Quantifying the Nonlocality of Greenberger-Horne-Zeilinger Quantum Correlations by a Bounded Communication Simulation Protocol

Cyril Branciard[1] and Nicolas Gisin[2]

[1]*School of Mathematics and Physics, The University of Queensland, St Lucia, QLD 4072, Australia*
[2]*Group of Applied Physics, University of Geneva, 20 rue de l'Ecole-de-Médecine, CH-1211 Geneva 4, Switzerland*

(Received 1 February 2011; published 5 July 2011)

The simulation of quantum correlations with finite nonlocal resources, such as classical communication, gives a natural way to quantify their nonlocality. While multipartite nonlocal correlations appear to be useful resources, very little is known on how to simulate multipartite quantum correlations. We present a protocol that reproduces tripartite Greenberger-Horne-Zeilinger correlations with bounded communication: 3 bits in total turn out to be sufficient to simulate all equatorial Von Neumann measurements on the tripartite Greenberger-Horne-Zeilinger state.

DOI: 10.1103/PhysRevLett.107.020401 PACS numbers: 03.65.Ud, 03.67.Mn

When measurements are performed on several quantum systems in an entangled state, the statistics of the results may contain correlations that cannot be simulated by shared local variables. Such correlations are called nonlocal. They can be identified by their capacity to violate the so-called Bell inequalities [1].

The observation that quantum theory predicts nonlocal correlations goes all the way back to the famous EPR argument [2]. Many experimental confirmations have been demonstrated all over the world during the last two decades of the last century [3]. During the first ten years of this century, the interest for nonlocal correlations has shifted from mere skepticism and incredulity to more constructive questions. First, physicists raised the question of the power of nonlocal correlations for information processing, such as "device-independent" quantum key distribution [4–6] and random number generation [7,8]. Second, theorists realized that quantum correlations, although possibly nonlocal, are never maximally nonlocal, hence the question "why is quantum theory not more nonlocal?" [9]; note the great advances since the original question "Why is quantum theory not local?".

Thirdly, and this is the topic of this Letter, physicists and computer scientists tried to quantify nonlocality; that is, to treat nonlocality as a physical quantity. Indeed, the violation of a Bell inequality only proves that the correlations are not local, but does not tell us anything about how far from local they are. Intuitively, a larger violation should signal more nonlocality. But this naïve approach is insufficient as some correlations may violate different Bell inequalities by different amounts. A quite natural measure of nonlocality is the number of classical bits that need to be communicated from one party to another, in addition to using shared randomness (a local resource), in order to simulate the full statistics of the observed data. For local correlations, no communication is needed, as shared local variables suffice; they thus have a "communication measure" of nonlocality equal to zero, as it should be. Let us stress that the idea is not to imagine that nature uses communication to produce nonlocal correlations, it is only to quantify the amount of nonlocality by the quantity of communication required to simulate the correlation.

That such a measure of nonlocality is natural is testified by the fact that it has been introduced by 3 independent papers [10–12]. More precisely, in this Letter we adopt as a measure the number of bits communicated between all partners in the worst case [10,11]. An alternative could be to count the number of bits sent on average [12,13].

For the case of 2 qubits in a maximally entangled state, Toner and Bacon [14] proved that one single bit of communication suffices (if one restricts the analysis to projective Von Neumann measurements, as we do here). Hence the nonlocality of the singlet state is 1 bit. For the general case of 2 qubits in a partially entangled state it is known that 2 bits of communication are enough [14], though it is still unproven that 1 bit is not sufficient. At first, one may think that the nonlocality of a partially entangled state should not be larger than that of maximally entangled states, but this is not so clear once one realizes the difficulty of simulating at the same time the nonlocal correlation and the nontrivial marginal probabilities [15,16].

GHZ correlations.—In this Letter we consider 3-qubit Greenberger-Horne-Zeilinger (GHZ) quantum correlations and present the first known protocol to simulate such nonlocal correlations with bounded communication. This problem is the straightforward next step after the 2-qubit case; it attracted the attention of most of the specialists. After years of unsuccessful efforts, the feeling started to spread that it might be impossible with finite communication [17]. Some hope, however, appeared when Bancal *et al.* [18] presented a protocol with unbounded, but finite average communication. Moreover, a team recently presented a nonconstructive existence proof of a protocol with 6 bits of communication [19]; the proof turned out to be flawed, but the impulse was given!

