Chapter 8
Reductions to IID: Parallel Interaction

Multi-round parallel boxes, discussed in Sect. 6.1, can display an almost arbitrary behaviour and hence are complicated to analyse. However, some additional structure of the boxes can be assumed when certain types of symmetries are present in the considered information processing task. In this chapter we focus on the analysis of parallel boxes that are *permutation invariant*. Permutation invariance is an inherent symmetry in many information processing tasks, device-independent tasks among them. Thus, analysing permutation invariant boxes (as defined below) is of special interest.

A well known family of tools used to study permutation invariant systems[1] is the family of "de Finetti-type theorems". A de Finetti-type theorem is any theorem that relates (in one way or another) *permutation invariant systems* to a more structured system, having the form of a *convex combination of IID systems*, called a de Finetti system (or state). The relation given by the theorem can be used, in certain cases, to argue that instead of analysing permutation invariant systems one can restrict the attention to the simpler to analyse (convex combination of) IID systems. A de Finetti theorem therefore acts as a reduction to IID.

The first de Finetti theorem [1] established that the collection of infinitely exchangeable sequences, i.e., distributions on infinite strings that are invariant under all permutations, exactly coincides with the collection of all convex combinations of IID distributions. Subsequent results gave quantitative bounds of different forms [2–9]. de Finetti-type theorems had proven to be useful in various proofs. The quantum de Finetti theorems, for example, enable a substantially simplified analysis of many quantum information tasks such as quantum cryptography [7, 10], tomography [11], channel capacities [12] and complexity [9].

[1] Depending on the context, the term system may refer to a probability distribution, a quantum state, or a box.

R. Arnon-Friedman, *Device-Independent Quantum Information Processing*, Springer Theses, https://doi.org/10.1007/978-3-030-60231-4_8

The de Finetti theorems listed above cannot be used in the device-independent setting for various reasons.[2] In this chapter we present a de Finetti-type theorem, which was introduced in [13], that is applicable when working with parallel boxes. Our de Finetti theorem, termed "de Finetti reduction for correlations", is then used in the analysis of one of our showcases, namely, non-signalling parallel repetition, in Chap. 10.

The chapter is arranged as follows. We start by explaining the notion of permutation invariance in the device-independent context in Sect. 8.1. The de Finetti reduction is presented and proven in Sect. 8.2. Section 8.3 exemplifies how the reductions can be used in two different general ways (while Chap. 10 deals with a specific application). The theorems proven in Sect. 8.3 clarify in what sense we think of a de Finetti reduction as a reduction to IID in the device-independent setting.

In accordance with the rest of the thesis, the chapter focuses only on the case of two parties. All the statements can be extended to any number of parties, as can be seen in [13].

8.1 Permutation Invariance

As mentioned above, we are interested in considering permutation invariant parallel multi-round boxes. Let n be the number of games that can be played with the parallel box of interest $\mathrm{P}_{\boldsymbol{AB}|\boldsymbol{XY}}$. A permutation π is a bijective function $\pi : [n] \to [n]$. We denote $\pi(\boldsymbol{x}) = x_{\pi^{-1}(1)}, x_{\pi^{-1}(2)}, \ldots, x_{\pi^{-1}(n)}$ and similarly for $\pi(\boldsymbol{y})$, $\pi(\boldsymbol{a})$, and $\pi(\boldsymbol{b})$. A permutation invariant box[3] is defined as follows.

Definition 8.1 (*Permutation invariant box*) Given a parallel multi-round box $\mathrm{P}_{\boldsymbol{AB}|\boldsymbol{XY}}$, defined over $\mathcal{X}^n, \mathcal{Y}^n, \mathcal{A}^n, \mathcal{B}^n$, and a permutation $\pi : [n] \to [n]$ we denote by $\mathrm{P}_{\boldsymbol{AB}|\boldsymbol{XY}} \circ \pi$ the box defined by

$$\forall \boldsymbol{a}, \boldsymbol{b}, \boldsymbol{x}, \boldsymbol{y} \quad \left(\mathrm{P}_{\boldsymbol{AB}|\boldsymbol{XY}} \circ \pi\right)(\boldsymbol{a}, \boldsymbol{b}|\boldsymbol{x}, \boldsymbol{y}) = \mathrm{P}_{\boldsymbol{AB}|\boldsymbol{XY}}(\pi(\boldsymbol{a}), \pi(\boldsymbol{b})|\pi(\boldsymbol{x}), \pi(\boldsymbol{y})) \ . \quad (8.1)$$

A parallel multi-round box $\mathrm{P}_{\boldsymbol{AB}|\boldsymbol{XY}}$ is said to be permutation invariant if and only if

$$\forall \pi \quad P_{\boldsymbol{AB}|\boldsymbol{XY}} = \mathrm{P}_{\boldsymbol{AB}|\boldsymbol{XY}} \circ \pi \ .$$

Figure 8.1 illustrate the action of permuting a parallel box. The action of the permuted box can be understood as follows: First, the box applies the permutation π on the inputs. Second, it uses the initial box $\mathrm{P}_{\boldsymbol{AB}|\boldsymbol{XY}}$ to produce the intermediate outputs. Lastly, it applies the inverse permutation π^{-1} on the intermediate outputs

[2] The mentioned theorems rely on some initial subsystem structure and/or a bound on the dimension of the subsystems. In the device-independent setting one cannot start with such assumptions regarding the considered boxes in general.

[3] The definition and the derived theorem are independent of the nature of the box, i.e., if it is classical, quantum, non-signalling, or even signalling. This will be addressed in Sect. 8.2.

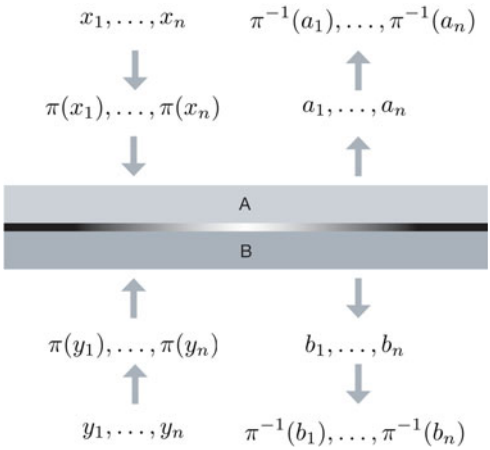

Fig. 8.1 Permutation of a box $\mathrm{P}_{\boldsymbol{AB|XY}}$. The permuted box, $\mathrm{P}_{\boldsymbol{AB|XY}} \circ \pi$ acts by first applying the permutation π on the inputs, then producing the outputs using the initial box $\mathrm{P}_{\boldsymbol{AB|XY}}$, and lastly applying the inverse permutation on the outputs. The input output distribution of the box is then defined according to Eq. (8.1). A box is said to be permutation invariant if for all π, $\mathrm{P}_{\boldsymbol{AB|XY}} = \mathrm{P}_{\boldsymbol{AB|XY}} \circ \pi$

and returns these final strings as the ultimate outputs. Note that only the inputs and the outputs of the box are being permuted, all using the same permutation π. In particular, we do not permute the parties, that is, Alice and Bob do not swap their inputs and outputs with one another.

