arXiv:2402.12318v2 [quant-ph] 2 May 2025

Memory attacks in network nonlocality and self-testing

Mirjam Weilenmann,[1] Costantino Budroni,[2] and Miguel Navascués[3]

[1] *Inria, Télécom Paris - LTCI, Institut Polytechnique de Paris, 91120 Palaiseau, France*[*]
[2] *Department of Physics "E. Fermi" University of Pisa, Largo B. Pontecorvo 3, 56127 Pisa, Italy*[†]
[3] *Institute for Quantum Optics and Quantum Information–IQOQI Vienna, Austrian Academy of Sciences, Boltzmanngasse 3, 1090 Vienna, Austria*[‡]

We study what can or cannot be certified in communication scenarios where the assumption of independence and identical distribution (iid) between experimental rounds fails. In this respect, we prove that membership tests for non-convex sets of correlations cannot be formulated in the non-iid regime. Similarly, it is impossible to self-test non-extreme quantum operations, such as mixed states, or noisy quantum measurements, unless one allows more than a single use thereof within the same experimental round. One consequence of our results is that non-classicality in causal networks without inputs cannot be experimentally demonstrated. By analyzing optimal non-iid strategies in the triangle scenario, we raise the need to take into account the prior communication required to set up a causal network.

I. INTRODUCTION

Hypothesis testing plays an important role in experiments for certifying properties of quantum systems. Statistical tools based on martingale theory or prediction-based-ratio analysis have been successfully applied [1–4], especially in the context of Bell inequality violations [5–7], where it is common to work in an adversarial setting. These techniques allow us to formulate binary hypothesis tests that are secure against adversaries that introduce variations between the different rounds of a protocol. As a consequence, these tests are valid beyond the *independent and identically distributed* (iid) regime and take into account the possibility of *memory attacks* [8].

In this work, we study the consequences of dropping the iid assumption in two standard certification tasks: (a) proving that the experimental devices can generate measurement statistics outside of a given set of correlations or (b) close to a given distribution. The first task is the basis of non-classicality detection, understood as the certification of quantum (or at least non-classical) effects within the experimental setup. The second task is instrumental for self-testing [9, 10]: certifying that the generated statistics are close enough to a given distribution, it is sometimes possible to make claims about the inner workings of the devices involved in the experiment.

Regarding the first task, we conclude that membership tests for non-convex sets of correlations cannot be formulated in the non-iid regime. This implies that, for general causal networks, there are correlations for which one cannot certify incompatibility with the network. In particular, no causal network without inputs, such as the famous triangle scenario [11, 12], allows certifying non-classicality of the observed correlations. Another consequence is that, in general, one cannot certify that a multipartite source is distributing separable states, due to the non-convexity of the set of (highly) entangled states.

Regarding the second task, we prove that, in the non-iid regime, robust self-testing is only possible if the considered distribution is an extreme point of the set of physical correlations. Thus it is impossible to self-test mixed quantum states and non-extreme quantum measurements or instruments, independently of the communication scenario, unless one allows multiple identical preparations or uses thereof in a single experimental round. This means that the constructions presented in [13, 14] to self-test arbitrary quantum states and measurements cannot be extended to non-iid scenarios.

We conclude our paper by analysing non-iid strategies that separate players in a network might follow to win a membership test devised for the iid case. We observe that many such strategies, while formally compatible with the network configuration, would require violating the network's causal constraints to be set up. Hence we raise the need to discuss how prior communication might compromise the conclusions of a causal experiment.

II. THE INPUT/OUTPUT SCENARIO

We consider a scenario where the experimenters have access to a device with an input and an output port. In every experimental round, the experimenters feed a symbol $x \in \{1, ..., X\}$ into the input port and read a symbol $a \in \{1, ..., A\}$ on the output. Inputs and outputs might be composite, e.g. in a bipartite Bell experiment, the input is of the form (x, x') and the output, (a, a'). In some cases, the input may also be trivial, i.e., take only one possible value. This input/output framework thus encompasses Bell tests, prepare-and-measure scenarios, and causal network experiments.

In general, the probability of obtaining output a given input x in round k depends on both k and the past history of inputs and outputs. Invoking Bayes' rule, the most general statistical behavior of a device in an input/output

[*] mirjam.weilenmann@inria.fr
[†] costantino.budroni@unipi.it
[‡] miguel.navascues@oeaw.ac.at

experiment is given by the marginals

$$P_1(a_1|x_1), P_2(a_2|x_2, s_1), ..., P_n(a_n|x_n, s_{n-1}), \quad (1)$$

where $s_k = (a_1, x_1, ..., a_k, x_k)$ represents the list of inputs and outputs occurring prior to or in round k. We will also denote by $P^{(k)}$ the prior distribution of the inputs and outputs in the first k rounds. A special type of behavior arises when, in every round k, the probability of obtaining output a_k is solely dependent on k and the input x_k, i.e., when $P_k(a_k|x_k, s_{k-1}) = P_k(a_k|x_k)$, for $k = 1, ..., n$. We will then denote $P^{(n)}$ by $\bigotimes_{k=1}^{n} P_k$. If $P_k = P, \forall k$, we say that the device's behavior is iid. In that case, we write $P^{(n)} = P^{\otimes n}$.

