

Article

Tsirelson's Bound Prohibits Communication through a Disconnected Channel

Avishy Carmi ^{1,2,*} and Daniel Moskovich ^{1,2,*}

¹ Center for Quantum Information Science and Technology, Ben-Gurion University of the Negev, Beersheba 8410501, Israel

² Faculty of Engineering Sciences, Ben-Gurion University of the Negev, Beersheba 8410501, Israel

* Correspondence: avcarmi@bgu.ac.il (A.C.); dmoskovich@gmail.com (D.M.)

Received: 4 December 2017; Accepted: 24 February 2018; Published: 27 February 2018

Abstract: Why does nature only allow nonlocal correlations up to Tsirelson's bound and not beyond? We construct a channel whose input is statistically independent of its output, but through which communication is nevertheless possible if and only if Tsirelson's bound is violated. This provides a statistical justification for Tsirelson's bound on nonlocal correlations in a bipartite setting.

Keywords: nonlocality; Bell inequality; Tsirelson's bound; no-signaling; information causality; Fisher information

1. Introduction

Some of the predictions made by quantum mechanics appear to be at odds with common sense. Yet quantum mechanics remains the most precisely tested and successful quantitative theory of nature. It is therefore believed that even if quantum mechanics is someday replaced, any successor will have to inherit at least some of its "preposterous" but highly predictive principles. Perhaps the most counter-intuitive quantum mechanical feature is *nonlocality* [1]: the correlations exhibited by remote parties may exceed those allowed by any local realistic model.

The mystery of nonlocality is not only why nature is as nonlocal as it is, but why nature is not *more* nonlocal than it is. There are alternative *Non-Signaling* theories which permit nonlocality beyond the quantum limit [2,3]; why doesn't nature choose one of these theories over quantum mechanics? In Section 1.1 we review several previously proposed explanations. This paper presents another explanation, from statistics.

In this paper we construct a protocol (a repeated oblivious transfer) which sends messages through a disconnected channel. We show that Alice can communicate nontrivial information to Bob via this protocol if and only if the maximal quantum mechanical violation of the Bell-CHSH inequality [1,4], *Tsirelson's bound* [5], is exceeded. We thus provide a statistical explanation of this bound that is independent of the mathematical formalism of quantum mechanics.

We briefly recall the setting for the Bell-CHSH experiment. Section 2 provides a more detailed account. A famous application of nonlocality is to construct an 1-2 *oblivious transfer protocol* between two distant agents (A)lice and (B)ob. Alice and Bob each hold a box. Alice's box might, for example, contain one half of a singlet state of spin- $\frac{1}{2}$ particles, with Bob's box containing the other half [1,4]. In addition, Alice possesses a pair of bits x_0 and x_1 , each of which is a zero or a one. Using boolean algebra and her boxes (the protocol will be described later), Alice encodes her pair of bits into a single bit $x^{(1)}$ which she sends across a classical channel to Bob. Bob wants to know the value either of x_0 or of x_1 , but Alice doesn't know which of these Bob wants to know. Bob uses the received bit $x^{(1)}$, his box, and some boolean algebra to construct an estimate y_i for his desired bit x_i . See Figure 2 later on.

What is the probability that Bob correctly estimates the bit he wishes to know? He has two possible sources of knowledge—the bit $x^{(1)}$ he received from Alice, and some mysterious "nonlocal"

correlation between his box and Alice's. The strength of such a nonlocal coordination between two systems is captured by a parameter $c \in [-1, 1]$ called the *Bell–CHSH correlator*. Bob's probability of guessing the value of Alice's bit correctly is $(1 + |c|)/2$. The *Bell–CHSH inequality* states that $|c| \leq 1/2$ in a world governed by classical (non-quantum) mechanics [1,4]. *Nonlocality* is the state of affairs in which the Bell–CHSH inequality is violated. To the best of our knowledge, real world physics is nonlocal. Over the years, the violation of the Bell–CHSH inequality has been measured in increasingly accurate and loophole-free experiments, culminating in celebrated loophole-free verifications [6–8].

Thus, we know that $|c|$ can exceed $1/2$. How large can $|c|$ be? Tsirelson's bound tells us that $|c|$ cannot exceed $1/\sqrt{2}$ in a world described by quantum mechanics [5]. This quantum bound on nonlocality:

$$|c| \leq \frac{1}{\sqrt{2}}, \quad (1)$$

has been tested experimentally, with the current state of the art being an experiment which has achieved a value of c which is only 0.00084 ± 0.00051 distant from Tsirelson's bound [9]. Such experimental evidence supports the contention that Tsirelson's bound indeed holds true in the real world. Tsirelson's result as presented in the original paper is a specifically quantum mechanical fact, following from the Hilbert-space mathematical formalism for quantum mechanics, for which there has been no good conceptual physical explanation. How fundamental is Tsirelson's bound? Must this inequality also hold for any future theory which might someday supersede quantum mechanics [10]? We are led to the following question: *Can we identify a plausible physical principle, independent of quantum mechanics (or independent of functional analysis), which is necessary and sufficient to guarantee that $|c| \leq 1/\sqrt{2}$?*

1.1. Existing Principles

For the last two decades, people have searched for physical principles that bound nonlocality. It was initially expected that the physical principle of relativistic causality (no-signaling) itself restricts the strength of nonlocality [11–13]. But then it was discovered that no-signaling theories may exist for which $|c| > 1/\sqrt{2}$. This led to the device-independent formalism of *No-Signaling (NS)–boxes* [2,14] (see also [3]). In particular, maximum violation of the Bell–CHSH inequality is achieved by *Popescu–Rohrlich (PR)–boxes* which are consistent with relativistic causality.