As we are merely permuting the classical inputs and outputs, the box itself need not to have a subsystem structure. That is, we do not require, e.g., $\mathrm{P}_{A_1|X_1}$ to be a valid system (i.e., a conditional probability distribution). This is in contrast to, e.g., quantum de Finetti-type theorems such as [5, 7], where the permutation is applied on the quantum states themselves.[4] This distinction is relevant when wishing to discuss general parallel boxes (recall Sect. 6.1).

In some applications (e.g., the showcase considered in Chap. 10) one can easily show that it is sufficient to consider permutation invariant boxes without loss of generality. If this is not the case, it is also possible to *enforce* permutation invariance. A protocol, for example, can be modified to enforce the symmetry by adding a step in which a random permutation is applied[5] on the box and by this make it permutation invariant. Precisely: given *any* parallel box $\mathrm{P}_{\boldsymbol{AB|XY}}$, let

$$\tilde{\mathrm{P}}_{\boldsymbol{AB|XY}} = \frac{1}{n!} \sum_{\pi} \mathrm{P}_{\boldsymbol{AB|XY}} \circ \pi$$

be the result of applying a permutation π, chosen uniformly at random out of all permutations, on the original box. It can be easily verified that $\tilde{\mathrm{P}}_{\boldsymbol{AB|XY}}$ is indeed a permutation invariant box.

[4] In a quantum de Finetti statement a permutation takes a state $|\phi_1\rangle \otimes \ldots |\phi_n\rangle$ to $\left|\phi_{\pi^{-1}(1)}\right\rangle \otimes \ldots \left|\phi_{\pi^{-1}(n)}\right\rangle$. That is, the quantum states themselves are being permuted.

[5] Depending on the considered scenario, the application of the permutation may be a purely theoretical step or needs to be done in practice.

8.2 de Finetti Reductions for Correlations

A de Finetti-type theorem is any theorem that relates a permutation invariant system to a much more structured system called a de Finetti system. In our context, we consider permutation invariant and de Finetti boxes. A *de Finetti box* is defined as follows.

Definition 8.2 (*de Finetti box*[6]) A de Finetti box is any box of the form of a convex combination of IID boxes. That is, it is a box $\tau_{\boldsymbol{AB|XY}}$, defined over $\mathcal{X}^n, \mathcal{Y}^n, \mathcal{A}^n, \mathcal{B}^n$, such that

$$\tau_{\boldsymbol{AB|XY}} = \int \mathrm{O}_{AB|XY}^{\otimes n} \mathrm{dO}_{AB|XY} \ ,$$

where $\mathrm{dO}_{AB|XY}$ is some measure on the space of bipartite boxes over $\mathcal{A}, \mathcal{B}, \mathcal{X}$, and $\mathcal{Y}$ and $\mathrm{O}_{AB|XY}^{\otimes n}$ is the IID box defined by $\mathrm{O}_{AB|XY}$, i.e.,

$$\mathrm{O}_{AB|XY}^{\otimes n}(\boldsymbol{a}, \boldsymbol{b}|\boldsymbol{x}, \boldsymbol{y}) = \prod_{i\in[n]} \mathrm{O}_{AB|XY}(a_i, b_i|x_i, y_i) \ .$$

As seen from the above definition, by choosing different measures $\mathrm{dO}_{AB|XY}$ we define different de Finetti boxes. Depending on the measure, $\tau_{\boldsymbol{AB|XY}}$ may be classical, quantum, non-signalling, or even signalling between the two parties. If the measure $\mathrm{dO}_{AB|XY}$ assigns weight only to, e.g., non-signalling boxes $\mathrm{O}_{AB|XY}$, then the de Finetti box $\tau_{\boldsymbol{AB|XY}}$ is non-signalling as well. The other direction does not necessarily hold—there are convex combinations of signalling boxes that result in over-all non-signalling boxes.

A de Finetti reduction is a de Finetti-type theorem of a specific form: it sets an *inequality relation* between any permutation invariant box to a certain de Finetti box. Specifically, the following theorem is a de Finetti reduction for any permutation invariant conditional probability distribution [13].[7]

Theorem 8.3 (de Finetti reduction for conditional probability distributions) *For any $\mathcal{X}, \mathcal{Y}, \mathcal{A}, \mathcal{B}$, and n there exists a de Finetti box $\tau_{\boldsymbol{AB|XY}}$, defined over $\mathcal{X}^n, \mathcal{Y}^n, \mathcal{A}^n, \mathcal{B}^n$, such that for every permutation invariant box $\mathrm{P}_{\boldsymbol{AB|XY}}$*

$$\forall \boldsymbol{a}, \boldsymbol{b}, \boldsymbol{x}, \boldsymbol{y} \quad \mathrm{P}_{\boldsymbol{AB|XY}}(\boldsymbol{a}, \boldsymbol{b}|\boldsymbol{x}, \boldsymbol{y}) \leq (n+1)^{|\mathcal{X}||\mathcal{Y}|(|\mathcal{A}||\mathcal{B}|-1)} \ \tau_{\boldsymbol{AB|XY}}(\boldsymbol{a}, \boldsymbol{b}|\boldsymbol{x}, \boldsymbol{y}) \ . \quad (8.2)$$

To see why Theorem 8.3 is not trivial and what needs to be done to prove it, let us first consider a "bad choice" of a de Finetti box, $\tau^{\mathrm{bad}}_{\boldsymbol{AB|XY}}$. Imagine that we choose our de Finetti box to be the uniform distribution over $\mathcal{A}^n \times \mathcal{B}^n$ for all $\boldsymbol{x}$ and $\boldsymbol{y}$. With

[6] As previously mentioned, we focus on the case of two parties. The definition extends to any number of parties trivially.

[7] In [13], a more general version of Theorem 8.3 was proven, in which further symmetries of $\mathrm{P}_{\boldsymbol{AB|XY}}$ (on top of permutation invariance) can be exploited to construct more structured de Finetti boxes and prove de Finetti reductions with improved parameters. Theorem 8.3 was then derived as a corollary. To keep things (relatively) concise, we present in this thesis a direct proof of Theorem 8.3.

this choice, $\tau^{\text{bad}}_{\boldsymbol{AB}|\boldsymbol{XY}}(\boldsymbol{a},\boldsymbol{b}|\boldsymbol{x},\boldsymbol{y}) = (|\mathcal{A}||\mathcal{B}|)^{-n}$ for all $\boldsymbol{a}$, $\boldsymbol{b}$, $\boldsymbol{x}$, and $\boldsymbol{y}$. Then, the only inequality relation that holds is

$$\forall \boldsymbol{a},\boldsymbol{b},\boldsymbol{x},\boldsymbol{y} \quad \mathrm{P}_{\boldsymbol{AB}|\boldsymbol{XY}}(\boldsymbol{a},\boldsymbol{b}|\boldsymbol{x},\boldsymbol{y}) \leq (|\mathcal{A}||\mathcal{B}|)^{n} \ \tau^{\text{bad}}_{\boldsymbol{AB}|\boldsymbol{XY}}(\boldsymbol{a},\boldsymbol{b}|\boldsymbol{x},\boldsymbol{y}) \ ,$$

i.e., a relation with a pre-factor exponential in n. By choosing a "good" de Finetti box, we are able to get a pre-factor polynomial in n instead; this is crucial for applications of de Finetti reductions. In Sect. 8.3 we show how Theorem 8.3 can be utilised as a reduction to IID in certain scenarios.[8]

The proof of the theorem proceeds in two steps. In the first, an explicit de Finetti box $\tau_{\boldsymbol{AB}|\boldsymbol{XY}}$ is constructed and a lower-bound on its entries is calculated. In the second step the permutation invariance of $\mathrm{P}_{\boldsymbol{AB}|\boldsymbol{XY}}$ is used to upper-bound its entries. The theorem follows by combining the two bounds.

