Nonlocality beyond quantum mechanics: Excludible Information Causality

Amber Halsall

H.H. Wills Physics Laboratory, Bristol, United Kingdom

Abstract

There exists nonlocal correlations that exceed the predictions of quantum mechanics. To limit nonlocality to the quantum bound, this report examines a proposed physical principle known as Information Causality (IC). We present a reformulation of IC through a new form of information, 'Exclusion Information'. We analyse the behaviour of exclusion information within IC communication protocols, leading to the proposal of a new figure of merit for IC, 'mutual exclusion information'.

1 Introduction

Nonlocality is an inherent quality of our universe, as John Bell proved in 1964 [1]. This revelation traces it's roots to the pioneering work of Einstein, Podolsky, and Rosen in their seminal 'EPR' paper, which used entanglement to attempt to prove locality [2]. Entanglement defies classical mechanics, due to correlations that are fundamentally inaccessible within classical frameworks, giving the basis for investigating nonlocality [3]. Bell's Theorem states that if quantum mechanics truly governs our universe, then nonlocality is an inevitable consequence. However, nonlocality is more than a by-product of quantum theory; it is a foundational property of the universe, as intrinsic as space and time [4].

Following Bell's 1964 paper, experimental efforts, collectively termed Bell tests, were designed to probe Bell's inequality. A violation of Bell's inequality signifies nonlocal behaviour. The most simple Bell test, the Clauser-Horne-Shimony-Holt (CHSH) test is a bipartite game which involves two players who share a no-signalling device, which does not allow faster than light communication [5]. By employing entangled particles in the CHSH game, researchers consistently observed violations of Bell's theorem, showing the correlations enabled by quantum mechanics are inexplicable without considering Nonlocality [6]. In contrast, when the game is played under classical mechanics, Bell's Theorem remains satisfied.

Maximally entangled particles were expected to achieve the theoretical upper bound of Nonlocality permitted by our universe. However, in 1994, Popescu and Rohrlich found nonlocal correlations exceeding those predicted by quantum mechanics, yet consistent with special relativity [7]. This was done using a Popescu-Rohrlich (PR) box, which is a model independent construct that simplified the exploration of such correlations. This discovery raises fundamental questions: how nonlocal can nature be, and what determines its upper limit?

This discrepancy between quantum and super-quantum correlations necessitates the formulation of a physical principle to define the upper limit of Nonlocality. In the absence of such a principle, quantum mechanics remains unable to determine the maximal extent of nonlocal correlations. Thus, to further the development of quantum theory, it is essential to establish a principle that constrains nonlocality to the quantum bound. Several candidates have been proposed, including Communication Complexity [8], Information Causality [9], and Macroscopic Locality [10].

In 2009, Information Causality emerged as the first principle to precisely sever the quantum-super-quantum boundary in the CHSH game, suggesting its potential as a fundamental axiom. Initially, its scope was limited to a specific scenario, leaving open questions about its broader applicability. However, in 2024, a less strict constraint was proven to extend to all bipartite cases, marking a major advancement in it's theoretical foundation [11]. However, nature is described by multipartite scenarios, which a Bell test involving more than 2 players, and information causality has showed limited success in this case [12].

In light of its continued development, this report focuses exclusively on Information Causality through the examination of a new communication problem. It introduces a new form of information, Exclusion Information [13], which differs from the information measure employed in the original Information Causality framework. To do this, a new communication protocol was formulated and a new figure of merit 'Mutual Exclusion Information' was devised. This hopes to provide a more robust constraint on nonlocality than the original principle.

2 The Clauser-Horne-Shimony-Holt (CHSH) test

2.1 Introducing Bell tests

In a Bell test game, the players are referred to alphabetically as Alice, Bob... and are all on the same team [14, 15]. Each game consists of many rounds, each independent of previous rounds. The players are situated in separate laboratories, where they each receive an input and will provide an answer (output). The players are allowed to prepare a common strategy before the game, and are allowed no-signalling resources, meaning no devices which will enable Alice and Bob to communicate their outcomes faster than light to find out if they have won the game. It is possible to describe the complexity of a Bell test through the following notation:

$$(M_A, m_a; M_B, m_b). \tag{1}$$

Where the number of Alice's (Bob's) inputs M_A (M_B) and outputs m_A (m_B) are defined as such, and all of these parameters satisfy the inequality that:

$$M_A, m_a, M_B, m_b \geqslant 2, \tag{2}$$

Meaning all of the players' inputs and outputs must be larger than or equal to 2.

2.2 Describing the CHSH test

The Clauser-Horne-Shimony-Holt (CHSH) test can be written as:

$$(2, 2; 2, 2).$$

Therefore, the CHSH test is the most simple Bell test, as all inputs of (Eq. 1) are the minimum value they can be. The CHSH test is a bipartite scenario, as it has 2 players: Alice and Bob who have respective inputs, $x \in \{0, 1\}$ and $y \in \{0, 1\}$, and corresponding outputs, $a_x \in \{0, 1\}$ and $b_y \in \{0, 1\}$.

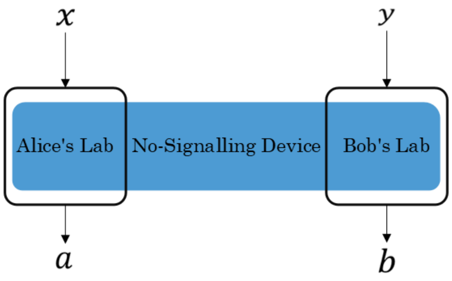

Figure 1: The CHSH game generalised: where Alice and Bob share a No-signalling device.

The winning conditions are that when $a = b$:

$$(x, y) \in \{(0, 0), (0, 1), (1, 0)\}, \tag{3}$$

and when $a \neq b$:

$$(x, y) = (1, 1). \tag{4}$$

Each input pair (x, y) is equally probable, ensuring a uniform distribution of $P(x, y) = \frac{1}{4}$.

2.3 Key Metrics

To evaluate how effective a strategy is at winning the CHSH game, two key metrics are defined: success probability, P_{success}, and score, S. The success probability is defined as:

$$P^{success} = P(a_x \oplus b_y = xy). \tag{5}$$

This has been simplified using addition modulo 2, which is a binary operation.

$0 \oplus 0$	0
$0 \oplus 1$	1
$1 \oplus 0$	1
$1 \oplus 1$	0

Table 1: Addition modulo 2

The rules and results of addition modulo 2 are shown in Table 1. The second metric is the Score defined as:

$$S = E_{00} + E_{01} + E_{10} + E_{11}, \tag{6}$$

which is written in terms of correlators , E_{xy} where:

$$E_{xy} = P(a = b|x, y) - P(a \neq b|x, y). \tag{7}$$

The correlator expression (Eq. 7) is a more concise way of writing the probabilities of the winning conditions of the CHSH game (Eqs. 3, 4).

There are four possible ways to win the game, meaning the maximal score is $S = 4$ and the hypothetical maximum success probability is $P_{\text{success}} = 1$. These metrics are have a linear relationship, namely:

$$P_{\text{success}} = \frac{S + 4}{8} \tag{8}$$

The proof for this can be found in [14].

2.4 Classical strategy

To prove that this test qualifies as a Bell test, the maximum score achievable under the assumption of local hidden variables (LHVs) must be determined. This will define the largest score and success probability possible while adhering to locality. It may be useful to think of a local hidden variable as a probabilistic source, such as a dice. It is assumed that this source of hidden variables is deterministic, meaning that the probability distribution $P_{source}(\lambda, \mu)$ is equal to 1 for some choice of λ and μ and 0 otherwise.

