Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Almost-quantum correlations violate information causality

Anandamay Das Bhowmik

ananda.adb@gmail.com

S N Bose National Centre for Basic Sciences https://orcid.org/0000-0003-3306-3940

Manik Banik

S. N. Bose National Centre for Basic Sciences https://orcid.org/0000-0001-8036-790X

Article

Keywords:

Posted Date: November 11th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-11606954/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: There is **NO** Competing Interest.

Almost-quantum correlations violate information causality

Anandamay Das Bhowmik[1,†] and Manik Banik[1,*]

[1]S. N. Bose National Centre for Basic Sciences, Block JD, Sector III, Salt Lake, Kolkata 700106, India
[†]e-mail: ananda.adb@gmail.com [*]e-mail: manik11ju@gmail.com

Abstract

Information causality (IC), a generalization of the no-signalling principle, states that communicating m classical bits cannot give the receiver access to more than m bits of information about the sender's independent data. Although IC holds in quantum theory and excludes a broad class of supra-quantum correlations, its validity for the almost-quantum set has remained open. This semidefinite relaxation of the quantum set satisfies nontrivial communication complexity, no advantage for non-local computation, macroscopic locality, local orthogonality, and numerical evidence has suggested that it may also satisfy IC. Here we show that almost-quantum correlations violate IC, and do so without bound. Unlike earlier violations of IC, which rely on biased guesses, ours is driven by zero-error certificates: each is rare but never wrong, carries information linear in its probability, and vouches for many of the sender's bits at once. Our result establishes a sharp dichotomy: either IC is a valid physical principle that excludes these correlations, or any nonsignalling theory realizing them admits no mutual information obeying consistency, data processing and the chain rule. In the latter case, we discuss why the chain rule is the natural property to relinquish, and how this possibility relates to histories-based formulations and to locality defined relative to the state rather than presupposed in a fixed spacetime.

Introduction

Bell's theorem[1] marks one of the sharpest departures of quantum theory from classical physics[2–4]. Addressing the question raised by Einstein, Podolsky and Rosen of whether the quantum-mechanical description of physical reality is complete[5], Bell derived an inequality that the statistics of local measurements on separated systems must obey whenever they admit a local-causal explanation, and showed that quantum mechanics predicts its violation[1,6]. Such violations have since been observed in several milestone experiments[7–14]. Beyond its foundational significance, Bell nonlocality is a resource for device-independent information processing, in which conclusions are drawn from the observed statistics alone, without trusting the internal workings of the devices[4,15]. Examples include quantum key distribution based on Bell tests and its device-independent versions, randomness certification and amplification, self-testing of quantum states and measurements, and device-independent witnesses of entanglement and of Hilbert-space dimension, along with other applications[16–38].

Quantum nonlocality is nevertheless restricted compared with what relativistic causality alone would permit. For the Clauser–Horne–Shimony–Holt (CHSH) expression[6], local hidden-variable models reach at most 2 and quantum theory at most $2\sqrt{2}$, Tsirelson's bound[39], whereas nonsignalling Popescu–Rohrlich (PR) boxes[40,41] attain the algebraic maximum 4. Explaining this gap, and ideally singling out the set of quantum correlations from physical or information-theoretic principles, is a long-standing programme. Proposed principles include nontrivial communication complexity[42–44], no advantage for nonlocal computation[45], information causality (IC)[46], macroscopic locality[47] and local orthogonality[48]. Each excludes a large class of supra-quantum correlations, but none is known to single out the quantum set. IC generalizes the no-signalling principle,

which it contains as the case of zero communication: m bits of communication cannot give the receiver access to more than m bits of information about the sender's independent data. IC holds in quantum theory, recovers Tsirelson's bound[46] and part of the boundary of the quantum set[49], and has been developed in several directions[50–53].

Almost-quantum (AQ) correlations[54] are the most demanding test case for this programme. They form the "$1 + AB$" level of the Navascués–Pironio–Acín (NPA) hierarchy[55,56], a set that strictly contains the quantum set yet is characterized by a single semidefinite program. They also arise from strongly positive decoherence functionals in Sorkin's quantum measure theory[57] when later measurements may depend on earlier outcomes[58], and from a principle of macroscopic noncontextuality[59]. AQ correlations satisfy nontrivial communication complexity, no advantage for nonlocal computation, macroscopic locality and local orthogonality[54]. For IC the question has remained open. IC is violated by the first level of the NPA hierarchy, which contains the AQ set[60], whereas numerical evidence suggested that the AQ set satisfies it[54].

Here we show that AQ correlations violate IC, and do so without bound. A single use of one explicit AQ box and one classical bit suffice; Alice's data are independent fair bits, every run produces a guess, and nothing is postselected. The box provides certificates of equality: whatever the number N of settings, its outcomes certify with probability $1/17$ that both parties chose the same setting, and they never do so when the settings differ. Quantum boxes can certify equality in this way with probability at most $1/N$ (ref. 61). Such certificates are exactly what IC cannot tolerate: an answer that is rarely given but always correct carries information linear in its probability, and a single certificate can vouch for many of Alice's bits at once. The same box is studied in detail in a companion paper[61], which separates almost-quantum from commuting-operator correlations in the zero-error certification of equality and does not concern IC; the present work is self-contained in its main result.

Results

Information causality

The principle of IC concerns the information a receiver can access about a distant sender's data when shared nonsignalling correlations are supplemented by limited classical communication. It can be appreciated simply with the communication task of random access codes (RACs)[62–64]. Alice receives D independent, uniformly distributed bits $Z_1, \ldots, Z_D$, and Bob receives an index $r \in \{1, \ldots, D\}$. They share a nonsignalling resource that is independent of these inputs. Alice sends Bob an m-bit message, and Bob outputs a guess G_r of Z_r. IC requires[46]

$$\mathcal{I} \equiv \sum_{r=1}^{D} I(Z_r : G_r) \leq m, \tag{1}$$

where $I(Z_r : G_r)$ is the Shannon mutual information in runs in which Bob's index is r. The sum runs over alternative questions, not over bits that Bob learns simultaneously. Pawłowski *et al.*[46] derived Eq. (1) for any theory in which a mutual information $I(X : Y)$ can be defined for all pairs of systems with three properties: (i) *consistency*, it reduces to the Shannon mutual information when both systems are classical; (ii) *data processing*, local operations on either system cannot increase it; and (iii) the *chain rule*, $I(X : YW) = I(X : W) + I(X : Y|W)$. Data processing bounds each term of Eq. (1) by the information that the message M and Bob's share $\mathcal{B}$ of the resource carry about Z_r. The chain rule and the independence of the Z_r bound the sum of these terms by the single quantity $I(Z_1 \cdots Z_D : M\mathcal{B})$. Finally, because the resource is

Table 1 | The almost-quantum box $\boldsymbol{p}^\star(a,b|x,y)$. It depends only on whether the settings coincide, has marginals $p_A(0|x) = p_B(0|y) = 3/17$, and satisfies Eq. (2) with $s = 1/17$ for every number of settings.

