Chapter 5
Single-Round Box

In the device-independent framework we use "boxes" to describe the physical devices, or resources, of interest. A box, formally modelled as a conditional probability distribution (recall Sect. 3.1), is always defined with respect to a *specific* task or protocol. More specifically, note the following:

1. To define a box $P_{AB|XY}$ we need to fix the sets of the inputs $\mathcal{X}$, $\mathcal{Y}$ and the outputs $\mathcal{A}$, $\mathcal{B}$ of the box. These sets are chosen according to the task in which the box is being used. For example, if a box is used to play a single CHSH game then the sets are all chosen to be $\{0, 1\}$. The box's action is undefined when it is used with, e.g., the input $x = 2$.

2. The location of the used devices in space (or space-time) also sets the conditions that the box describing the devices must fulfil. For example, if a protocol demands two devices, separated in space, that cannot communicate during the execution of the protocol then the defined box should fulfil certain non-signalling conditions.[1]

3. When considering boxes that are used to execute a complex protocol, in which many games are being played with the box (as done in the succeeding chapters), we also need to take into account the type of interaction when defining the box. For example, some protocols require boxes with which we can interact sequentially—in each round of the protocol we give one input to the box, wait for the output, and only then give the next input. Other protocols involve boxes which accepts all the

[1] Interestingly, if one considers protocols with more than two parties in which the devices can only be used in specific space-time coordinates and merely assumes that the box modelling the devices respects relativistic causality (in the sense that it cannot lead to casual loops) then the conditions defining the box are different than the non-signalling ones [1]. This acts as another example for how the specific use of the devices effects the mathematical model of the box.

R. Arnon-Friedman, *Device-Independent Quantum Information Processing*, Springer Theses, https://doi.org/10.1007/978-3-030-60231-4_5

inputs and only then produces all the outputs. If we only give one input to such a box we do not expect it to output anything and its action is undefined. Thus, these differences in the behaviour of the boxes depend on the way we intend to use it in the task of interest and effect the mathematical model of the considered boxes.

To grasp the dependence of the box on the considered task, as described above, one can contrast it with the standard formalism used to define quantum states and measurements. For example, the definition of a quantum state in terms of a density operator is completely independent of the way we might want to measure it. Consider, for example, a quantum state used to play the CHSH game with the measurements σ_x and σ_z for one of the parties. Even though we only intend to perform these measurements, the formalism also tells us what will happen if we choose to measure σ_y instead. This stands in contrast to Item 1 above.[2]

The current chapter as well as Chap. 6 are devoted to the way one models the different boxes used in device-independent information processing, depending on the considered setting and interaction with the boxes. In Chap. 6 we will be interested in boxes, or devices, which can be used to implement certain protocols. Before we explain how such boxes can be described let us focus on a simpler object—the "single-round box".

We think of a single-round box as illustrated in Fig. 5.1, as a small device that can be used to play a *single* round of a Bell game. That is, in the case of the CHSH game, for example, Alice and Bob can input their bits $x, y \in \{0, 1\}$ to the box and receive the outcomes $a, b \in \{0, 1\}$. After that the box can no longer be used (i.e., Alice and Bob cannot play another game with it). Mathematically, such a box can be described by a non-signalling conditional probability distribution $\mathrm{P}_{AB|XY}$ as explained in Sect. 3.1. Physically, an example of a single-round box is a single EPR pair together with a set of possible measurements for each party.

A single-round box is *not* a useful resource in the *operational sense*. Since our starting point in the device-independent setting is that we do not know how the device operates, we must interact with it to test it. However, since a single-round box allows us to play just a single game we can hardly conclude anything regarding its inner-working. One can imagine Alice and Bob playing the CHSH game with their box and observing $(a, b, x, y) = (0, 0, 0, 0)$. Then what? It can always be the case that they are sharing a classical device that always outputs $(a, b) = (0, 0)$ for the inputs $(x, y) = (0, 0)$. Thus, Alice and Bob cannot learn anything regarding, e.g., the randomness of their outputs, from this single game. As the information collected in a single game is not sufficient to test the box we start, instead, with an *assumption* regarding the box, e.g., that it can be used to win the CHSH game with winning probability ω. As will be shown below, various fundamental properties can be concluded by starting with such an assumption.

[2]One can rightfully say that this property of boxes, among several other properties, renders them an "unphysical description" of real systems and resources. With this respect, the formalism of the so called "generalised probabilistic theories" [2, 3] is a more appropriate mathematical setting to discuss physical theories which extend, or abstract, quantum physics. In contrast, boxes are merely a simplified mathematical model sufficient for certain analyses.