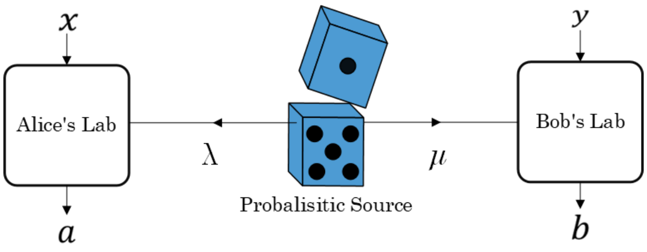

Figure 2: Diagram of the CHSH protocol using local hidden variables. The inputs are denoted by $x \in \{0, 1\}$ and $y \in \{0, 1\}$, and the outputs are denoted by $a_x \in \{0, 1\}$ and $b_y \in \{0, 1\}$. The dice represent the probabilistic source—local hidden variables.

A diagram illustrating the CHSH game protocol under a local hidden variable framework is shown in fig.2. The No-signalling device in this case is the probabilistic source, $P_{source} = (\lambda, \mu)$ which produces local hidden variables, λ and μ which are distributed to Alice and

Bob. Alice and Bob will input their respective queries x, y, and the probabilistic source will determine their respective outcomes via the local hidden variables they are sent.

$P_{success}(a \oplus b \,|\, x, y)$	
$P(0 \,|\, 0,0)$	$= 1$
$P(0 \,|\, 0,1)$	$= 1$
$P(0 \,|\, 1,0)$	$= 1$
$P(1 \,|\, 1,1)$	$= 0$

Table 2: Table of success probability playing the CHSH game using local hidden variables

Table 2 is the success probabilities for one predetermined strategy, but in all strategies one combination of inputs will evaluate a success probability of zero. Therefore, the success probability is bounded by:

$$P^{\text{classical}}_{\text{success}} = \frac{3}{4}. \tag{9}$$

Thus, the CHSH game demonstrates that any local hidden variable model can win the game at most three out of four times, resulting in a maximal score of:

$$S_{\text{classical}} \leq 2, \tag{10}$$

whilst adhering to locality.

2.5 Nonlocality & Quantum Mechanics

To demonstrate how Nonlocality is an inherent quality of quantum mechanics, Alice and Bob will play the CHSH game by sharing a maximally entangled state of two qubits:

$$|\phi\rangle = \frac{|0\rangle|0\rangle + |1\rangle|1\rangle}{\sqrt{2}}, \tag{11}$$

as their no-signalling device. If a success probability larger than $\frac{3}{4}$ then the local bound will be exceeded, proving Nonlocality, as the correlations between maximally entangled states are inexplicable using classical correlations.

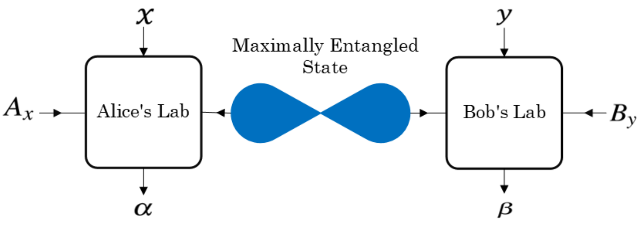

Figure 3: Diagram of the CHSH protocol using a maximally entangled state defined by Eq.11. Alice and Bob use operators A_x and B_y to measure their respective qubits. The inputs are denoted by x & y, and the eigenvalues are denoted by α & g, which are associated with outputs a_x & b_y respectively.

Alice (Bob) will measure an operator A_0 or A_1 (B_0 or B_1), depending on whether they have received $x = 0$ or $x = 1$ ($y = 0$ or $y = 1$). These operators have eigenvalues $\alpha \in \{+1, -1\}$, and $g \in \{+1, -1\}$ respectively. These can be mapped onto a and b using:

$$a = \begin{cases} 0 & \text{if} \quad \alpha = +1 \\ 1 & \text{if} \quad \alpha = -1 \end{cases}, \quad b = \begin{cases} 0 & \text{if} \quad g = +1 \\ 1 & \text{if} \quad g = -1 \end{cases}$$

which allows the outputs to be in binary. Using this method, the resulting success probabilities are:

$P_{success}(a \oplus b \,|\, x, y)$	
$P(0 \,|\, 0,0)$	≈ 0.854
$P(0 \,|\, 0,1)$	≈ 0.854
$P(0 \,|\, 1,0)$	≈ 0.854
$P(1 \,|\, 1,1)$	≈ 0.854

Table 3: Table of success probability playing the CHSH game using maximally entangled states

Regardless of the combinations of inputs and outputs, the success probability is always:

$$P^{quantum}_{success} = \frac{2 + \sqrt{2}}{4} \approx 0.854, \tag{12}$$

which is known as the Tsirelson bound [6]. Consquently the score is:

$$S_{quantum} = 2\sqrt{2}, \tag{13}$$

when Alice and Bob share a maximally entangled state. Quantum mechanics reveals correlations that defy explanation by any classical (LHV) model. Despite the no-signaling principle, entangled particle measurements exhibit correlations that cannot be accounted for by classical physics. While these quantum correlations may appear to imply faster-than-light communication, they do not violate relativity as Alice and Bob due to the no-signaling constraints of the CHSH test and all Bell tests. Classical communication remains necessary to verify outcomes. As Shimony aptly described, the probabilistic nature of quantum mechanics ensures the ”peaceful coexistence of relativity and nonlocality” [17]. This underscores that quantum mechanics cannot be replaced by a deeper, local theory.

2.6 Nonlocality Beyond Quantum Mechanics

Alice and Bob can achieve a 100% success rate in the CHSH game using a model-independent framework known as a Popescu-Rohrlich (PR) box. Formally, a PR box is a bipartite no-signaling probability distribution with binary inputs and outputs [18]. It can be conceptualized as an automated laboratory, preconfigured to conduct specific experiments with a predetermined set of possible outcomes while respecting no-signaling constraints.

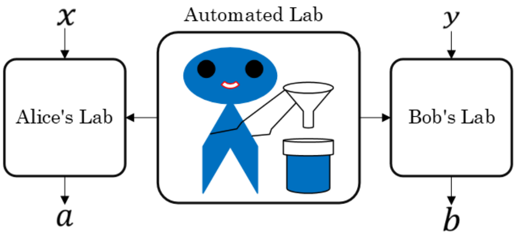

Figure 4: Diagram of the CHSH protocol using a PR-box as the no-signallin device. The inputs are denoted by $x \in \{0,1\}$ and $y \in \{0,1\}$, and the outputs are denoted by $a_x \in \{0,1\}$ and $b_y \in \{0,1\}$.

This concept is illustrated in fig.4, where the PR box functions as a no-signalling device. It Alice and Bob to be perfected correlated, leading to the following success probabilities:

$P_{success}(a \oplus b \mid x, y)$	
$P(0 \mid 0, 0)$	$= 1$
$P(0 \mid 0, 1)$	$= 1$
$P(0 \mid 1, 0)$	$= 1$
$P(1 \mid 1, 1)$	$= 1$

Table 4: Table of success probability playing the CHSH game using PR-correlations

This results in:

$$P^{PR}_{success} = 1, \tag{14}$$

and therefore,

$$S_{PR} = 4 \tag{15}$$

These metrics ($P_{success}$ & S_{PR}) are determined using a 'perfect' PR box; however, noise can be introduced to lower these metrics. This is briefly noted here, with a detailed explanation provided in Section 5 for the sake of continuity. By sharing these super-quantum correlations, Alice and Bob attain the maximum possible success probability and score. This raises a fundamental question: is there a fundamental physical principle that imposes a limit on the nonlocality of such correlations?