	$p(0,0)$	$p(0,1)$	$p(1,0)$	$p(1,1)$
$x = y$	$1/17$	$2/17$	$2/17$	$12/17$
$x \neq y$	0	$3/17$	$3/17$	$11/17$

nonsignalling, $\mathcal{B}$ alone carries no information about Alice's data, and the m-bit classical message contributes at most m. The quantum mutual information has all three properties, so every protocol with quantum resources, including arbitrary shared entanglement, satisfies Eq. (1)[46]. A set of correlations violates IC if some protocol that uses correlations from the set violates Eq. (1). By the derivation above, no theory whose physical systems realize such correlations admits a mutual information with properties (i)–(iii).

Certificate boxes

A bipartite correlation experiment involves two spatially separated parties, Alice and Bob, each performing local measurements on their respective parts of a shared system. laboratories that share a source. In each round, Alice chooses a measurement setting $x \in \mathcal{X}$ and records an outcome $a \in \mathcal{A}$; Bob independently chooses $y \in \mathcal{Y}$ and records $b \in \mathcal{B}$. All four alphabets are finite. Repeating the experiment produces the *behaviour* (or *box*) $\boldsymbol{p} = \{p(a,b|x,y)\}$, with $p(a,b|x,y) \geq 0$ and $\sum_{a,b} p(a,b|x,y) = 1$. A correlation is called nonsignalling (NS) if local outcome statistics of each party does not depend on the measurement choice of the other party, i.e.

$$\sum_b p(a,b|x,y) = p(a|x) \qquad \text{and} \qquad \sum_a p(a,b|x,y) = p(b|y).$$

Consider a bipartite NS box $\boldsymbol{p}_s = \{p(a,b|x,y)\}$ with N settings per party, $x, y \in \{1,\ldots,N\} = [N]$, and binary outcomes $a, b \in \{0,1\}$, such that

$$p(0,0|x,y) = s\,\delta_{xy} \qquad \text{for some } s > 0. \tag{2}$$

The outcome pair $(0,0)$ then certifies with certainty that $x = y$, and it occurs with probability s whenever $x = y$; we call such a box a certificate box and s its certification rate. As shown in ref. 61, for commuting-operator correlations, and hence for all quantum correlations, a box with $N \geq 3$ settings and $p(0,0|x,y) = 0$ for $x \neq y$ obeys $\sum_x p(0,0|x,x) \leq 1$, so every quantum certificate box has $s \leq 1/N$. Shared randomness attains this value: the parties share a uniformly random label and each outputs 0 exactly when its setting equals that label. In contrast, the box $\boldsymbol{p}^\star$ of Table 1 satisfies Eq. (2) with $s = 1/17$ for every N, and it is almost quantum.

Definition 1 (Almost-quantum correlations[54])**.** A box $\boldsymbol{p}$ belongs to the AQ set $\mathrm{C_{AQ}}$ if there exist a Hilbert space $\mathcal{H}$, a unit vector $\psi \in \mathcal{H}$, and projective measurements $\{A_{a|x}\}_a$ and $\{B_{b|y}\}_b$ on $\mathcal{H}$ such that, for all a, b, x, y, $A_{a|x}B_{b|y}\psi = B_{b|y}A_{a|x}\psi$ and $p(a,b|x,y) = \langle \psi, A_{a|x}B_{b|y}\psi\rangle$.

Quantum correlations, in the commuting-operator framework, require $[A_{a|x}, B_{b|y}] = 0$ as an operator identity; the AQ set requires commutation only on the state ψ, and it strictly contains the quantum set[54]. That $\boldsymbol{p}^\star$ is almost quantum was shown in ref. 61; for completeness, the short proof is given in Methods (Lemma 1).

Random-access block certification

Pawłowski *et al.* used the RAC version of the IC game to show that PR boxes violate IC[46]. To show that the AQ box $\boldsymbol{p}^\star$ violates IC, we first formulate a zero-error certification task in the spirit of a RAC. In random-access block certification (RABC), Alice receives a uniformly random string $\boldsymbol{Z} \in \{0,1\}^{kN}$ (equivalently, kN independent fair bits), which we divide into N blocks of k bits, $\boldsymbol{Z} = (\boldsymbol{Z}_1, \ldots, \boldsymbol{Z}_N)$ with $\boldsymbol{Z}_i = (Z_{i,1}, \ldots, Z_{i,k}) \in \{0,1\}^k$ (Fig. 1a). Bob receives a block index $i \in [N]$, independent of $\boldsymbol{Z}$. Alice sends Bob one bit $M \in \{0,1\}$, which may depend on $\boldsymbol{Z}$ but not on i, and Bob either certifies that block i consists only of ones, $C_i = 1$, or gives no certificate, $C_i = 0$. A certificate must never be false:

$$\Pr\left(C_i = 1,\ \boldsymbol{Z}_i \neq 1^k\right) = 0 \qquad (i \in [N]), \tag{3}$$

where 1^k denotes the all-ones string of length k. The figure of merit is the total certification probability $\mathcal{W} = \sum_{i=1}^{N} \Pr(C_i = 1)$, where $\Pr(C_i = 1)$ refers to runs in which Bob's index is i. As in a RAC, Bob is asked about one part of Alice's string, but, unlike in a RAC, he does not guess a bit; instead, he certifies, without error, that the whole block $\boldsymbol{Z}_i$ equals 1^k, and he may always decline. Since $\Pr(\boldsymbol{Z}_i = 1^k) = 2^{-k}$, Eq. (3) gives $\Pr(C_i = 1) \leq 2^{-k}$, and hence $\mathcal{W} \leq N2^{-k}$ whatever the resources. With shared randomness alone, $\mathcal{W} \leq 2^{-k}$, and this value is attained if Alice reports whether a randomly chosen block equals 1^k (Lemma 2 in Methods).

Certificates obtained in the RABC game are valuable in the IC game for two reasons. A guess that is made with probability t but is never wrong carries at least t bits about the requested bit, that is, information linear in its probability. Moreover, a certificate for block i reveals every bit of that block, so it answers correctly whichever of the k bits $Z_{i,1}, \ldots, Z_{i,k}$ Bob is asked for. The following proposition makes both points precise.