If we posit some physical model S generating $P_k(a_k|x_k, s_{k-1})$, we might find that the corresponding set of correlations $\mathcal{S} = \{P(a|x) : P(a|x)$ compatible with $S\}$ does not exhaust the set of all possible probability distributions. In particular, we might find a constraint of the form

$$F(P) \leq \alpha, \forall P \in \mathcal{S}, \quad (2)$$

where F is a function of the distribution $P(a|x)$ and $\alpha \in \mathbb{R}$, which is violated for some $P \notin \mathcal{S}$. Examples of such constraints are Bell inequalities (when $\mathcal{S}$ is the set of local realistic correlations [15, 16]) or prepare-and-measure dimension witnesses (when the experimental outcomes are generated by conducting measurements labeled by y on a D-dimensional quantum system in state x [17]).

Now, suppose that we wish to refute the (null) hypothesis that model S describes the device's behavior. Within the input/output framework, this is equivalent to proving that the device can generate a distribution $P \notin \mathcal{S}$. The most general way to proceed is by defining a binary hypothesis test.

Definition 1. ***Binary Hypothesis Test.*** *An n-round binary hypothesis test is a prescription to decide what symbol x_k to input into the device in each experimental round k, as well as how to decide on the final outcome of the test:* 0 *(signifying that the test aiming to reject the null hypothesis failed) or* 1 *(meaning that the null hypothesis is rejected).*

According to this definition, the most general statistical test T for an input/output device is defined in terms of the marginal distributions $Q_1(x_1), Q_2(x_2|s_1), ..., Q_n(x_n|s_{n-1})$, which generate the next input based on the past history of inputs and outputs, and the distribution $Q_f(o|s_n)$, with $o \in \{0, 1\}$, used to generate the final, binary outcome of the test. Given the n-round behavior $P^{(n)}$ of the experimental device, the probability to declare the null hypothesis falsified is thus

$$P_T(o = 1|P^{(n)}) := \sum_{s_n} P^{(n)}(s_n) Q_1(x_1) Q_2(x_2|s_1) ... \\ Q_n(x_n|s_{n-1}) Q_f(1|s_n). \quad (3)$$

To see that Eq. (3) captures the most general hypothesis test, note that the above does not only apply to hypothesis tests where the total number of rounds n is fixed *a priori*, but also to hypothesis tests where the total number of rounds dynamically depends on the sequence of outputs of the experimental device. Such variable-n protocols are indeed included in the formulation above, as long as they have a maximum number N of rounds (this is a realistic assumption, since there is no such thing as an infinitely long experiment). In that case, the protocol would be defined through marginals $Q_1, ..., Q_N$ and the condition of variable n can be modeled by making the outcome distribution $Q_f(o|s_N)$ to be of the form $Q_f(o|s_N) = Q_f(o|s_n)$, for some lists of inputs/outputs s_n. Namely, the device would still be probed after the n^{th} round, but the subsequent results would not be taken into account. Alternatively, one can define a new input $x = \emptyset$, signifying that the device is not to be measured in that round, and set the marginals $Q_1, ..., Q_n$ defining the test so that, if the data s_k collected so far contains any input labeled $\emptyset$, then the output of Q_k must be $\emptyset$ with certainty.

Suppose, then, that we wish to prove that our device can produce distributions $P(a|x)$ such that $F(P) > \alpha$, with F being a continuous function. Equivalently, we wish to refute the hypothesis that, in every round, the device generates a distribution P_k satisfying $F(P_k) \leq \alpha$.

In the iid scenario, all we need to do is input different values of $x_1, ..., x_n$ and note the outcomes $a_1, ..., a_n$. Then, we can approximate the probabilities $P(a|x)$ by the observed frequencies, i.e.,

$$\tilde{P}(a|x) := \frac{|\{a_i = a, x_i = x\}|}{|\{x_i = x\}|}, \quad (4)$$

where $|\{a_i = a, x_i = x\}|$ is the number of times $x_i = x$ and $a_i = a$ is observed. Finally, we evaluate $F(\tilde{P})$, corresponding to the average value of F in our experiment, and its standard deviation σ. We then declare the null hypothesis rejected if the result is larger than $\alpha + K\sigma$ for some predetermined $K > 0$. In other words, to declare the null hypothesis rejected we require that the average is K standard deviations away from the bound.

The instructions above are in effect an n-round binary hypothesis test, with the property that, for large n, the outcome will be 0 with high probability if the device cannot generate distributions beyond $\mathcal{S}$. On the contrary, if the device does generate distributions outside of $\mathcal{S}$, then the test will output 1 with high probability.

In the iid scenario, it is similarly easy to carry out a *self-testing* experiment. Let $\| \bullet \|$ be an arbitrary norm and suppose that $P \in \mathcal{S}$ is such that, for all $Q \in \mathcal{S}$, the relation $\|P - Q\| < \varepsilon$ implies that the physical realization of Q within theory S requires the device to prepare states and/or conduct operations close to some reference ones. Then we say that P *robustly self-tests* those states and/or operations.

What happens, though, if we drop the iid assumption? As shown in [4], if F is linear on the probabilities P, then

one can design a family of hypothesis tests $(T^n)_n$ with the property that

$$\lim_{n\to\infty} P_{T^n}(1|P^{\otimes n}) = 1, \forall P \text{ s.t. } F(P(a|x)) > \alpha$$
$$P_{T^n}(1|P^{(n)}) \leq \varepsilon_n, \forall P^{(n)} \text{ s.t. } F(P_k(a|x,s_k)) \leq \alpha, \forall k, s_k, \tag{5}$$

for some $\{\epsilon_n\}_n \subset \mathbb{R}^+$ with $\lim_{n\to\infty} \epsilon_n = 0$ (in the statistics literature, ϵ_n is known as the *p value* of test T^n).

