are nonlocal, meaning they cannot be described by a local hidden variable model. Certain quantum correlations are so strong that they cannot be reproduced even if one allows only a small fraction of the rounds to admit a local hidden variable description. These correlations are called fully nonlocal and they lead to Bell inequalities in which the quantum bound saturates the non-signaling bound. A famous and well-known example is the Peres-Mermin square in which the underlying state is a four dimensional maximally entangled state. Surprisingly, examples of full nonlocality are so-far only known for maximally entangled states. In this work, we show that in every local Hilbert space dimension $d \geq 3$ there are non-maximally entangled states that are fully nonlocal. In fact, we derive simple criteria to ensure full nonlocality that are only based on the smallest and largest Schmidt coefficient. Furthermore, we show that all pure entangled states can be activated to show full nonlocality in the many-copy scenario.

arXiv:2604.26605

* These two authors contributed equally.

Robust certification of high-dimensional quantum devices

Javier Fernández,[1,2] Albert Rico,[1,3] Adam Vallès,[1,2] David Viedma,[1] Verònica Ahufinger,[1,2] Evelyn A. Ortega,[2] Valerio Pruneri,[2] Anna Sanpera,[1] and Some S. Bhattacharya[1]

[1)] *UAB - Autonomous University of Barcelona, Bellaterra, Spain*

[2)] *ICFO - Institute of Photonic Sciences, Castelldefels, Spain*

[3)] *USiegen - University of Siegen, Siegen, Germany*

(Dated: 10 September 2026)

Probing quantum behavior from classically accessible correlations is essential for secure communication and scalable quantum technologies. While powerful certification methods using nonlocal correlations, their experimental demonstrations remain largely confined to low-dimensional systems. Here we establish noise-tolerant quantum certification in high dimensions with minimal setups. We propose, design, and experimentally implement a protocol that certifies quantumness between two distant parties without the need of expensive resources like entanglement, nonlocality and even measurement incompatibility. The experiments are carried out using the orbital angular momentum degrees of freedom of single photons, chosen for providing increased dimensionality that is scalable. Our results provide a practical route to validating high-dimensional quantum communication systems and open new possibilities for secure and dimension-efficient quantum information processing.

Quantum mechanics enables correlations and information-processing capabilities that cannot be explained within a classical framework, forming the foundation of emerging quantum technologies such as secure communication, quantum simulation, and quantum computation[1–5]. A central challenge in quantum information science is therefore to identify and certify genuinely quantum behaviour using only classically accessible data, without relying on detailed assumptions about the underlying devices[6–8]. This task, known as *quantum certification*, exploits the fact that classical theories cannot reproduce the full range of correlations achievable in quantum systems. Prominent manifestations include Bell nonlocality[1,6], quantum steering[7,9], and contextuality[8,10], each revealing fundamental departures from classical hidden-variable descriptions. More recently, related approaches have explored quantum signatures encoded in correlations between state preparations and measurement outcomes, where incompatibility of quantum measurements provides an operational resource[11–15].

Certifying quantum properties is particularly important for establishing security in quantum communication protocols, which typically involve only three ingredients in the following structure: Alice encodes an input, transmits it to Bob, and Bob performs a decoding measurement without any external inputs[16–22]. This contrasts with more standard certification in other prepare-measure scenarios with additional structure, for example preshared entanglement or conditional measurement choices. In the absence of these resources, quantum behavior reduces to the ability to prepare and measure superposition states, making certification considerably more challenging.

However, existing quantum certification proposals for communication setups are largely confined to theoretical models and low-dimensional systems. *Here we overcome this current limitation by proposing a theoretical method, design its encoding into physical photons, and experimentally implement it successfully.* In turn, we establish a robust high-dimensional prepare-measurement protocol to certify the ability of remote parties to prepare and measure quantum superpositions. We use orbital angular momentum (OAM) degree of freedom of light, which offers access to a discrete and in principle unbounded Hilbert space, and demonstrate robust certification of quantum devices of dimension up to seven. The proposed protocol with OAM of single photons enables compact implementations of quantum communications protocols with increased channel capacity[23], security[24], and robustness to noise[25]. This proposal is particularly applicable to quantum communication setups with limited carrier system size, in free space links and few-mode optical fibers for future long-distance communication networks.