So relativistic causality doesn't limit nonlocality after all; Why then does nature not permit (1) to be violated (as far as we know)? Several suggestions have been made. Superquantum correlations lead to violations of the Heisenberg uncertainty principle [15,16], which is another seemingly purely quantum result. PR–boxes would allow distributed computation to be performed with only one bit of communication [17], which looks unlikely but doesn't violate any known physical law. Similarly, in stronger-than-quantum nonlocal theories some computations exceed reasonable performance limits [18]. The principle of *Information Causality* [19] shows that no sensible measure of mutual information exists between pairs of systems in superquantum nonlocal theories. Our approach is most directly comparable with Information Causality, with a conceptual difference being that we use variance of an efficient estimator, therefore Fisher information, whereas information causality uses mutual information (Shannon information). The relationship between our approach and theirs is the topic of Section 6. Finally, it was shown that superquantum nonlocality does not permit local (non-nonlocal) physics to emerge in the limit of infinitely many microscopic systems [20,21].

1.2. Tsirelson's Bound from a Statistical No-Signaling Condition

Here we show that Tsirelson's bound follows from the following principle applied to a certain limiting Bell–CHSH setting:

Statistical No-Signaling: It is impossible to communicate a nontrivial message through a channel whose output is independent of its input.

Our strategy is to construct a channel whose input is a Bernoulli random variable X of mean θ and whose output is another Bernoulli random variable Y (Section 3.2). The construction of our channel is not new—it is a reinterpretation of the well-known van Dam protocol [17]. Through the channel, Alice sends 2^n samples $\mathcal{A} \stackrel{\text{def}}{=} \{x_0, x_1, \dots, x_{2^n-1}\}$ from X , and at the other end Bob receives a set of values $\mathcal{B} \stackrel{\text{def}}{=} \{y_0, y_1, \dots, y_{m-1}\}$.

We imagine $\theta \in [-1, 1]$ as encoding a message, perhaps in the digits of its binary expansion. Bob’s task is to estimate θ . The following theorem states that he can do so if and only if Tsirelson’s bound fails.

Theorem 1.1.

1. The channel from X to Y we construct is described by the conditional probability $p(Y = x \mid X = x) = (1 + c^n)/2$, where c is the Bell–CHSH correlator. Its output satisfies:

$$p(Y = 1 \mid \theta) = \frac{1}{2} + \frac{c^n \cdot \theta}{2} .$$

In the $n \rightarrow \infty$ limit it disconnects for $p(Y \mid X) = p(Y)$ (i.e. we can arrange that $c < 1$).

2. The unbiased estimator:

$$\hat{\theta} \stackrel{\text{def}}{=} \frac{1}{2^n c^n} \sum_{i=0}^{2^n-1} y_i ,$$

for θ has variance:

$$\text{Var} [\hat{\theta} \mid \theta] = \lim_{n \rightarrow \infty} \frac{1 - c^{2n} \theta^2}{(2c^2)^n} = \begin{cases} 0, & 2c^2 > 1 \text{ (signaling)} \\ 1, & 2c^2 = 1 \text{ (randomness)} \\ \infty, & 2c^2 < 1 \text{ (no-signaling)} \end{cases}$$

3. The estimator $\hat{\theta}$ is efficient, i.e. it has the minimal variance of any estimator of θ constructed from Bob’s set of samples \mathcal{B} for all $n \in \mathbb{N}$.

The theorem is visually summarized by Figure 1.

The theorem shows that failure of Tsirelson’s bound leads to failure of the following consequence of Statistical No-Signaling—Consequence of Statistical No-Signaling—In the above notation, if X and Y are independent, then no estimator constructed from \mathcal{B} has both mean θ and variance 0.

Section 5 shows that a violation of Uffink’s inequality [22], a generalization of Tsirelson’s bound, also leads to the failure of the same consequence of Statistical No-Signaling. Uffink’s inequality is also known to be recovered by Information Causality [23].

Theorem 1.1 is formulated as an asymptotic construction, but in practice a finite number of samples suffices because for any experimental setup there exists a nonzero minimal possible environmental noise level $\epsilon > 0$. By Theorem 1.1, $p(Y = 1 \mid \theta)$ is physically indistinguishable from $1/2$ when the absolute value of $c^n \theta / 2$ is less than ϵ . Since $|\theta| \leq 1$, we need $n \geq \ln 2\epsilon / \ln c$ trials. As an example, for a photon pair where ϵ is greater than or equal to the reduced Planck constant \hbar , we find that $n \geq 244$ suffices to make $p(Y = 1 \mid \theta)$ physically indistinguishable from $1/2$ when $|c| \leq 1/\sqrt{2}$. Thus, if we can still distinguish $p(Y = 1 \mid \theta)$ from $1/2$ for $n = 244$, we know that Tsirelson’s bound has been violated, and if not then it holds.

