PHYSICAL REVIEW A **87**, 020302(R) (2013)

Relationship between semi- and fully-device-independent protocols

Hong-Wei Li,[1,2,3] Piotr Mironowicz,[4,5] Marcin Pawłowski,[4,6] Zhen-Qiang Yin,[1] Yu-Chun Wu,[1] Shuang Wang,[1] Wei Chen,[1] Hong-Gang Hu,[2] Guang-Can Guo,[1] and Zheng-Fu Han[1]

[1]*Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei, 230026, China*

[2]*Department of Electronic Engineering and Information Science, University of Science and Technology of China, Hefei, 230027, China*

[3]*Zhengzhou Information Science and Technology Institute, Zhengzhou, 450004, China*

[4]*Instytut Fizyki Teoretycznej i Astrofizyki, Uniwersytet Gdański, PL-80-952 Gdańsk, Poland*

[5]*Department of Microwave and Antenna Engineering, Faculty of Electronics, Telecommunications and Informatics, Gdańsk University of Technology, PL-80-233 Gdańsk, Poland*

[6]*Department of Mathematics, University of Bristol, Bristol BS8 1TW, United Kingdom*

(Received 4 October 2012; published 14 February 2013)

We study the relation between semi- and fully-device-independent protocols. As a tool, we use the correspondence between Bell inequalities and dimension witnesses. We present a method for converting the former into the latter, and vice versa. This relation provides us with interesting results for both scenarios. First, we find random-number-generation protocols with higher bit rates for both the semi- and fully-device-independent cases. As a byproduct, we obtain classes of Bell inequalities and dimension witnesses. Then, we show how optimization methods used in studies on Bell inequalities can be adopted for dimension witnesses.

DOI: 10.1103/PhysRevA.87.020302 PACS number(s): 03.67.Ac, 03.65.Ud, 03.67.Dd, 03.67.Mn

Introduction. In device-independent (DI) protocols, two distant parties either do not know all the relevant parameters of their machines or do not trust them. This was formally presented in [1]. Initially, this approach was very successful in quantum cryptography [2–5]. Later, Colbeck [6,7] proposed a true random-number-expansion protocol based on the Greenberger-Horne-Zeilinger (GHZ) test, while Pironio *et al.* [8] proposed a protocol based on Bell inequality violations. All these protocols require entanglement, which has a negative effect on the complexity of the devices and the rates of randomness generation [8] and key distribution. To cope with this problem, the semi-device-independent (SDI) scenario was introduced in [9]. In this approach, we consider prepare-and-measure protocols without making any assumptions about the internal operations of the preparation and measurement devices. The only assumption made is about the size of the communicated system. We assume there is a single qubit in each round of the experiment. This approach is a very good compromise between the fully DI scenario and experimental feasibility. The possibility of using prepare-and-measure protocols implies no need for entanglement, which makes the experiments easier by several orders of magnitude. However, the price to pay for this is that one extra assumption means the possibility of a loophole if the assumption is not met. This lowers the overall security of the protocol, albeit not significantly, since it is relatively easy to find the dimension of the system in which Alice's device encodes information, even through superficial inspection of the device. However, it is almost impossible to test each part of the device to check whether it indeed works as advertised. The first SDI protocol, presented in [9], was for quantum key distribution. Shortly thereafter, the first SDI randomness-expansion protocol was proposed [10]. This work studies the relation between DI and SDI protocols. We show how and under what conditions one can be converted into the other and how this change affects their parameters. This relation provides us with interesting results for both scenarios. First, we find random-number-generation protocols with higher bit rates for both semi- and fully-device-independent cases. As a byproduct, we obtain classes of Bell inequalities and dimension witnesses. Then, we show how optimization methods used in studies on Bell inequalities can be adopted for dimension witnesses. Our Rapid Communication is structured as follows. First, we describe the method for converting DI protocols to SDI, and vice versa. Then we apply our method to SDI random generators to obtain DI protocols with higher bit rates. We also present a family of Bell inequalities. Next we take a class of DI protocols and turn these into SDI protocols with better rates. This time our byproduct is a family of dimension witnesses. Finally, we show how semi-definite-programming (SDP) methods, which are a powerful tool in the DI scenario, can be used in an SDI one.