Proposition 1. *Take any zero-error RABC protocol. In the IC game with $D = kN$ bits, $Z_r \equiv Z_{i,j}$ for $r = (i-1)\,k + j$, let Alice send the same message as in the RABC protocol, and let Bob, asked for $Z_{i,j}$, run the protocol with block index i and guess $G_{i,j} = C_i$. Then $\mathcal{I} \geq k\,\mathcal{W}$; consequently, IC with $m = 1$ implies $\mathcal{W} \leq 1/k$.*

Proof. Alice's message does not depend on Bob's index, so the construction is a valid protocol for the IC game. Fix a question (i, j) and let $t_i = \Pr(C_i = 1)$. By Eq. (3), a certificate requires $\boldsymbol{Z}_i = 1^k$, so $t_i \leq 2^{-k} \leq 1/2$.

Let Z be a fair bit and G a binary guess with $\Pr(G = 1, Z = 0) = 0$ and $\Pr(G = 1) = t \leq 1/2$. The joint distribution is then $\Pr(Z = 1, G = 1) = t$, $\Pr(Z = 1, G = 0) = 1/2 - t$ and $\Pr(Z = 0, G = 0) = 1/2$, yielding

$$I(Z : G) = h(t) - \tfrac{1}{2}h(2t) \ \geq\ t. \tag{4}$$

The inequality holds because $f(t) = h(t) - \frac{1}{2}h(2t) - t$ vanishes at $t = 0$ and has derivative $f'(t) = \log_2[(1-t)/(1-2t)] \geq 0$ for $0 \leq t < 1/2$. For small t the bound is nearly an equality: $h(t) - \frac{1}{2}h(2t) = t + t^2/(2\ln 2) + O(t^3)$, so the information carried by a certificate is linear in its probability. Since Bob's question is independent of Alice's data, $Z_{i,j}$ is a fair bit. By Eq. (3), the pair $(Z_{i,j}, G_{i,j}) = (Z_{i,j}, C_i)$ satisfies the assumptions above with $t = t_i$. Hence $I(Z_{i,j} : G_{i,j}) \geq t_i$. The guess $G_{i,j} = C_i$ does not depend on j, so each of the k questions about block i contributes at least t_i, and

$$\mathcal{I} = \sum_{i=1}^{N}\sum_{j=1}^{k} I(Z_{i,j} : G_{i,j}) \ \geq\ k\sum_{i=1}^{N} t_i = k\,\mathcal{W}.$$

If IC holds, then $\mathcal{I} \leq 1$, and hence $\mathcal{W} \leq 1/k$. □

Violation of information causality

The bound $\mathcal{W} \leq 1/k$ of Proposition 1 lies far above the classical value 2^{-k}. A certificate box nevertheless exceeds it with the following block-certification protocol (Fig. 1a). Alice finds the first block that consists only of ones, $L = \min\{\, i : \boldsymbol{Z}_i = 1^k \,\}$. If such a block exists, she inputs $x = L$ into the box, obtains a, and sends the one-bit message $M = a$. If no block consists only of ones, she sends $M = 1$ and does not use the box. Bob, asked about block i, inputs $y = i$ and obtains b. He certifies, $C_i = 1$, if $M = b = 0$, and gives no certificate otherwise. Alice's message thus depends only on her string and her outcome, and Bob's setting only on his index.

Theorem 1. *For a box obeying Eq. (2) and every integer $k \geq 1$, the block-certification protocol uses the box at most once and one bit of communication, never certifies falsely, and achieves*

$$\mathcal{W} = s\left[1 - (1 - 2^{-k})^N\right]. \tag{5}$$

Consequently, in the IC game with $D = kN$ data bits,

$$\mathcal{I} \;\geq\; k\, s\left[1 - (1 - 2^{-k})^N\right]. \tag{6}$$

Proof. Write $u = 2^{-k}$ for the probability that a given block equals 1^k. The blocks are independent, and the box is independent of Alice's string and of Bob's index. Bob certifies only if $M = 0$ and $b = 0$. Alice sends $M = 0$ only if some block equals 1^k, in which case she inputs $x = L$, and only if her outcome is $a = 0$. Bob, asked about block i, inputs $y = i$. By Eq. (2) the outcome pair $(a, b) = (0, 0)$ has probability zero unless $x = y$. Hence $C_i = 1$ implies $L = i$, so $\boldsymbol{Z}_i = 1^k$, and Eq. (3) holds.

The event $L = i$ occurs exactly when $\boldsymbol{Z}_{i'} \neq 1^k$ for all $i' < i$ and $\boldsymbol{Z}_i = 1^k$, so $\Pr(L = i) = (1-u)^{i-1}u$ for $i \in [N]$. If $L = i$, the box is used with settings $x = y = i$ and returns $(a, b) = (0, 0)$ with probability $p(0, 0|i, i) = s$. If $L \neq i$, Bob does not certify: either no block equals 1^k and $M = 1$, or $x = L \neq y = i$ and $(0, 0)$ is impossible. Therefore

$$t_i \equiv \Pr(C_i = 1) = s \Pr(L = i) = s\, u\, (1 - u)^{i-1}. \tag{7}$$

Summing Eq. (7) over the blocks, and using $u(1 - u)^{i-1} = (1 - u)^{i-1} - (1 - u)^i$, we obtain

$$\mathcal{W} = \sum_{i=1}^{N} t_i = s\left[1 - (1 - u)^N\right],$$

which is Eq. (5); here $1 - (1 - u)^N$ is the probability that at least one block equals 1^k. Since the protocol is a zero-error RABC protocol, Proposition 1 applies, with Bob guessing $G_{i,j} = C_i$ when asked for $Z_{i,j}$, and gives Eq. (6). □

Corollary 1 (Almost-quantum correlations violate IC)**.** *The AQ box $\boldsymbol{p}^\star$ violates IC without bound. (i) With $k = 18$ and $N = 757\,693$ settings, $\mathcal{I} \geq 1.00000018 > 1$. (ii) With $N = k2^k$, $\mathcal{I} \geq k(1 - e^{-k})/17$, which grows without bound.*

Proof. Part (i) is a direct evaluation of Eq. (6) with $s = 1/17$, using $D = 13\,638\,474$ data bits. For part (ii), write $u = 2^{-k}$. For $0 \leq u < 1$, $\ln(1 - u) \leq -u$. Hence $(1 - u)^N = e^{N \ln(1-u)} \leq e^{-Nu}$, and with $N = k2^k$, so that $Nu = k$, we obtain $(1 - 2^{-k})^{k2^k} \leq e^{-k}$. Equation (6) then gives $\mathcal{I} \geq (k/17)\,(1 - e^{-k})$. □

Figure 1b shows the bound (6), maximized over k, for the AQ box, for the level-1 boxes of the NPA hierarchy and at the quantum limit. Few observations are in order.