Building on this observation, for any convex set $\mathcal{S}$ of correlations the authors of [4] provide a hypothesis test to falsify the null hypothesis that $P_k(a_k|x_k, s_k) \in \mathcal{S}\ \forall k$.

There exist, however, interesting sets of correlations that are not convex. These sets appear, for instance, in the study of causal networks [12]. To partially characterize these sets, non-linear functions such as polynomials or linear combinations of entropies have been proposed [18–21]. As we saw, verifying that a system violates a non-linear constraint in the iid case is a trivial endeavor. But, how about the non-iid case? Can one extend the results of [4] to non-linear functions?

One can ask the same questions regarding self-testing. In [13], Miklin and Oszmaniec propose a scheme, relying on the iid assumption, to self-test arbitrary quantum states and Positive Operator Valued Measures (POVMs) in prepare-and-measure scenarios. In particular, they can self-test states and measurements giving rise to single-shot input/output distributions P that are not extreme in the set of 2-dimensional quantum realizations. Can this scheme be extended to the non-iid regime?

III. TESTING NON-CONVEX SETS

Let us consider a set of correlations $\mathcal{S}$. If the null hypothesis holds, namely, if $P_k(a|x, s_k) \in \mathcal{S}, \forall k, s_k$, then we wish our hypothesis test to output 1 with very low probability. At the same time, we wish the test to be meaningful, i.e., for some $P \notin \mathcal{S}$ we wish that the probability of detection of $P^{\otimes n}$ be close to 1. This defines the following problem.

Problem 1 (Membership Problem)**.** *Let $\mathcal{S}$ be a set of correlations. For $P \notin \mathcal{S}$, we aim to develop a family of hypothesis tests $(T^n)_n$, s.t.*

$$\lim_{n\to\infty} P_{T^n}(1|P^{\otimes n}) = 1. \tag{6}$$

In addition, for all $P^{(n)}$ with $P_k(a_k|x_k, s_k) \in \mathcal{S}, \forall k, s_k$,

$$P_{T^n}(1|P^{(n)}) \leq \varepsilon_n,$$
$$\lim_{n\to\infty} \varepsilon_n = 0. \tag{7}$$

Now, if $P \notin \text{conv}(\mathcal{S})$, where conv$(\cdot)$ denotes the convex hull, then we can use the results of [4] to devise a test to disprove the (stronger) null hypothesis $P_k \in \text{conv}(\mathcal{S}), \forall k, s_k$. The following proposition shows that it is *not* possible to devise a hypothesis test that rejects the null hypothesis and yet detects $P \notin \mathcal{S}$, $P \in \text{conv}(\mathcal{S})$.

Proposition 2. *There does not exist a solution to Problem 1 for $P \in \text{conv}(\mathcal{S}) \setminus \mathcal{S}$.*

Proof. By contradiction. Let $(T^n)_n$ be a family of hypothesis tests satisfying Eqs. (6) and (7). Since $P \in \text{conv}(\mathcal{S})$, we consider any decomposition of $P = \sum_i \lambda_i P_i$ as a convex combination of distributions $\{P_i\}_i \subset \mathcal{S}$. Then we have that

$$\begin{aligned} P_{T^n}(1|P^{\otimes n}) &= \sum_{i_1,\dots i_n} \lambda_{i_1} \cdots \lambda_{i_n} P(1|P_{i_1} \otimes \cdots \otimes P_{i_n}) \\ &\leq \varepsilon_n \sum_{i_1,\dots i_n} \lambda_{i_1} \cdots \lambda_{i_n} = \varepsilon_n, \end{aligned} \tag{8}$$

where we used first the linearity of P_{T^n} with respect to $P^{(n)}$, see Eq. (3), and then Eq. (7). It follows that, $\lim_{n\to\infty} P_{T^n}(1|P^{\otimes n}) = 0$, contradicting Eq. (6). □

Proposition 2 implies that the membership tests for non-convex sets currently used in experiments, e.g., non-convex probability or correlator inequalities for the analysis of quantum networks [22–26], are no longer sound when the iid assumption is not satisfied. In fact, for any set of correlations $\mathcal{S}$, it is only possible to certify that the device is capable of producing correlations outside conv$(\mathcal{S})$. In any communication scenario, the convexification of set $\mathcal{S}$ can be interpreted as having all the communicating parties share an arbitrary source of classical randomness. By this reasoning, causal networks without inputs, such as the triangle scenario [12], cannot exhibit any quantum advantage in the non-iid regime. Indeed, in any such network, a source of shared randomness allows all possible correlations to be achieved with classical resources.

Another consequence of Proposition 2 is that, in general, it is impossible to certify that a source of quantum states is distributing separable states. Indeed, let $\mathcal{E}$ denote the set of entangled states and consider the separable two-qubit state $\rho = \frac{1}{2}(|\psi^+\rangle\langle\psi^+| + |\psi^-\rangle\langle\psi^-|)$, with $|\psi^\pm\rangle := \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B \pm |1\rangle_A|0\rangle_B)$. Since $\rho \in \text{conv}(\mathcal{E})$, by Proposition 2 it is impossible to devise a test that outputs 0 with high probability when the source is generating highly entangled states and 1 when the source is distributing n independent copies of ρ.

IV. SELF TESTING WITHOUT IID

Let $\mathcal{S}$ be a set of physical correlations, and let $P \in \mathcal{S}$. Without relying on the iid assumption, under which circumstances can we guarantee that our device has prepared a distribution Q such that $\|P - Q\| < \delta$? More formally, we consider the following problem.