More precisely, our goal is to simulate the quantum correlations obtained by performing equatorial

Von Neumann measurements on a tripartite GHZ state. Namely: 3 parties, Alice, Bob and Charlie, each receive an input angle ϕ_A, ϕ_B and $\phi_C \in [0, 2\pi]$ (corresponding to a measurement setting on the equator of the Bloch sphere $\mathcal{S}^2$), and they must output binary outcomes α, β, $\gamma \in \{+1, -1\}$, such that the expectation values satisfy

$$\langle \alpha\beta\gamma \rangle = \cos(\phi_A + \phi_B + \phi_C), \tag{1}$$

while all single- and bipartite marginals vanish. Note that although the choice of equatorial measurements is restrictive, these are enough to come up with the "GHZ paradox" [20]. We will show that our problem can be solved with finite communication. For that, we first introduce a protocol that provides "stronger" correlations, before showing how to adequately transform these and obtain the desired cosine correlations.

Simulation with classical communication.—Consider the following protocol, that uses 3 bits of communication: 2 from Bob to Alice, and 1 from Charlie to Alice. The sign function is defined as $\text{sgn}(x) = +1$ if $x \geq 0$, $\text{sgn}(x) = -1$ if $x < 0$.

Protocol 1.—Let Alice and Bob share two random vectors $\vec{\lambda}_1$ and $\vec{\lambda}_2$, uniformly distributed on the sphere $\mathcal{S}^2$, together with a random bit $\xi \in \{0, 1\}$; let Alice and Charlie share a random variable φ_c, uniformly distributed on $[0, 2\pi]$. After reception of their measurement settings ϕ_A, ϕ_B and ϕ_C, the three parties proceed as follows: (a) Bob defines $\hat{b}$ to be the equatorial vector with azimuthal angle $\frac{\pi}{2} - 2\phi_B$; he calculates $\sigma_0 = \text{sgn}(\hat{b} \cdot \vec{\lambda}_1)\text{sgn}(\hat{b} \cdot \vec{\lambda}_2)$, and sends the bit $\tau_0 = \frac{1-\sigma_0}{2}$ to Alice. Alice and Bob can then both determine the azimuthal angle $\varphi_0 \in [0, 2\pi]$ of $\vec{\lambda}_0 = \vec{\lambda}_1 + (-1)^{\tau_0}\vec{\lambda}_2$; they calculate $\varphi_b = \frac{\varphi_0}{2} + \xi\pi \in [0, 2\pi]$. (b) Alice, Bob, and Charlie define $\tilde{\phi}_A = \phi_A - \varphi_b - \varphi_c$, $\tilde{\phi}_B = \phi_B + \varphi_b$ and $\tilde{\phi}_C = \phi_C + \varphi_c$, respectively. (c) Bob calculates $\sigma_b = \text{sgn}(\sin 2\tilde{\phi}_B)$, and sends $\tau_b = \frac{1-\sigma_b}{2}$ to Alice; he outputs $\beta = \text{sgn}(\sin\tilde{\phi}_B)$. Similarly, Charlie calculates $\sigma_c = \text{sgn}(\sin 2\tilde{\phi}_C)$, and sends $\tau_c = \frac{1-\sigma_c}{2}$ to Alice; he outputs $\gamma = \text{sgn}(\sin\tilde{\phi}_C)$. (d) Alice outputs $\alpha = \text{sgn}[\sin(-\tilde{\phi}_A - \tau_b\frac{\pi}{2} - \tau_c\frac{\pi}{2})]$.