In the proofs below we use the following notation.

1. $|\mathcal{X}||\mathcal{Y}| = l$ and we identify each pair $(x, y) \in \mathcal{X} \times \mathcal{Y}$ with a label $j \in [l]$ by writing $(x, y) = j$.
2. $|\mathcal{A}||\mathcal{B}| = m$ and we identify each pair $(a, b) \in \mathcal{A} \times \mathcal{B}$ with a label $k \in [m]$ by writing $(a, b) = k$.
3. For all $j \in [l]$ and $k \in [m]$, $p^j_k \in [0, 1]$ such that $\sum_k p^j_k = 1$.
4. For all $j \in [l]$ and $k \in [m]$, $c^j_k = 1 - \sum_{t<k} p^j_t$.
5. For all $\boldsymbol{x}$, $\boldsymbol{y}$, and $j \in [l]$, $n^j = |\{i : (x_i, y_i) = j\}|$, i.e., n^j denotes the number of indices of $(\boldsymbol{x}, \boldsymbol{y})$ in which the type of inputs is $(x, y) = j$.
6. For all $\boldsymbol{x}$, $\boldsymbol{y}$, $\boldsymbol{a}$, $\boldsymbol{b}$, $j \in [l]$, and $k \in [m]$, $n^j_k = |\{i : (x_i, y_i) = j \wedge (a_i, b_i) = k\}|$, i.e., n^j_k denotes the number of indices of $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{a}, \boldsymbol{b})$ in which the type of inputs is $(x, y) = j$ and the type of outputs is $(a, b) = k$.

Note that by definition:

1. For all $j \in [l]$ and $k \in [m-1]$, $p^j_k \in [0, c^j_k]$ and $p^j_m = c^j_m$.
2. For all $j \in [l]$, $n^j_m = n^j - \sum_{k=1}^{m-1} n^j_k$.

According to Definition 8.2, a de Finetti box is defined via the choice of measure $\mathrm{dO}_{AB|XY}$. We think of a bipartite box $\mathrm{O}_{AB|XY}$ as a set of probabilities p^j_k, with the identification $\mathrm{O}_{AB|XY}(a, b|x, y) = p^j_k$ for $(x, y) = j$ and $(a, b) = k$. Thus, we can define a measure over $\mathrm{O}_{AB|XY}$ by a measure over the probabilities p^j_k. Our chosen measure is

$$\mathrm{dO}_{AB|XY} = \prod_{j=1}^{l} \frac{\mathrm{d}p^j_1}{c^j_1} \cdots \frac{\mathrm{d}p^j_{m-1}}{c^j_{m-1}} \ ,$$

where $\mathrm{d}p^j_k$ is the uniform measure over $[0, c^j_k]$ for c^j_k defined above. The resulting de Finetti box is given by

[8] A curious reader may already take a glimpse of Theorems 8.11 and 8.15.

$$\begin{aligned}\tau_{\boldsymbol{AB}|\boldsymbol{XY}}(\boldsymbol{a},\boldsymbol{b}|\boldsymbol{x},\boldsymbol{y}) &= \int \mathrm{O}_{AB|XY}^{\otimes n}\,\mathrm{dO}_{AB|XY} \\ &= \prod_{j=1}^{l}\left[\int_0^{c_1^j}\frac{\mathrm{d}p_1^j}{c_1^j}\left(p_1^j\right)^{n_1^j}\right]\cdots\left[\int_0^{c_{m-1}^j}\frac{\mathrm{d}p_{m-1}^j}{c_{m-1}^j}\left(p_{m-1}^j\right)^{n_{m-1}^j}\right] \\ &\quad\cdot\left(p_m^j\right)^{n^j-\sum_{k=1}^{m-1}n_k^j}\,.\end{aligned} \tag{8.3}$$

The measure $\mathrm{dO}_{AB|XY}$ assigns some weight to *all* conditional probability distributions $\mathrm{O}_{AB|XY}$. As a result, the de Finetti box in Eq. (8.3) is *signalling*. This is discussed in Sect. 8.4 below.

The following lower-bound on the entries of the above de Finetti box is proven in Appendix A.1:

Lemma 8.4 *For all* $\boldsymbol{a}$, $\boldsymbol{b}$, $\boldsymbol{x}$, *and* $\boldsymbol{y}$,

$$\tau_{\boldsymbol{AB}|\boldsymbol{XY}}(\boldsymbol{a},\boldsymbol{b}|\boldsymbol{x},\boldsymbol{y}) \geq \prod_{j=1}^{l}\binom{n^j}{n_1^j,\ldots,n_m^j}^{-1}\frac{1}{(n^j+1)^{m-1}}\,,$$

where $\tau_{\boldsymbol{AB}|\boldsymbol{XY}}$ *is as in Eq.* (8.3).

Next, we exploit the permutation invariance of $\mathrm{P}_{\boldsymbol{AB}|\boldsymbol{XY}}$ to prove the following upper-bound on it:

Lemma 8.5 *For every permutation invariant box* $\mathrm{P}_{\boldsymbol{AB}|\boldsymbol{XY}}$, *as in Definition 8.1, and for all* $\boldsymbol{a}$, $\boldsymbol{b}$, $\boldsymbol{x}$, *and* $\boldsymbol{y}$,

$$\mathrm{P}_{\boldsymbol{AB}|\boldsymbol{XY}}(\boldsymbol{a},\boldsymbol{b}|\boldsymbol{x},\boldsymbol{y}) \leq \prod_{j=1}^{l}\binom{n^j}{n_1^j,\ldots,n_m^j}^{-1}\,.$$

Proof To prove the lemma we bound the value of a specific entry $\mathrm{P}_{\boldsymbol{AB}|\boldsymbol{XY}}(\boldsymbol{a},\boldsymbol{b}|\boldsymbol{x},\boldsymbol{y})$ by counting how many entries $\mathrm{P}_{\boldsymbol{AB}|\boldsymbol{XY}}(\tilde{\boldsymbol{a}},\tilde{\boldsymbol{b}}|\boldsymbol{x},\boldsymbol{y})$ must have the same value as $\mathrm{P}_{\boldsymbol{AB}|\boldsymbol{XY}}(\boldsymbol{a},\boldsymbol{b}|\boldsymbol{x},\boldsymbol{y})$ due to permutation invariance. The normalisation of $\mathrm{P}_{\boldsymbol{AB}|\boldsymbol{XY}}$ then implies a bound on the value of the entries.