Problem 2. *Given $\delta' > 0$, a closed set $\mathcal{P}$ of correlations and $P \in \mathcal{P}$, we aim to devise a family of hypothesis tests $(T^n)_n$ such that, for some $\delta \in (0, \delta')$,*

$$\lim_{n\to\infty} P_{T^n}(1|Q^{\otimes n}) = 1, \tag{9}$$

for all $Q \in \mathcal{P}$ with $\|P - Q\| < \delta$. Moreover, there exists a sequence $(\epsilon_n)_n$ of real, non-negative numbers satisfying

$$\lim_{n\to\infty} \epsilon_n = 0, \tag{10}$$

such that

$$P_{T^n}(1|P^{(n)}) \leq \epsilon_n, \tag{11}$$

holds for all $P^{(n)}$ with marginals $\{P_k(a|x, s_k) : k, s_k\} \subset \mathcal{P}$ satisfying $\|P_k(a|x, s_k) - P\| > \delta'$, $\forall k, s_k$.

Not surprisingly, the answer of this problem depends on the relation between P and $\text{conv}(\mathcal{P})$.

Proposition 3. *Problem 2 can be solved for arbitrarily small $\delta' > 0$ iff P is an extreme point of conv$(\mathcal{P})$.*

Proof. First, we prove that the problem cannot be solved for all $\delta' > 0$ if P is not an extreme point of conv$(\mathcal{P})$. Suppose, instead, that such is the case. By Caratheodory's theorem, there exist $\{\lambda_i\}_{i=1}^m \subset \mathbb{R}^+$, and $\{P_i\}_{i=1}^m$, with $m \leq \|P\|_0 + 1$ such that

$$P = \sum_{i=1}^{m} \lambda_i P_i, \tag{12}$$

where $\|P\|_0$ denotes the number of non-zero probabilities of the behavior $P(a|x)$. Now, suppose that there exists a family of binary hypothesis tests $(T^n)_n$ satisfying Eqs. (9), (10) and (11) for $\delta' < \min_i \|P_i - P\|$ and arbitrary positive $\delta < \delta'$. Those tests comply with Eqs. (6), (7) for $\mathcal{S} := \{P_i\}_i$. Since $P \in \text{conv}(\mathcal{S}) \setminus \mathcal{S}$, their existence contradicts the statement of Proposition 2.

Assume, on the contrary, that P is an extreme point of conv$(\mathcal{P})$, and, for arbitrarily small $\delta' > 0$, define the closed set $\mathcal{A} := \{Q \in \text{conv}(\mathcal{P}) : \|Q - P\| \geq \delta'\}$. Since $P \notin \mathcal{A} \subset \text{conv}(\mathcal{P})$ and P is extremal in conv$(\mathcal{P})$, it follows that P does not belong to the closed set conv$(\mathcal{A})$. Therefore, by the Hahn-Banach theorem, there exist $\alpha \in \mathbb{R}$ and a separating linear functional c, which we can take to be normalized, such that $c(Q) \leq \alpha$, for all $Q \in \text{conv}(\mathcal{A})$ and $c(P) > \alpha$. Setting $0 < \delta < c(P) - \alpha$, we find that, for any $Q \in \mathcal{P}$ with $\|Q - P\| < \delta$, $c(Q) - \alpha \geq c(P) - \delta - \alpha > 0$. To summarize, the linear functional c satisfies $c(Q) \leq \alpha$, for all $Q \in \mathcal{P}$ with $\|Q - P\| \geq \delta'$ and $c(Q) > \alpha$, for all $Q \in \mathcal{P}$ with $\|Q - P\| < \delta$. Using the construction by [4], we can thus find a family of tests $(T^n)_n$ satisfying Eq. (5) and thus the conditions of the proposition. □

A corollary of this proposition is that, in the non-iid regime, one cannot devise an experiment to self-test any physical operation $\tilde{O}$ that is not extreme in the set of operations allowed by the experimental setup, unless two or more uses of $\tilde{O}$ are allowed at each experimental round.

Suppose, indeed, that we wished to certify that a given operation O of our device is $\tilde{O}$, and let us assume that only one use of O is allowed within an experimental round. By Bayes rule, this implies that, all other operations being fixed, the single-shot distribution $P(a|x, O)$ depends in a linear affine way on O.

Now, suppose that $\tilde{O} = \sum_i \lambda_i O_i$, where $\{O_i\}_i$ are extreme operations and the weights $\{\lambda_i\}_i \subset \mathbb{R}^+$ add up to 1. Define $P_i := P(a|x, O_i)$. Then, there is the possibility that $P_i = P$, for some i. In that case, one could not distinguish the non-extreme operation $\tilde{O}$ from the extreme O_i with the considered setup. That is, it would be impossible to self-test $\tilde{O}$. Alternatively, it could be that $P_i \neq P$, for all i, in which case $P = \sum_i \lambda_i P_i$ would not be extreme in the set of allowed behaviors. Thus, by the above proposition, one cannot certify that the device generated a distribution arbitrarily close to P in any experimental round, and so one cannot self-test $\tilde{O}$.

The impossibility of self-testing mixed states and non-extremal POVMs in Bell scenarios was already known [27]. Self-testing has, however, been studied in communication scenarios other than Bell's, such as causal networks, where protocols to self-test arbitrary quantum states and measurements exist [14]. In a similar vein, self-testing results for mixed states and non-extremal measurements can be found for prepare-and-measure scenarios [13], also under the iid assumption.