Table I. **Results: robust quantum certification.** We compare the Hilbert space dimension d_Q used in our protocol with the operational dimension d_C that would be needed in order to reproduce the correlations by classical preparations and measurements. We report robustness in the tolerance at the the certification bound $\sigma_{d_{\exp}}(P)$ and the next singular value $\sigma_{d_{\exp}+1}(P)$. Robustness is reported for dimensions $d_C = d_{\exp}$ where $\sigma_{d_{\exp}}(P) \leq \|E\|_2$.

n	d_Q	$d_{\exp}$	$\sigma_{d_{\exp}}(P)$	$\|E\|_2$	$\sigma_{d_{\exp}+1}(P)$
9	3	6	2.00×10^{-1}	$(6.57\pm0.29)\times10^{-2}$	9×10^{-17}
15	5	8	1.24×10^{-1}	$(5.87\pm0.13)\times10^{-2}$	4.00×10^{-2}
21	7	12	8.10×10^{-2}	$(6.41\pm0.12)\times10^{-2}$	2.00×10^{-2}
9	3	6	6.67×10^{-2}	$(2.21\pm0.09)\times10^{-2}$	2×10^{-17}
25	5	15	1.44×10^{-2}	$(1.22\pm0.02)\times10^{-2}$	2×10^{-17}
49	7	28	1.061×10^{-2}	$(1.045\pm0.007)\times10^{-2}$	2×10^{-17}

REFERENCES

[1] J. S. Bell, "On the Einstein Podolsky Rosen paradox," Physics Physique Fizika **1**, 195 (1964).

[2] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," Phys. Rev. Lett. **70**, 1895–1899 (1993).

[3] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," Theoretical computer science **560**, 7–11 (2014).

[4] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, "Concentrating partial entanglement by local operations," Physical Review A **53**, 2046 (1996).

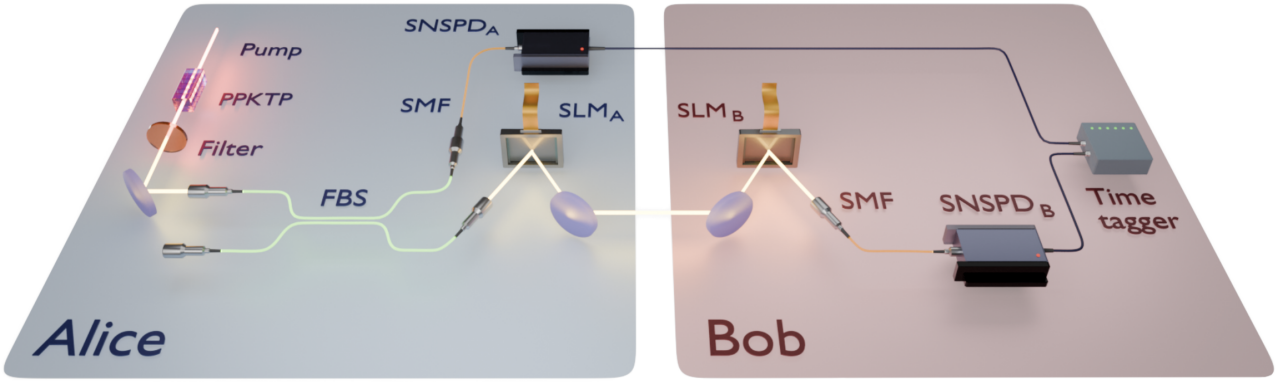


Fig. 1. **Simplified scheme of the experimental setup.** Alice encodes a message in the orbital angular momentum (OAM) of a photon prepared in the spatial light modulator (SLM$_A$). She sends this photon to Bob, who decodes it in his system (SLM$_B$) and detects it at the superconducting nanowire single-photon detector (SNSPD$_B$). Although the conceptual protocol occurs in these two devices, further components are needed for the experiment. We use a fiber beam splitter (FBS) to create two entangled photons. This entanglement is not used to certify quantumness, but we use it in the experiment to verify the callibration rounds via coincidence counting at the Time tagger.

[5] Y.-H. Kim, S. P. Kulik, and Y. Shih, "Quantum teleportation of a polarization state with a complete bell state measurement," Phys. Rev. Lett. **86**, 1370–1373 (2001).