Denote

$$\mathcal{N}(\boldsymbol{a},\boldsymbol{b},\boldsymbol{x},\boldsymbol{y}) = \left|\left\{(\tilde{\boldsymbol{a}},\tilde{\boldsymbol{b}})\in\mathcal{A}\times\mathcal{B}:\mathrm{P}_{\boldsymbol{AB}|\boldsymbol{XY}}(\tilde{\boldsymbol{a}},\tilde{\boldsymbol{b}}|\boldsymbol{x},\boldsymbol{y}) = \mathrm{P}_{\boldsymbol{AB}|\boldsymbol{XY}}(\boldsymbol{a},\boldsymbol{b}|\boldsymbol{x},\boldsymbol{y})\right\}\right|\,.$$

The permutation invariance of $\mathrm{P}_{\boldsymbol{AB}|\boldsymbol{XY}}$ implies that $\mathcal{N}(\boldsymbol{a},\boldsymbol{b},\boldsymbol{x},\boldsymbol{y})$ is lower-bounded by the number permutations π for which $\pi(\boldsymbol{x}) = \boldsymbol{x}$, $\pi(\boldsymbol{y}) = \boldsymbol{y}$. To keep $\pi(\boldsymbol{x}) = \boldsymbol{x}$ and $\pi(\boldsymbol{y}) = \boldsymbol{y}$, the relevant permutations π are only allowed to permute indices with the same input type (x, y). The number of such permutations is exactly $\prod_{j=1}^{l}\binom{n^j}{n_1^j,\ldots,n_m^j}$. Thus,

$$\mathcal{N}(\boldsymbol{a},\boldsymbol{b},\boldsymbol{x},\boldsymbol{y}) \geq \prod_{j=1}^{l} \binom{n^j}{n_1^j,\ldots,n_m^j}$$

and

$$\mathrm{P}_{\boldsymbol{AB}|\boldsymbol{XY}}(\boldsymbol{ab}|\boldsymbol{xy}) \leq \frac{1}{\mathcal{N}(\boldsymbol{a},\boldsymbol{b},\boldsymbol{x},\boldsymbol{y})} \leq \prod_{j=1}^{l} \binom{n^j}{n_1^j,\ldots,n_m^j}^{-1}. \qquad \square$$

Proof of Theorem 8.3. Using Lemmas 8.4 and 8.5 one can easily prove Theorem 8.3. For all $\boldsymbol{a}$, $\boldsymbol{b}$, $\boldsymbol{x}$, and $\boldsymbol{y}$,

$$\begin{aligned}\frac{\mathrm{P}_{\boldsymbol{AB}|\boldsymbol{XY}}(\boldsymbol{a},\boldsymbol{b}|\boldsymbol{x},\boldsymbol{y})}{\tau_{\boldsymbol{AB}|\boldsymbol{XY}}(\boldsymbol{a},\boldsymbol{b}|\boldsymbol{x},\boldsymbol{y})} &\leq \frac{\prod_{j=1}^{l}\binom{n^j}{n_1^j,\ldots,n_m^j}^{-1}}{\prod_{j=1}^{l}\binom{n^j}{n_1^j,\ldots,n_m^j}^{-1}(n^j+1)^{-(m-1)}} \\ &\leq \prod_{j=1}^{l}(n^j+1)^{m-1} \\ &\leq (n+1)^{l(m-1)}\,. \end{aligned}$$

$\square$

To end this section let us give a last remark regarding Theorem 8.3. Notice the order of the quantifiers; *there exists one* de Finetti box for which Eq. (8.2) holds for *all* permutation invariant box. For the purpose of applications, one could also imagine a different statement in which for each permutation invariant box a de Finetti box is constructed (i.e., different permutation invariant boxes may be related to different de Finetti boxes). Such a statement has the potential of improving the obtained parameters and simplifying the use of the reduction in applications (see also [13] for examples of such statements).

8.3 Ways of Using the Reductions

The main motivation for considering de Finetti reductions as in Theorem 8.3 is to allow us to simplify the analysis of device-independent information processing tasks. However, it is a priori not clear how one can bring an inequality as that in Eq. (8.2) into work. The aim of this section is to exemplify the usage of the inequality in a mathematical way by considering two types of abstract applications. Chapter 10 discusses a more concrete application of the reduction to prove a non-signalling parallel repetition theorem.

To derive the results presented in this section we use an alternative, but equivalent, version of the de Finetti reduction; this is the topic of Sect. 8.3.1 below. Sections 8.3.2

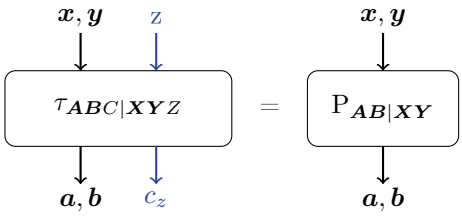

Fig. 8.2 post-selecting a box $\mathrm{P}_{\boldsymbol{AB|XY}}$ from an extension of $\tau_{\boldsymbol{AB|XY}}$. Conditioned on the output c_z, the resulting box is $\mathrm{P}_{\boldsymbol{AB|XY}}$. After [13]

and 8.3.3 present two ways of using the de Finetti reduction via the alternative formulation.

8.3.1 Post-selecting Permutation Invariant Boxes

Lemma 8.6 *There exists a de Finetti box $\tau_{\boldsymbol{AB|XY}}$ and a non-signalling extension*[9] *of it (Definition 3.2) to a larger box $\tau_{\boldsymbol{ABC|XYZ}}$ such that for every permutation invariant box $\mathrm{P}_{\boldsymbol{AB|XY}}$ there exists an input z and an output of this input c_z for which*

$$\forall \boldsymbol{a}, \boldsymbol{b}, \boldsymbol{x}, \boldsymbol{y} \quad \tau_{\boldsymbol{ABC|XYZ}}(\boldsymbol{a}, \boldsymbol{b}, c_z|\boldsymbol{x}, \boldsymbol{y}, z) = \frac{1}{(n+1)^{l(m-1)}} \mathrm{P}_{\boldsymbol{AB|XY}}(\boldsymbol{a}, \boldsymbol{b}|\boldsymbol{x}, \boldsymbol{y}) \ ,$$

where $l = |\mathcal{X}||\mathcal{Y}|$ and $m = |\mathcal{A}||\mathcal{B}|$.

This lemma states that there exists a de Finetti box $\tau_{\boldsymbol{AB|XY}}$ and a non-signalling extension of it $\tau_{\boldsymbol{ABC|XYZ}}$ such that any permutation invariant box $\mathrm{P}_{\boldsymbol{AB|XY}}$ can be *post-selected* from it with probability greater or equal to $\frac{1}{(n+1)^{l(m-1)}}$. When we say that $\mathrm{P}_{\boldsymbol{AB|XY}}$ can be post-selected we mean that there exists an input z to $\tau_{\boldsymbol{ABC|XYZ}}$ and an output c_z of this input such that with probability $\tau_{C|Z}(c_z|z) \geq \frac{1}{(n+1)^{l(m-1)}}$ the resulting box (the "post-measurement box", using terminology borrowed from quantum physics) is $\mathrm{P}_{\boldsymbol{AB|XY}}$ (see Fig. 8.2). Note that we consider a single extension $\tau_{\boldsymbol{ABC|XYZ}}$ of the box $\tau_{\boldsymbol{AB|XY}}$, and by choosing different inputs z we can post-select different boxes $\mathrm{P}_{\boldsymbol{AB|XY}}$.