By our previous observation, though, any such protocol is vulnerable to memory attacks. A more positive consequence of Proposition 3 is that the work of [28] completely characterizes self-testing in the prepare-and-measure scenario (in the non-iid regime). There the authors provide a general protocol to self-test any ensemble of extreme (pure) quantum preparations and extreme POVMs. By Proposition 3, no other states and measurements can be self-tested.

What happens if we allow more than one use of O within a single experimental round? That would be a form of iid *within* rounds, rather than *between* rounds. It might be a good approximation in many experimental setups, though, if all the calls to O take place in a very short time span.

If we allow, say, up to two uses of O per round, then each of the probabilities of the single-shot behavior $P(a|x, O)$ will be a second-degree polynomial on the parameters defining O. Equivalently, it will be an affine linear expression on O and $O \otimes O$. Hence, the relevant set to consider is not the set $\mathcal{O}$ of all physical operations, but the set $\mathcal{O}^2 := \text{conv}\left(\{(O, O \otimes O) : O \in \mathcal{O}\}\right)$. While $\tilde{O} \in \mathcal{O}$ might not be an extreme point of $\mathcal{O}$, it is possible that $(\tilde{O}, \tilde{O}^{\otimes 2})$ is an extreme point of $\mathcal{O}^2$, in which case the no-go argument above does not apply.

Suppose, for instance, that $\mathcal{O}$ is the set $\mathcal{Q}_D$ of D-dimensional quantum states. Then, $\mathcal{O}^2$ would correspond to the set $\mathcal{Q}_D^2$ of pairs of matrices that can be expressed as convex combinations of pairs of the form $(\rho, \rho^{\otimes 2})$, where ρ is a quantum state. It turns out that, for *any* $\rho \in \mathcal{Q}_D$, $(\rho, \rho^{\otimes 2})$ is an exposed, extreme point of $\mathcal{Q}_D^2$. Indeed, consider the following $D^2 \times D^2$ matrix:

$$W_\rho = V + \text{tr}(\rho^2)\mathbb{I}_D^{\otimes 2} - 2\mathbb{I}_D \otimes \rho, \tag{13}$$

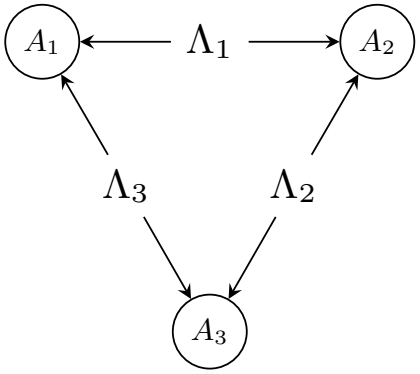


FIG. 1. Triangle network. Three parties, Alice, Bob and Charlie, make observations captured by random variables A_1, A_2, A_3 respectively. In the example in the main text these are binary, i.e., take values in $\{0, 1\}$. For this, each pair of parties shares a bipartite source of shared randomness, in terms of a random variable $\Lambda_1, \Lambda_2, \Lambda_3$ respectively (see diagram). In the quantum case these are replaced by quantum states, which increases the number of distributions $P(a_1, a_2, a_3)$ that can be generated.

where $V|j\rangle|k\rangle = |k\rangle|j\rangle$ denotes the permutation operator. This matrix gives rise to the linear functional $\mathcal{W}_\rho : \mathcal{Q}_D^2 \to \mathbb{R}$ through the relation $\mathcal{W}_\rho((\alpha, \beta)) := \mathrm{tr}\{W_\rho \beta\}$, for $(\alpha, \beta) \in \mathcal{Q}_D^2$. It can be verified that, for any $\sigma \in \mathcal{Q}_D$, $\mathcal{W}_\rho((\sigma, \sigma^{\otimes 2})) = \mathrm{tr}\{(\sigma - \rho)^2\}$. Thus, the linear optimization problem

$$\begin{aligned} &\min \mathcal{W}_\rho(q) \\ &\text{such that } q \in \mathcal{Q}_D^2 \end{aligned} \tag{14}$$

has $q = (\rho, \rho^{\otimes 2})$ as a unique solution, and so $(\rho, \rho^{\otimes 2})$ is an exposed point of $\mathcal{Q}_D^2$. This argument can be extended to any set $\mathcal{O}$ that can be embedded in a countable vector space and such that there exists a linear functional $\omega : \mathcal{O} \to \mathbb{R}$ with $\omega(O) = 1$, for all $O \in \mathcal{O}$. This includes the set of all D-dimensional POVMs/quantum channels/quantum instruments.

Hence, Proposition 3 does not preclude the possibility of self-testing, e.g., all D-dimensional POVMs when more than a single measurement is allowed within a given round. These ideas have been investigated by [29, 30]. Indeed, the sequential measurement protocol proposed in [29] does precisely that: it self-tests arbitrary (i.e., non-necessarily extreme) D-dimensional POVMs through a witness linear in the input/output distribution $P(a_1, a_2|x_1, x_2)$.

V. PRIOR COMMUNICATION IN CAUSAL NETWORK EXPERIMENTS

Consider the triangle causal network [11, 12], depicted in Figure 1. In the triangle scenario three separate agents locally generate random variables by combining three bipartite sources. Thus, a tri-variate distribution $P(a_1, a_2, a_3)$ is compatible with the triangle network if there exist distributions $p_1, p_2, p_3, q_1, q_2, q_3$ such that

$$\begin{aligned} P(a_1, a_2, a_3) = \sum_{\lambda_1, \lambda_2, \lambda_3} & p_1(\lambda_1) p_2(\lambda_2) p_3(\lambda_3) q_1(a_1|\lambda_1, \lambda_3) \\ & q_2(a_2|\lambda_1, \lambda_2) q_3(a_3|\lambda_2, \lambda_3). \end{aligned} \tag{15}$$

Call $\mathcal{S}$ the set of all single-site distributions satisfying the decomposition above. Remarkably, some tri-variate distributions cannot be arbitrarily well approximated by any distribution in $\mathcal{S}$. One of these is the distribution $P_c(0, 0, 0) = P_c(1, 1, 1) = \frac{1}{2}$, which violates a number of non-linear inequalities satisfied by all triangle-feasible distributions [11, 12, 19, 31, 32].