3 A Physical Principle: Information Causality

To address the presence of super-quantum nonlocal correlations, an additional axiom is required to complete the foundational principles of the quantum mechanical framework. In 1999, the physical principle of *Communication Complexity* was proposed as a potential constraint on such correlations [8]. By 2006, it was established that this principle is only violated when the success probability of the CHSH game reaches or exceeds:

$$P_{\text{success}} \geq \frac{3+\sqrt{6}}{6} \approx 0.908 \tag{16}$$

[16]. While this provided an initial restriction on super-quantum correlations, a more stringent principle was introduced in 2011: *Information Causality*. Notably, Information Causality is violated precisely at Tsirelson's bound,

$$P^{\text{quantum}}_{\text{success}} = \frac{2+\sqrt{2}}{4} \approx 0.854. \tag{17}$$

This made Information Causality the first principle to impose a strict separation between quantum and super-quantum correlations. This suggests that Information Causality could serve as the necessary axiom; however, it has several limitations, which will be discussed in a section 3.7 and the discussion (section 7).

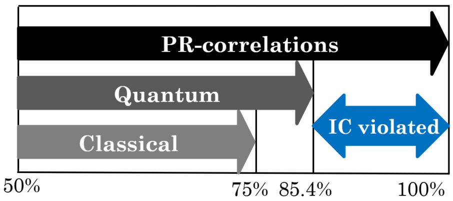

Figure 5: Visualisation of the various success probabilities, $P_{success}$ of playing the CHSH game using different strategies: Classical, Quantum and 'perfect' PR correlations. Also shows where the proposed physical principle, *Information Causality* must be violated.

3.1 Defining Information Causality

To introduce the principle of Information Causality, it is useful to consider a bipartite scenario involving Alice and Bob. Suppose Alice possesses a dataset that is initially unknown to Bob. By utilizing all of his local resources and receiving m classical bits of communication from Alice, the maximum amount of information Bob can **potentially** gain is limited to m bits.

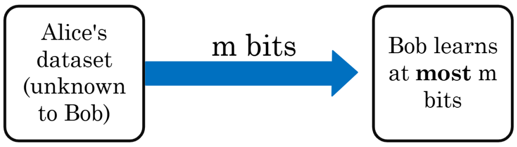

Figure 6: Flow diagram illustrating Information Causality in bipartite scenarios.

An example to understand this principle is the following: Suppose Alice provides Bob with a single key that grants access to a specific piece of information, this is permitted under Information Causality. However, if Alice were to send Bob a single key capable of unlocking her entire dataset, this would constitute a violation of the principle.

Information Causality imposes a fundamental limit, ensuring that the amount of information Bob can access does not exceed what has been explicitly transmitted to him. The principle of information causality is independent of any underlying physical theory, as it is fully determined by Alice and Bob's inputs and outputs. In this sense, it resembles Bell's parameter, which only involves random variables and can be used to test different physical theories.

3.2 Expressing Information Causality

Information Causality can be expressed in terms of Mutual Information. Mutual information, I quantifies how much information is communicated, on average, in one random variable about another. Applying this to Alice and Bob, the amount of information that Alice has is $x_i = \{x_0, x_1, ...\}$ and Bob's information about Alice's data is $g_i = \{g_0, g_1, ...\}$ corresponding to his guess for each bit in Alice's string. This means their mutual information can be defined by $I(x_i : g_i)$, quantifying how much information Bob has about Alice's string, x_i. The condition for Information Causality is then:

$$\sum_{i=1}^{N} I(x_i : g_i) \leqslant m, \tag{18}$$

where m is the number of bits Alice has sent to Bob. This says that the mutual information between sum of all of the bits in Alice's string, and Bob's guess about each bit in Alice's string must be less than or equal to the number of bits Alice sent to Bob. This will be explained through a communication task.

3.3 A classical communication task

Alice wants to send Bob a message that enables him to correctly output the bit which corresponds to the subscript of Alice's string. Let's say Alice has a 2-bit string, denoted by $x_i = \{x_0, x_1\}$, and Bob has $y = \{0, 1\}$ and he wants to output g_y. Bob's input is unknown to Alice, and therefore classically, in order to win this game 100% of the time, Alice must send both 2 bits: x_0 and x_1 for Bob to output the correct bit each time.

What happens if Alice is restricted to sending 1 bit? Classically, her best strategy is to just send the first bit in her string, x_0 every time, regardless of Bob's input, as this is unknown to Alice. This means $p_{success}(x_0) = 1$ and $p_{success}(x_1) = \frac{1}{2}$ as Bob knows nothing about x_1, but he can guess from two options (0 and 1), meaning he can still win 50% of the time. As Bob's inputs, $y = 0$ and $y = 1$ have an equal probability of occurring the success probability when Alice is restricted to sending one bit is:

$$P^{classical}_{success} = \underbrace{\frac{1}{2} \cdot 1}_{\text{when y=0}} + \underbrace{\frac{1}{2} \cdot \frac{1}{2}}_{\text{when y=1}} = \frac{3}{4}. \tag{19}$$

Interestingly, it is possible to win this game 100% of the time, and therefore violate Information Causality when Alice and Bob share a PR box, following a 'Random Access Code'.

3.4 Random Access Code

Using a Random access code, a proof of how a PR Box violates Information causality will be shown. A random access code is basically a fancy name for a scheme that compresses an initial amount of data into a smaller amount, such that any initial bit can be recovered with high probability [19].

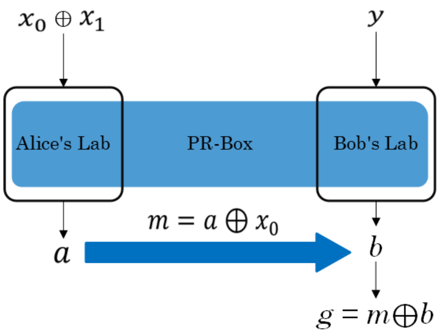

Figure 7: Diagram of the Random Access Code protocol, where Alice and Bob share a PR-box. Alice sends a one bit message to Bob, allowing him perfectly guess the value either bit in her string.

Consider the following situation shown in fig.(7). Alice inputs the sum of her two bits, $x_0 \oplus x_1$, which can be denoted as a into the shared PR-box. Using the output of this she can multiply this by the first bit in her string x_0. Then using the PR box she can send a one bit message, m to Bob. Bob obtains the output b from the PR box, unknown to Alice. Then Bob makes his guess, g by adding Alice's one bit message m and his output b together:

$$g = m \oplus b. \tag{20}$$

This protocol enables Bob to be able to correctly output $g_y = x_i$, regardless of Bob's input y, (see appendix A.1 for proof). This means he has the potential to access any bit of Alice's string, in this case he has the potential to access x_0 or x_1. Therefore Alice and Bob's mutual information is larger than the number of bits Alice sent Bob, which directly violates Information causality. This begs the question, is it possible for Alice to send Bob a one bit message, which will enable him to access more than 2 bits of Alice's dataset? This is possible, using a nested protocol.

3.5 Nested Protocol

To explain the nested protocol, Alice will now have a 4-bit string, denoted by $x_i = \{x_0, x_1, x_2, x_3\}$. Bob has 4 possible inputs $y \in \{0, 1, 2, 3\}$, which can be described by $y = 2y_1 + y_0$, where $y_0, y_1 \in \{0, 1\}$ in binary. Again, Alice is restricted to sending a 1-bit message. Alice and Bob can share 3 PR boxes, to do this.

Alice will input the first 2 bits of her string x_0 and x_1 into the 1st PR box, and the second 2 bits of her string x_2 and x_3 into the 2nd PR box. From this she will output m_0 and m_1 from the 1st and 2nd PR boxes respectively. Then, Alice will input m_0 and m_1 into the 3rd PR box, and she will output a. Finally, she will send m where is defined by:

$$m = a \oplus m_0. \tag{21}$$

Bob can now input y_1 into the 3rd PR box. If $y_1 = 0$ then Bob must retrieve either x_2 or x_3, which is done by retrieving m_1, and inputting y_0 into the second box, following the random access code, outlined in fig.(7).