[6] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, "Bell nonlocality," Reviews of modern physics **86**, 419–478 (2014).

[7] 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).

[8] S. Kochen and E. P. Specker, "The problem of hidden variables in quantum mechanics," in *Ernst Specker Selecta* (Springer, 2011) pp. 235–263.

[9] R. Uola, A. C. S. Costa, H. C. Nguyen, and O. Gühne, "Quantum steering," Rev. Mod. Phys. **92**, 015001 (2020).

[10] C. Budroni, A. Cabello, O. Gühne, M. Kleinmann, and J.-A. Larsson, "Kochen-specker contextuality," Rev. Mod. Phys. **94**, 045007 (2022).

[11] R. Gallego, N. Brunner, C. Hadley, and A. Acín, "Device-independent tests of classical and quantum dimensions," Phys. Rev. Lett. **105**, 230501 (2010).

[12] M. Pawłowski and N. Brunner, "Semi-device-independent security of one-way quantum key distribution," Phys. Rev. A **84**, 010302 (2011).

[13] A. Tavakoli, M. Smania, T. Vértesi, N. Brunner, and M. Bourennane, "Self-testing nonprojective quantum measurements in prepare-and-measure experiments," Science Advances **6**, eaaw6664 (2020).

[14] S. Puliyil, L. Leppäjärvi, and M. Ziman, "Semi-device-independent channel identification with communication matrices," (2025), arXiv:2511.14273 [quant-ph].

[15] S. Halder and A. Streltsov, "Quantum advantage in a unified scenario and secure detection of resources," Phys. Rev. A **111**, 022446 (2025).

[16] Z. Ma, M. Rambach, K. Goswami, S. S. Bhattacharya, M. Banik, and J. Romero, "Randomness-free test of nonclassicality: A proof of concept," Phys. Rev. Lett. **131**, 130201 (2023).

[17] T. Heinosaari, O. Kerppo, L. Leppäjärvi, and M. Plávala, "Simple information-processing tasks with unbounded quantum advantage," Phys. Rev. A **109**, 032627 (2024).

[18] C. Ding, E. P. Lobo, M. Alimuddin, X.-Y. Xu, S. Zhang, M. Banik, W.-S. Bao, and H.-L. Huang, "Quantum advantage: a single qubit's experimental edge in classical data storage," Physical Review Letters **133**, 200201 (2024).

[19] A. Diebra, S. Llorens, E. Bagan, G. Sentís, and R. Muñoz-Tapia, "Quantum state exclusion for group-generated ensembles of pure states," Physical Review Research **8**, L012001 (2026).

[20] T. Heinosaari and O. Kerppo, "Maximal Elements of Quantum Communication," Quantum **8**, 1515 (2024).

[21] A. Chakraborty, S. Gopalkrishna Naik, E. P. Lobo, R. K. Patra, S. Sen, M. Alimuddin, A. Mukherjee, and M. Banik, "Unlocking the advantage of qubit communication in multi-node network configurations," New Journal of Physics **27**, 023027 (2025).

[22] B. Doolittle, F. Leditzky, and E. Chitambar, "An operational framework for nonclassicality in quantum communication networks," (2025), arXiv:2403.02988 [quant-ph].

[23] J. T. Barreiro, T.-C. Wei, and P. G. Kwiat, "Beating the channel capacity limit for linear photonic superdense coding," Nature physics **4**, 282–286 (2008).

[24] F. Bouchard, R. Fickler, R. W. Boyd, and E. Karimi, "High-dimensional quantum cloning and applications to quantum hacking," Science advances **3**, e1601915 (2017).

[25] S. Ecker, F. Bouchard, L. Bulla, F. Brandt, O. Kohout, F. Steinlechner, R. Fickler, M. Malik, Y. Guryanova, R. Ursin, *et al.*, "Overcoming noise in entanglement distribution," Physical Review X **9**, 041042 (2019).

Communication complexity games and Continuous variable Bell inequalities

Abhyoudai S. Shaleena [1], Chithra Raj[1], Michał Studziński[1], Paweł Horodecki[1,2].