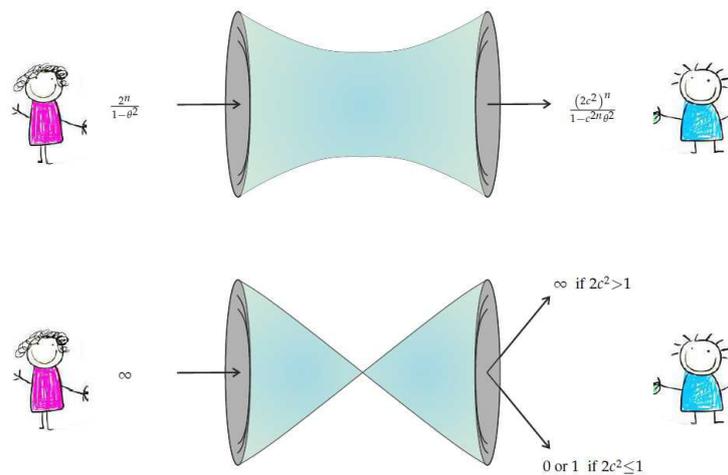


Figure 1. The Statistical No-Signaling condition. The van Dam protocol defines an underlying channel which becomes disconnected in the $n \rightarrow \infty$ limit. The upper illustration shows this channel and the Fisher information (one over the variance) of the maximum likelihood estimators for θ at its input and at its output. When the number of nonlocal resources increases unboundedly, the two ends of the channel become disconnected as illustrated by a vanishing bottleneck in the lower illustration. Statistical No-Signaling dictates that in this case no information can pass through. This occurs if and only if $2c^2 \leq 1$. The case of $2c^2 > 1$ leads to a physically unreasonable limit where Bob can fully read off the value of Alice's θ through a disconnected channel.

1.3. Organization of This Paper

Section 2 recalls the bipartite Bell experiment and exhibits the Bell–CHSH correlator c as the correlator of a certain noisy symmetric channel. Section 3 presents the van Dam protocol as an extension of the Bell–CHSH setup, and explain how it defines a noisy symmetric channel with correlator c^n . Section 4 computes the means and variance of an estimator $\hat{\theta}$ for θ , and proves that $\hat{\theta}$ is an efficient estimator. Section 5 extends Theorem 1.1 to recover Uffink's inequality [22,23] for anisotropic correlators from Statistical No-Signaling. Finally, Section 6 discusses the relationship of Statistical No-Signaling with Information Causality.

2. The Bipartite Bell Experiment as a Noisy Symmetric Channel

In this section we recall the definition of the Bell–CHSH correlator c and we formulate the Bell–CHSH inequality, establishing notation. We then exhibit c as the correlator of a symmetric binary channel.

2.1. The Bell–CHSH Inequality

Let us recall the classical bipartite Bell experiment [1]. Alice and Bob each hold one half of an EPR pair (a pair of particles with certain properties summarized below) such as a singlet state of spin- $\frac{1}{2}$ particles. They each possess two different measuring instruments. Alice measures her particle using one of the instruments, and Bob measures his particles using one of his. We write i for the index of the instrument used by Alice, and a for its reading. Similarly, we let j and b denote the index of an instrument chosen by Bob and its reading correspondingly. In the language of probability, a and b are ± 1 -valued Bernoulli random variables. The choices of measuring instrument, i and j , may be either parameters or 0/1-valued Bernoulli random variables.

Repeating the experiment for many different EPR pairs, Alice and Bob may compute the two-point correlator $E[ab | i, j]$ of their readings a and b for any given pair of indices i and j , where $E[\cdot]$ is the statistical expectation operator. We now define the *Bell–CHSH correlator* c by the formula:

$$c \stackrel{\text{def}}{=} \frac{1}{4} \left\{ E[ab | 0,0] + E[ab | 0,1] + E[ab | 1,0] - E[ab | 1,1] \right\} . \quad (2)$$

In a theory in which both Alice and Bob's choices, and the readings of their measuring devices, are *local*, the Bell–CHSH inequality [4] holds:

$$|c| \leq \frac{1}{2} . \quad (3)$$

Operationally speaking, locality means that Alice's readings may only be affected by her own choices (and perhaps by other variables hidden locally at her site), and similarly for Bob's readings. Quantum mechanically, however, Alice and Bob may violate (3). Correlators violating (3) are said to be *nonlocal*.

2.2. The Bell–CHSH Correlator c as a Channel Correlator

Non-signaling (NS)–boxes provide an abstraction and an extension of the Bell–CHSH experiment [2,14]. This time, Alice and Bob each owns a box. Such a box may be thought of as a complete laboratory containing two measuring devices. Either participant inserts their choice of measuring device into their box. The box output is the respective reading of the chosen measuring device.

Alice and Bob share a pair of NS–boxes whose 0/1–valued inputs are i and j and whose ± 1 –valued outputs are Bernoulli random variables a and b . We will show that the Bell–CHSH correlator (2) represents the correlator of a symmetric binary channel whose input is the Bernoulli random variable $X \stackrel{\text{def}}{=} (-1)^{ij}$ and whose output is the Bernoulli random variable $Y \stackrel{\text{def}}{=} a \cdot b$.

Let $x \in \{-1, 1\}$. Define the *channel correlators* c_x as follows:

$$c_x \stackrel{\text{def}}{=} E[XY | X = x] = p(Y = x | X = x) - p(Y \neq x | X = x) = 2p(Y = x | X = x) - 1 . \quad (4)$$

With respect to a particular choice of measuring devices i and j and for $x = (-1)^{ij}$, (4) becomes:

$$c_x(i, j) = E[a \cdot b \cdot (-1)^{ij} | i, j] = 2p(a \cdot b = (-1)^{ij} | i, j) - 1 . \quad (5)$$

Assume the underlying channel is symmetric and therefore that $c_x(i, j)$ is fixed for all i, j . By (5) the Bell–CHSH correlator (2) may be written as:

$$c = \frac{1}{4} (c_1(0,0) + c_1(0,1) + c_1(1,0) + c_{-1}(1,1)) = c_x(i, j) = 2p(a \cdot b = ij | i, j) - 1 . \quad (6)$$

which is our promised interpretation of the Bell–CHSH correlator as a correlator of a noisy symmetric binary channel.