Before analyzing the correlation given by Protocol 1, let us give an intuitive understanding of it. Forget for now the rather technical step (a) [21], and note that after step (b), one has $\tilde{\phi}_A + \tilde{\phi}_B + \tilde{\phi}_C = \phi_A + \phi_B + \phi_C$; the first two steps will ensure that the final tripartite correlation depends on the sum $\phi = \phi_A + \phi_B + \phi_C$ only, and that all marginals vanish. Assume now that $\tilde{\phi}_B, \tilde{\phi}_C \in [0, \pi]$ (and hence $\beta = \gamma = +1$); if this is not the case, Bob and Charlie can locally subtract π to $\tilde{\phi}_B$ or $\tilde{\phi}_C$ and flip their output, so that the correlation $E(\phi) = \langle\alpha\beta\gamma\rangle$ is unchanged—this is precisely why we ask them to output $\beta = \text{sgn}(\sin\tilde{\phi}_B)$ and $\gamma = \text{sgn}(\sin\tilde{\phi}_C)$. In step (c), Bob and Charlie tell Alice in which quadrant ($[0, \frac{\pi}{2}]$ or $[\frac{\pi}{2}, \pi]$) their angles $\tilde{\phi}_B$ and $\tilde{\phi}_C$ are. From this information, Alice knows in which half-circle $\tilde{\phi}_B + \tilde{\phi}_C$ is (more precisely, she knows $\text{sgn}[\sin(\tilde{\phi}_B + \tilde{\phi}_C)]$ or $\text{sgn}[\cos(\tilde{\phi}_B + \tilde{\phi}_C)]$, depending on whether $\tau_b = \tau_c$ or $\tau_b \neq \tau_c$); if $-\tilde{\phi}_A$ is in the same half-circle, she wants to obtain a good correlation with $\beta\gamma = +1$ (if by chance $-\tilde{\phi}_A = \tilde{\phi}_B + \tilde{\phi}_C$, she wants a perfect correlation), and will thus output $\alpha = +1$; otherwise, she will output $\alpha = -1$; this corresponds precisely to step (d).

As shown in [22], Protocol 1 gives vanishing marginals, and the following tripartite correlation $E_1(\phi) := \langle\alpha\beta\gamma\rangle$:

$$\begin{aligned} E_1(\phi) &= \frac{32}{\pi^2}\sum_{n\geq 0}\frac{1}{(2n+1)^2}\,\frac{1}{4-(2n+1)^2}\cos[(2n+1)\phi] \\ &= 1 - \frac{2\phi - \sin 2\phi}{\pi} \quad \text{for } \phi \in [0, \pi]. \end{aligned} \tag{2}$$

$E_1(\phi)$ is shown in Fig. 1. One can notice that it is stronger than the desired $\cos\phi$ correlation, in the sense that $|E_1(\phi)| \geq |\cos\phi|$ for all ϕ. Intuitively, one should be able to add some noise and weaken the correlation; this is however not trivial, since this weakening must depend on ϕ and should, in particular, not weaken the extreme correlations for $\phi = 0$ and π. Starting from a 2π-periodic correlation function such that $E(0) = -E(\pi) = 1$, one can nonetheless try to mix correlations of the form $E((2m+1)\phi)$, with $m \in Z$, as this will preserve the perfect (anti-)correlations for $\phi = 0$ and π. The following lemma gives a sufficient condition under which such a mixture can indeed give the desired cosine correlation.

Lemma 1.—Let $E(\phi)$ be a real function with a Fourier decomposition of the form

$$E(\phi) = \sum_{n\geq 0} e_{2n+1}\cos[(2n+1)\phi], \tag{3}$$

such that

$$\begin{aligned} &e_1 > 0, \qquad e_{2n+1} \leq 0 \quad \text{for all } n \geq 1, \\ &E(0) = \sum_{n\geq 0} e_{2n+1} = 1, \\ &E''(0) = -\sum_{n\geq 0}(2n+1)^2 e_{2n+1} \leq 0. \end{aligned} \tag{4}$$

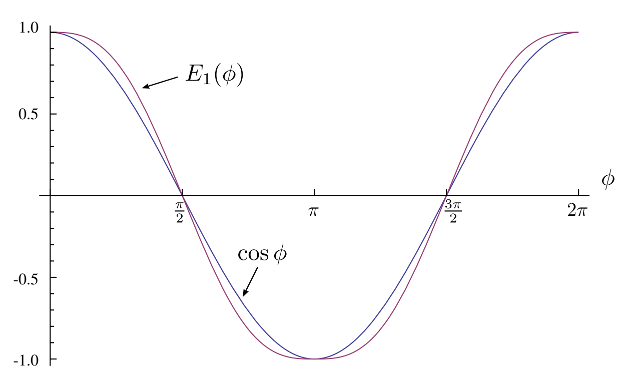

FIG. 1 (color online). Correlation $E_1(\phi) = E_1(\phi_A + \phi_B + \phi_C)$ obtained from Protocol 1, compared to the desired correlation $\cos(\phi)$.