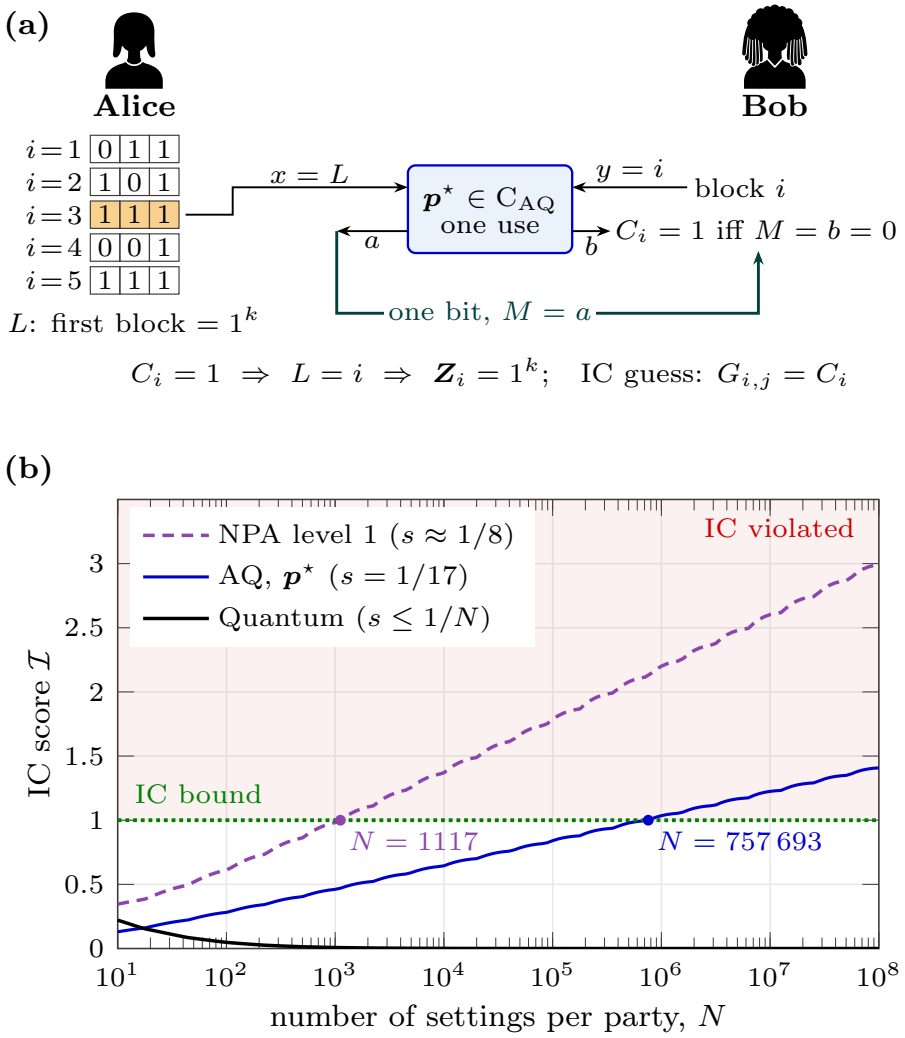


Fig. 1 | Violating information causality with a certificate box. a The block-certification protocol, drawn for $N = 5$ blocks of $k = 3$ bits. Alice inputs the index L of the first block equal to 1^k and sends her outcome as one bit. Bob, asked about block i, inputs $y = i$ and certifies it, $C_i = 1$, only if the message and his outcome both equal 0. By Eq. (2) this happens only if $L = i$, so a certificate is never false. In the IC game, Bob answers a question about any bit $Z_{i,j}$ of block i with $G_{i,j} = C_i$. **b** The bound (6), maximized over k, versus the number of settings per party N: for the AQ box $\boldsymbol{p}^\star$ ($s = 1/17$, solid), for the level-1 boxes of Lemma 3 (Methods) with $s = N/[8(N-2)]$ (dashed), and for the largest certification rate compatible with quantum theory, $s = 1/N$ (black). Dots mark the first violations of IC.

Quantum certificate boxes respect information causality. Quantum boxes never yield a violation in this protocol. A quantum certificate box has $s \leq 1/N$, and the union bound gives $1-(1-2^{-k})^N \leq N2^{-k}$, so the right-hand side of Eq. (6) is at most $k\,s\,N2^{-k} \leq k2^{-k}$. Since $k2^{-k}$ equals $1/2$ for $k = 1, 2$ and decreases thereafter, this bound never exceeds $1/2$, consistent with the validity of IC in quantum theory (Fig. 1b). A violation requires certification rates far above this limit. It needs $ks > 1$ together with $N \gtrsim 2^k$, the scale on which the bracket in Eq. (6) approaches one; hence $s \gtrsim 1/\log_2 N$, whereas quantum boxes have $s \leq 1/N$. Correspondingly, at the threshold of Corollary 1(i), $\boldsymbol{p}^\star$ gives $\sum_x p(0,0|x,x) = N/17 \approx 4.5 \times 10^4$, while every commuting-operator box with $p(0,0|x,y) = 0$ for $x \neq y$ obeys $\sum_x p(0,0|x,x) \leq 1$ (ref. 61).

Number of settings. The violation requires many settings. With $s = 1/17$, the bound (6) exceeds one only for $k \geq 18$, and hence only for $N \gtrsim 2^{18}$; the precise threshold is $N = 757\,693$ (Corollary 1). Such scenarios lie far beyond the reach of numerical searches, consistent with the earlier numerical evidence[54]. The protocol itself applies to every box obeying Eq. (2). The first level of the NPA hierarchy contains such boxes with $s = N/[8(N-2)] \to 1/8$ (ref. 61); with $k = 9$ they violate IC for every $N \geq 1117$ (Fig. 1b), an independent confirmation that this level violates IC[60].

Certainty versus bias. What makes certificates so effective? A binary guess of a fair bit that is correct with probability $(1+E)/2$ carries $1 - h\big((1+E)/2\big) = E^2/(2\ln 2) + O(E^4)$ bits, with $h(\cdot)$ the binary entropy. IC therefore constrains squared biases, as in the condition $E_1^2 + E_2^2 \leq 1$ derived from it[46,49]. A certificate behaves differently: by Eq. (4) in Methods, an answer given with probability t but never wrong carries at least t bits, linearly in t. In our protocol a certificate for block i occurs with probability $t_i \leq s2^{-k}$, but it vouches for all k bits of that block, and the $N \gtrsim 2^k$ blocks compensate for its rarity. The resulting score, $ks[1-(1-2^{-k})^N]$, approaches ks and exceeds one once $ks > 1$ and N is large enough. Quantum boxes cannot exploit this mechanism, because their certification rate is at most $1/N$, whereas the AQ box keeps $s = 1/17$ for every N.