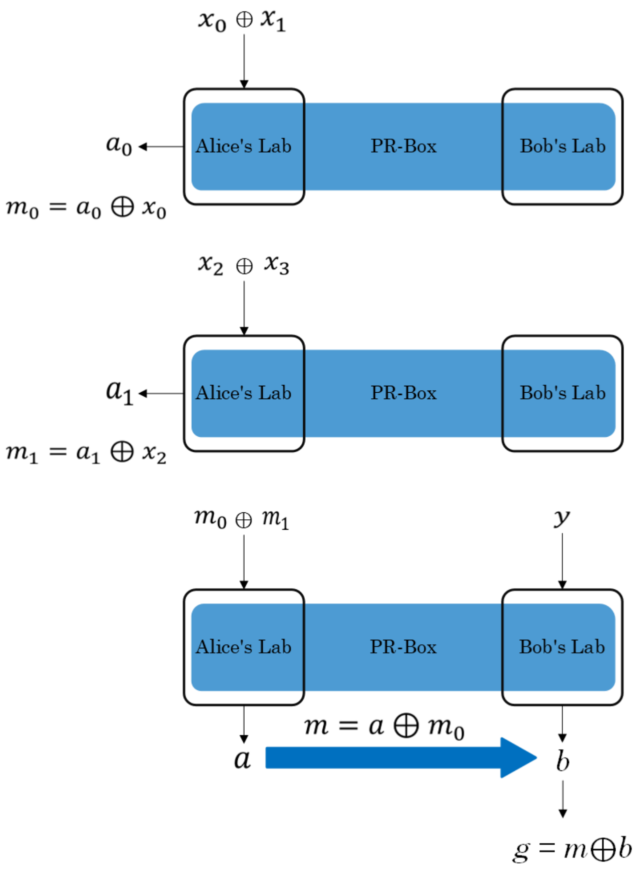

Figure 8: Diagram of the nested protocol, where Alice and Bobs share 3 PR-boxes [14]. Alice sends a one bit message to Bob, allowing him to perfectly guess the value of any of the 4 bits in her string.

3.6 Generalizing to an N-bit string

The nested protocol, shown for a 4-bit string (fig. 8) can be generalised to an N-bit string, where

$$x_i = \{x_0, x_1, ...x_{N-1}\},$$

and,

$$y \in \{0, 1, ..(N-1)\},$$

for every $N = 2^n$ where n is an integer. To do this, $N - 1$ PR-boxes must be used, and using this protocol it is possible to, with just one bit of communication from Alice, for Bob to retrieve any of her N bits with certainty, whilst learning nothing about the others. Here Information Causality works as the physical principle to limit nonlocal correlations stronger than those found using quantum theory, however this is not always the case. The following section will discuss the current shortcomings of Information Causality.

3.7 Current Shortcomings of Information Causality

Generalising Information Causality (IC) to various Bell scenarios has proven challenging, these difficulties are discussed in depth in the discussion (section 7). In 2024, IC was extended to all bipartite Bell scenarios [11], but the constraint on nonlocality was lowered to allow for this. Therefore, it remains uncertain whether all correlations which respect IC lie within the quantum limit. Extending IC to multipartite scenarios introduces additional challenges, requiring higher-dimensional resources for maximal violations of Bell inequalities [14].

4 Excludible Information Theory

These shortcomings and the small set of Bell tests which Information causality can currently be applied to form the basis for attempting to find a stronger figure of merit for information causality. Thus, this report aims to look at Information causality through the examination of a communication problem, using a new type of information, *Exclusion Information*. This hopes to widen the use of Information causality, or show that it is not the proposed principle. This section will describe this new type of information through an example.

4.1 An example of Exclusion Information

Unlike conventional communication problems, which focus on maximizing information transfer, this report explores transdering some information. While this distinction may appear redundant, the following example will illustrate its significance as a novel perspective on information transmission.

Contrasting a usual communication problem, which is about the ability for a process to send the maximal amount of information possible, this report aims to ask the best way to communicate some information. This may seem redudant, but hopefully the below example will prove that this is an interesting and new way to look to communicating information.

Let's digest this through an example. It is Alice's birthday, and she is allergic to peanuts. Bob wants to get Alice a cake, but he can't remember what she is allergic to. So he calls Alice, but the phone line is noisy at the shops. What is the safest way to communicate her allergy?

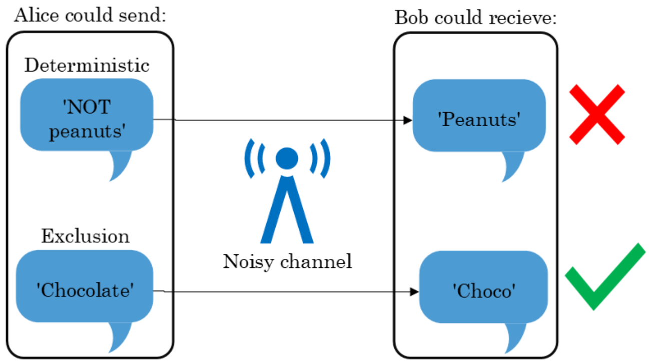

Figure 9: An example of a communication problem solved using Exclusion Information.

Instead of Alice attempting to communicate 'NOT peanuts' , which could be mistaken as 'peanuts', it may be a better coding strategy for Alice to communicate 'chocolate', which is much less likely to be wrongly decoded as 'peanuts'. In this way, Bob does not learn Alice's allergy, but he still gains enough information to successfully buy her a cake, and not send her into anaphylactic shock on her birthday!

Through this example, it is apparent that the ability of a channel to transfer deterministic information (a cake Alice is allergic to) may be completely different from its ability to transfer excludible information (which cake Alice is not allergic to). Hence different coding strategies should be employed.

4.2 Mutual exclusion information

These different coding strategies require different 'exclusion information' metrics, which are different from those found from sending 'deterministic information' [13]. These metrics will be defines below, leading to a formulation of the 'mutual exclusion information' which will be used to evaluate 'exclusion information causality' later in this report.

A cornerstone of *Information Theory* is the idea of quantifying how much information there is in a message. The mutual information, I of two variables, X and Y can be found by computing the difference in entropies, H associated with error probabilities, P_{error}. Consider in a communication task there is a random variable, X distributed according to $p(x)$. The error probability:

$$P_{\text{error}}(X) = min_x p(x), \tag{22}$$

defines the probability that one option is not successfully excluded. Let's consider a case where more than one option is excluded from a dataset. Then the error probability becomes:

$$P_{\text{error}}(x) = min_x \sum_{i=0}^{N-1} p(x_i), \tag{23}$$

Where the summation is over each individual bit in Alice's string. The associated entropy with this error probability is a order minus-infinity Rényi Entropy, which will be referred to as the 'exclusion entropy':

$$H_{excl}(X) = -log(P_{\text{error}}(X)). \tag{24}$$

A Rényi Entropy is quantity which has generalized various notions of entropy [20]. However, this quantity $H_{excl}(X)$ doesn't consider Bob's input, y, therefore the conditional probability distribution $p(y|x)$ must be considered. The associated error probability of this quantity is then:

$$P_{\text{error}}(X|Y) = \sum_y p(y) min_x p(x|y), \tag{25}$$

and the associated conditional exclusion entropy is:

$$H_{excl}(X|Y) = -log(P_{\text{error}}(X|Y)). \tag{26}$$

This information theory is able to define the mutual exclusion information between X and Y as:

$$I_{excl}(X:Y) = H_{excl}(X|Y) - H_{excl}(X). \tag{27}$$

This defines the reduction in exclusion entropy. This quantity can be used to evaluate Excludible Information Causality.