[1]International Centre for Theory of Quantum Technologies (ICTQT), University of Gdańsk,
[2]Faculty of Applied Physics and Mathematics, Gdańsk University of Technology, Gdańsk, Poland.

Beyond its foundational significance, Bell nonlocality is being harnessed as a powerful resource for quantum information processing tasks, such as device-independent quantum key distribution, randomness certification, and self-testing of quantum devices, etc. Moreover, in the communication complexity scenario, quantum correlations can reduce the amount of classical communication required to solve distributed computational tasks. There have been works that have given insight into the relationship between Bell inequality violations and communication complexity advantages.

What could be the possible significance if we were to allow a continuous spectrum? In this work, we develop a framework that provides insight into continuous-variable Bell inequalities in terms of a corresponding communication-complexity task.

References

[1] Č. Brukner, M. Żukowski, J-W. Pan, A. Zeilinger, Bell's Inequalities and Quantum Communication Complexity. Phys. Rev. Lett. 92, 127901 (2004). https://doi.org/10.1103/PhysRevLett.92.127901.

[2] A. S. Shaleena, C. Raj, et al. (2026), work in progress.

Certifying measurement incompatibility under bounded classical communication

Oxana Shaya[1] and Ritu Dhaulakhandi[2]

[1]Institute for Information Processing (tnt/L3S), Leibniz Universität Hannover, Appelstraße 9A, 30167 Hannover, Germany
[2]Institute for Theoretical Physics, Universität Innsbruck, Technikerstraße 21A, 6020 Innsbruck, Austria

Can an experiment certify that an untrusted device carries out incompatible measurements? The standard routes need either a Bell test, which forbids communication, or a trusted Hilbert-space dimension. We propose a test whose only quantitative assumption is a cap on classical communication: a one-way message of at most k bits per round. The message may be public, and the devices may share arbitrary entanglement. A linear program turns the statistics into a new prior-free score, the exponentiated union maximal leakage, built on the maximal leakage of quantitative information flow [1]. Jointly measurable readouts score below 2^k. How large the score can be is a Tsirelson question: for a natural three-input witness the answer is exactly the chained Tsirelson bound [2]. We then outline a key-distribution primitive for an assumption class no existing framework covers, where both devices are untrusted and the eavesdropper hears every message, and prove that at the ideal point the eavesdropper is completely decoupled.

References

[1] I. Issa, A. B. Wagner and S. Kamath, IEEE Trans. Inf. Theory **66**, 1625 (2020) [2] S. Wehner, Phys. Rev. A **73**, 022110 (2006)

Maximum randomness and perfect key generation from a Genuine Nonlocal Bell Inequality

Ritesh K. Singh[1], Rajdeep Paul[1], Alok K. Pan[1]

[1] Indian Institue of Technology Hyderabad, Kandi, Sangareddy, Telangana, India

The secure generation and distribution of cryptographic keys is a foundational problem in cryptography. Quantum mechanics offers a solution through Device-Independent Quantum Key Distribution (DIQKD), which requires minimal assumptions about the underlying devices by relying on nonlocal correlations. While the maximal violation of Bell inequalities has been successfully utilized to generate secure keys in bipartite scenarios, extending this to multipartite systems remains challenging due to the complex landscape of possible multipartite correlations. The strongest nonlocality among these are correlations exhibiting genuine multipartite nonlocality. While key distribution based on genuinely nonlocal correlations has been demonstrated using Mermin-Ardehali-Belinskii-Klyshko (MABK) Bell functionals, certifying genuineness with these functionals is typically restricted to scenarios with an even number of parties. In this work, we propose an n-partite Bell functional where correlations achieving the maximal quantum violation are genuinely nonlocal and yield a perfect key for any arbitrary number of parties. Furthermore, we demonstrate that achieving the maximal quantum value of this proposed functional self-tests the n-qubit GHZ state along with the appropriate observables acting on local two-dimensional Hilbert spaces. We establish this self-testing result by explicitly constructing a SWAP isometry.

On the relationship between quantum adiabatic evolution and quantum signal processing

Shawn Skelton
Institut für Theoretische Physik, Leibniz Universität Hannover, Hannover, Germany

Quantum signal processing (QSP) is a template for designing algorithms in the quantum circuit model, becoming increasingly popular in recent years. It is well-known that the circuit model of quantum computation can be related to adiabatic quantum computing with polynomial resource overhead.