Bell inequalities and dimension witnesses. In a DI protocol, distant parties receive systems in an unknown, (possibly) entangled state from an untrusted sender. In each round, they choose their inputs and make measurements to obtain the outcomes. In our Rapid Communication, we are interested in bipartite protocols, and, thus, we have two parties, Alice and Bob, with their setting choice denoted by x and y, respectively, and their outcome denoted by a and b, respectively. In some randomly chosen rounds of the protocol, both parties will publicly compare their settings and outcomes to estimate the conditional probability distribution $P(a,b|x,y)$. From this, they can calculate the value of some Bell inequality,

$$I = \sum_{a,b,x,y} \alpha_{a,b,x,y} P(a,b|x,y), \tag{1}$$

which is their security parameter. This parameter can then be used as the lower bound on the amount of randomness or secrecy in the remaining rounds. In an SDI protocol, Alice chooses her input x', but she does not have any outcome. Instead, in each round, she prepares a state depending on x' and sends it to Bob. Bob chooses his measurement setting y and obtains outcome b. Although the devices that prepare the system and then measure it are not trusted, we assume that the communicated states are described by a Hilbert space with

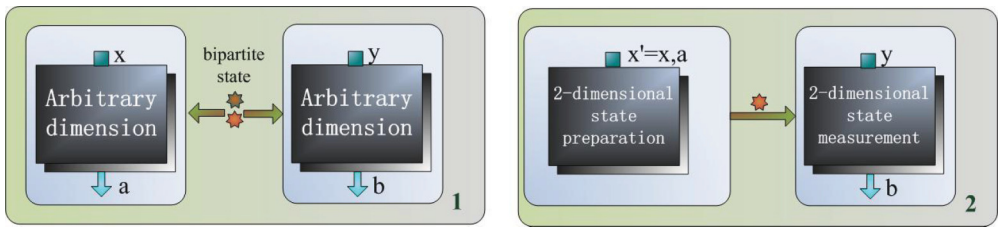

FIG. 1. (Color online) Schematic representation of (1) DI and (2) SDI protocols and of our method for finding the corresponding ones.

a fixed dimension (here we assume they are qubits) and that there is no entanglement between the devices of Alice and Bob. Again, in some rounds, x',y, and b are announced to estimate the value of some dimension witness

$$W = \sum_{b,x',y} \beta_{b,x',y} P(b|x',y), \tag{2}$$

which has exactly the same function as I in the DI case. Both of these scenarios are illustrated in Fig. 1.

Dimension witnesses were introduced in [11]. Just as violation of a Bell inequality in the DI case tells us that the measured system cannot have a classical description, violation of a dimension witness in the SDI case tells us that the communicated system cannot be a classical bit (in the case of the witness for dimension 2). In both cases, violation of the classical bound is a necessary (though not always sufficient) condition for the protocol to work. Moreover, in both cases, the form of I or W is the most important part of the protocol description. Therefore, finding the correspondence between these two objects is equivalent to finding the correspondence between the protocols. Our method for doing so is quite straightforward: Let us rewrite I as $\sum_{a,b,x,y} \alpha_{a,b,x,y} P(a|x,y)P(b|a,x,y)$ and start by considering a as part of Alice's input. This is a purely mathematical operation and has no meaning at the protocol level. Now Alice's input is $x' = (x,a)$. We can consider $P(a|x,y)$ as the probability that part of Alice's input is a. Because in the parameter estimation phase of the protocol the inputs are chosen according to a uniform distribution, we set $P(a|x,y) = \frac{1}{A}$, where A is the size of the alphabet of a. Our I is now $\sum_{b,x',y} \alpha_{b,x',y} \frac{1}{A} P(b|x',y)$ and has the form of (2) with $\beta_{b,x',y} = \frac{1}{A}\alpha_{b,x',y}$. Our method is quite heuristic and there is no guarantee that a Bell inequality with a quantum bound higher than the classical one will lead to a dimension witness that can be violated. Also, using it to go from a dimension witness to a Bell inequality is not always possible. To do so, Alice's input x' must be divided into a pair comprising a setting and an outcome. This is only possible if the alphabet of x' has a composite size. These are serious drawbacks, but they are easily outweighed by the advantages of simplicity and the fact that the method works. In the following paragraphs, we apply it to generate useful witnesses, inequalities, and protocols.