5 Noisy PR-correlations

Following from section 2.6, it is possible to introduce noise into a PR box. This noise is added to Alice's message when she sends it via a PR box using random access code, (section 3.4). When this message is sent, an additional noise parameter, r is added such that:

$$g = m \oplus b \oplus \underbrace{r}_{\text{noise}}, \tag{28}$$

Where r can take the values 0 or 1. When $r = 0$, Alice's message becomes $g = m \oplus b \oplus 0$, which is the same as her original message. This means that when $r = 0$, Bob receives the message Alice intended to send. However, when $r = 1$, Alice's message becomes $g = m \oplus b \oplus 1$ meaning Bob will always receive the wrong message, which is the opposite of what Alice intended to send. Thus, Bob's output becomes:

$$\overline{g} = g \oplus 1, \tag{29}$$

where the overline represents $\oplus 1$, changing the original message.

The amount of noise introduced into the PR-box can be defined by setting probabilities of when $r = 0$ or $r = 1$. The probability of $r = 0$ can be defined by:

$$P_{\text{no noise}}(r = 0) = q, \tag{30}$$

Where q is a probability that a message will be unaffected by noise. The probability of $r = 1$ is:

$$P_{\text{noise}}(r = 1) = 1 - q, \tag{31}$$

If $q = 0$ then the PR box has no noise at all, conversely, if $q = 1$ then there will be so much noise that Bob will always output the wrong result. This parameter q can be varied from 0 (perfect) to 1 (most imperfect).

6 Results

6.1 A communication task using Excludible Information

To evaluate whether Excludible Information is able to reconcile any of the shortcomings of Information Causality, a game was created. This game considers favourite colours, of Alice's friends: Claire and Dave. Alice knows Claire's favourite colour is a_0 = blue and Dave's favourite colour is a_1 = red. These two favourite colours are each chosen from a list of four colours:

$$x_i = \{\underbrace{a_0}_{\text{blue}}, \underbrace{a_1}_{\text{red}}, \underbrace{a_2}_{\text{yellow}}, \underbrace{a_3}_{\text{green}}\}. \tag{32}$$

Bob wishes to learn some information about either Claire's or Dave's favourite colour so that he can successfully exclude half of the colours in the dataset (Eq.32). Which friend he chooses to learn about is unknown to Alice, due to the No-signalling condition of the game.

The winning condition of the game are if Bob can exclude the possibilities of favourite colours from 4 possibilities down to 2 possibilites, for either Claire or Dave.

Alice must send Bob the information required to do this using the minimum number of bits, m necessary. To do this, Alice must send Bob the correct colour, and another possibility for both Claire and Dave, as such:

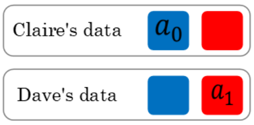

Figure 10: Information Alice needs to send to Bob.

To learn about some information about Claire's or Dave's favourite colour, Bob will query with either $y = 0$ or $y = 1$. Then using either $y = 0$ or $y = 1$ and Alice's message, m Bob makes a guess, g. This guess can be defined as:

$$g = \overline{m} \oplus b = \overline{x_y} \quad \text{Where} \quad y \in \{0, 1\}, \tag{33}$$

Where $\overline{x_y} = x_y \oplus 1$. This says that Bob will output the opposite of what Alice sends, to successfully exclude colours that the favourite colour is not, which is the winning condition of the game.

6.2 Organising Colours

Alice and Bob must come up with a pre-arranged strategy to encode these colours into the minimum number of bits possible. This is done by firstly denoting the colours in binary notation such that:

Colour	1st Bit	2nd Bit
Blue	0	0
Red	0	1
Yellow	1	0
green	1	1

Table 5: Assignment of colours to bits.

Alice and Bob can write the 4 colours within their datasets as seen in table 5. However, there is a smarter way for them to organise their data. As Bob needs to exclude half of a dataset, it is possible to group the colours into two categories: 0 and 1.

0	Blue,	Red
1	Yellow,	green

Table 6: Grouping colours based on the 1st bit of each of the colours.

In this case, Alice and Bob choose to split their data using the first bit of each of the colours, resulting in the groupings found in table 6. There are 2 other groupings of this data that are possible (see Appendix B). It is important to note that these variations in grouping do not affect Alice and Bob's success. Using this grouping, it is now possible for Alice to send Bob a 1 bit message for each friend: Claire and Dave. Then Bob can successfully exclude two colours which the favourite colour is not. This will be digested through the following example.

6.2.1 An example

Claire and Dave's favourite colours are red and blue respectively, therefore Alice must send $x_0 = 0$ and $x_1 = 0$, as both Claire and Dave's favourite colours are grouped into the 0 category, using table 6. Let's say Bob inputs $y = 0$ his guess will be:

$$g = \overline{x_{y=0}} = 0 \oplus 1 = 1. \tag{34}$$

If Bob inputs $y = 1$ instead, then his guess would be:

$$g = \overline{x_{y=1}} = 0 \oplus 1 = 1. \tag{35}$$

Bob can then use the key in table 6, and as both outputs are 1, Bob knows to exclude yellow and green. Therefore, he knows Claire and Dave's favourite colours must be either blue or red.

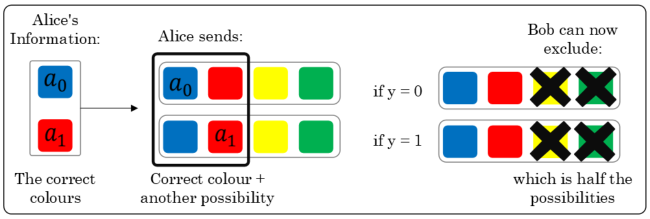

Figure 11: The exclusion game explained through an example, where Claire and Dave's favourite colours are a_0 = blue and a_1 = red, and Bob successfully excludes yellow and green from both datasets.

The overall process of this game is shown in fig.11. In the following sections, this game will be played using no signalling resources with correlations of increasing strength. It can be established at what strength of correlations Information Causality has been violated, by evaluating a new figure of merit called the 'Mutual exclusion information'.

6.3 Quantifying Excludible IC

At this point, it is necessary to introduce a new proposed figure of merit for IC. This is called the Mutual Exclusion information, $I_{\text{Exclusion}}$ which is defined as:

$$I_{\text{exclusion}} = \sum_{i=0}^{N-1} I_{excl}(\overline{x_i} : g|y = i) \tag{36}$$

In this equation, $\overline{x_i}$ is the bit in Alice's string which has the information required to exclude half the possibilities within a dataset and g is Bob's guess. It is possible to think that the strategy that Alice and Bob use is encoded within Bob's guess. Therefore by adapting Eq. 27, $I_{\text{exclusion}}$ can be written as:

$$I_{excl}(\overline{x_i} : g) = H_{excl}(\overline{x_i}|g) - H_{excl}(\overline{x_i}). \tag{37}$$

This means it is possible to find the mutual exclusion information for different strategies. This metric can be used to answer at what strength of correlations information causality is violated, and if this is at the same limit as seen in the original formulation of IC [9].

6.3.1 Generalising number of colours

It is possible to extend the number of colours to choose from such that :

$$x_i \in \{a_0, a_1, a_2, ..., a_{C-1}\}, \tag{38}$$

Where C is the number of colours in a string, x_i. C can be defined as:

$$C = 2^b, \quad b \in \mathbb{Z}, \quad b \geqslant 2,$$

where b is the number of bits used to define a colour. It is important that b starts at 2, as $b = 1$ results in $C = 2$, oversimplifying the game and yielding an identical game to the one utilized for illustrating information causality in Section 3.3. Alice can then group the colours as such:

0	$a_0, a_1, ..., a_{\frac{C}{2}-2}, a_{\frac{C}{2}-1}$
1	$a_{\frac{C}{2}}, a_{\frac{C}{2}+1} ..., a_{C-2}, a_{C-1}$

Table 7: Grouping based on the 1st bit of each of the colours.