The reader might wonder what would happen if we ran a family of tests $(T^n)_n$, tailor-made to detect $P_c \in \mathcal{S}$ under the iid assumption, but otherwise allowed the three triangle-constrained players to use non-iid strategies. By Proposition 2, it follows that $(T^n)_n$ cannot satisfy Eq. (7). Thus, there must exist non-iid behaviors $P^{(n)} \in \mathcal{S}^{\otimes n}$ that allow the parties to pass T^n with non-negligible probability in the limit $n \to \infty$. But, what do these behaviors look like?

As it turns out, for any such family of tests there exist many feasible behaviors that asymptotically pass the test with probability tending to 1. Moreover, some of them do not depend on the specific single-shot witness function F employed to decide the outcome, see Eq. (2). One of these behaviors is the 'clock strategy' $P_{clock}^{(n)} := (P_0 \otimes P_1)^{\otimes n/2}$, with $P_b(a_1, a_2, a_3) := \delta_{b,a_1}\delta_{b,a_2}\delta_{b,a_3}$. For $n = 2m \geq 2$, the observed average frequencies $\tilde{P}(a_1, a_2, a_3)$, see (4), would satisfy $\tilde{P} = P_c$ exactly and so the three parties would pass the hypothesis test.

The clock strategy requires each player i to keep track of an internal variable $a_i \in \{0, 1\}$, which tells them what digit to output and gets updated at each round. In this case, the update rule is very simple: $a_i \to a_i \oplus 1$. The scheme demands the three players to have the same values of the variables (a_1, a_2, a_3) at round 1: should player 1 not be synchronized with the other two, the frequency average would change to $\tilde{P}(1, 0, 0) = \tilde{P}(0, 1, 1) = \frac{1}{2}$. This single-shot distribution is also unrealizable within the triangle network, but might not maximize functional F.

The reader might not think remarkable that three independent binary counters coincide. In fact, it is easy to find natural mechanisms to ensure this, e.g.: the memory system storing a_i might decay to state $a_i = 0$ in the absence of frequent updates. That all three players also independently come up with the same local update rule is less clear, but may still seem plausible. Consider, though, the following strategy $R^{(n)}$: let q be a n-bit random sequence, sampled from a uniform distribution. Then, at round k each party just needs to output q_k to generate $\tilde{P} \approx P_c$ with high probability. At the same time, with high probability no n-round test can distinguish this *deterministic* strategy from $P_c^{\otimes n}$.

The behavior $R^{(n)}$ is deterministic and thus compatible

with the triangle scenario. However, it does not seem *plausible* that three separate parties happen to come up with the same sequence q of numbers out of the blue, even though it is in principle possible. Coordinating strategies of this sort requires communication between the agents *before* the test starts.

To our knowledge, the role of prior communication in causal network experiments has not been discussed, except for comments on the role of *shared reference frames* in specific examples [33, 34]. This is most likely because this discussion is irrelevant both in the iid regime and in any causal network with a common source of randomness, such as a Bell test or the recent experimental disproofs of real quantum mechanics [35–38]. In non-iid scenarios without common classical sources, though, prior communication makes a difference. Depending on the goal of the subsequent test, it might be completely forbidden, but also partially or fully allowed, as long as it is accounted for. We next examine these three possibilities. In each case, we will take for granted that all the parties are informed of the test they are about to take. This premise is characteristic of cryptographic scenarios, where the protocol to be implemented is assumed to 'leak' to the public.

Unlimited prior communication, while harmless in the iid case, would in general allow separate parties to run strategies using unlimited amounts of shared randomness, such as $R^{(n)}$. In such a scenario, the set of feasible behaviors is indistinguishable from those generated by a network with a common randomness source.

Other scenarios might allow a limited amount of prior communication between the parties, before or after the test is leaked. In this regard, a minimal paradigm would allow some known, prior, bounded, test-independent knowledge common to all the parties involved in the communication game, e.g. all the parties speak English.

This paradigm would preclude the implementation of strategy $R^{(n)}$, for $n \gg 1$. It is, however, sufficient to run $P^{(n)}_{clock}$; in fact, it allows the players to pass any hypothesis test with maximum probability. In effect, all they need to do is follow this meta-strategy: once they receive the description of the game, each party (locally) computes all the optimal deterministic strategies to win it. Among those, they follow the first optimal strategy in lexicographic order (here we need to demand that the three players know the meta-strategy, and hence the notion of lexicographic order). This procedure guarantees that, no matter the test, the three parties will implement an optimal strategy, not only among all deterministic ones, but in general. This is so due to the following trivial identity:

$$\max_{P^{(n)}\in\mathbb{P}} P_T(1|P^{(n)}) = \max_{P^{(n)}\in\mathbb{P}_{det}} P_T(1|P^{(n)}), \tag{16}$$

where $\mathbb{P}$ ($\mathbb{P}_{det}$) denotes the set of all (deterministic) n-round behaviors. This meta-strategy can be straightforwardly generalized to any classical causal network without inputs.