3. The Van Dam Protocol as a Noisy Symmetric Channel

In this section we recall the construction of the van-Dam protocol [17,19]. We then reinterpret this protocol as underlying a noisy symmetric binary channel, as a special case of the construction of Section 2. We compute its correlator, and establish the effect of noise on its classical component.

3.1. The Van Dam Protocol

The van Dam protocol realizes an *oblivious transfer protocol* by means of a classical channel and a collection of NS-boxes. Each of Alice’s boxes has a corresponding box on Bob’s side, and different pairs of boxes are statistically independent. Suppose that Alice has in her possession the bits x_0, \dots, x_{m-1} where $m = 2^n$, $n \geq 1$. Bob wishes to know the value of one of her bits. He may do so by specifying the address of the bit whose value he wishes to know via its binary address $j = j_{n-1}j_{n-2} \dots j_0$. For example, if $n = 2$ then Bob may specify which of the bits x_0 to x_3 he wants by specifying a binary address, 00, 01, 10, or 11. Alice bits and Bob addresses are encoded into the inputs of $2^n - 1$ NS-boxes following a particular protocol which is described next.

Alice uses outputs of boxes and choices of measuring device to determine choices of measuring device for other boxes. Such a procedure is called *wiring*. The wiring of boxes on Alice side admits a recursive description which we now give. Let $a_i^{k,l}$ denote the output of Alice’s l th box on the k th level for the input i . We follow the convention that box outputs for the van Dam protocol are 0/1-valued (rather than ± 1 -valued) random variables. Let also:

$$f^{k,l}(q_1, q_2) \stackrel{\text{def}}{=} q_1 \oplus a_{q_1 \oplus q_2}^{k,l} . \tag{7}$$

Suppose that Alice wishes to encode $m = 4$ bits with her boxes. To do so, she first picks two boxes and computes:

$$x_1^{(1)} \stackrel{\text{def}}{=} f^{1,1}(x_0, x_1), \quad x_2^{(1)} \stackrel{\text{def}}{=} f^{1,2}(x_2, x_3) . \tag{8}$$

This forms the first level in her construction. The second level then follows:

$$x^{(2)} \stackrel{\text{def}}{=} f^{2,1}(x_1^{(1)}, x_2^{(1)}) . \tag{9}$$

In this example there are only two levels and so $x^{(2)}$ is the bit which Alice transmits to Bob through the classical channel. In case where $m = 2^n$ there will be n levels and thus $x^{(n)}$ is the bit Bob will receive from Alice.

Unbeknownst to Alice, Bob now decides which bit x_j he would like to know the value of. He takes its binary address $j = j_{n-1}j_{n-2} \dots j_0$, and inserts j_{k-1} into all of his boxes whose counterparts are on the k level on Alice’s side. He then uses the values $b_{j_{k-1}}^{k,l}$ that he obtains, together with the bit $x^{(n)}$ he received from Alice, to construct the decoding function:

$$y_j \stackrel{\text{def}}{=} x^{(n)} \oplus b_{j_0}^{1,l_1} \oplus b_{j_1}^{2,l_2} \oplus \dots \oplus b_{j_{n-1}}^{n,l_n} . \tag{10}$$

The values l_1, \dots, l_n (which boxes Bob uses) are determined by the binary address $j = j_{n-1}j_{n-2} \dots j_0$ via the recursive formula $l_{h-1} = 2l_h - 1 + l_{h-1}$ for $h = 1, 2, \dots, n - 1$ starting from $l_n = 1$.

The van Dam protocol we have described above is summarized in Figure 2.

The probability that Bob will decode the correct value of the bit he desires is governed by the NS-box correlator c . In general, decoding any bit out of 2^n possible bits involves using n pairs of NS boxes. Noting that an even number of errors, $a \oplus b \neq ij$, will cancel out in such a construction, we obtain the following expression [19]:

$$c^n = 2p(y_j = x_j \mid x_j) - 1 . \tag{11}$$

For example, for $n = 2$:

$$\begin{aligned}
 p(a_{i_1} \oplus b_{j_1} \oplus a_{j_2} \oplus b_{j_2} = i_1 j_1 \oplus i_2 j_2 \mid i_{1,2}, j_{1,2}, i_1 j_1 \oplus i_2 j_2) = \\
 p(a_{i_1} \oplus b_{j_1} = i_1 j_1 \mid a_1, b_1) p(a_{i_2} \oplus b_{j_2} = i_2 j_2 \mid i_2, j_2) + \\
 p(a_{i_1} \oplus b_{j_1} \neq i_1 j_1 \mid i_1, j_1) p(a_{i_2} \oplus b_{j_2} \neq i_2 j_2 \mid i_2, j_2) = \\
 \frac{1}{2}(1+c) \cdot \frac{1}{2}(1+c) + \frac{1}{2}(1-c) \cdot \frac{1}{2}(1-c) = \frac{1}{2}(1+c^2) . \quad (12)
 \end{aligned}$$