Then $\cos\phi$ can be decomposed as

$$\cos\phi = \sum_{m\geq 0} p_{2m+1} E((2m+1)\phi), \tag{5}$$

with $p_{2m+1} \geq 0$ for all $m \geq 0$.

In particular, for $\phi = 0$, one gets $\sum_{m\geq 0} p_{2m+1} = 1$. The coefficients $p_{2m+1} \geq 0$ can be interpreted as probabilities, and the "inverse Fourier decomposition" (5) is indeed a probabilistic mixture of correlations $E((2m+1)\phi)$.

A proof of Lemma 1 is given in [22] together with the explicit form of the p_{2m+1}. It is easy to check that E_1 satisfies the conditions (4). Hence, $\cos\phi$ can be obtained from $E_1(\phi)$ as in (5). The following protocol therefore gives the desired cosine correlation and solves our problem, with the same 3 classical bits as in Protocol 1:

Protocol 2.—Let Alice, Bob, and Charlie share, in addition to the randomness already introduced in Protocol 1, a random variable M that takes the value $M = 2m+1$ with probability p_{2m+1}, where $\{p_{2m+1}\}_{m\geq 0}$ are the coefficients of the decomposition (5) for $E = E_1$.

After reception of their measurement settings ϕ_A, ϕ_B, and ϕ_C, the three parties run Protocol 1 with input angles $(2m+1)\phi_A$, $(2m+1)\phi_B$, and $(2m+1)\phi_C$, respectively.

Variants of our communication protocol.—For convenience, let us from now on consider the equivalent 0 or 1 bit values corresponding to the 3 parties' outputs in Protocol 1 (or 2): $a = \frac{1-\alpha}{2}$, $b = \frac{1-\beta}{2}$, and $c = \frac{1-\gamma}{2}$; the additions below will be modulo 2. Writing explicitly $a = a_{\tau_0\tau_b\tau_c}$ as a function of the classical communication that Alice receives, one has

$$a_{\tau_0 11} = a_{\tau_0 00} + 1 \quad \text{and} \quad a_{\tau_0 01} = a_{\tau_0 10}. \tag{6}$$

One can see that our communication protocol can actually be declined in different forms. In particular, Alice might not need to know the individual values of the bits τ_b and τ_c, but only their sum $\tau_{bc} = \tau_b + \tau_c$. Charlie's bit τ_c could, for example, be sent to Bob instead; Bob would then send τ_{bc} to Alice, who would output $a'_{\tau_0\tau_{bc}} = a_{\tau_0\tau_{bc}0}$; in the case when $\tau_b = \tau_c = 1$, the "+1" term in (6) can be introduced by Bob, who should output $b'_{\tau_c} = b + \tau_b\tau_c$. With similar considerations, one can come up with many different variants with varied communication patterns [23]. These variants and the original protocol look different, though they all require 3 bits of communication and lead to the same correlation. All of them have severe timing constraints (which is common for communication protocols): there are always some players that cannot produce their output before some other partners receive their input and send them some information.

Simulation with PR boxes.—An interesting alternative to measure nonlocality is to estimate the number of nonlocal Popescu-Rohrlich (PR) boxes [24] (some kind of "unit of nonlocality" [25]) required to simulate the correlations. Since the correlations we consider in this Letter have no single- nor bipartite marginals, all the variant communication protocols introduced above can be translated into PR-box-based protocols [25]. Indeed, using (6) one can always decompose the sum $a+b+c$ as follows:

$$\begin{aligned} a_{\tau_0\tau_b\tau_c} + b + c = {} & a_{000} + b + c + \tau_0(a_{000} + a_{100}) \\ & + \tau_b(a_{000} + a_{010}) + \tau_0\tau_b(a_{000} + a_{010} \\ & + a_{100} + a_{110}) + \tau_b\tau_c + \tau_c(a_{000} + a_{010}) \\ & + \tau_0\tau_c(a_{000} + a_{010} + a_{100} + a_{110}). \end{aligned}$$

The product terms above can be generated by using nonlocal boxes: 5 PR boxes can be used for the first 5 products (3 between Alice and Bob, 1 between Bob and Charlie and 1 between Alice and Charlie); the last product can be generated by a tripartite GHZ box, which can in turn be constructed from 3 PR boxes [26]. Hence, 8 PR boxes suffice to simulate the tripartite GHZ correlations.