From SDI to DI protocols. Let us consider the family of SDI protocols for randomness generation introduced in [12], which are based on $n \to 1$ quantum random access codes [13]. Alice's input x' is a collection of n independent bits, $a_0,\ldots,a_{n-1}$. For Bob, $y = 0,\ldots,n-1$. The dimension witness is defined by $\beta_{b,x',y} = \delta_{a_y,b}$. There are many ways of dividing Alice's input into pairs of settings and outcomes, but, because of the independence of the bits, they are all equivalent. Let us then take outcome a to be a_0 and setting x to be $a_1,\ldots,a_{n-1}$. In this way, we obtain a family of Bell inequalities,

$$I_n = \sum_{a,b,x,y} \delta_{a_y,b} P(a,b|y,x). \tag{3}$$

Systems obtaining a high value of I_n can be used to implement entanglement-assisted random access codes [14]. In these codes, Alice has n independent bits and Bob is interested in only one of them. Alice can send only one bit of classical communication to Bob, but they can share entanglement. If we denote the bits that Alice wants to encode by $c_0,\ldots,c_{n-1}$, then Alice can choose her setting by taking $a_i = c_i \oplus c_0$ for all $i > 0$ and transmit the message $m = a \oplus c_0$ to Bob. If he XORs his outcome b with the message, it is easy to calculate that he obtains the correct value of a_y with average probability $P_n = \frac{I_n}{n2^n}$. Therefore, we see that there is indeed a correspondence between the dimension witness and the Bell inequality related by our method, also at the level of protocols. In this case, they are both a measure of the success probability for the different kinds of random access codes. I_2 is equivalent to the Clauser-Horne-Shimony-Holt (CHSH) inequality. However, members of this family for $n > 2$ have never been studied. Because it is possible to use them for entanglement-assisted random access codes, the bounds on their efficiency derived in [14] apply and they translate to the maximum quantum value of P_n, that is, $P_n^{\max} = \frac{1}{2}(1 + \frac{1}{\sqrt{n}})$. Now we show how our Bell inequalities perform in DI randomness generation. The quantity that we wish to optimize is the min entropy $H_\infty(a,b|x,y) = -\log \max_{a,b} P(a,b|x,y)$. To find the lower bound on this for a given value of P_n, we use the methods described in [15]. More precisely, we bound the set of allowed probability distributions by the second level of their hierarchy. Table I shows the lower bounds on the min entropy for the maximal quantum values of P_n that we obtained.

Compared with the randomness obtained from the SDI protocols, the main difference is that it grows with n instead of reaching a maximum at $n = 3$. In fact, the upper bound is $H_\infty(a,b|x,y) = 1 - \log P_n^{\max} = 2 - \log(1 + \frac{1}{\sqrt{n}})$, which approaches 2 as $n \to \infty$. We conjecture that this is reached for any n, but the second level of the SDP hierarchy form [15] that we use for the lower bound is sufficient only for $n = 2$. Proving this conjecture is one of the open areas of research. The lower bounds as a function of P_n are plotted in Fig. 2.