Quantum adiabatic computing is inspired by the quantum adiabatic theorem (QAT), which gives conditions for when the physical time evolution of some Hamiltonian $H(s)$ is close to the evolution of some eigenstate, up to a geometric phase. When it holds, then we can approximate the physical evolution with an adiabatically evolved state, $|\psi_{adia}(s)\rangle$.

In QSP circuits, a ”black-box” oracle and a set of rotation gate parameters (”phase-factors”) fully determines the circuits, in QAT the evolution is determined by a choice of scheduler and delay time. We consider cases where a specific formal connection can be made between the adiabatic scheduler of a QAT evolution and a QSP circuit.

Specifically, we show that in the high-degree and small-signal limit, when the chosen adiabatic schedule is Lipschitz continuous, the quantum adiabatic evolution of a scheduler eigenstate is close to a QSP circuit applied to the same eigenstate. Crucially, our formalism establishes is a direct functional relationship between the adiabatic schedule and the set of phase factors that determine the QSP circuit.

Our work can provide intuition for QSP, which is more accessible to physics researchers outside of quantum algorithms than the QSP formalism. The adiabatic scheduler we have proposed is itself quite amenable to analysis; it has an eigenspectrum that naturally encodes two-dimensional subspaces for each eigenvalue of the oracle. This behavior is also the key feature that allows QSP to succeed.

No-local-broadcasting theorem for non-signalling behaviours and assemblages

Adrian Solymos[1,2], Carlos Vieira[3], Cristhiano Duarte[4,5,6,7], Zoltán Zimborás[1,8]

[1]HUN-REN Wigner Research Centre for Physics, Budapest, Hungary; [2]Eötvös Loránd University, Budapest, Hungary; [3]Universidade Estadual de Campinas, Campinas, Brazil; [4]Chapman University, Orange, USA; [5]Universidade Federal da Bahia, Ondina, Brazil; [6]Fundação Maurício Grabois, São Paulo, Brazil; [7]Universidade Federal de Juiz de Fora, Juiz de Fora, Brazil; [8]University of Helsinki, Helsinki, Finland

Abstract

The no-broadcasting theorem is a fundamental result in quantum information theory. It guarantees that a class of attacks on quantum protocols, based on eavesdropping and indiscriminate copying of quantum information, are impossible. Due to its fundamental importance, it is natural to ask whether it is an intrinsic quantum property or whether it also holds for a broader class of non-classical theories. To address this question, one could use the framework of correlation scenarios. Under this standpoint, Joshi, Grudka, and Horodecki$^{\otimes 4}$ conjectured that one cannot locally broadcast nonlocal behaviours [1]. In this poster, we present the result of our article [2], which proves their conjecture based on the monotonicity of the relative entropy for behaviours. Additionally, following a similar reasoning, we obtain an analogous no-go theorem for steerable assemblages.

References

[1] Pankaj Joshi, Andrzej Grudka, Karol Horodecki, Michal Horodecki, Pawel Horodecki, and Ryszard Horodecki. No-broadcasting of non-signalling boxes via operations which transform local boxes into local ones. *Quantum Information and Computation*, 13(7-8):567–582, 2013.

[2] Adrian Solymos, Carlos Vieira, Cristhiano Duarte, and Zoltán Zimborás. No-local-broadcasting theorem for nonsignaling behaviors and assemblages. *Physical Review A*, 113(3):032209, Mar 2026.

Non-signaling assistance in prepare-and-measure scenarios with classical communication

José Nogueira[1], Carlos Vieira[2,3], Lucas E. A. Porto[3],
Lucas Pollyceno[4], Rafael Rabelo[1], Otfried Gühne[5]

[1]Instituto de Física Gleb Wataghin, Universidade Estadual de Campinas, CEP 13083-859 Campinas, Brazil
[2]Instituto de Matemática, Estatística e Computação Científica, Universidade Estadual de Campinas, CEP 13083-859 Campinas, Brazil
[3]Sorbonne Université, CNRS, LIP6, F-75005 Paris, France
[4]International Centre for Theory of Quantum Technologies, University of Gdańsk, 80-308 Gdańsk, Poland
[5]Naturwissenschaftlich-Technische Fakultät, Universität Siegen, Walter-Flex-Straße 3, 57068 Siegen, Germany

Prepare-and-measure scenarios provide a natural black-box framework for studying communication under minimal assumptions [1]. A sender encodes an input into a bounded message; a receiver selects a setting and produces an output. I will discuss classical communication assisted by arbitrary non-signaling (NS) correlations [2]. Non-adaptive receivers query the shared resource independently of the message and use it only in classical post-processing. Adaptive receivers can choose their query based on the message, enabling advantages [3].