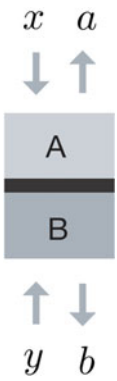

Fig. 5.1 A single-round box. We think of a single-round box as a small device, shared between Alice and Bob, which can be used to play a single round of a Bell game, such as the CHSH game. It is described by a conditional probability distribution $\mathrm{P}_{AB|XY}$

Although a single-round box is not a valuable resource in practice, it is useful as a simple abstract object that allows us to study the fundamental implications of violating a Bell inequality (while putting aside many technical details that arise when considering the complex devices used in protocols). Furthermore, it is the goal of this thesis to explain how "single-round box statements" can be lifted to operational statements regarding more complex scenarios such as the analysis of device-independent protocols.

5.1 The Model

Mathematically, we model a single-round black box by a non-signalling conditional probability distribution $\mathrm{P}_{AB|XY}$ that can be used to play a single Bell game G defined over the sets of inputs $\mathcal{X}, \mathcal{Y}$ and outputs $\mathcal{A}, \mathcal{B}$ for Alice and Bob (see Sect. 3.2.1 for complete definitions). $\mathrm{P}_{AB|XY}$ is also sometimes referred to as a strategy for G.

As mentioned above, when considering single-round boxes one usually assumes that the box $\mathrm{P}_{AB|XY}$ can be used to win the game with a certain winning probability ω. That is, $\mathrm{P}_{AB|XY}$ is such that

$$\mathbb{E}_{x,y} \sum_{\substack{a,b| \\ w(a,b,x,y)=1}} \mathrm{P}_{AB|XY}(ab|xy) = \omega \,, \tag{5.1}$$

where the expectation $\mathbb{E}_{x,y}$ is defined with respect to the input distribution of the considered game and $w : \mathcal{A} \times \mathcal{B} \times \mathcal{X} \times \mathcal{Y} \to \{0, 1\}$ is the winning function of the game.

Depending on the context, one can consider quantum single-round boxes or non-signalling ones.

5.1.1 Quantum Single-Round Boxes

When we say that a single-round box is quantum we mean that its inner-working can be described within the quantum formalism. Specifically:

Definition 5.1 (*Quantum single-round box*) Given a Bell game G, a quantum single-round box is a quantum box $\mathrm{P}_{AB|XY}$, as in Definition 3.3, defined for the inputs and outputs of the game G – $\mathcal{X}, \mathcal{Y}, \mathcal{A}, \mathcal{B}$. That is, there exist a bipartite state $\rho_{Q_A Q_B}$ and measurements $\{M_a^x\}$ and $\{M_b^y\}$ such that

$$\mathrm{P}_{AB|XY}(ab|xy) = \mathrm{Tr}\left(M_a^x \otimes M_b^y \ \rho_{Q_A Q_B}\right) \quad \forall a, b, x, y \ . \tag{5.2}$$

The quantum single-round box is said to win G with winning probability ω when the state and measurements are such that Eq. (5.1) holds.

Note that mathematically a quantum single-round box is merely a quantum box (Definition 3.3). What makes it *single-round* is that $\mathrm{P}_{AB|XY}$ is defined for the inputs and outputs of a single game G.

When considering cryptographic applications where a quantum adversary is present we extend the box to the adversary. That is, we let $\rho_{Q_A Q_B E}$ be the purification of $\rho_{Q_A Q_B}$ where E is a quantum register belonging the the adversary and $\rho_{Q_A Q_B} = \mathrm{Tr}_E\left(\rho_{Q_A Q_B E}\right)$ is Alice and Bob's marginal satisfying Eqs. (5.1) and (5.2).

5.1.1.1 Non-signalling Single-Round Boxes

Instead of restricting our attention to quantum boxes we can also consider non-signalling single-round boxes. These are defined in a similar way to their quantum counterparts.

Definition 5.2 (*Non-signalling single-round box*) Given a Bell game G, a non-signalling single-round box is a non-signalling box $\mathrm{P}_{AB|XY}$, as in Definition 3.1, defined for the inputs and outputs of the game G – $\mathcal{X}, \mathcal{Y}, \mathcal{A}, \mathcal{B}$. That is, for all $a \in \mathcal{A}$, $b \in \mathcal{B}$, $x, x' \in \mathcal{X}$ and $y, y' \in \mathcal{Y}$,

$$\sum_b \mathrm{P}_{AB|XY}(a, b|x, y) = \sum_b \mathrm{P}_{AB|XY}(a, b|x, y')$$
$$\sum_a \mathrm{P}_{AB|XY}(a, b|x, y) = \sum_a \mathrm{P}_{AB|XY}(a, b|x', y) \ .$$

The non-signalling single-round box is said to win G with winning probability ω when $\mathrm{P}_{AB|XY}$ is such that Eq. (5.1) holds.