Interestingly, the variant communication protocols we came up with all lead to a PR-box-based protocol with the same configuration of 8 PR boxes, all used precisely in the same way. In addition to this invariance, and similarly to quantum correlations, the PR-box-based protocol does not suffer from any timing constraint. Hence, it might be a more faithful tool to measure quantum nonlocality (at least, for correlations without marginals)—this general question would require further scrutinies beyond the scope of this Letter. Note that reciprocally, simulating the PR boxes by communication gives a systematic way to generate different variants of our protocol, depending on which way the communication goes.

Detection loophole.—Another interesting connection is between our communication protocol and simulation models based on the detection loophole [13,27]. A more symmetric variant of our protocol, where each party sends one bit, naturally leads to a detection-loophole-based protocol that simulates the GHZ correlations with "detection efficiencies" of 50% for Alice, Bob, and Charlie [23]. Other variants can lead to detection-loophole-based protocols with asymmetric detection efficiencies.

Conclusion.—We have proven that 3 bits of communication (or 8 PR boxes) suffice to simulate 3-qubit GHZ equatorial correlations; hence, their nonlocality is at most of 3 bits (8 PR boxes). In the course of our derivation, we introduced a strategy to obtain a cosine correlation as a mixture of other ("harmonic") correlations (Lemma 1) that could be used in other contexts as well.

In this Letter we considered correlations with random single- and bipartite marginals. If one considers measurements on the GHZ state out of the equatorial plane [28], or other states such as biased GHZ-like states for instance, then the marginals will no longer vanish, and simulating the entire probability distribution is likely to be significantly harder [16].

Two other important open problems are the questions of the optimality of our protocol and of its generalization to more parties. For 3 parties, since the GHZ correlations are truly tripartite [29], a minimum of 2 bits is necessary to connect the 3 parties. We could find a 2-bit protocol

(Protocol 1, without step (a), see [21]) that gives stronger correlations than $\cos\phi$ and that can approximate it to a very good accuracy, but not perfectly. For the N-partite case, it is easy to generalize protocol 1, again without step (a), using $(N-1)\log_2(N-1)$ bits of communication, by dividing the equator of the Bloch sphere into $2(N-1)$ equal sectors. This leads again to a protocol giving stronger correlations than $\cos\phi$, with a number of bits that is asymptotically equivalent to the lower bound derived in [17] for the simulation of GHZ correlations. Unfortunately, we did not find a generalization that would give a correlation satisfying the assumptions of Lemma 1, so that the exact cosine correlation could then be obtained as in Protocol 2.

These observations lead us to formulate the following question: Should we understand a "stronger" correlation as being "more nonlocal"? If our goal is to quantify the power of nonlocality as a resource for achieving some information processing task, then the next question follows: Is there any (useful) task, for which a stronger correlation might actually be less powerful than a weaker one? If this is not the case, then one could be happy with simulation protocols that give stronger correlations than the desired ones, and for this operational interpretation of the nonlocality measure, we could conclude that the nonlocality of the tripartite GHZ correlations is at most 2 bits (or 3 PR boxes), and that of the N-partite GHZ correlations is at most $(N-1)\log_2(N-1)$ bits.

Nonlocal quantum correlations are fascinating. First, because they cannot be simulated by mere shared local variables; next, because even if finite communication is allowed, their simulation remains tedious and quite artificial. This underlines the power of nonlocal correlations. Yet, such simulations seem to give a good measure of nonlocality (whether we are interested in the exact simulation or in the "operational nonlocality" measure), possibly the best together with PR-box-based simulations, and provide the only story that takes place in space and time about how they could occur.

We acknowledge discussions with G. Brassard, M. Kaplan, S. Pironio, and I. Villanueva. This work profited from financial support from the ARC Centre of Excellence for Quantum Computer Technology, the Swiss NCCR-QP and NCCR-QSIT, and the EU AG-QORE.