Finally, a third experimental scenario would ban any form of communication between the parties prior to the test, other than the knowledge of the test itself. This prescription would rule out all multipartite quantum experiments conducted so far on causal networks without a common source of randomness, even under the iid assumption. Indeed, those experiments, which require all the parties to conduct appropriate quantum operations, are impossible to set up without contacting all the parties involved. Furthermore, experiments that involve independent sources generally also require a synchronisation of the sources in different rounds, which according to this viewpoint would also be considered part of the (forbidden) communication.

VI. CONCLUSIONS

In this paper, we have proven that basic primitives of quantum information theory cannot be implemented when one drops the iid assumption. More specifically, we showed that, in the non-iid regime, one cannot devise: (1) binary hypothesis tests to decide membership within a non-convex set and (2) self-tests of non-extreme operations (as long as we only allow the use of one operation per experimental round).

As a consequence of (1), currently used membership criteria for nonconvex sets, typically associated with causal network inequalities, do not satisfy the requirements of a general hypothesis test for the non-iid scenario. Moreover, the non-classicality of causal networks without inputs, such as the triangle network, cannot be certified. A consequence of (2) is that existing self-testing protocols for mixed density matrices and quantum measurements [13, 14] cannot resist memory attacks. On a more positive note, (2) also implies that the recent result by one of us [28] completely characterizes self-testing in prepare-and-measure scenarios.

While analyzing the form of optimal n-round strategies in network communication tests, we raised the need to account for prior communication between the parts of the experiment involved. As we saw, given unrestrained communication, the statistics generated by the parties are indistinguishable from those corresponding to a causal network with a common classical source node. In fact, just knowing the test to be conducted is enough for the players to 'simulate' the presence of such an extra node. On the other hand, banning prior communication altogether would not allow setting up most feasible iid strategies. Ultimately, deciding what is or not allowed is determined by the practical use we want to make of the network.

ACKNOWLEDGMENTS

This project was supported by the Swiss National Science Foundation (Ambizione PZ00P2_208779); by the QuantERA II Programme that has



received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No 101017733 and by the Austrian Science Fund (FWF) through project I-6004, project ZK 3, and project F 7113.

[1] R. D. Gill, Accardi contra Bell (cum mundi): the impossible coupling, IMS Lecture Notes-Monograph Series **42**, 133 (2003).

[2] R. D. Gill, Time, finite statistics, and bell's fifth position, in *Proceedings of Foundations of Probability and Physics - 2*, Ser. Math. Modelling in Phys., Engin., and Cogn. Sc., Vol. 5 (Växjö Univ. Press., 2003) p. 179–206, arXiv:quant-ph/0301059 [quant-ph].

[3] Y. Zhang, S. Glancy, and E. Knill, Asymptotically optimal data analysis for rejecting local realism, Phys. Rev. A **84**, 062118 (2011).

[4] Y. Zhang, S. Glancy, and E. Knill, Efficient quantification of experimental evidence against local realism, Phys. Rev. A **88**, 052119 (2013).

[5] M. Giustina, M. A. M. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner, J. Kofler, J.-A. Larsson, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, J. Beyer, T. Gerrits, A. E. Lita, L. K. Shalm, S. W. Nam, T. Scheidl, R. Ursin, B. Wittmann, and A. Zeilinger, Significant-loophole-free test of bell's theorem with entangled photons, Phys. Rev. Lett. **115**, 250401 (2015).

[6] L. K. Shalm, E. Meyer-Scott, B. G. Christensen, P. Bierhorst, M. A. Wayne, M. J. Stevens, T. Gerrits, S. Glancy, D. R. Hamel, M. S. Allman, K. J. Coakley, S. D. Dyer, C. Hodge, A. E. Lita, V. B. Verma, C. Lambrocco, E. Tortorici, A. L. Migdall, Y. Zhang, D. R. Kumor, W. H. Farr, F. Marsili, M. D. Shaw, J. A. Stern, C. Abellán, W. Amaya, V. Pruneri, T. Jennewein, M. W. Mitchell, P. G. Kwiat, J. C. Bienfang, R. P. Mirin, E. Knill, and S. W. Nam, Strong loophole-free test of local realism, Phys. Rev. Lett. **115**, 250402 (2015).

[7] S. Storz, J. Schär, A. Kulikov, and et al., Loophole-free bell inequality violation with superconducting circuits, Nature **617**, 265–270 (2023).

[8] J. Barrett, D. Collins, L. Hardy, A. Kent, and S. Popescu, Quantum nonlocality, bell inequalities, and the memory loophole, Phys. Rev. A **66**, 042111 (2002).

[9] B. Tsirelson, Some results and problems on quantum bell-type inequalities, Hadronic Journal Supplement **8**, 329 (1993).

[10] D. Mayers and A. Yao, Self testing quantum apparatus, Quantum Information & Computation **4**, 273 (2004).

[11] B. Steudel and N. Ay, Information-theoretic inference of common ancestors, Entropy **17**, 2304 (2015).

[12] T. Fritz, Beyond Bell's theorem: correlation scenarios, New Journal of Physics **14**, 103001 (2012).

[13] N. Miklin and M. Oszmaniec, A universal scheme for robust self-testing in the prepare-and-measure scenario, Quantum **5**, 424 (2021).

[14] S. Sarkar, A. C. Orthey, Jr., and R. Augusiak, A universal scheme to self-test any quantum state and measurement (2023), arXiv:2312.04405 [quant-ph].