This is following the same methodology as used to group 4 colours (see section 6.2). This demonstrates that the number of colours, C, does not influence Alice and Bob's probability of success in the game. Regardless of the total number of colours available to Claire and Dave, it is always possible to separate them into two equal groups, assigning one group to 0 and the other to 1. Consequently, upon receiving a one-bit message from Alice, Bob can consistently eliminate 50% of the dataset.

6.4 Sending Excludible Information

6.4.1 Using Classical Correlations

Playing this game classically results in the same success probabilities as seen in section 3.3. Although the winning conditions are now different, as Bob is required to output information entirely different then the original protocol. The number of bits Alice must send to obtain a success probability of 100% is still two bits, and when Alice is restricted to playing with one bit $P_{success}$ is $\frac{3}{4}$, (as outlined in section 5). It is also possible to add noise to a PR-correlation by setting:

$$q = \frac{3}{4}.$$

Then, when no noise is added:

$$P_{\text{No noise}}(r = 0) = \frac{3}{4}, \tag{39}$$

and when noise is added:

$$P_{\text{Noise}}(r = 1) = \frac{1}{4}. \tag{40}$$

As Alice has a two bit string, and random access code is used, it is possible to set $P_{\text{No Noise}} = P_{success}$ as this is when Alice's message is unaffected by the Noise, and therefore $P_{\text{Noise}} = P_{\text{error}}$. Meaning that using Noisy PR-correlations with a q value of $\frac{3}{4}$ evaluates to the same success probabilities as playing this game classically.

6.4.2 Using Quantum Correlations

It is also possible, to set:

$$q = \frac{2+\sqrt{2}}{4} \approx 0.854,$$

resulting in:

$$P_{\text{No noise}}(r = 0) = P_{success} = \frac{2+\sqrt{2}}{4} \approx 0.854, \tag{41}$$

$$P_{\text{Noise}}(r = 1) = P_{\text{error}} = \frac{2-\sqrt{2}}{4} \approx 0.146. \tag{42}$$

Which recovers the Tsirelson's bound for this excludible information game.

6.4.3 Using PR correlations

Using PR- correlations it is possible for Alice and Bob to win the game 100% of the time, only sending one bit. This can be done by Alice using the random access code outlined in section 3.4 to send her message, m to Bob. Therefore this exclusion protocol yields results consistent with those originally reported in the original Information Causality protocol. Furthermore, as seen in section 3.5 no matter how large Alice's string is, Bob will still be able to retrieve any of her N bits with certainty, whilst learning nothing about the others. Therefore:

$$P^{PR, N-bit}_{success} = 1. \tag{43}$$

$$P^{PR, N-bit}_{\text{error}} = 0, \tag{44}$$

However, as soon as noise is introduced, the $P_{success}$ and P_{error} are affected by the string size N. This will be shown in the next section.

6.5 Mutual Information & N: Classical Correlations

Alice has a 4-bit string which is represented by:

$$x_i \in \{x_0, x_1, x_2, x_3\},$$

which corresponds to four friends favourite colours. Alice sends the answer for the first bit, x_0, regardless of how many bits are in her string. The resulting success probability is:

$$P^{cl,\ 4-bit}_{success} = \underbrace{\frac{1}{4} \cdot 1}_{\text{when } y=0} + \underbrace{\frac{1}{4} \cdot \frac{1}{2} + \frac{1}{4} \cdot \frac{1}{2} + \frac{1}{4} \cdot \frac{1}{2}}_{\text{when} \quad y \neq 0} = \frac{5}{8}. \tag{45}$$

This shows that as the string size increases in any protocol where there is noise, the success probability of the protocol decreases. This is because, as Alice's string size increases, the one bit message she sends, which is x_0 is less and less useful to Bob. It is possible to approximate the success and error probabilities to an N-bit string such that:

$$P^{classical}_{success} = \frac{N+1}{2N}, \tag{46}$$

$$P^{classical}_{\text{error}} = \frac{N-1}{2N}. \tag{47}$$

Which means that both $P^{classical}_{success}$ and $P^{classical}_{\text{error}}$ tend towards $\frac{1}{2}$ as N tends to infinity. This is because the information Alice sends Bob x_0 becomes less and less useful as Alice's string size increases (proof in appendix A.2). The relationship between mutual information and number of bits in Alice's string can be described by (proof in appendix A.3):

$$I(x_i : g) = log_2(\frac{N}{N-1}). \tag{48}$$

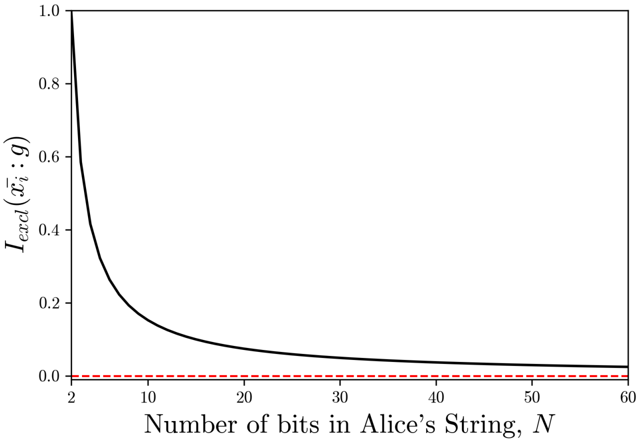

Figure 12: Graph of $I_{\text{excl}}(\overline{x_i} : g)$ against number of bits in Alice's string for classical correlations.

This means that when Alice has a 2-bit string, the mutual information is one, however as Alice's string size increases, the mutual information tends to 0, as shown in fig. 12.

6.6 Using Noisy PR-correlations to emulate Quantum Correlations

Using the nested protocol (section 3.5) and noisy PR-boxes with a q set to the Tsirelson bound, it is possible to evaluate how $P_{success}$ and P_{error} are affected as string size increases. This results in success and error probabilities such that:

$$P^{quant,4-bit}_{success} = \frac{3}{4}, \tag{49}$$

$$P^{quant,4-bit}_{\text{error}} = \frac{1}{4}. \tag{50}$$

Again, this shows that as string size increases, the success probability decreases, in this case from ≈ 0.854 to 0.75. It can be useful to think of this as, by using more PR boxes, the errors introduced by the noise accumulate, reaching a larger error probability.

An important note to make is that it is unknown whether this is best protocol using maximally entangled states, as this method just takes the Tsirelson's bound as q. Although, the Tsirelson's bound defines the most nonlocal correlations for the CHSH game that does not necessary mean the same applies to this exclusion game for any string size beyond a 2-bit string.

6.7 Mutual exclusion information and q

For a 2-bit string, and a 4-bit string, a relationship between the strength of correlations, q and the mutual information between Alice and Bob, $I(\overline{x_i} : g)$ can be found. This relationship is derived from the relationship between P_{error} and q, namely:

$$P^{2-bit}_{\text{error}} = 1 - q, \tag{51}$$

and,

$$P^{4-bit}_{\text{error}} = 2q(1-q). \tag{52}$$

These lead to this relationship between mutual information and q:

$$I^{2-bit}_{excl}(\overline{x_i} : g) = -log_2(2(1-q)), \tag{53}$$

and,

$$I^{4-bit}_{excl}(\overline{x_i} : g) = -log_2(4q(1-q)). \tag{54}$$

Derivations of these $I_{\text{Exclusion}}$ can be found in Appendix A.4 & A.5 respectively.