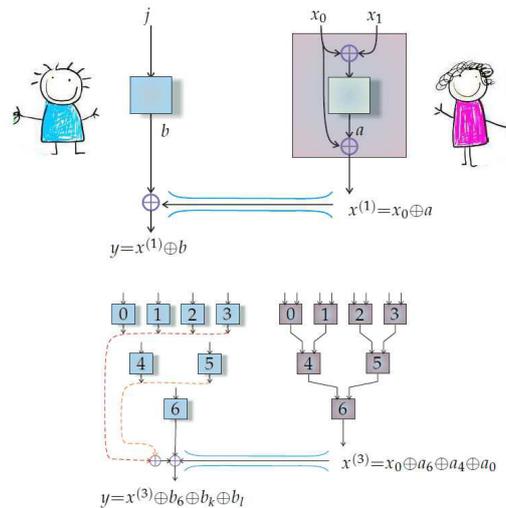


Figure 2. Distributed oblivious transfer (van Dam) protocol [17]. Its basic building block is on the left, where Alice inserts $x_0 \oplus x_1$ into her box, receives a , and sends $x_0 \oplus a$ to Bob. Bob decides that he wants to know the value of x_j , and he feeds j into his box, which outputs b . Bob’s estimate of x_i is then $x^{(1)} \oplus b$. When there are multiple boxes, Alice concatenates (the process is called *wiring*). For example, with seven boxes, Alice begins with a collection of bits x_0, x_1, \dots, x_7 , and she inputs $x_{2i} \oplus x_{2i+1}$ into box i , where $i = 0, 1, 2, 3$, receiving a_0, a_1, a_2, a_3 correspondingly. The bits fed into the next level of boxes become $x_i^{(1)} \stackrel{\text{def}}{=} x_{2i} \oplus a_i$ with $i = 0, 1, 2, 3$. The final output $x^{(3)}$ is sent to Bob. Bob encodes the address of the bit he wants as the binary number $j_3 j_2 j_1$ —for example, if he wants x_2 , then he sets $j_3 = 0, j_2 = 1$, and $j_1 = 0$ because 10 is 2 in binary. This binary encoding describes a path in his binary tree from a root to a branch, where 0 means ‘go left’ and 1 means ‘go right’. Bob inserts j_3 into the lowermost box to obtain b_6 . Setting $k \stackrel{\text{def}}{=} 5 - (1 - j_3)$, he then inserts j_2 into box k to obtain b_k . Finally, setting $l \stackrel{\text{def}}{=} k - (3 - j_3) - (1 - j_2)$, Bob inserts j_1 into box l to obtain B_l . His final estimate for x_j is $y_j = x^{(3)} \oplus b_6 \oplus b_k \oplus b_l$.

3.2. Van Dam Protocol as a Symmetric Channel

This section describes the modification of the van Dam protocol that we use.

Alice has in her possession an information source that is a ± 1 -valued Bernoulli random variable X whose mean is θ . Alice takes m iid samples, $\tilde{x}_0, \dots, \tilde{x}_{m-1}$, from X and converts them into 0/1-valued bits, x_0, x_1, \dots, x_{m-1} by mapping 0 to -1 and 1 to 1. Alice and Bob repeat the van Dam protocol m times, once for each of Alice’s samples. Each time, Bob uses the protocol to estimate Alice’s bit, first x_0 , then x_1 , and so on until x_{m-1} .

As in (12), the van Dam protocol has a *memoryless* property:

$$p(y_i = x_i \mid x_0, x_1, \dots, x_{m-1}) = p(y_i = x_i \mid x_i) . \quad (13)$$

From this it follows that if Alice’s inputs x_0, x_1, \dots, x_{m-1} are iid then Bob’s outputs y_0, y_1, \dots, y_{m-1} are also iid. Therefore the set of $\tilde{y}_i \stackrel{\text{def}}{=} (-1)^{y_i}$ determines a Bernoulli random variable Y . In this way, the van Dam protocol may be viewed as a symmetric binary channel whose input is X and whose output is Y . By (11) the channel correlator is:

$$E [XY | X = \tilde{x}_i] = 2p(Y = \tilde{x}_i | X = \tilde{x}_i) - 1 = 2p(y_i = x_i | x_i) - 1 = c^n . \tag{14}$$

We generalize slightly, for the purpose of treating the $|c| = 1$ case in the next section. Suppose that Alice’s bits are contaminated with noise and therefore might be flipped once injected into her boxes. Let $[1 - (c')^n]/2$ be the probability that the bit x_i is flipped where $|c'| \leq 1$. In this case the corresponding channel correlator (14) is $E [XY | X = \tilde{x}_i] = (cc')^n$, which follows from (4) and:

$$p(Y = \tilde{x}_i | X = \tilde{x}_i) = p(Y = \tilde{x}_i | X' = \tilde{x}_i)p(X' = \tilde{x}_i | X = \tilde{x}_i) + p(Y = \tilde{x}_i | X' \neq \tilde{x}_i)p(X' \neq \tilde{x}_i | X = \tilde{x}_i) = \frac{1}{2}[1 + (cc')^n] , \tag{15}$$

where $p(Y = \tilde{x}_i | X' = \tilde{x}_i) = [1 + c^n]/2$ underlies the channel defined by the ordinary van Dam protocol, and $p(X' \neq \tilde{x}_i | X = \tilde{x}_i) = [1 - (c')^n]/2$ is the probability of x_i having been flipped.

3.3. The Van Dam Channel Disconnects in the $n \rightarrow \infty$ Limit

If $|c| < 1$ or $|c'| < 1$ then it follows that:

$$E[XY] = 2p(Y = i | X = i) - 1 = (cc')^n \xrightarrow{n \rightarrow \infty} 0 . \tag{16}$$

Therefore, in the $n \rightarrow \infty$ limit:

$$p(Y = i | X = i) = 1/2 . \tag{17}$$

But also:

$$p(Y = i) = p(Y = i | X = i)p(X = i) + p(Y = i | X \neq i)p(X \neq i) = \frac{1}{2}(p(X = i) + p(X \neq i)) = \frac{1}{2} . \tag{18}$$

Combining (17) with (18) gives:

$$p(Y | X) \xrightarrow{n \rightarrow \infty} p(Y) . \tag{19}$$

Thus X and Y are statistically independent in the $n \rightarrow \infty$ limit, proving the first part of Theorem 1.1.