It is easy to see how to derive Lemma 8.6 from Theorem 8.3 by using the formalism introduced in [14, 15] of partitions of a conditional probability distribution. We repeat here the relevant statements.

Definition 8.7 A partition of a box $\mathrm{Q}_{\boldsymbol{AB|XY}}$ is a family of pairs $\left\{\left(q_c, \mathrm{Q}^c_{\boldsymbol{AB|XY}}\right)\right\}_c$ where $q_c \geq 0$, $\sum_c q_c = 1$, and the boxes $\mathrm{Q}^c_{\boldsymbol{AB|XY}}$ are such that

$$\mathrm{Q}_{\boldsymbol{AB|XY}} = \sum_c q_c \cdot \mathrm{Q}^c_{\boldsymbol{AB|XY}} \ .$$

[9] Note that $\tau_{\boldsymbol{AB|XY}}$ may be signalling, as in our previous statements. The fact that we are considering non-signalling extensions only means that the marginals $\tau_{\boldsymbol{AB|XY}}$ and $\tau_{C|Z}$ of $\tau_{\boldsymbol{ABC|XYZ}}$ are well defined.

Lemma 8.8 (Lemma 9 in [14]) *Given a box* $Q_{AB|XY}$*, there exists a partition with element* $\left(q_c, Q^c_{AB|XY}\right)$ *if and only if*

$$\forall \boldsymbol{a}, \boldsymbol{b}, \boldsymbol{x}, \boldsymbol{y} \quad q_c \cdot Q^c_{AB|XY}(\boldsymbol{a}, \boldsymbol{b}|\boldsymbol{x}, \boldsymbol{y}) \leq Q_{AB|XY}(\boldsymbol{a}, \boldsymbol{b}|\boldsymbol{x}, \boldsymbol{y}) \ .$$

Lemma 8.9 (Lemma 3.2 in [15]) *Given a box* $Q_{AB|XY}$*, let* Z *be the set of all partitions* $\left\{\left(q_{c_z}, Q^{c_z}_{AB|XY}\right)\right\}_{c_z}$ *of* $Q_{AB|XY}$*. Then, there exist a non-signalling extension* $Q_{ABC|XYZ}$ *of* $Q_{AB|XY}$*, an input* z*, and an output* c_z *such that*

$$\forall \boldsymbol{a}, \boldsymbol{b}, \boldsymbol{x}, \boldsymbol{y} \quad Q_{ABC|XYZ}(\boldsymbol{a}, \boldsymbol{b}, c_z|\boldsymbol{x}, \boldsymbol{y}, z) = q_{c_z} \cdot Q^{c_z}_{AB|XY}(\boldsymbol{a}, \boldsymbol{b}|\boldsymbol{x}, \boldsymbol{y}) \ .$$

Using the lemmas above and Theorem 8.3 we can now prove Lemma 8.6.

Proof of Lemma 8.6. The above lemmas together with Theorem 8.3 imply that for any permutation invariant box $P_{AB|XY}$, $\left(\frac{1}{(n+1)^{l(m-1)}}, P_{AB|XY}\right)$ is an element of a partition of $\tau_{AB|XY}$. Moreover, there exists a box $\tau_{ABC|XYZ}$ and an input z such that with probability $\frac{1}{(n+1)^{l(m-1)}}$ the resulting box is $P_{AB|XY}$:

$$\forall \boldsymbol{a}, \boldsymbol{b}, \boldsymbol{x}, \boldsymbol{y} \quad \tau_{ABC|XYZ}(\boldsymbol{a}, \boldsymbol{b}, c_z|\boldsymbol{x}, \boldsymbol{y}, z) = \frac{1}{(n+1)^{l(m-1)}} P_{AB|XY} \ . \qquad \square$$

Lemma 8.6 is used in the following sections to illustrate two ways in which de Finetti reductions can be used in applications.

8.3.2 Failure Probability of a Test

We start by considering the following abstract application. Let $\mathcal{T}$ be a test which interacts with a box $P_{AB|XY}$ and outputs "success" or "fail" with some probabilities. One can think about this test, which can be chosen according to the application being considered, as a way to quantify the success probability of a protocol when the box $P_{AB|XY}$ is given as input. For example, if one considers an estimation, or a tomography, protocol a test can be chosen to output "success" when the estimated box is close to the actual box [7]. Another type of test will be considered explicitly in Sect. 10.2.

A test $\mathcal{T}$ interacts with $P_{AB|XY}$ by supplying it with inputs $\boldsymbol{x}, \boldsymbol{y}$, according to some probability distribution $\Pr_{\mathcal{T}}(\boldsymbol{x}, \boldsymbol{y})$ over $\mathcal{X}^n \times \mathcal{Y}^n$, and collecting its outputs $\boldsymbol{a}, \boldsymbol{b}$. This is illustrated in Fig. 8.3. The test then decides whether to output 0 or 1 depending on $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{a}$, and $\boldsymbol{b}$. Given a test $\mathcal{T}$, we denote by $\Pr_{\text{fail}}(P_{AB|XY})$ the failure probability of the test, i.e., the probability that $\mathcal{T}$ outputs 0 after interacting with $P_{AB|XY}$:

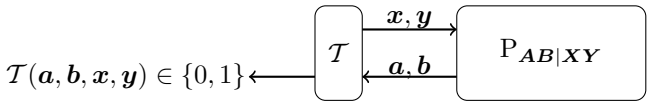

Fig. 8.3 The test $\mathcal{T}$ interacts with $\mathrm{P}_{\boldsymbol{AB|XY}}$ by supplying it with inputs $\boldsymbol{x}$, $\boldsymbol{y}$ and collecting its outputs $\boldsymbol{a}$, $\boldsymbol{b}$. The test then decides whether to output 0 or 1 depending on $\boldsymbol{x}$, $\boldsymbol{y}$, $\boldsymbol{a}$, and $\boldsymbol{b}$. If the output is 0 then we say that the test failed. After [13]

$$\Pr_{\text{fail}}(\mathrm{P}_{\boldsymbol{AB|XY}}) = \sum_{\boldsymbol{x},\boldsymbol{y}} \Pr_{\mathcal{T}}(\boldsymbol{x},\boldsymbol{y}) \sum_{\boldsymbol{a},\boldsymbol{b}:\mathcal{T}(\boldsymbol{a},\boldsymbol{b},\boldsymbol{x},\boldsymbol{y})=0} \mathrm{P}_{\boldsymbol{AB|XY}}(\boldsymbol{a},\boldsymbol{b}|\boldsymbol{x},\boldsymbol{y}) \ .$$

The event of failing the test can therefore be defined as an event over $\mathcal{X}^n \times \mathcal{Y}^n \times \mathcal{A}^n \times \mathcal{B}^n$.

We consider permutation invariant tests, defined as follows.