Discussion

Our construction shows that almost-quantum correlations permit unbounded violations of information causality with one classical bit and a single use of a bipartite box. It thus provides explicit counterexamples to the compatibility of AQ correlations with IC suggested by numerical evidence[54]. Earlier obstructions to AQ correlations invoked Specker's principle in contextuality scenarios[65] and the no-restriction hypothesis for theories reproducing the AQ set[66]. Our violation depends only on the bipartite input–output probabilities and the classical operations specified in the protocol.

Since IC is a *proposed physical principle*, its violation does not by itself establish unphysicality. It nevertheless imposes a precise obstruction: no nonsignalling theory that realizes our family and permits the protocol can admit a mutual information with properties (i)–(iii). The violation alone does not identify which property fails. For the generalized mutual information of Wakakuwa and Murao, defined through optimal rates of classical communication over channels with general probabilistic outputs, consistency and data processing hold, and together with no-signalling the chain rule would imply IC[67]; within their framework, it is therefore the chain rule that must fail. Composite systems may remain well defined, but their operational information content cannot obey the usual decomposition into conditional contributions.

This obstruction has a concrete connection to generalized histories formulations. In bipar-

tite Bell scenarios, the existence of a strongly positive joint decoherence functional reproducing the experimental probabilities, including branching measurement contexts, characterizes the AQ set[57,58]. Our family therefore shows that strong positivity and consistency under outcome-dependent measurement choices can coexist with unbounded IC violations. These histories conditions alone do not recover the information constraints of quantum theory.

A broader possibility is that such violations signal the need for a revised operational account of subsystems and informational composition. Questions of this kind arise independently in causal-set approaches[68] and in frameworks with dynamical or indefinite causal structure[69,70]. These developments motivate examining alternatives to state-independent operator locality. AQ correlations provide a precise statistical relaxation: in their Hilbert-space characterization, distant projectors need commute only on the prepared state. Whether this relaxation acquires a physical interpretation in any such framework remains open. A physical completion might require a different information calculus, or additional dynamical and compositional requirements might exclude the offending correlations. Our result constrains these possibilities without selecting a particular spacetime mechanism.

Our construction uses many settings, leaving the economy of the violation as an important question. Concatenating copies of smaller boxes, as in Ref.[46], does not help, because the conclusive probabilities of successive certificates multiply while their information content is only linear. More economical violations will require different resources, such as almost-quantum boxes with more outcomes or behaviours that do not rely on certificates. The exact zeros $p(0,0|x,y) = 0$ for $x \neq y$ make the certification mechanism transparent but are not essential to a finite violation. Determining useful noise thresholds, particularly as the number of settings grows, remains important. More broadly, rare conclusive outcomes contribute information at first order in their probability, whereas small symmetric prediction biases contribute only at second order in the bias. Certification tasks therefore provide a natural setting in which to uncover operational differences that average guessing performance alone can conceal.

Methods

0.1 Almost-quantum realization of the box

Lemma 1. *For every $N \geq 1$, the box $\boldsymbol{p}^\star$ of Table 1, with settings $x, y \in \{1, \ldots, N\}$, belongs to* $\mathrm{C_{AQ}}$.

Proof. Let $\{\psi, e_1, e_2, f_x, g_x : x = 1, \ldots, N\}$ be an orthonormal basis of $\mathbb{R}^{2N+3}$, and define

$$c_x = \tfrac{3}{17}\psi + \tfrac{\sqrt{15}}{34}\, e_2 + \tfrac{\sqrt{5}}{2\sqrt{17}}\, g_x, \qquad d_x = \tfrac{\sqrt{51}}{34}\, e_1 + \tfrac{1}{2\sqrt{17}}\, f_x,$$
$$u_x = c_x + d_x, \qquad v_x = c_x - d_x, \qquad w_x = \tfrac{1}{17}\psi - \tfrac{2\sqrt{15}}{85}\, e_2 + \tfrac{2}{\sqrt{85}}\, g_x.$$

These are the vectors a_x, b_x and w_x of ref. 61, with $u_x = a_x$ and $v_x = b_x$. Direct multiplication gives $\langle \psi, u_x\rangle = \|u_x\|^2 = \langle \psi, v_x\rangle = \|v_x\|^2 = 3/17$, $\langle \psi, w_x\rangle = \|w_x\|^2 = \langle u_x, w_x\rangle = \langle v_x, w_x\rangle = \langle u_x, v_x\rangle = 1/17$, and $\langle u_x, v_y\rangle = \langle u_x, w_y\rangle = \langle v_x, w_y\rangle = 0$ for $x \neq y$. Let $A_{0|x}$ be the projector onto $\mathrm{span}\{u_x, w_x\}$ and $B_{0|y}$ the projector onto $\mathrm{span}\{v_y, w_y\}$, and set $A_{1|x} = \mathbf{I} - A_{0|x}$ and $B_{1|y} = \mathbf{I} - B_{0|y}$. By the inner products above, each of $\psi - u_x$, $v_x - w_x$ and v_y $(y \neq x)$ is orthogonal to both u_x and w_x, so $A_{0|x}\psi = u_x$, $A_{0|x}v_x = w_x$ and $A_{0|x}v_y = 0$; exchanging the roles of u and v gives $B_{0|y}\psi = v_y$, $B_{0|y}u_y = w_y$ and $B_{0|y}u_x = 0$. Hence $A_{0|x}B_{0|y}\psi = B_{0|y}A_{0|x}\psi = \delta_{xy}w_x$, and the commutation on ψ in Definition 1 extends to all outcome pairs because $A_{1|x} = \mathbf{I} - A_{0|x}$ and $B_{1|y} = \mathbf{I} - B_{0|y}$. Finally,

$p(0,0|x,y) = \delta_{xy}\langle\psi, w_x\rangle = \delta_{xy}/17$ and $p_A(0|x) = \langle\psi, u_x\rangle = p_B(0|y) = \langle\psi, v_y\rangle = 3/17$. For binary outcomes these values fix all entries of Table 1. □

0.2 Classical value of random-access block certification

Lemma 2 (Classical value)**.** *For all $N \geq 1$ and $k \geq 1$, every zero-error protocol for RABC that uses a one-bit message and shared randomness, but no other resource, satisfies $\mathcal{W} \leq 2^{-k}$. The value 2^{-k} is attained.*

Proof. All local randomness can be absorbed into the shared random variable λ. For fixed λ, Alice's message is a function $M = f_\lambda(\boldsymbol{Z})$, and Bob certifies block i after message m if and only if $c_\lambda(m,i) = 1$, for some function c_λ. The value $\mathcal{W}$ is the average over λ of the value $\mathcal{W}_\lambda$ of the deterministic strategy (f_λ, c_λ). Moreover, the protocol has zero error only if every strategy that occurs with positive probability does. It therefore suffices to show $\mathcal{W}_\lambda \leq 2^{-k}$ for a zero-error deterministic strategy, and we drop the index λ.