We characterize both forms of assistance in arbitrary prepare-and-measure scenarios. Non-adaptive realizability reduces to classical realizability in each fixed-setting subscenario. Combined with Frenkel and Weiner's theorem [4], this implies that non-adaptive non-signaling assistance simulates qudit transmission using a classical dit of the same alphabet size, even with multiple receiver settings. Adaptive behaviours are exactly those satisfying a family of input-discrimination inequalities, connecting the problem to channel simulation.

Comparing the models, we identify all scenarios exhibiting an adaptive advantage and prove that any such advantage must already appear at a single receiver setting. Thus, unlike entanglement-assisted protocols [3], arbitrary non-signaling assistance yields no genuinely multi-setting adaptive advantages. These results distinguish consequences of non-signaling alone from restrictions specific to quantum resources.

References

[1] R. Gallego, N. Brunner, C. Hadley, and A. Acín, Phys. Rev. Lett. **105**, 230501 (2010).
[2] J. Nogueira, C. Vieira, L. E. A. Porto, L. Pollyceno, R. Rabelo, and O. Gühne, arXiv:2607.01193v1 (2026).
[3] J. Pauwels, S. Pironio, E. Z. Cruzeiro, and A. Tavakoli, Phys. Rev. Lett. **129**, 120504 (2022).
[4] P. E. Frenkel and M. Weiner, Commun. Math. Phys. **340**, 563–574 (2015).

Towards rigorous tests of Bell nonlocality with time-bin entanglement

Bell tests provide an experimental way to identify correlations that cannot be explained by local realistic theories. Given measurement choices (x, y) and outcomes (a, b), correlations $P(a, b|x, y)$ that violate a Bell inequality cannot be reproduced by a local hidden-variable model, provided that the assumptions underlying the test are satisfied. In practical experiments, however, apparent violations may arise when these assumptions are weakened by experimental *loopholes*. Closing such loopholes is therefore essential for strengthening the validity of the Bell test.

Here we demonstrate a fiber-compatible platform for a Clauser–Horne–Shimony–Holt (CHSH) Bell test using time-bin entangled photons that simultaneously addresses the locality, freedom-of-choice, and postselection loopholes.

Time-bin encoding is particularly attractive for quantum networks because it is naturally compatible with optical fiber transmission and can be extended beyond two-dimensional encoding. Conventional time-bin measurements, however, generally use passive unbalanced interferometers. Only the temporally indistinguishable events are then retained, introducing a postselection loophole through which local hidden-variable models can reproduce correlations that would otherwise appear nonlocal [1]. We eliminate this temporal postselection by replacing the passive input beamsplitter of each receiver interferometer with a fast electro-optic switch. The switch deterministically routes the early and late time bins through complementary paths so that the interfering alternatives arrive in the same temporal mode. Independent quantum random-number generators determine Alice's and Bob's settings at 125 MHz.

The experiment is arranged such that the relevant measurement-setting and detection events at Alice and Bob satisfy the required spacelike-separation conditions. The two stations are separated by only 49.0 ± 0.7 m, demonstrating that the locality and freedom-of-choice constraints can be simultaneously satisfied within a compact architecture. All detected coincidences are included without temporal filtering, and we obtain

$$S = 2.583 \pm 0.002,$$

corresponding to a violation of the local-realistic CHSH bound $S \leq 2$ by more than 265 standard deviations. Tests of marginal statistics using the complete detection records are also consistent with the no-signalling conditions within statistical uncertainty.