Definition 8.10 A test $\mathcal{T}$ is permutation invariant if and only if for all boxes $\mathrm{P}_{\boldsymbol{AB|XY}}$ and all permutations π we have

$$\Pr_{\text{fail}}(\mathrm{P}_{\boldsymbol{AB|XY}}) = \Pr_{\text{fail}}(\mathrm{P}_{\boldsymbol{AB|XY}} \circ \pi) \ .$$

Using the de Finetti reduction in Theorem 8.3 we can prove upper bounds of the following type:

Theorem 8.11 *Let $\mathcal{T}$ be a permutation invariant test. Then for every box $\mathrm{P}_{\boldsymbol{AB|XY}}$*

$$\Pr_{\text{fail}}(\mathrm{P}_{\boldsymbol{AB|XY}}) \leq (n+1)^{l(m-1)} \Pr_{\text{fail}}(\tau_{\boldsymbol{AB|XY}}) \ ,$$

where $\tau_{\boldsymbol{AB|XY}}$ is the de Finetti box given in Eq. (8.3).

The importance of de Finetti reductions is already obvious from Theorem 8.11—if one wishes to prove an upper bound on the failure probability of the test $\mathcal{T}$, then instead of proving it for all boxes $\mathrm{P}_{\boldsymbol{AB|XY}}$, it is sufficient to prove it for the de Finetti box $\tau_{\boldsymbol{AB|XY}}$ and "pay" for it with the additional polynomial pre-factor of $(n+1)^{l(m-1)}$. Since the de Finetti box can be written as a convex combination of IID boxes, this can highly simplify the calculations of the bound. In this sense the de Finetti reduction acts as a *reduction to IID*.

In many cases one finds that the bound on $\Pr_{\text{fail}}(\tau_{\boldsymbol{AB|XY}})$ is exponentially small in n. For an estimation protocol, the failure probability of the test, when interacting with an IID box, can be shown to be exponentially small in the number of boxes n used for the estimation, using Chernoff bounds. This is also the case when dealing with security proofs—the failure probability of a protocol, when a de Finetti box is given as input, is usually exponentially small in the number of boxes n used in the protocol. If this is indeed the case then the polynomial pre-factor of $(n+1)^{l(m-1)}$ becomes irrelevant in the asymptotic limit of large n. In other words, an exponentially small bound on $\Pr_{\text{fail}}(\tau_{\boldsymbol{AB|XY}})$ implies an exponentially small bound on $\Pr_{\text{fail}}(\mathrm{P}_{\boldsymbol{AB|XY}})$.

Let us prove Theorem 8.11 using the de Finetti reduction given as Theorem 8.3.

Proof of Theorem 8.11. We follow here a similar proof given in [16] for the quantum post-selection theorem [7]. First, since the test $\mathcal{T}$ is permutation invariant it is sufficient to consider only permutation invariant boxes. To see this recall that for any box $\mathrm{P}_{\boldsymbol{AB|XY}}$ and permutation π we have $\Pr_{\text{fail}}(\mathrm{P}_{\boldsymbol{AB|XY}}) = \Pr_{\text{fail}}(\mathrm{P}_{\boldsymbol{AB|XY}} \circ \pi)$ according to Definition 8.10. Therefore we also have by linearity[10]

$$\Pr_{\text{fail}}(\mathrm{P}_{\boldsymbol{AB|XY}}) = \frac{1}{n!}\sum_{\pi} \Pr_{\text{fail}}(\mathrm{P}_{\boldsymbol{AB|XY}} \circ \pi) = \Pr_{\text{fail}}\left(\frac{1}{n!}\sum_{\pi} \mathrm{P}_{\boldsymbol{AB|XY}} \circ \pi\right) .$$

The box $\frac{1}{n!}\sum_{\pi} \mathrm{P}_{\boldsymbol{AB|XY}} \circ \pi$ is permutation invariant and therefore we can consider only permutation invariant boxes without loss of generality.

Next we define the following probabilities. Let $\Pr_{\text{fail}\wedge c_z}(\tau_{\boldsymbol{ABC|XYZ}})$ be the probability that the second part of the box, $\tau_{C|Z}$, is used with the input z and the output is c_z and that the first part of the box, $\tau_{\boldsymbol{AB|XY}}$, fails the test $\mathcal{T}$ at the same time. That is,

$$\Pr_{\text{fail}\wedge c_z}(\tau_{\boldsymbol{ABC|XYZ}}) = \Pr_{\text{fail}}(\tau_{\boldsymbol{AB|XY}}) \cdot \tau_{C|Z}(c_z|z) .$$

In a similar way we define $\Pr_{\text{fail}|c_z}(\tau_{\boldsymbol{ABC|XYZ}})$ to be the probability that $\tau_{\boldsymbol{AB|XY}}$ fails the test $\mathcal{T}$ *given* that c_z is the output of $\tau_{C|Z}$ when used with the input z. We have

$$\Pr_{\text{fail}|c_z}(\tau_{\boldsymbol{ABC|XYZ}}) = \frac{\Pr_{\text{fail}\wedge c_z}(\tau_{\boldsymbol{ABC|XYZ}})}{\tau_{C|Z}(c_z|z)} \leq \frac{\Pr_{\text{fail}}(\tau_{\boldsymbol{AB|XY}})}{\tau_{C|Z}(c_z|z)}$$

since $\Pr_{\text{fail}\wedge c_z}(\tau_{\boldsymbol{ABC|XYZ}}) \leq \Pr_{\text{fail}}(\tau_{\boldsymbol{AB|XY}})$ always holds.

Lemma 8.6 implies that $\tau_{C|Z}(c_z|z) \geq \frac{1}{(n+1)^{l(m-1)}}$ and that $\Pr_{\text{fail}|c_z}(\tau_{\boldsymbol{ABC|XYZ}}) = \Pr_{\text{fail}}(\mathrm{P}_{\boldsymbol{AB|XY}})$ (given that the output was c_z, the resulting box is $\mathrm{P}_{\boldsymbol{AB|XY}}$). All together we get $\Pr_{\text{fail}}(\mathrm{P}_{\boldsymbol{AB|XY}}) \leq (n+1)^{l(m-1)} \Pr_{\text{fail}}(\tau_{\boldsymbol{AB|XY}})$ as required. □

8.3.3 Diamond Norm

Theorem 8.3 allows for a simple treatment of cases that can be analysed using the notation of a test. In some information processing tasks this is not possible and different ways of utilising the reductions are needed. In this section we consider the task of distinguishing two channels acting on boxes. The channels can describe, for example, a cryptographic protocol.[11]

[10] Linearity refers here to the linearity of the test in the box $\mathrm{P}_{\boldsymbol{AB|XY}}$, which follows from the fact that the test interacts only once with $\mathrm{P}_{\boldsymbol{AB|XY}}$ (or, in other words, the test gets only a single copy of the box).