From DI to SDI protocols. Now we apply our method to show that we can go the other way and convert a DI protocol to an SDI one. We start from the randomness-generation protocol

TABLE I. Lower bounds on the min entropy for the protocols corresponding to the $n \to 1$ random access codes. The values in the rightmost column are for the family of protocols defined in [12] and are taken from there. The values in the middle column correspond to the min entropy of the outcomes in Bell inequalities I_n for the maximal quantum values thereof. These were obtained using the SDP methods in [15]. The inequalities I_n were derived from the protocols in [12] using the method depicted in Fig. 1.

n	DI: $H_\infty(a,b\|x,y)$	SDI: $H_\infty(b\|a,x,y)$
2	1.2284	0.2284
3	1.3421	0.3425
4	1.4126	0.1388
5	1.4652	0.1024

form [16] based on Bell inequality I_α, which expressed in the form (1) is

$$I_\alpha = \sum_{a,b,y} \delta_{a,b}\alpha P(a,b|x=0,y) + \sum_{a,b,y} \delta_{a,b\oplus y} P(a,b|x=1,y). \quad (4)$$

Converting this to a dimension witness, we get

$$W_\alpha = \sum_{a,b,y} \frac{\alpha\delta_{a,b}}{2} P(b|a,x=0,y) + \sum_{a,b,y} \frac{\delta_{a,b\oplus y}}{2} P(b|a,x=1,y). \quad (5)$$

The lower bound on the min entropy as a function of coefficient α is plotted in Fig. 3. For large values of α, the amount of randomness is clearly greater than that for the best of the protocols described in [12]. The intuitive explanation for this is that W_α also corresponds to a kind of quantum random access code. In this case, it is a $2 \to 1$ code with different weights assigned to the cases with $x = 0$ or $x = 1$. For large α, it is much more important for the protocol to be correct when $x = 0$ than in the case of $x = 1$. This means that the protocols reaching maximum quantum value will tend to give the correct value of b for $x = 0$. Here correct means

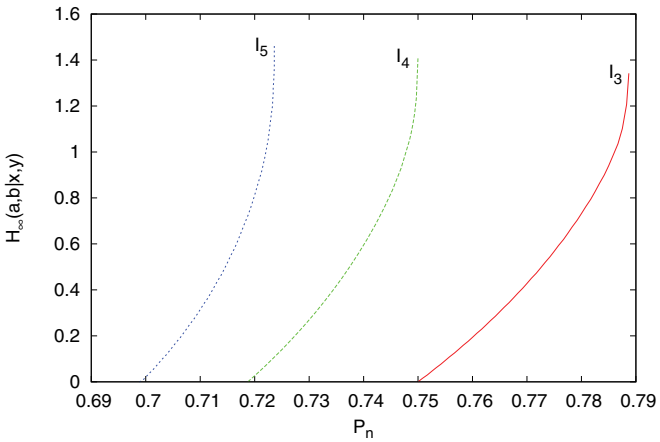

FIG. 2. (Color online) The lower bounds on $H_\infty(a,b|x,y)$ as functions of P_n.

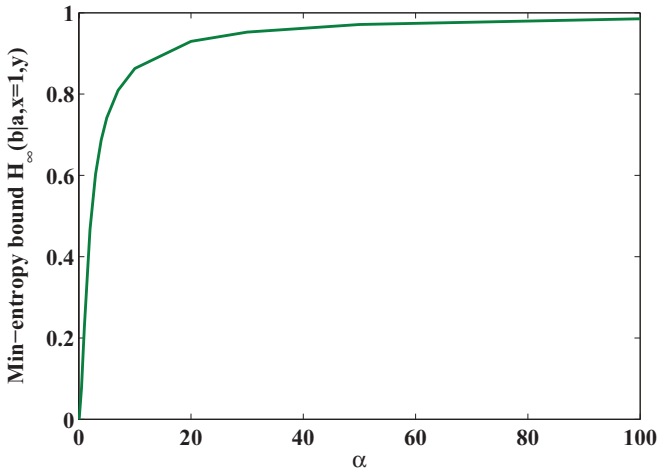

FIG. 3. (Color online) Lower bound on the min entropy $H_\infty(b|a,x=1,y)$ as a function of coefficient α for the maximal quantum value of W_α. In [16], a large amount of randomness is generated only for one setting of x. Here we observe the same result with high randomness for $x = 1$ and low randomness for $x = 0$.