Every string $\boldsymbol{Z} \in \{0,1\}^{kN}$ occurs with probability $2^{-kN} > 0$. Hence zero error [Eq. (3)] requires that $c(m,i) = 1$ only if $\boldsymbol{Z}_i = 1^k$ for every $\boldsymbol{Z}$ with $f(\boldsymbol{Z}) = m$.

Let $m_0 = f(0^{kN})$ be the message sent for the all-zero string. No block of 0^{kN} equals 1^k, so $c(m_0,i) = 0$ for every i. Let $\bar{m}$ be the other message and $T = \{i : c(\bar{m},i) = 1\}$. Bob certifies block i exactly when $i \in T$ and $f(\boldsymbol{Z}) = \bar{m}$, so

$$\mathcal{W} = \sum_{i=1}^{N} \Pr(C_i = 1) = |T| \Pr\big(f(\boldsymbol{Z}) = \bar{m}\big).$$

By the zero-error condition, every string with $f(\boldsymbol{Z}) = \bar{m}$ satisfies $\boldsymbol{Z}_i = 1^k$ for all $i \in T$. The blocks are independent and uniformly distributed, so

$$\Pr\big(f(\boldsymbol{Z}) = \bar{m}\big) \leq \Pr\big(\boldsymbol{Z}_i = 1^k \;\forall\, i \in T\big) = 2^{-k|T|},$$

and hence $\mathcal{W} \leq g(|T|)$ with $g(t) \equiv t\,2^{-kt}$. We have $g(0) = 0$, and for every integer $t \geq 1$, $g(t+1)/g(t) = (1+1/t)\,2^{-k} \leq 2 \cdot 2^{-k} \leq 1$. So g is non-increasing on $t \geq 1$, and $\mathcal{W} \leq g(1) = 2^{-k}$.

For attainability, the parties share a uniformly random index $\ell \in \{1,\ldots,N\}$. Alice sends $M = 1$ if $\boldsymbol{Z}_\ell = 1^k$ and $M = 0$ otherwise. Bob certifies block i if $i = \ell$ and $M = 1$. A certificate for block i then requires $\boldsymbol{Z}_i = 1^k$, so the protocol has zero error, and

$$\mathcal{W} = \sum_{i=1}^{N} \Pr(\ell = i) \Pr(\boldsymbol{Z}_i = 1^k) = \sum_{i=1}^{N} \frac{1}{N}\, 2^{-k} = 2^{-k},$$

which completes the proof. □

0.3 Level-1 certificate boxes

The first level of the NPA hierarchy[55] is the set of vector correlations.

Definition 2 (Vector correlations)**.** A box $\boldsymbol{p}$ belongs to $\mathrm{C}_{\mathrm{Vec}}$ if there exist a unit vector ψ and vectors $\xi_{a|x}$, $\zeta_{b|y}$ in a real or complex Hilbert space such that $\xi_{a|x} \perp \xi_{a'|x}$ for $a \neq a'$, $\zeta_{b|y} \perp \zeta_{b'|y}$ for $b \neq b'$, $\sum_a \xi_{a|x} = \psi = \sum_b \zeta_{b|y}$, and $p(a,b|x,y) = \langle\xi_{a|x}, \zeta_{b|y}\rangle$ for all a,b,x,y.

Given an almost-quantum realization (Definition 1), the vectors $\xi_{a|x} = A_{a|x}\psi$ and $\zeta_{b|y} = B_{b|y}\psi$ form a vector realization, so $\mathrm{C}_{\mathrm{AQ}} \subseteq \mathrm{C}_{\mathrm{Vec}}$.

Lemma 3. *Let $N \geq 4$ and $q = N/[8(N-2)]$. The box $\boldsymbol{p}_N^{\mathrm{Vec}}$ with settings $x, y \in [N]$, binary outcomes and*

$$p(0,0|x,y) = q\,\delta_{xy}, \qquad p(0,1|x,y) = p(1,0|x,y) = \tfrac{1}{4} - q\,\delta_{xy}, \qquad p(1,1|x,y) = \tfrac{1}{2} + q\,\delta_{xy}$$

belongs to $\mathrm{C}_{\mathrm{Vec}}$. It satisfies Eq. (2) with certification rate $s = N/[8(N-2)]$.

Proof. Let ψ and e be orthonormal, let $g_1, \ldots, g_N$ be orthonormal and orthogonal to both, and put $f_x = g_x - \frac{1}{N}\sum_y g_y$, so that $\langle f_x, f_y\rangle = \delta_{xy} - 1/N$. With $\tau = \sqrt{(N-4)/[16(N-2)]}$, which is real for $N \geq 4$, define

$$\xi_{0|x} = \tfrac{1}{4}\psi + \tau e + \sqrt{q}\, f_x, \qquad \zeta_{0|y} = \tfrac{1}{4}\psi - \tau e + \sqrt{q}\, f_y,$$

and $\xi_{1|x} = \psi - \xi_{0|x}$, $\zeta_{1|y} = \psi - \zeta_{0|y}$. Direct multiplication gives $\langle \psi, \xi_{0|x}\rangle = \|\xi_{0|x}\|^2 = \frac{1}{4}$, $\langle \psi, \zeta_{0|y}\rangle = \|\zeta_{0|y}\|^2 = \frac{1}{4}$ and $\langle \xi_{0|x}, \zeta_{0|y}\rangle = \frac{1}{16} - \tau^2 + q\big(\delta_{xy} - \frac{1}{N}\big) = q\,\delta_{xy}$. The first two identities make $\xi_{0|x} \perp \xi_{1|x}$ and $\zeta_{0|y} \perp \zeta_{1|y}$, and each pair sums to ψ by construction. The remaining inner products follow by linearity, e.g. $\langle \xi_{0|x}, \zeta_{1|y}\rangle = \frac{1}{4} - q\,\delta_{xy}$, which reproduces the stated box. All entries are nonnegative because $\frac{1}{4} - q = (N-4)/[8(N-2)] \geq 0$. The vectors lie in the $(N+1)$-dimensional span of ψ, e and the f_x. □

The rate $N/[8(N-2)]$ is the largest certification rate of any level-1 box with $N \geq 4$ settings and binary outcomes, and it decreases to $1/8$[61]. For every $N \geq 5$ it exceeds the largest almost-quantum rate, so $\boldsymbol{p}_N^{\mathrm{Vec}} \notin \mathrm{C}_{\mathrm{AQ}}$[61]. Inserting $s = N/[8(N-2)]$ into Eq. (6) with $k = 9$ gives $\mathcal{I} > 1$ for every $N \geq 1117$. This is the dashed curve in Fig. 1b.