[15] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Bell nonlocality, Reviews of Modern Physics **86**, 419 (2014), arXiv:1303.2849 [quant-ph].

[16] V. Scarani, *Bell Nonlocality*, Oxford Graduate Texts (Oxford University Press, 2019).

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

[18] R. Chaves, Polynomial bell inequalities, Phys. Rev. Lett. **116**, 010402 (2016).

[19] E. Wolfe, R. W. Spekkens, and T. Fritz, The Inflation Technique for Causal Inference with Latent Variables, Journal of Causal Inference 10.1515/jci-2017-0020 (2016).

[20] M. Weilenmann and R. Colbeck, Analysing causal structures with entropy, Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences **473**, 20170483 (2017).

[21] R. Chaves, C. Majenz, and D. Gross, Information-theoretic implications of quantum causal structures, Nature communications **6**, 5766 (2015).

[22] G. Carvacho, F. Andreoli, L. Santodonato, M. Bentivegna, R. Chaves, and F. Sciarrino, Experimental violation of local causality in a quantum network, Nature communications **8**, 14775 (2017).

[23] D. J. Saunders, A. J. Bennet, C. Branciard, and G. J. Pryde, Experimental demonstration of nonbilocal quantum correlations, Science Advances **3**, e1602743 (2017).

[24] Q.-C. Sun, Y.-F. Jiang, B. Bai, W. Zhang, H. Li, X. Jiang, J. Zhang, L. You, X. Chen, Z. Wang, *et al.*, Experimental demonstration of non-bilocality with truly independent sources and strict locality constraints, Nature Photonics **13**, 687 (2019).

[25] D. Poderini, I. Agresti, G. Marchese, E. Polino, T. Giordani, A. Suprano, M. Valeri, G. Milani, N. Spagnolo, G. Carvacho, *et al.*, Experimental violation of n-locality in a star quantum network, Nature communications **11**, 2467 (2020).

[26] E. Polino, D. Poderini, G. Rodari, I. Agresti, A. Suprano, G. Carvacho, E. Wolfe, A. Canabarro, G. Moreno, G. Milani, *et al.*, Experimental nonclassicality in a causal network without assuming freedom of choice, Nature Communications **14**, 909 (2023).

[27] P. Baptista, R. Chen, J. Kaniewski, D. R. Lolck, L. Mančinska, T. G. Nielsen, and S. Schmidt, A mathematical foundation for self-testing: Lifting common assumptions (2023), arXiv:2310.12662 [quant-ph].

[28] M. Navascués, K. F. Pál, T. Vértesi, and M. Araújo, Self-testing in prepare-and-measure scenarios and a robust version of wigner's theorem, Phys. Rev. Lett. **131**, 250802 (2023).

[29] D. Das, A. G. Maity, D. Saha, and A. S. Majumdar, Robust certification of arbitrary outcome quantum measurements from temporal correlations, Quantum **6**, 716 (2022).

[30] J. Nöller, N. Miklin, M. Kliesch, and M. Gachechiladze, Classical certification of quantum gates under the dimen-

sion assumption (2024), arXiv:2401.17006 [quant-ph].
[31] M. Weilenmann and R. Colbeck, Non-Shannon inequalities in the entropy vector approach to causal structures, Quantum **2**, 57 (2018).
[32] R. Chaves, L. Luft, and D. Gross, Causal structures from entropic information: geometry and novel scenarios, New Journal of Physics **16**, 043001 (2014).
[33] F. Andreoli, G. Carvacho, L. Santodonato, M. Bentivegna, R. Chaves, and F. Sciarrino, Experimental bilocality violation without shared reference frames, Phys. Rev. A **95**, 062315 (2017).
[34] A. Suprano, D. Poderini, E. Polino, I. Agresti, G. Carvacho, A. Canabarro, E. Wolfe, R. Chaves, and F. Sciarrino, Experimental genuine tripartite nonlocality in a quantum triangle network, PRX Quantum **3**, 030342 (2022).
[35] M.-O. Renou, D. Trillo, M. Weilenmann, T. P. Le, A. Tavakoli, N. Gisin, A. Acín, and M. Navascués, Quantum theory based on real numbers can be experimentally falsified, Nature **600**, 625–629 (2021).
[36] M.-C. Chen, C. Wang, F.-M. Liu, J.-W. Wang, C. Ying, Z.-X. Shang, Y. Wu, M. Gong, H. Deng, F.-T. Liang, Q. Zhang, C.-Z. Peng, X. Zhu, A. Cabello, C.-Y. Lu, and J.-W. Pan, Ruling out real-valued standard formalism of quantum theory, Phys. Rev. Lett. **128**, 040403 (2022).
[37] Z.-D. Li, Y.-L. Mao, M. Weilenmann, A. Tavakoli, H. Chen, L. Feng, S.-J. Yang, M.-O. Renou, D. Trillo, T. P. Le, N. Gisin, A. Acín, M. Navascués, Z. Wang, and J. Fan, Testing Real Quantum Theory in an Optical Quantum Network, Phys. Rev. Lett. **128**, 040402 (2022).
[38] D. Wu, Y.-F. Jiang, X.-M. Gu, L. Huang, B. Bai, Q.-C. Sun, X. Zhang, S.-Q. Gong, Y. Mao, H.-S. Zhong, M.-C. Chen, J. Zhang, Q. Zhang, C.-Y. Lu, and J.-W. Pan, Experimental Refutation of Real-Valued Quantum Mechanics under Strict Locality Conditions, Phys. Rev. Lett. **129**, 140401 (2022).