4. Bob’s Estimator

4.1. Bob’s Estimator

In Section 3 we used the van Dam protocol to construct a symmetric channel whose input is a ± 1 -valued Bernoulli random variable X and whose output is another ± 1 -valued Bernoulli random variable Y . The channel correlator is c^n .

Alice sends m iid random samples $\mathcal{X} \stackrel{\text{def}}{=} \{X_1, \dots, X_m\}$ through the channel. Denote the set of respective outputs $\mathcal{Y} \stackrel{\text{def}}{=} \{Y_1, \dots, Y_m\}$. Assume a prior distribution for X given by:

$$p(X = -1 | \theta) = \frac{1}{2}(1 + \theta) , \tag{20}$$

with parameter $\theta \in [-1, 1]$.

Bob attempts to estimate θ using the estimator:

$$\hat{\theta} \stackrel{\text{def}}{=} \frac{1}{2^n c^n} \sum_{i=0}^{2^n-1} Y_i . \quad (21)$$

We will show that Bob's estimator is unbiased, $E[\hat{\theta} | \theta] = \theta$. Note that

$$E[Y_i | \theta] = p(Y = 1 | \theta) - p(Y = -1 | \theta) . \quad (22)$$

and

$$p(Y = -1 | \theta) = p(Y = -1 | X = -1)p(X = -1 | \theta) + p(Y = -1 | X = 1)p(X = 1 | \theta) = \frac{1+c^n\theta}{2} . \quad (23)$$

From (22) and (23) together, deduce:

$$E[Y_i | \theta] = c^n \theta . \quad (24)$$

and therefore, $E[\hat{\theta} | \theta] = \theta$.

As for variance, by (24):

$$\text{Var}[Y_i | \theta] = E[Y_i^2 | \theta] - E[Y_i | \theta]^2 = 1 - c^{2n} \theta^2 . \quad (25)$$

Therefore:

$$\text{Var}[\hat{\theta} | \theta] = \frac{1 - c^{2n} \theta^2}{(2c^2)^n} . \quad (26)$$

We have proved the second part of Theorem 1.1.

4.2. Bob's Estimator $\hat{\theta}$ is Efficient

We prove efficiency of $\hat{\theta}$ by calculating the Fisher information about θ contained in Bob's set of samples \mathcal{B} . The Cramer–Rao Theorem tells us that one over this Fisher information is a lower bound for the variance of an estimator for θ constructed from \mathcal{B} . By showing that $\hat{\theta}$ saturates this bound, we will have proven that it is efficient. In the derivation that follows, we assume that $|c| < 1$ by replacing c by cc' if necessary.

We compute the Fisher information. The *likelihood* of θ given the set \mathcal{B} is given by the expression:

$$p(\mathcal{B} | \theta) = \left[p(Y = -1 | \theta) \right]^{\sum_{i=1}^{2^n} \mathbf{1}_{\{Y_i=-1\}}} \left[p(Y = 1 | \theta) \right]^{\sum_{i=1}^{2^n} \mathbf{1}_{\{Y_i=1\}}} , \quad (27)$$

where the *indicator* random variable of a random event A is given as:

$$\mathbf{1}_A \stackrel{\text{def}}{=} \begin{cases} 1, & A \text{ occurred;} \\ 0, & \text{otherwise.} \end{cases} \quad (28)$$

According to (27) the log-likelihood is given by the expression:

$$\mathcal{L}(\theta) \stackrel{\text{def}}{=} \log p(\mathcal{B} | \theta) = \left[\sum_{i=1}^{2^n} \mathbf{1}_{\{Y_i=-1\}} \right] \log p(Y = -1 | \theta) + \left[\sum_{i=1}^{2^n} \mathbf{1}_{\{Y_i=1\}} \right] \log p(Y = 1 | \theta) . \quad (29)$$

The Fisher information about θ contained in the set \mathcal{B} is defined as:

$$\mathcal{I}_{\mathcal{B}}(\theta) \stackrel{\text{def}}{=} E \left[\left(\frac{\partial \mathcal{L}(\theta)}{\partial \theta} \right)^2 \right] = -E \left[\frac{\partial^2 \mathcal{L}(\theta)}{\partial \theta^2} \right]. \tag{30}$$

Note that:

$$E \left[\sum_{i=1}^{2^n} \mathbf{1}_{\{Y_i=s\}} \right] = \sum_{i=1}^{2^n} E \left[\mathbf{1}_{\{Y_i=s\}} \right] = 2^n p(Y = s | \theta), \quad s = -1, 1. \tag{31}$$

Using this, (30) reads:

$$\mathcal{I}_{\mathcal{B}}(\theta) = \frac{(2c^2)^n}{1 - c^{2n}\theta^2}. \tag{32}$$

Indeed the Fisher information about θ in \mathcal{B} as given by Equation (32) equals one over the variance of $\hat{\theta}$ as given by Equation (26). Thus, by the Cramer–Rao Theorem, $\hat{\theta}$ is an efficient estimator for θ . Parenthetically, note that the minimum of $\mathcal{I}_{\mathcal{B}}(\theta)$ is obtained for $\theta = 0$ in which case $p(X | \theta) = 1/2$ and $\mathcal{I}_{\mathcal{B}}(0) = (2c^2)^n$. We have proved the final part of Theorem 1.1.

5. Uffink’s Inequality from Statistical No-Signalling

The basic protocol in Section 3 assumes all box correlators are identical in absolute value. When this assumption is relaxed, Statistical No-Signaling leads to Uffink’s inequality, which is a necessary condition for quantum mechanical Bell-CHSH correlators [22,23]. Our approach is based on evaluating the total Fisher information $\mathcal{I}_{\mathcal{B}}(\theta)$ gained by Bob in 2^n trials of the experiment.