Here as well one can consider an extension of the single-round box to an additional party describing a non-signalling (super-quantum) adversary. This will not be needed in this thesis so we do not explain how this is done. The interested reader is referred to [4, Sect. 3.2].

5.2 Showcase: Device-Independent Quantum Cryptography

As mentioned above, a single-round box is useful as a simple abstract object that allows us to study the fundamental implications of violating a Bell inequality. More specifically, certain properties of the box can be concluded if we assume to know the probability of winning a Bell game using a single-round box described by $\mathrm{P}_{AB|XY}$. We consider out showcase of device-independent cryptography as an example.

The most crucial observation when considering device-independent cryptographic protocols is the fact that high winning probability in a Bell game not only implies that the measured system is non-local, but more importantly that the kind of non-locality it exhibits cannot be shared: the higher the winning probability, the less information any eavesdropper can have about the outcomes produced by the box.

There are different ways of making such a statement quantitive. One possible way (that will also be of relevance later on) is to consider the conditional von Neumann entropy $H(A|XYE)$ where A is the random variable describing Alice's outcome bit, X and Y are the random variables describing the inputs of Alice and Bob and E is a quantum register holding the quantum side information belonging to the adversary. If the adversary is completely oblivious to the value of a bit A even given X, Y and E then takes its maximal value $H(A|XYE) = 1$.

A tight trade-off between the winning probability of a single-round box ω and the entropy $H(A|XYE)$ generated by the box was derived in [5, 6] and is stated in the following lemma.

Lemma 5.3 ([5, 6][3]) *For any quantum single-round box* $\mathrm{P}_{AB|XY}$ *with winning probability* $\omega \in \left[\frac{3}{4}, \frac{2+\sqrt{2}}{4}\right]$ *in the* CHSH *game,*

$$H(A|XYE) \geq 1 - h\left(\frac{1}{2} + \frac{1}{2}\sqrt{16\omega\,(\omega - 1) + 3}\right)\,, \tag{5.3}$$

where E *denotes the quantum side-information belonging to the adversary and* $h(\cdot)$ *is the binary entropy function.*

The relation stated in Eq. (5.3) is plotted in Fig. 5.2. One can see that the entropy increases as the winning probability ω increases. That is, the amount of secret randomness in Alice's outcome is directly related to the winning probability of the single-round box. In particular, we observe that $H(A|XYE) = 0$ (i.e., the adversary knows the value of A) for the optimal classical winning probability and $H(A|XYE) = 1$ (i.e., A looks completely random to the adversary) for the optimal quantum winning probability.[4] Note that there can be many different boxes $\mathrm{P}_{AB|XY}$ (and hence extensions to the adversary) with the same winning probability ω. That is, the assumption

[3] Lemma 5.3 is stated in the form appearing in [7]. To see how the original results of [5] can be used to derive the lemma as we state it, follow the proof given in Appendix C.1.

[4] These two extreme cases are easy to understand. When the box employs a classical strategy the adversary can simply hold a copy of A. When the box employs the optimal quantum strategy the

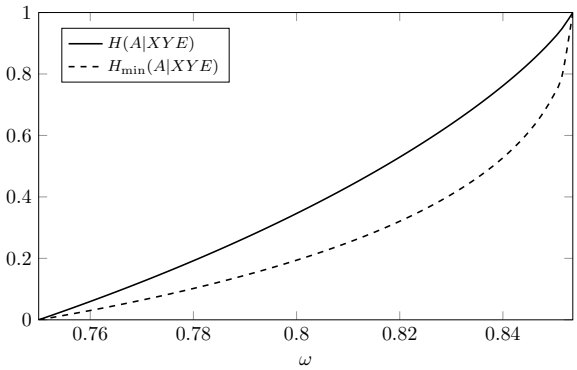

Fig. 5.2 Secrecy versus winning probability ω in the CHSH game for a *single-round box*. Two lower-bounds are shown: one for the conditional von Neumann entropy $H(A|XYE)$ [5] and the other for the conditional min-entropy $H_{\min}(A|XYE)$ [8]; both bounds are tight. As soon as the winning probability is above the classical threshold of 75% some secret randomness is produced

regarding the winning probability of the box does not pin down the full probability distribution. The bound given in Eq. (5.3) is thus very strong—it says that for *any* single-round box with winning probability ω and *any* purification to the adversary the stated lower bound holds.