[11] Let us briefly explain why the notation of a test considered in Sect. 8.3.1 is not appropriate in the cryptographic setting. When considering tests, we were interested in events defined over $\mathcal{X}^n \times \mathcal{Y}^n \times \mathcal{A}^n \times \mathcal{B}^n$. Whether an output of a protocol (a key, for example) is secure to use cannot

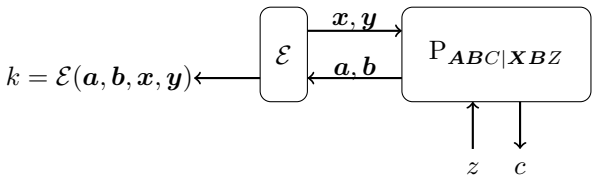

Fig. 8.4 The channel $\mathcal{E} \otimes \mathbb{I}$ acts on an extension $\mathrm{P}_{\boldsymbol{ABC}|\boldsymbol{XBZ}}$ of $\mathrm{P}_{\boldsymbol{AB}|\boldsymbol{XY}}$ and outputs a classical string $k \in \{0,1\}^t$ according to the probability $\mathrm{E}_K(k)$. After [13]

When considering quantum protocols the distinguishing advantage is given by the diamond norm [17]. The distance between two channels $\mathcal{E}$ and $\mathcal{F}$ which act on quantum states ρ_{AB} is given by $\|\mathcal{E} - \mathcal{F}\|_\diamond = \max_{\rho_{ABC}} \|(\mathcal{E} - \mathcal{F}) \otimes \mathbb{I}\, \rho_{ABC}\|_1$ where ρ_{ABC} is a purification of ρ_{AB} and $\|\cdot\|_1$ is the trace distance. Informally, the idea is that in order to distinguish two channels we are not only allowed to choose the input state to the channels, ρ_{AB}, but also keep to ourselves a purifying state ρ_C.

Although the definition of the diamond norm includes a maximisation over all states ρ_{ABC} it was proven, using the quantum post-selection theorem [7], that when considering permutation invariant channels it is sufficient to calculate the distance for a specific quantum de Finetti state. Motivated by this, we give a similar bound on a distance analogous to the diamond norm for channels which act on boxes (instead of quantum states).

In the following, we denote by $\mathcal{P}$ the set of all boxes $\mathrm{P}_{\boldsymbol{AB}|\boldsymbol{XY}}$ and by $\mathcal{K}$ the set of all probability distributions P_K over $\{0,1\}^t$ for some $t \in \mathbb{N}$. We consider channels of the form $\mathcal{E} : \mathcal{P} \to \mathcal{K}$ which interact with boxes $\mathrm{P}_{\boldsymbol{AB}|\boldsymbol{XY}}$ and output a classical bit string $k \in \{0,1\}^t$ of some length $t \geq 0$ with some probability $\mathrm{P}_K(k)$. The connection between the channel and the box is illustrated in Fig. 8.4.[12]

The probability distribution of the output depends on the channel $\mathcal{E}$ itself and is given by the following definition.

Definition 8.12 The probability that a channel $\mathcal{E}$ outputs a string $k \in \{0,1\}^t$ when interacting with $\mathrm{P}_{\boldsymbol{AB}|\boldsymbol{XY}}$ is

$$\mathrm{E}_K(k) = \sum_{\boldsymbol{x},\boldsymbol{y}} \mathrm{Pr}_{\mathcal{E}}(\boldsymbol{x},\boldsymbol{y}) \sum_{\substack{\boldsymbol{a},\boldsymbol{b}: \\ \mathcal{E}(\boldsymbol{a},\boldsymbol{b},\boldsymbol{x},\boldsymbol{y})=k}} \mathrm{P}_{\boldsymbol{AB}|\boldsymbol{XY}}(\boldsymbol{a},\boldsymbol{b}|\boldsymbol{x},\boldsymbol{y})$$

where $\mathrm{Pr}_{\mathcal{E}}(x)$ is the probability that $\mathcal{E}$ inputs $\boldsymbol{x}$, $\boldsymbol{y}$ to $\mathrm{P}_{\boldsymbol{AB}|\boldsymbol{XY}}$ and $\mathcal{E}(\boldsymbol{a},\boldsymbol{b},\boldsymbol{x},\boldsymbol{y})$ is the function according to which the output of the channel is determined. Analogously,

$$\mathrm{E}_{K|C}(k|c) = \sum_{\boldsymbol{x},\boldsymbol{y}} \mathrm{Pr}_{\mathcal{E}}(\boldsymbol{x},\boldsymbol{y}) \sum_{\substack{\boldsymbol{a},\boldsymbol{b}: \\ \mathcal{E}(\boldsymbol{a},\boldsymbol{b},\boldsymbol{x},\boldsymbol{y})=k}} \mathrm{P}_{\boldsymbol{AB}|\boldsymbol{XYC}}(\boldsymbol{a},\boldsymbol{b}|\boldsymbol{x},\boldsymbol{y},c)\ .$$

be defined as an event. Security depends on the *process* of producing the key rather on the specific *data* that was produced during the run of the protocol.

[12] Figure 8.4 is almost identical to Fig. 8.3, describing a test. The difference between the two scenarios lies in the quantity that we wish to bound; see the previous footnote.

Definition 8.13 The distance between two channels $\mathcal{E}, \mathcal{F} : \mathcal{P} \to \mathcal{K}$ according to the diamond norm is

$$\|\mathcal{E} - \mathcal{F}\|_\diamond = \max_{\mathrm{P}_{\boldsymbol{ABC|XYZ}}} \| (\mathcal{E} - \mathcal{F}) \otimes \mathbb{I}(\mathrm{P}_{\boldsymbol{ABC|XYZ}})\|_1 \ ,$$

where the maximisation is over all boxes $\mathrm{P}_{\boldsymbol{AB|XY}}$ and all possible extensions of them and

$$\begin{aligned} \mathcal{E} \otimes \mathbb{I}(\mathrm{P}_{\boldsymbol{ABC|XYZ}}) &= \mathcal{E} \otimes \mathbb{I}(\mathrm{P}_{\boldsymbol{AB|XYC}} \cdot \mathrm{P}_{C|Z}) \\ &= \mathrm{E}_{K|C} \cdot \mathrm{P}_{C|Z} \ . \end{aligned}$$

$\mathcal{F} \otimes \mathbb{I}(\mathrm{P}_{\boldsymbol{ABC|XYZ}})$ is defined in a similar way.

Similarly to the concept of a permutation invariant test presented in Definition 8.10, we define a permutation invariant channel:

Definition 8.14 A channel $\mathcal{E}$ is permutation invariant if for all boxes $\mathrm{P}_{\boldsymbol{AB|XY}}$ and all permutations π we have

$$\mathcal{E}(\mathrm{P}_{\boldsymbol{AB|XY}}) = \mathcal{E}(\mathrm{P}_{\boldsymbol{AB|XY}} \circ \pi) \ .$$

Using the de Finetti reduction, Theorem 8.3, we prove the following theorem.

Theorem 8.15 *For any two permutation invariant channels* $\mathcal{E}, \mathcal{F} : \mathcal{P} \to \mathcal{K}$

$$\|\mathcal{E} - \mathcal{F}\|_\diamond \leq (n+1)^{l(m-1)} \max_{\tau_{\boldsymbol{ABC|XYZ}}} \| (\mathcal{E} - \mathcal{F}) \otimes \mathbb{I}(\tau_{\boldsymbol{ABC|XYZ}})\|_1 \tag{8.4}$$

where $\tau_{\boldsymbol{ABC|XYZ}}$ *is a non-signalling extension of the de Finetti box* $\tau_{\boldsymbol{AB|XY}}$ *where given in Eq.* (8.3).