fully specified by a,y, and x, in other words, deterministic. The price paid for this is that for $x = 1$, the probability of the correct (predetermined by a,y, and x) value is small, which implies a lot of randomness. Previously, in [10,12], the bounds on the entropy in SDI protocols were calculated using the Levenberg-Marquardt algorithm [17], which is not guaranteed to find global minima. SDP, on the other hand, always finds these; however, it was previously not known how this could be applied in the SDI case. Below we give a solution to this problem.

Optimization in SDI protocols. It is not possible to use SDP optimization directly in the SDI case because of the nonlinear target function. Neither can methods from [15] be applied because they do not allow the dimension of the system to be set. Therefore, we need to find another solution. We do it by proving the following theorem:

Theorem. If $H_\infty(b|a,x,y)$ is the min entropy obtained in the SDI case and $H_\infty(a,b|x,y)$ is the min entropy obtained in the corresponding DI protocol, then

$$H_\infty(b|a,x,y) \geqslant H_\infty(a,b|x,y) - 1 \quad (6)$$

for the same value of the security parameter.

Proof. See the Supplemental Material in Ref. [20].

Let us stress that (6) holds only when the values of the dimension witness and the Bell inequality are the same. Consider Table I once again. For $n = 2$, we have equality $H_\infty(b|x,a,y) = H_\infty(a,b|x,y) - 1$. For $n = 3$, $H_\infty(b|x,a,y)$ is slightly larger than $H_\infty(a,b|x,y) - 1$. This most likely stems from the fact that the bound in the table is not tight for $n = 3$. In fact, the upper bound on $H_\infty(a,b|x,y)$ is exactly $H_\infty(b|x,a,y) + 1$. The situation changes for $n = 4,5$. In these cases, (6) does not seem to hold. This is because the values in the table are given for the maximal quantum values of witnesses and inequalities, which, for $n = 4,5$, are not the same. If we calculate the entropy bound for the DI case when the value of the Bell inequality is equal to the maximal quantum value of the dimension witness, then the values are in

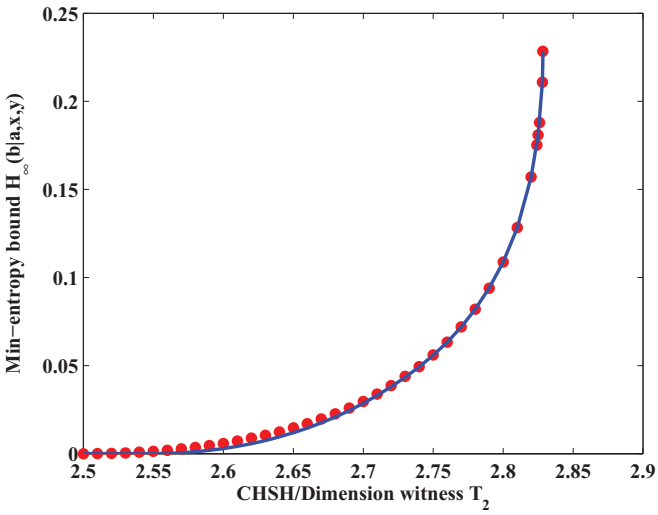

FIG. 4. (Color online) Min entropy bounds for the SDI randomness-generation protocol based on the $2 \to 1$ quantum random access code. The dots are obtained from the Levenberg-Marquardt algorithm used in [10], which is not guaranteed to find global minima, while the line depicts the SDP method described here. Note that state preparation in the SDI protocol assumes that $p(a|x,y) = \frac{1}{2}$.

agreement with (6). Using this method, we were able to refine the results in [10], as shown in Fig. 4.