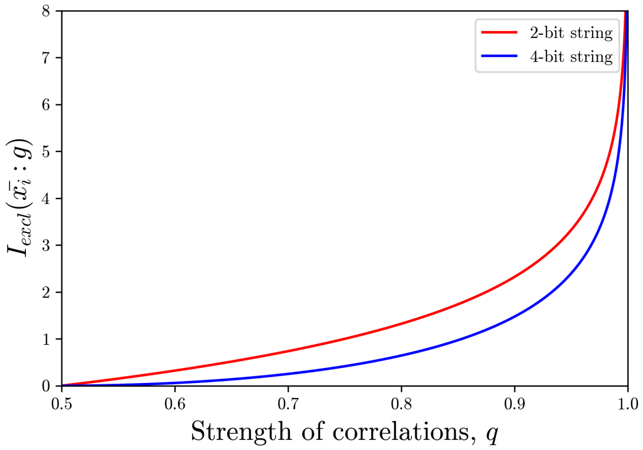

Figure 13: Graph of $I_{\text{excl}}(\overline{x_i} : g)$ against the strength of correlations.

This is graphically displayed in fig.13, where it is evident that the 2-bit string results in higher mutual information than the 4-bit string for all values of q. Both curves exhibit a rapid increases as q approaches 1, but the 2-bit string's curve grows more steeply than the 4-bit string.

	Classical	Quantum	Super-Quantum
q	$\frac{3}{4}$	$\frac{2+\sqrt{2}}{4}$	$\frac{7}{8}$
2-bit string:	1	1.77	2
4-bit string:	0.42	1	1.19

Table 8: Mutual Exclusion information for strategies of varying strength, where the strength of the correlations is determined by the q values.

Some key points from figure 13 have been quantified in table 8, and their relevance will be discussed below.

7 Discussion

7.1 Results

The communication task using excludible information was formulated, introducing a new parameter: the number of colours excluded from the dataset. This report focused on cases where 50% of the dataset was excluded. Given more time, it would be valuable to explore varying exclusion percentages and evaluate their impact on exclusion mutual information. The relationship between mutual exclusion information and the number of bits in Alice's string for classical correlations was examined, revealing that as N increased, the mutual information tended towards zero.

The noise parameter r was varied using the parameter q for 2-bit and 4-bit strings. Figure 12 and table 8 indicate that as q decreased, I_{excl} also decreased. Furthermore, when $q = 1$, corresponding to a 'perfect' PR-box, Bob has the potential to access all of Alice's data, meaning the mutual exclusion information becomes very large as Bob never makes a mistake, as seen by in the graph. Extending this analysis to an N-bit string would be insightful to determine the q value at which exclusion information causality is violated. This would show if exclusion information causality recovers the Tsirelson bound. Unfortunately, this requires demanding computation, which results in increasing large polynomials for the P_{error}, due to the nature of the nested protocol.

7.2 Figures of Merit

Different figures of merit can be used to assess the point at which information causality is violated, notably success probability and mutual information in the literature. The original information causality framework [9] used mutual information as the figure of merit, yielding the result:

$$I^{\text{classical}} = I^{\text{quantum}} < I^{\text{PR-correlations}}. \tag{55}$$

This implies that quantum entanglement does not provide an advantage over classical strategies when using mutual information as the figure of merit. In contrast, this report employs mutual exclusion information as the figure of merit, leading to:

$$I_{excl}^{\text{classical}} < I_{excl}^{\text{quantum}} < I_{excl}^{\text{PR-correlations}}. \tag{56}$$

This hierarchy of strategies aligns with the findings of Al-Safi et al [21]. who used success probability as the figure of merit. Their findings suggest that entangled quantum states outperform classical strategies when considering success probability. While success probability and mutual information are not monotonically related, this report establishes a connection between these metrics by adapting mutual information from the original information causality framework which in turn reproduces the bounds observed in Al-Safi et al.

7.3 Issues with information causality

The first issue is defining the quantum bound itself. While the Tsirelson bound is well-defined in simple Bell scenarios such as the CHSH game, computing quantum bounds becomes increasingly complex as the scenarios grow in complexity. Some success has been found by Allcock et al. [22] who found that part of the boundary of quantum correlations in a more complex space actually emerges from the principle of information causality. This was done by introducing an additional noise parameter. A particularly counter-intuitive result is that maximal quantum correlations can emerge from measurements on non-maximally entangled states, further complicating their computation [14]. Ensuring a protocol optimally achieves the nonlocal upper bound is a fundamental challenge. How can one be certain that a given protocol retrieves the maximal possible nonlocality?

As a result, the precise threshold at which information causality should be violated remains unknown in Bell scenarios where the quantum bounds have yet to be established. This uncertainty raises fundamental questions: how can one define a physical principle distinguishing quantum from super-quantum correlations when the boundary remains unclear?

Generalizing information causality across more complex Bell scenarios remains a significant challenge. Information causality on all bipartite Bell scenarios has been proposed by Jain et al. [11], however, their proposed constraint is weaker than the original proposal of IC. This proposed constraint raises uncertainty regarding whether all correlations respecting it remain within the quantum limit.

Another major difficulty is extending information causality to multipartite scenarios, which are crucial for modelling real-world systems. Multipartite Bell scenarios introduce additional complexities, such as requiring systems with higher dimensions than the number of possible outcomes [14]. Furthermore, this report relied on a nested protocol (3.5), which is designed for a bipartite scenario. Therefore, attempting to apply this protocol to multipartite cases is problematic and potentially ineffective, thus contributing to the difficulty in establishing a bound for multipartite scenarios.

Furthermore, if the nested protocol is not the most optimal way to organise and send bits, it has far reaching consequences as all results are derived from this. This means that it is possible that the figure of merit for Information Causality would hold for more complex scenarios, if a smarter protocol than the nested protocol were to be devised. Finding the 'smartest' protocol and the maximal quantum boundary in increasingly complex bell scenarios are the keys to finding a physical principle to limit nonlocal correlations. Consequently, while mutual exclusion information may offer a promising figure of merit, the core issue leading to stagnation in this field likely lies within the excludible protocol itself. Developing a smarter protocol may be key to unlocking the full potential of this new figure of merit. This report hopes that by applying this type of information to IC, we may possess the key to beginning to answer these questions.

8 Conclusions

In this report, information causality is explored through the concept of Exclusion Information and its associated figure of merit, Mutual Exclusion Information. However, several challenges remain in defining the maximal quantum boundary, particularly in multipartite scenarios and the complexity of achieving optimal protocols. The use of a nested protocol, while informative, may not be the most effective strategy, and developing more sophisticated protocols maybe be the next step in advancing the study of nonlocality. The development of a clearer and more universal principle that constrains nonlocality to the quantum limit remains an open challenge, but the introduction of exclusion information offers a promising direction for future research in quantum information theory.

References

[1] J. Bell, *On the Einstein Podolsky Rosen paradox* **3, 195-200**, Physics Physique Fizika, (1964).

[2] A. Einstein, B. Podolsky, & N. Rosen, *Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?*, **10, 777–780**, Physical Review Letters, (1935).

[3] R. Horodecki, P. Horodecki, M. Horodecki, & K. Horodecki, *Quantum entanglement*, **2, 865–942**, Physical Review Letters, (2009).

[4] S. Popescu, *Nonlocality Beyond Quantum Mechanics*, **10, 264–270**, Nature Physics, (2014).

[5] J. Clauser, M. Horne, A. Shimony, and R. Holt, *Proposed Experiment to Test Local Hidden-Variable Theories*, **23, 15, 880-884**, Physical Review Letters, (1970)

[6] B. S. Cirel'son, *Quantum generalizations of Bell's inequality*, **100, 93**, Letters in Mathematical Physics, (1980).

[7] S. Popescu, D. Rohrlich, *Quantum Nonlocality as an axiom*, **24, 3, 379-385**, Foundations of Physics, (1994).