Instead of considering the von Neumann entropy as above, one can also study lower-bounds on the conditional min-entropy $H_{\min}(A|XYE)$ as a function of the winning probability of a single-round box—as was done in [8]. We plot the resulting bound in Fig. 5.2. As can be seen in the figure, for non-optimal Bell violation the min-entropy can be significantly lower than the von Neumann entropy. Indeed, the min-entropy is always upper-bounded by the von Neumann entropy (hence the name). Still, in some cases a bound on the min-entropy, rather than the von Neumann entropy, is needed or, at the least, is easier to derive. In particular, lower-bounds on the min-entropy for *single-round boxes* can be found using general techniques based on the semidefinite programming hierarchies of [9] while, up to date, there is no general technique to derive (or even estimate) such bounds on the von Neumann entropy.

Similar bounds were derived also for other Bell inequalities. For example, lower-bounds on the min-entropy produced by a single-round box were found as a function of the violation of the Mermin inequality [10, Eq. (6)] and the tilted-CHSH inequality [11, Lemma 2]. Another result in the same spirit is that of [12, Sect. 5], where a bound on the min-entropy is derived as a function of several Bell inequalities all at once.[5] Lower-bounds on the von Neumann entropy were derived as a function of

used state is the maximally entangled state. Then, due to monogamy of entanglement, the adversary is completely decoupled from the Alice and Bob's state. For more details see Sect. 4.2.

[5] That is, instead of assuming that we know just the winning probability of the single-round box in a specific game, we assume we know its winning probabilities in several different games. In the context of single-round boxes this is a stronger assumption regarding the device. However, in actual application this is not an issue, as will be mentioned later on.

the violation of the MDL inequalities [13, Sect. 3] and the MABK inequality [14, Lemma S5].

Before continuing to the next chapter, we emphasise once again that single-round statements as mentioned above should not be understood as operational statements. If we are given a single-round box but we do not assume to know its winning probability ω then we cannot conclude anything about its properties (e.g., the entropy of the outputs). When considering, for example, device-independent cryptographic protocols one must test the device in order to estimate whether it can violate a Bell inequality or not. This is done by playing several games with the device and collecting statistic regarding its input-output behaviour. For this purpose we need to consider *multi-rounds* boxes, as done in the following sections.

References

1. Horodecki P, Ramanathan R (2016) Relativistic causality versus no-signaling as the limiting paradigm for correlations in physical theories. arXiv preprint arXiv:1611.06781
2. Barrett J (2007) Information processing in generalized probabilistic theories. Phys Rev A 75(3):032304
3. Chiribella G, D'Ariano GM, Perinotti P (2010) Probabilistic theories with purification. Phys Rev A 81(6):062348
4. Hänggi E (2010) Device-independent quantum key distribution. PhD thesis
5. Pironio S, Acín A, Massar S, de La Giroday AB, Matsukevich DN, Maunz P, Olmschenk S, Hayes D, Luo L, Manning TA et al (2010) Random numbers certified by Bell's theorem. Nature 464(7291):1021–1024
6. Acín A, Massar S, Pironio S (2012) Randomness versus nonlocality and entanglement. Phys Rev Lett 108(10):100402
7. Arnon-Friedman R, Renner R, Vidick T (2019) Simple and tight device-independent security proofs. SIAM J Comput 48(1):181–225
8. Masanes L, Pironio S, Acín A (2011) Secure device-independent quantum key distribution with causally independent measurement devices. Nat Commun 2:238
9. Navascués M, Pironio S, Acín A (2008) A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. New J Phys 10(7):073013
10. Gallego R, Masanes L, De La Torre G, Dhara C, Aolita L, Acín A (2013) Full randomness from arbitrarily deterministic events. Nat Commun 4
11. Bamps C, Massar S, Pironio S (2017) Device-independent randomness generation with sublinear shared quantum resources. arXiv preprint arXiv:1704.02130
12. Nieto-Silleras O, Bamps C, Silman J, Pironio S (2016) Device-independent randomness generation from several bell estimators. arXiv preprint arXiv:1611.00352
13. Kessler M, Arnon-Friedman R (2017) Device-independent randomness amplification and privatization. arXiv preprint arXiv:1705.04148
14. Ribeiro J, Murta G, Wehner S (2017) Fully device independent conference key agreement. arXiv preprint arXiv:1708.00798