Suppose that the mean of Alice’s bits, x_i , is θ' for even i , and θ otherwise. Consider now a pair of NS-boxes with correlators, $c(i, j) \stackrel{\text{def}}{=} E[ab | i, j]$. The channel underlying the van Dam protocol in this case is described by

$$p(y_j = x_j | x_0, x_1) = p(a \oplus b = ij | j, i = x_0 \oplus x_1) = [1 + c(x_0 \oplus x_1, j)] / 2, \tag{33}$$

where y_j is Bob’s guess of Alice’s bit x_j . It now follows that

$$\begin{aligned} p(y_j = 1 | \theta', \theta) = & \\ p(y_j = x_j | x_j = 1, x_{1-j} = 1) & p(x_j = 1)p(x_{1-j} = 1) + p(y_j \neq x_j | x_j = 0, x_{1-j} = 0)p(x_j = 0)p(x_{1-j} = 0) + \\ p(y_j = x_j | x_j = 1, x_{1-j} = 0) & p(x_j = 1)p(x_{1-j} = 0) + p(y_j \neq x_j | x_j = 0, x_{1-j} = 1)p(x_j = 0)p(x_{1-j} = 1) = \\ \frac{1}{2} \left[1 + \frac{1}{2}(c(0, j) + (-1)^j c(1, j))\theta' + \frac{1}{2}(c(0, j) - (-1)^j c(1, j))\theta \right]. & \end{aligned} \tag{34}$$

For simplicity, assume that $\theta' = 0$. It can now be verified that for a n -level construction in the van Dam protocol

$$p(y_{j_1, \dots, j_n} = 1 | \theta) = \frac{1}{2} [1 + c_{j_1} c_{j_2} \dots c_{j_n} \theta], \tag{35}$$

where $c_j \stackrel{\text{def}}{=} (c(0, j) - (-1)^j c(1, j)) / 2$. According to (32) the Fisher information about θ contained in y_{j_1, \dots, j_n} is

$$\mathcal{I}_{j_1, \dots, j_n}(\theta) = \frac{(c_{j_1} \dots c_{j_n})^2}{1 - (c_{j_1} \dots c_{j_n})^2 \theta^2}. \tag{36}$$

Assuming $|c(i, j)| < 1$, Bob’s total amount of information about θ in 2^n trials is

$$\mathcal{I}_{\mathcal{B}}(\theta) = \sum_{j_1=0,1} \dots \sum_{j_n=0,1} \mathcal{I}_{j_1, \dots, j_n}(\theta) \approx \sum_{j_1=0,1} \dots \sum_{j_n=0,1} (c_{j_1} \dots c_{j_n})^2 = [c_0^2 + c_1^2]^n, \tag{37}$$

for large n . As before, the underlying channel asymptotically disconnects for $c_{j_1} \cdots c_{j_n} \rightarrow 0$ in the $n \rightarrow \infty$ limit. Statistical No-Signaling dictates that in this case the variance of Bob's estimator $\lim_{n \rightarrow \infty} \text{Var} [\hat{\theta} | \theta] = \lim_{n \rightarrow \infty} \mathcal{I}_B(\theta)^{-1} \geq 1$, which holds if and only if Uffink's inequality holds [22],

$$c_0^2 + c_1^2 = \frac{1}{4} [c(0,0) - c(1,0)]^2 + \frac{1}{4} [c(0,1) + c(1,1)]^2 \leq 1. \quad (38)$$

6. Relation to Information Causality

Of previous non-quantum justifications of Tsirelson's bound, Information Causality (IC) is perhaps the closest to Statistical No-Signaling [19]. IC is also stated as a limit on communication: *Information gain that Bob can reach about a previously unknown to him data set of Alice, by using all his local resources and m classical bits communicated by Alice, is at most m bits.*

IC is formally a restriction on the classical channel capacity. Detecting violation of this principle therefore requires the utilization of nonlocal resources, which the authors achieve through the application of IC to the van Dam protocol, that is the same communication protocol used in this paper.

The Information Causality quantity I is defined as the Shannon mutual information of Alice's input and Bob's output given the value of the single bit transmitted in the van Dam protocol. IC holds if $I \leq 1$ and is violated if $I > 1$. At the end of the supplementary section of [19], the following expression for the IC quantity is obtained:

$$I \geq \frac{1}{2 \ln(2)} \left(c_1^2 + c_{-1}^2 \right)^n, \quad (39)$$

where $c_i \stackrel{\text{def}}{=} E [XY | X = i]$ as in (4). In the symmetric setting, $c_1 = c_{-1} = c$, and for $\theta = 0$, Equations (39) and (32) combine to yield:

$$I \geq \frac{2^n c^{2n}}{2 \ln(2)} = \frac{[1 - c^{2n} \theta^2] \mathcal{I}_B(\theta)}{2 \ln(2)}. \quad (40)$$

In particular, in the $n \rightarrow \infty$ limit, if $2c^2 > 1$ then $\mathcal{I}_B(\theta) \rightarrow \infty$ implying that $I \rightarrow \infty$. Thus, violation of Statistical No-Signaling implies violation of IC. Conversely, as (39) is an inequality, it is unknown whether Tsirelson's bound being satisfied implies $I \leq 1$ (IC for the van Dam protocol), although, by our main theorem, it does imply $\mathcal{I}_B(\theta) \leq 1$ (Statistical No-Signaling for the van Dam protocol).