[8] W. Van Dam, *Nonlocality & Communication Complexity*, **28-30**, University of Physics, (1999).

[9] M. Pawłowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter & M. Żukowski, *Information Causality as a physical principle*, **461, 1101–1104**, Nature, (2009).

[10] M Navascués, & A Wunderlich, *glance beyond the quantum model.*, **466, 881 –890**, Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences, (2010).

[11] P. Jain, M Gachechiladze, & N. Miklin, *Information Causality as a Tool for Bounding the Set of Quantum Correlations*, **133, 1079-7114**, Physical Review Letters, (2024).

[12] L. Pollyceno, R. Chaves & R. Rabelo, *Information causality in multipartite scenarios*, **107, 2469-9934**, Physical Review A, (2023).

[13] A Ducuara, & P Skrzypczyk, *Weight of informativeness, state exclusion games and excludible information*, **1908.10347** arXiv (Quantum Physics), (2024).

[14] S. Valerio, *Bell Nonlocality* , **1-3, 8-11,** , Oxford University Press, (2019).

[15] N. Linden & P. Skrzypczyk, *Quantum Information Theory, 2023-4 Course Notes* **65-80**, University of Bristol, (2023).

[16] G. Brassard, H. Buhrman, N. Linden, A. Méthot, A. Tapp, and F. Unger, *Limit on Nonlocality in Any World in Which Communication Complexity Is Not Trivial*, **96, 25, 250401-(1-4)** Physical Review Letters, (2006)

[17] A. Shimony, *Foundations of Quantum Mechanics in the Light of New Technology* **225-230**, Physical Society of Japan, (1983)

[18] M. Pawłowski, S. Valerio, *Information Causality*, (2011).

[19] J. Doriguello & A. Montanaro, *Quantum Random Access Codes for Boolean Functions*, **5, 402**, Verein zur Förderung des Open Access Publizierens in den Quantenwissenschaften, (2021).

[20] A Rényi, *On measures of entropy and information*, **4, 547–562**, Proceedings of the fourth Berkeley symposium on mathematical statistics and probability, University of California Press, (1961).

[21] S. Al-Safi & A. Short, *Information causality from an entropic and a probabilistic perspective*, **84, 4, 042323, 6**, Physical Review A, (2011).

[22] J. Allcock, N. Brunner, M. Pawlowski, & S. Valerio, *Recovering part of the boundary between quantum and nonquantum correlations from information causality*, **80, 4**, Physical Review A, (2009).

Appendix A: Derivations & Proofs

This appendix covers all the additional derivations used throughout the report.

A.1 Proving $m \oplus b = x_y$

Alice inputs $x = x_0 \oplus x_1$ into the PR box, and she outputs a. Bob inputs y into the PR box and outputs $g = m \oplus b$, which also equals $g = (a \oplus b) \oplus x_0$. A known rule for PR-boxes it that $a \oplus b = xy$ is always satisfied, since $P_{\text{success}} = 1$. These can be substituted into Bob's output, g which will result in:

$$g = (x_0 \oplus x_1)y \oplus x_0 \tag{57}$$

Factorising this obtains:

$$g = x_0(y \oplus 1) \oplus x_1 y \tag{58}$$

From this, if Bob's input is y=0, then $g = x_0$ and conversely if y=1, then $g = x_1$, exactly as is required.

A.2 Deriving $P^{classical}_{\textbf{error}} = \frac{N-1}{2N}$

Extending from Eq.45, it is possible to approximate P_{error} to an N-bit string. Let's say Alice now has an infinite string length $x_i = \{x_0, x_1, ...x_{N-1}\}$. The error probability then becomes:

$$P^{cl,N-bit}_{\text{error}} = \underbrace{\frac{1}{N} \cdot 0}_{y=0} + \underbrace{\frac{1}{N} \cdot \frac{1}{2} \cdot (N-1)}_{0<y<N}. \tag{59}$$

The first term is the probability of making an error on the 1st bit, which will never happen as Bob knows the value of x_0, as Alice sent him that. The second term, is when Bob makes a guess, hence he has a 50% of getting the wrong answer. Since this happens for every bit in his string except the first bit, this is multiplied by $N-1$. This results in an overall error probability of:

$$P^{cl,N-bit}_{\text{error}} = \frac{N-1}{2N}, \tag{60}$$

as seen in Eq.47.

A.3 Deriving $I_{excl}(\overline{x_y} : g) = log_2(\frac{N}{N-1})$

From the above derivation, it is possible to find an Equation for mutual information between Bob's guess, g and the bit of Alice's string Bob wants to output, $\overline{x_y}$. In this case the entropies are:

$$H_{excl}(\overline{x_y}) = -log_2(\frac{1}{2}), \tag{61}$$

which is when Alice has sent Bob no information, therefore he makes a completely uneducated guess. This is when Alice has sent Bob x_0 in this case, so he has some information about Alice's dataset:

$$H_{excl}(\overline{x_y}|g) = -log_2(\frac{N-1}{2N}), \tag{62}$$

This results in a mutual information of:

$$I_{excl}(\overline{x_y} : g) = -log_2(\frac{N-1}{2N}) + log_2(\frac{1}{2}). \tag{63}$$

Which results in the equation:

$$I_{excl}(\overline{x_y} : g) = log_2(\frac{N}{N-1}). \tag{64}$$

A.4 Deriving a relationship between *mutual exclusion information* and q for a 2-bit string

Using random access code (section 3.4), it is possible to see that the probability that noise is added to Alice's message, $P_{\text{Noise}}(r = 1)$ equals the error probability, P_{error} therefore:

$$P_{\text{error}} = 1 - q \tag{65}$$

The entropy if Bob has no information from Alice about which bits to exclude within a dataset is always:

$$H_{excl}(\overline{x_y}) = -log_2\frac{1}{2} \tag{66}$$

The conditional exclusion entropy, corresponding to when Alice has sent some information so that he is able to make a more 'informed' guess is:

$$H_{excl}(\overline{x_y}|g) = -log_2(1-q). \tag{67}$$

This results in a exclusion mutual information such that:

$$I_{excl}(\overline{x_y}:g) = -log_2(1-q) - log_2\frac{1}{2}, \tag{68}$$

which is simplified to:

$$I_{excl}(\overline{x_y}:g) = -log_2(2(1-q)), \tag{69}$$

as seen in eq. 53.

A.5 Deriving a relationship between *mutual exclusion information* and q for a 4-bit string

Unlike in the 2-bit string case, it is not possible to equate the probability of noise being added to Alice's message to the error probability. This is because more than one PR-box is used, (3 are used) therefore:

$$P_{\text{error}} = -2q^2 + 2q. \tag{70}$$

Then, the same formulas are used as seen for the 2-bit derivation above, so that:

$$H_{excl}(\overline{x_y}|g) = -log_2(-2q^2 + 2q). \tag{71}$$

This results in a exclusion mutual information such that:

$$I_{excl}(\overline{x_y}:g) = -log_2(-2q^2 + 2q) - log_2\frac{1}{2}, \tag{72}$$

which is simplified to:

$$I_{excl}(\overline{x_y}:g) = -log_2(4q(1-q)), \tag{73}$$

as seen in eq. 54.

Appendix B: Possible mappings

This section covers different ways to organise the colours as seen in section 6.2. All these mappings do not affect any of the results, they are simply put in to make a point that there are several combinations that are equally effective in the 'exclusion protocol'.

Red, green	0
Yellow, Blue	1

Table 9: Grouping colours based on the 2nd bit of each of the colours

Red, Blue	0
Yellow, green	1

Table 10: Grouping colours based on adding the 1st bit of each colour to the 2nd bit of each colour, $b_1 \oplus b_2$