Statement of AI Use

The problem was conceived and the principal results were obtained by the authors. The large language model Claude (Anthropic) was used to assist with editing the prose, checking the numerical thresholds and preparing the figure.

Data availability

No datasets were generated or analyzed during the current study.

Note added

The almost-quantum box used here is studied in detail in a companion paper, "*An Unbounded Separation of Almost-Quantum and Commuting-Operator Correlations in Zero-Error Communication*" by R. Gazi, B. Chatterjee, J. Karmakar, R. K. Patra, M. Banik and A. Das Bhowmik[61]. That paper separates almost-quantum from commuting-operator correlations in the zero-error certification of equality; its results do not concern information causality. The present work is self-contained in its main result.

References

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

[2] Bell, J. S. On the Problem of Hidden Variables in Quantum Mechanics. *Rev. Mod. Phys.* **38**, 447 (1966).

[3] Mermin, N. D. Hidden variables and the two theorems of John Bell. *Rev. Mod. Phys.* **65**, 803 (1993).

[4] Brunner, N., Cavalcanti, D., Pironio, S., Scarani, V. & Wehner, S. Bell nonlocality. *Rev. Mod. Phys.* **86**, 419 (2014).

[5] Einstein, A., Podolsky, B. & Rosen, N. Can Quantum-Mechanical Description of Physical Reality Be Considered Complete? *Phys. Rev.* **47**, 777 (1935).

[6] Clauser, J. F., Horne, M. A., Shimony, A. & Holt, R. A. Proposed Experiment to Test Local Hidden-Variable Theories. *Phys. Rev. Lett.* **23**, 880 (1969).

[7] Freedman, S. J. & Clauser, J. F. Experimental Test of Local Hidden-Variable Theories. *Phys. Rev. Lett.* **28**, 938 (1972).

[8] Aspect, A., Grangier, P. & Roger, G. Experimental Tests of Realistic Local Theories via Bell's Theorem. *Phys. Rev. Lett.* **47**, 460 (1981).

[9] Aspect, A., Grangier, P. & Roger, G. Experimental Realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: A New Violation of Bell's Inequalities. *Phys. Rev. Lett.* **49**, 91 (1982).

[10] Aspect, A., Dalibard, J. & Roger, G. Experimental Test of Bell's Inequalities Using Time-Varying Analyzers. *Phys. Rev. Lett.* **49**, 1804 (1982).

[11] Weihs, G., Jennewein, T., Simon, C., Weinfurter, H. & Zeilinger, A. Violation of Bell's Inequality under Strict Einstein Locality Conditions. *Phys. Rev. Lett.* **81**, 5039 (1998).

[12] Hensen, B. *et al.* Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres. *Nature* **526**, 682 (2015).

[13] Giustina, M. *et al.* Significant-Loophole-Free Test of Bell's Theorem with Entangled Photons. *Phys. Rev. Lett.* **115**, 250401 (2015).

[14] Shalm, L. K. *et al.* Strong Loophole-Free Test of Local Realism. *Phys. Rev. Lett.* **115**, 250402 (2015).

[15] Scarani, V. The device-independent outlook on quantum physics. *Acta Phys. Slovaca* **62**, 347 (2012). arXiv:1303.3081.

[16] Ekert, A. K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **67**, 661 (1991).

[17] Mayers, D. & Yao, A. Quantum cryptography with imperfect apparatus. In *Proceedings 39th Annual Symposium on Foundations of Computer Science*, 503–509 (IEEE Computer Society, 1998).

[18] Acín, A. *et al.* Device-Independent Security of Quantum Cryptography against Collective Attacks. *Phys. Rev. Lett.* **98**, 230501 (2007).

[19] Vazirani, U. & Vidick, T. Fully Device-Independent Quantum Key Distribution. *Phys. Rev. Lett.* **113**, 140501 (2014).

[20] Arnon-Friedman, R., Dupuis, F., Fawzi, O., Renner, R. & Vidick, T. Practical device-independent quantum cryptography via entropy accumulation. *Nat. Commun.* **9**, 459 (2018).

[21] Nadlinger, D. P. *et al.* Experimental quantum key distribution certified by Bell's theorem. *Nature* **607**, 682 (2022).

[22] Zhang, W. *et al.* A device-independent quantum key distribution system for distant users. *Nature* **607**, 687 (2022).

[23] Pironio, S. *et al.* Random numbers certified by Bell's theorem. *Nature* **464**, 1021 (2010).

[24] Colbeck, R. & Renner, R. Free randomness can be amplified. *Nat. Phys.* **8**, 450 (2012).

[25] Gallego, R. *et al.* Full randomness from arbitrarily deterministic events. *Nat. Commun.* **4**, 2654 (2013).

[26] Acín, A. & Masanes, L. Certified randomness in quantum physics. *Nature* **540**, 213 (2016).

[27] Mayers, D. & Yao, A. Self testing quantum apparatus. *Quantum Inf. Comput.* **4**, 273–286 (2004).

[28] Šupić, I. & Bowles, J. Self-testing of quantum systems: a review. *Quantum* **4**, 337 (2020).

[29] Rai, A. *et al.* Device-independent bounds from Cabello's nonlocality argument. *Phys. Rev. A* **103**, 062219 (2021).

[30] Rai, A. *et al.* Self-testing quantum states via nonmaximal violation in Hardy's test of nonlocality. *Phys. Rev. A* **105**, 052227 (2022).

[31] Bancal, J.-D., Gisin, N., Liang, Y.-C. & Pironio, S. Device-Independent Witnesses of Genuine Multipartite Entanglement. *Phys. Rev. Lett.* **106**, 250404 (2011).

[32] Brunner, N. *et al.* Testing the Dimension of Hilbert Spaces. *Phys. Rev. Lett.* **100**, 210503 (2008).

[33] Mukherjee, A. *et al.* Hardy's test as a device-independent dimension witness. *Phys. Rev. A* **92**, 022302 (2015).

[34] Cubitt, T. S., Leung, D., Matthews, W. & Winter, A. Improving Zero-Error Classical Communication with Entanglement. *Phys. Rev. Lett.* **104**, 230503 (2010).