[1] J. Bell, *Speakable and Unspeakable in Quantum Mechanics* (Cambridge University Press, Cambridge, England, 2004), 2nd ed..
[2] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).
[3] A. Aspect, Nature (London) **398**, 189 (1999).
[4] J. Barrett, L. Hardy, and A. Kent, Phys. Rev. Lett. **95**, 010503 (2005).
[5] A. Acín *et al.*, Phys. Rev. Lett. **98**, 230501 (2007).
[6] S. Pironio *et al.*, New J. Phys. **11**, 045021 (2009).
[7] R. Colbeck and A. Kent, J. Phys. A **44**, 095305 (2011).
[8] S. Pironio *et al.*, Nature (London) **464**, 1021 (2010).
[9] S. Popescu, Nature Phys. **2**, 507 (2006).
[10] T. Maudlin, in *Proceedings of the 1992 Meeting of the Philosophy of Science Association*, edited by D. Hull, M. Forbes, and K. Okruhlik (Philosophy of Science Association, East Lansing, MI, 1992), Vol. 1, pp. 404–417.
[11] G. Brassard, R. Cleve, and A. Tapp, Phys. Rev. Lett. **83**, 1874 (1999).
[12] M. Steiner, Phys. Lett. A **270**, 239 (2000).
[13] N. Gisin and B. Gisin, Phys. Lett. A **260**, 323 (1999).
[14] B.F. Toner and D. Bacon, Phys. Rev. Lett. **91**, 187904 (2003).
[15] A. A. Méthot and V. Scarani, Quantum Inf. Comput. **7**, 157 (2007).
[16] N. Brunner *et al.*, Phys. Rev. A **78**, 052111 (2008).
[17] A. Broadbent, P.-R. Chouha, and A. Tapp, in *3rd Int. Conf. on Quantum, Nano, and Micro Technologies* (IEEE, New York, 2009), pp. 59–62.
[18] J.-D. Bancal, C. Branciard, and N. Gisin, Adv. Theor. Math. Phys. **2010**, 293245 (2010).
[19] C. Palazuelos, D. Perez-Garcia, and I. Villanueva, arXiv:1006.5318.
[20] D. M. Greenberger, M. A. Horne, and A. Zeilinger, in *Bells Theorem, Quantum Theory, and Conceptions of the Universe*, edited by M. Kafatos (Kluwer Academic, Dordrecht, 1989), pp. 69–72.
[21] Step (a) allows Alice and Bob to sample their shared random variable φ_b so that it follows an appropriate sine distribution (see [22]). One could also define a similar protocol as Protocol 1, without step (a), starting directly with φ_b uniformly distributed on $[0, 2\pi]$. This simpler protocol, that requires only 2 bits of communication (or 3 PR boxes, 1 between each pair of parties), would also give a stronger correlation $E_0(\phi) = \frac{32}{\pi^3}\sum_{n\geq 0}\frac{(-1)^n}{(2n+1)^3} \times \cos[(2n+1)\phi]$ $(= 1 - \frac{4\phi^2}{\pi^2}$ for $\phi \in [0, \frac{\pi}{2}])$ than $\cos\phi$. However, $E_0(\phi)$ does not satisfy the assumptions of Lemma 1; by mixing correlations of the form $E_0((2m+1)\phi)$, one can approximate the cosine correlation with a very good accuracy, but not exactly.
[22] See supplemental material at http://link.aps.org/supplemental/10.1103/PhysRevLett.107.020401 for the calculation of $E_1(\phi)$ and the proof of Lemma 1.
[23] C. Branciard and N. Gisin, arXiv:1102.0330.
[24] S. Popescu and D. Rohrlich, Found. Phys. **24**, 379 (1994).
[25] J. Barrett and S. Pironio, Phys. Rev. Lett. **95**, 140401 (2005).
[26] J. Barrett *et al.*, Phys. Rev. A **71**, 022101 (2005).
[27] P.M. Pearle, Phys. Rev. D **2**, 1418 (1970).
[28] When two or more parties perform nonequatorial measurements, our protocol fails to reproduce the nonvanishing marginals. However, if one is not interested in the marginals but only wants to simulate the tripartite correlation term $\langle\alpha\beta\gamma\rangle = \sin\theta_A \sin\theta_B \sin\theta_C \cos\phi$ (where θ_A, θ_B and θ_C are the zenith angles of the 3 measurement settings in $\mathcal{S}^2$), then our protocol can be used, as each party can locally add the appropriate amount of noise to introduce the factors $\sin\theta_I$.
[29] G. Svetlichny, Phys. Rev. D **35**, 3066 (1987).