7. Conclusions

We have formulated a *Statistical No-Signaling* principle which dictates that no information can pass through a disconnected channel. A violation of Tsirelson's bound, *i.e.* a value of $|c|$ greater than $1/\sqrt{2}$, allows us to violate Statistical No-Signaling by constructing a disconnected channel through which Bob can construct an unbiased estimator with variance 0 for Alice's parameter θ . Conversely, when Tsirelson's bound holds, then, through this channel, so does Statistical No-Signaling. Our construction thus provides a purely statistical justification for Tsirelson's bound, independent of quantum mechanics.

Acknowledgments: The authors thank Daniel Rohrlich for useful discussions. Avishy Carmi acknowledges support from Israel Science Foundation Grant No. 1723/16.

Author Contributions: Avishy Carmi and Daniel Moskovich have both written the text and worked out the mathematical proofs in this paper.

Conflicts of Interest: The authors declare no conflict of interest.

References

- Bell, J.S. On the Einstein-Podolsky-Rosen paradox. *Physics* **1964**, *1*, 195–200.
- Popescu, S.; Rohrlich, D. Quantum nonlocality as an axiom. *Found. Phys.* **1994**, *24*, 379–385.
- Popescu, S. Nonlocality beyond quantum mechanics. *Nature Phys.* **2014**, *10*, 264–270.
- Clauser, J.; Horne, M.; Shimony, A.; Holt, R. Proposed experiment to test local hidden—Variable theories. *Phys. Rev. Lett.* **1969**, *23*, 880–884.
- Cirel'son, B. S. Quantum generalizations of Bell's inequality. *Lett. Math. Phys.* **1980**, *4*, 93–100.
- Giustina, M.; Versteegh, M.A.M.; Wengerowsky, S.; Handsteiner, J.; Hochrainer, A.; Phelan, K.; Steinlechner, F.; Kofler, J.; Larsson, J.-A.; Abellán, C.; et al. Significant-loophole-free test of Bell's theorem with entangled photons. *Phys. Rev. Lett.* **2015**, *115*, 250401.
- Hensen, B.; Bernien, H.; Dréau, A.E.; Reiserer, A.; Kalb, N.; Blok, M.S.; Ruitenbergh, J.; Vermeulen, R.F.L.; Schouten, R.N.; Abellán, C.; et al. Experimental loophole-free violation of a Bell inequality using entangled electron spins separated by 1.3 km. *Nature* **2015**, *526*, 682–686.
- Shalm, L. K.; Meyer-Scott, E.; Christensen, B.G.; Bierhorst, P.; Wayne, M.A.; Stevens, M.J.; Gerrits, T.; Glancy, S.; Hamel, D.R.; Allman, M.S.; et al. Strong loophole-free test of local realism. *Phys. Rev. Lett.* **2015**, *115*, 250402.
- Poh, H.S.; Joshi, S.K.; Céré, A.; Cabello, A.; Kurtsiefer, C. Approaching Tsirelson's bound in a photon pair experiment. *Phys. Rev. Lett.* **2015**, *115*, 180408.
- Seife, C. Do deeper principles underlie quantum uncertainty and nonlocality? *Science* **2005**, *309*, 98.
- Shimony, A. Controllable and Uncontrollable Non-Localities. In *Proceedings of the International Symposium on Foundations of Quantum Mechanics in the Light of New Technology*; Kamefuchi, S., Ed; Physical Society of Japan: Tokyo, Japan, 1984; pp. 225–230.
- Shimony, A. Events and processes in the quantum world. In *Quantum Concepts in Space and Time*; Penrose, R., Isham, C.J., Eds.; Oxford University Press: Oxford, UK, 1986; pp. 182–203.
- Aharonov, Y.; Rohrlich, D. Nonlocality and Causality. In *Quantum Paradoxes: Quantum Theory for the Perplexed*; Wiley-VCH: Weinheim, Germany, 2005.
- Barrett, J.; Linden, N.; Massar, S.; Pironio, S.; Popescu, S.; Roberts, D. Non-local correlations as an information theoretic resource. *Phys. Rev. A* **2005**, *71*, 022101.
- Wolf, M.; Garcia, D.P.; Fernandez, C. Measurements incompatible in quantum theory cannot be measured jointly in any other no-signaling theory. *Phys. Rev. Lett.* **2009**, *103*, 230402.
- Oppenheim, J.; Wehner, S. The uncertainty principle determines the non-locality of quantum mechanics. *Science* **2010**, *330*, 1072–1074.
- van Dam, W. Implausible consequences of superstrong nonlocality. *Nat. Comput.* **2013**, *12*, 9–12.
- Linden, N.; Popescu, S.; Short, A.J.; Winter, A. Quantum nonlocality and beyond: Limits from nonlocal computation. *Phys. Rev. Lett.* **2007**, *99*, 180502.
- Pawlowski, M.; Paterek, T.; Kaszlikowski, D.; Scarani, V.; Winter, A.; Żukowski, M. Information causality as a physical principle. *Nature* **2009**, *461*, 1101–1104.
- Rohrlich, D. PR-box correlations have no classical limit. In *Quantum Theory: A Two-Time Success Story*; Struppa, D.C., Tollaksen, J.M., Eds.; Springer: Berlin/Heidelberg, Germany, 2014; pp. 205–211.
- Navascués, M.; Wunderlich, H. A glance beyond the quantum model. *Proc. R. Soc. A* **2010**, *466*, 881–890.
- Uffink, J. Quadratic Bell inequalities as tests for multipartite entanglement. *Phys. Rev. Lett.* **2002**, *88*, 230406.
- Allcock, J.; Brunner, N.; Pawłowski, M.; Scarani, V. Recovering part of the boundary between quantum and nonquantum correlations from information causality. *Phys. Rev. A* **2009**, *80*, 040103.