Beyond its foundational relevance, the results provide a route toward more rigorous Bell experiments in fiber networks. Active, postselection-free time-bin measurements are compatible with high-speed operation and, unlike polarization encoding, can naturally be generalized to high-dimensional systems. Such systems offer an interesting platform for exploring how higher-dimensional state and measurement spaces, together with stronger experimental constraints, can improve the certification of nonclassical correlations and ultimately enable device-independent quantum information protocols.

Improving device-independent quantum key distribution protocols through multiple routed Bell tests

Sujan Vijayaraj[1], Mauro Paternostro[1,2]
1 Università degli Studi di Palermo, Dipartimento di Fisica e Chimica - Emilio Segrè, via Archirafi 36, 90123 Palermo, Italy 2 Centre for Quantum Materials and Technologies, School of Mathematics and Physics, Queen's University Belfast, BT7 1NN, United Kingdom

Device-independent quantum key distribution (DI-QKD) is known for being provably secure with a minimal set of assumptions. However, a practical demonstration of DI-QKD has remained elusive. First, long-range Bell tests, which have been crucial for most DI-QKD protocols, are very hard to implement. Otherwise, in current demonstrations using event-ready setups, quantum memories have remained difficult to implement [1]. Routed Bell tests with a distant Bell state measurement (BSM) unit (for entanglement swapping) was recently proposed as a promising alternative, and it was suggested that strong local Bell tests may be sufficient for security [2]. However, non-ideal violations come up with critical efficiency requirements at the long-range BSM. Overlooking this can lead to overestimation of the secret key rate. We propose a modified DI-QKD protocol based on multiple sources and measurement devices where, in each round, routed tests are performed on randomly selected local devices. The violation of local Bell tests is thereby checked even when a successful BSM projection is achieved. By requiring that such conditional tests remain consistent with the overall one, we achieve improvements in the long-range BSM critical efficiencies of about 4 - 12% for high visibilities. Our approach enables long-distance DI-QKD, with access to a highly efficient loophole-free routing setup, and multiple local tests (possibly imperfect) with very high local detection efficiencies. It importantly avoids the requirement for long-range Bell tests.

References

[1] V. Zapatero, T. van Leent, R. Arnon-Friedman, W. Z. Liu, Q. Zhang, H. Weinfurter, and M. Curty, Advances in device-independent quantum key distribution, npj Quantum Information 9, 10 (2023). [2] G. Koßmann, M. Berta, and R. Schwonnek, Routed Bell tests with arbitrarily many local parties, arXiv preprint arXiv:2510.08405 10.48550/arXiv.2510.08405 (2025).

Field Test of Entanglement Assisted Classical Communication

Kläre Wienecke[1], René Schwonnek[1], Christian Deppe[2] and Tara Cubel Liebisch[3]

[1] Institut für Theoretische Physik, Leibniz Universität Hannover, Germany

[2] Institut für Nachrichtentechnik, TU Braunschweig, Germany

[3] Physikalisch-Technische Bundesanstalt, Braunschweig, Germany

Recent theoretical studies [1–3] have demonstrated quantum advantage in entanglement-assisted classical multiple access channels (EA-MACs). Using non-local games, these approaches quantify the advantage in transmission rates when the senders share entanglement.

We present an ansatz relating EA-MAC protocols to Bell inequalities and discuss how an experimental implementation of the protocol in [1–3] requires a loophole-free Bell test. Since loophole-free Bell tests are experimentally challenging, we also investigate other EA-MAC protocols that are more feasible to implement. These protocols bypass the need for loophole-free Bell tests, making it possible to experimentally demonstrate a quantum advantage in EA-MACs.

Our aim is to bridge the gap between theoretical proposals and practical implementations, providing a pathway toward experimental demonstration of entanglement-assisted communication protocols.

References

[1] Uzi Pereg, Christian Deppe, and Holger Boche. “The Multiple-Access Channel with Entangled Transmitters”. In: *GLOBECOM 2023 - 2023 IEEE Global Communications Conference*. 2023, pp. 3173–3178.

[2] Janis Nötzel. “Entanglement-Enabled Communication”. In: *IEEE Journal on Selected Areas in Information Theory* 1.2 (2020), pp. 401–415.

[3] Felix Leditzky et al. “Playing games with multiple access channels”. In: *Nature Communications* 11.1 (2020), p. 1497.