[35] Alimuddin, M. *et al.* Advantage of Hardy's nonlocal correlation in reverse zero-error channel coding. *Phys. Rev. A* **108**, 052430 (2023).

[36] Brunner, N. & Linden, N. Connection between Bell nonlocality and Bayesian game theory. *Nat. Commun.* **4**, 2057 (2013).

[37] Roy, A. *et al.* Nonlocal correlations: Fair and unfair strategies in Bayesian games. *Phys. Rev. A* **94**, 032120 (2016).

[38] Banik, M. *et al.* Two-Qubit Pure Entanglement as Optimal Social Welfare Resource in Bayesian Game. *Quantum* **3**, 185 (2019).

[39] Cirel'son, B. S. Quantum generalizations of Bell's inequality. *Lett. Math. Phys.* **4**, 93 (1980).

[40] Popescu, S. & Rohrlich, D. Quantum nonlocality as an axiom. *Found. Phys.* **24**, 379 (1994).

[41] Popescu, S. Nonlocality beyond quantum mechanics. *Nat. Phys.* **10**, 264 (2014).

[42] van Dam, W. Implausible consequences of superstrong nonlocality. *Nat. Comput.* **12**, 9 (2013).

[43] Brassard, G. *et al.* Limit on Nonlocality in Any World in Which Communication Complexity Is Not Trivial. *Phys. Rev. Lett.* **96**, 250401 (2006).

[44] Brunner, N. & Skrzypczyk, P. Nonlocality Distillation and Postquantum Theories with Trivial Communication Complexity. *Phys. Rev. Lett.* **102**, 160403 (2009).

[45] Linden, N., Popescu, S., Short, A. J. & Winter, A. Quantum Nonlocality and Beyond: Limits from Nonlocal Computation. *Phys. Rev. Lett.* **99**, 180502 (2007).

[46] Pawłowski, M. *et al.* Information causality as a physical principle. *Nature* **461**, 1101 (2009).

[47] Navascués, M. & Wunderlich, H. A glance beyond the quantum model. *Proc. R. Soc. A* **466**, 881 (2010).

[48] Fritz, T. *et al.* Local orthogonality as a multipartite principle for quantum correlations. *Nat. Commun.* **4**, 2263 (2013).

[49] Allcock, J., Brunner, N., Pawłowski, M. & Scarani, V. Recovering part of the quantum boundary from information causality. *Phys. Rev. A* **80**, 040103(R) (2009).

[50] Al-Safi, S. W. & Short, A. J. Information causality from an entropic and a probabilistic perspective. *Phys. Rev. A* **84**, 042323 (2011).

[51] Miklin, N. & Pawłowski, M. Information Causality without Concatenation. *Phys. Rev. Lett.* **126**, 220403 (2021).

[52] Patra, R. K. *et al.* Principle of Information Causality Rationalizes Quantum Composition. *Phys. Rev. Lett.* **130**, 110202 (2023).

[53] Miklin, N., Jain, P. & Gachechiladze, M. Communication complexity bounds from information causality (2026). arXiv:2602.10206.

[54] Navascués, M., Guryanova, Y., Hoban, M. J. & Acín, A. Almost quantum correlations. *Nat. Commun.* **6**, 6288 (2015).

[55] Navascués, M., Pironio, S. & Acín, A. Bounding the Set of Quantum Correlations. *Phys. Rev. Lett.* **98**, 010401 (2007).

[56] Navascués, M., Pironio, S. & Acín, A. A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. *New J. Phys.* **10**, 073013 (2008).

[57] Sorkin, R. D. Quantum Mechanics as Quantum Measure Theory. *Mod. Phys. Lett. A* **9**, 3119 (1994).

[58] Dowker, F., Henson, J. & Wallden, P. A histories perspective on characterizing quantum non-locality. *New J. Phys.* **16**, 033033 (2014).

[59] Henson, J. & Sainz, A. B. Macroscopic noncontextuality as a principle for almost-quantum correlations. *Phys. Rev. A* **91**, 042114 (2015).

[60] Cavalcanti, D., Salles, A. & Scarani, V. Macroscopically local correlations can violate information causality. *Nat. Commun.* **1**, 136 (2010).

[61] Gazi, R. *et al.* An Unbounded Separation of Almost-Quantum and Commuting-Operator Correlations in Zero-Error Communication (2026). arXiv:2610.41448.

[62] Wiesner, S. Conjugate coding. *SIGACT News* **15**, 78–88 (1983).

[63] Ambainis, A., Nayak, A., Ta-Shma, A. & Vazirani, U. Dense quantum coding and quantum finite automata. *J. ACM* **49**, 496–511 (2002).

[64] Pawłowski, M. & Żukowski, M. Entanglement-assisted random access codes. *Phys. Rev. A* **81**, 042326 (2010).

[65] Gonda, T., Kunjwal, R., Schmid, D., Wolfe, E. & Sainz, A. B. Almost Quantum Correlations are Inconsistent with Specker's Principle. *Quantum* **2**, 87 (2018).

[66] Sainz, A. B., Guryanova, Y., Acín, A. & Navascués, M. Almost-Quantum Correlations Violate the No-Restriction Hypothesis. *Phys. Rev. Lett.* **120**, 200402 (2018).

[67] Wakakuwa, E. & Murao, M. The chain rule implies Tsirelson's bound: an approach from generalized mutual information. *New J. Phys.* **14**, 113037 (2012).

[68] Bombelli, L., Lee, J., Meyer, D. & Sorkin, R. D. Space-Time as a Causal Set. *Phys. Rev. Lett.* **59**, 521 (1987).

[69] Hardy, L. Towards quantum gravity: a framework for probabilistic theories with non-fixed causal structure. *J. Phys. A* **40**, 3081 (2007).

[70] Oreshkov, O., Costa, F. & Brukner, Č. Quantum correlations with no causal order. *Nat. Commun.* **3**, 1092 (2012).

Acknowledgements

We thank R. Gazi, B. Chatterjee, J. Karmakar and R. K. Patra, our coauthors on the companion paper[61], for useful discussions. We also thank S. G. Naik, M. Alimuddin and A. Mukherjee for useful discussions on the role of certainty in information-causality scenarios. M.B. acknowledges financial support from the National Quantum Mission (NQM) of the Department of Science and Technology (DST), Government of India.

Author contributions

A.D.B. has pursued this problem over the past few years, in particular exploring how certainty, rather than bias, can lead to a violation of information causality. Both authors contributed to conceptualizing the idea, proving the results and preparing the manuscript.

Competing interests

The authors declare no competing interests.