Conclusions. We investigated the relation between DI and SDI protocols. Although our study focused on randomness generation, our results are also applicable to quantum key distribution since all the state-of-the-art proofs of security are based on the randomness of measurement outcomes [3,4]. To this end, we demonstrated a method for converting Bell inequalities into dimension witnesses, and vice versa. This allowed us to generate examples of both types of objects with very interesting properties. Our family of Bell inequalities gave rise to DI randomness-generation protocols with better bit rates, while our family of dimension witnesses did the same for SDI protocols. Finally, using the correspondence between the DI and SDI approach, we were able to modify the SDP-based methods by implementing in MATLAB using toolboxes [18,19], which were proven successful in the former case, to work in the latter one. Apart from the similarities, our study also showed interesting differences such as the completely different dependence on n in Table I. It also introduced many protocols for both scenarios. Comparison of their efficiency with that of existing ones, especially in the presence of noise and imperfect detectors, opened an interesting area of research.

H.-W.L. wishes to thank YaoYao for his helpful discussion. This work has been supported by the National Natural Science Foundation of China (Grant Nos. 61101137, 61201239, 61205118, 10974193, and 11275182), UK EPSRC, FNP TEAM, and ERC Grant No. QOLAPS.

[1] A. Acin, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).
[2] J. Barrett, L. Hardy, and A. Kent, Phys. Rev. Lett. **95**, 010503 (2005).
[3] E. Hänggi and R. Renner, arXiv:1009.1833; E. Hänggi, R. Renner, and S. Wolf, in *Advances in Cryptology - EUROCRYPT 2010*, Lecture Notes in Computer Science, Vol. 6110 (Springer, Berlin, 2010), pp. 216–234.
[4] Ll. Masanes, S. Pironio, and A. Acin, Nature Commun. **2**, 238 (2011).
[5] M. Dall'Arno, E. Passaro, R. Gallego, and A. Acin, Phys. Rev. A **86**, 042312 (2012).
[6] R. Colbeck and A. Kent, J. Phys. A **44**, 095305 (2011).
[7] R. Colbeck, arXiv:0911.3814.
[8] S. Pironio, A. Acin, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, Nature (London) **464**, 1021 (2010).
[9] M. Pawłowski and N. Brunner, Phys. Rev. A **84**, 010302(R) (2011).
[10] H.-W. Li, Z.-Q. Yin, Y.-C. Wu, X.-B. Zou, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, Phys. Rev. A **84**, 034301 (2011).
[11] R. Gallego, N. Brunner, C. Hadley, and A. Acin, Phys. Rev. Lett. **105**, 230501 (2010).
[12] H.-W. Li, M. Pawłowski, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han, Phys. Rev. A **85**, 052308 (2012).
[13] A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani, J. ACM **49**(4), 496 (2002).
[14] M. Pawłowski and M. Żukowski, Phys. Rev. A **81**, 042326 (2010).
[15] M. Navascues, S. Pironio, and A. Acin, New J. Phys. **10**, 073013 (2008).
[16] A. Acin, S. Massar, and S. Pironio, Phys. Rev. Lett. **108**, 100402 (2012).
[17] K. Levenberg, Q. Appl. Math. **2**,164 (1944).
[18] J. Sturm, SeDuMi, a MATLAB Toolbox for Optimization Over Symmetric Cones, http://sedumi.mcmaster.ca (unpublished).
[19] J. Löfberg, YALMIP: A Toolbox for Modeling and Optimization in MATLAB, http://control.ee.ethz.ch/joloef/yalmip.php (unpublished).
[20] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevA.87.020302 for the Proof of the Theorem.