Theorem 8.15 tells us that when looking to bound the diamond norm for permutation invariant channels, one does not need to optimise over all possible boxes (as in Definition 8.13) but can consider only extensions of de Finetti boxes[13] without loss of generality. This gives us another example as to why a de Finetti reduction is a *reduction to IID* technique. As in the case of Theorem 8.11 if one is able to find an exponentially small upper bound on $\| (\mathcal{E} - \mathcal{F}) \otimes \mathbb{I}(\tau_{\boldsymbol{ABC|XYZ}})\|_1$, an exponentially small upper bound on $\|\mathcal{E} - \mathcal{F}\|_\diamond$ follows. That is, the polynomial pre-factor $(n+1)^{l(m-1)}$ does not affect the asymptotic behaviour.

The proof of Theorem 8.15 builds on the following lemma.

Lemma 8.16 *For every two permutation invariant channels* $\mathcal{E}, \mathcal{F} : \mathcal{P} \to \mathcal{K}$ *where* P_K *is a probability distribution over* $k \in \{0,1\}^t$ *for some* $t > 0$*, and all* $\mathrm{P}_{\boldsymbol{ABC|XYZ}}$*,*

$$\| (\mathcal{E} - \mathcal{F}) \otimes \mathbb{I}(\mathrm{P}_{\boldsymbol{ABC|XYZ}})\|_1 \leq (n+1)^{l(m-1)} \| (\mathcal{E} - \mathcal{F}) \otimes \mathbb{I}(\tau^{\mathrm{P}_{\boldsymbol{ABC|XYZ}}}_{\boldsymbol{ABC|XYZ}})\|_1$$

[13] Note, however, that the extension $\tau_{\boldsymbol{ABC|XYZ}}$ itself cannot be written as a convex combination of IID boxes, only its marginal $\tau_{\boldsymbol{AB|XY}}$ is a de Finetti box. Furthermore, $\tau_{\boldsymbol{AB|XY}}$ may be signalling in general, as before.

where $\tau^{\mathrm{P}_{ABC|XYZ}}_{ABC|XYZ}$ *is a non-signalling extension of* $\tau_{AB|XY}$ *which depends on the specific box* $\mathrm{P}_{ABC|XYZ}$.

The proof of the lemma follows by using Lemma 8.6 in order to construct a specific convex decomposition of $\tau_{AB|XY}$ from a convex decomposition of $\mathrm{P}_{AB|XY}$. A detailed proof is given in Appendix A.2.

Theorem 8.15 now easily follows from Lemma 8.16:

Proof of Theorem 8.15 Using Lemma 8.16,

$$\begin{aligned}\|\mathcal{E}-\mathcal{F}\|_{\diamond} &= \max_{\mathrm{P}_{ABC|XYZ}} \|\,(\mathcal{E}-\mathcal{F})\otimes\mathbb{I}(\mathrm{P}_{ABC|XYZ})\|_1 \\ &\leq (n+1)^{l(m-1)} \max_{\substack{\mathrm{P}_{ABC|XYZ}\\ \tau_{ABC'|XYZ}}} \|\,(\mathcal{E}-\mathcal{F})\otimes\mathbb{I}(\tau^{\mathrm{P}_{ABC|XYZ}}_{ABC'|XYZ})\|_1 \\ &\leq (n+1)^{l(m-1)} \max_{\tau_{ABC|XYZ}} \|\,(\mathcal{E}-\mathcal{F})\otimes\mathbb{I}(\tau_{ABC|XYZ})\|_1\end{aligned}$$

where $\tau_{ABC|XYZ}$ is a non-signalling extension of $\tau_{AB|XY}$. □

8.4 Impossibility Results

Before concluding this chapter, let us discuss the directions in which one could hope to further develop the technique of device-independent de Finetti reductions. We do so by presenting several impossibility results with regards to different variants of Theorem 8.3.

8.4.1 Restricted de Finetti Box

First, as explained in the above sections, our de Finetti box, given in Eq. (8.3), is a *signalling* box. Clearly, this raises some difficulties when coming to use the different theorems presented in this chapter.[14] Ideally, we would have wished to have a de Finetti reduction in which the de Finetti box $\tau_{AB|XY}$ can be quantum or non-signalling when starting with a quantum or non-signalling box $\mathrm{P}_{AB|XY}$. That is, we wish to find reductions of the form (with some c polynomial[15] in n):

$$\mathrm{P}^{\mathrm{quant}}_{AB|XY} \leq c\cdot\tau^{\mathrm{quant}}_{AB|XY} \quad ; \quad \mathrm{P}^{\mathrm{ns}}_{AB|XY} \leq c\cdot\tau^{\mathrm{ns}}_{AB|XY}\,, \tag{8.5}$$

where $\mathrm{P}^{\mathrm{quant}}_{AB|XY}$ and $\tau^{\mathrm{quant}}_{AB|XY}$ are quantum boxes and, similarly, $\mathrm{P}^{\mathrm{ns}}_{AB|XY}$ and $\tau^{\mathrm{ns}}_{AB|XY}$ are non-signalling boxes.

[14] Though this does not make them useless; see Chap. 10.

[15] Weaker statements, e.g., with a pre-factor sub-exponential in n, may also be of interest in certain applications.

Sadly, such reductions cannot be true when considering general permutation invariant boxes $\mathrm{P}^{\text{quant}}_{\boldsymbol{AB|XY}}$ and $\mathrm{P}^{\text{ns}}_{\boldsymbol{AB|XY}}$. One way to see that this is the case is by considering the task of parallel repetition of games (which acts as one of our showcases; see Sect. 4.1). Reductions as those in Eq. (8.5) will imply very strong parallel repetition results. Indeed, if, e.g., $\mathrm{P}^{\text{quant}}_{\boldsymbol{AB|XY}} \leq c \cdot \tau^{\text{quant}}_{\boldsymbol{AB|XY}}$ holds for any permutation invariant quantum box $\mathrm{P}^{\text{quant}}_{\boldsymbol{AB|XY}}$, then it follows that, for *any* game,

$$w\left(\mathrm{P}^{\text{quant}}_{\boldsymbol{AB|XY}}\right) \leq c \cdot w\left(\tau^{\text{quant}}_{\boldsymbol{AB|XY}}\right) = \mathrm{poly}(n) \cdot \omega^n \ , \tag{8.6}$$

where $w(\circ)$ is the winning probability of the considered box in the repeated game, ω is the winning probability of the optimal quantum strategy in a single game, and $\mathrm{poly}(n)$ is some polynomial of n, possibly depending on the alphabet of the RVs A, B, X, and Y. However, there are examples of games (in the classical, quantum, and non-signalling case) for which a strong decrease in the winning probability with the number of games played n, as in Eq. (8.6), does not hold; recall Sect. 4.1. Thus, reductions as in Eq. (8.5) cannot be true.

Knowing that Eq. (8.5) is not more than a wishful thinking, one could hope for the next best thing, i.e., an approximate version of the reduction. Concretely, we are interested in reductions of the form

$$\mathrm{P}^{\text{quant}}_{\boldsymbol{AB|XY}} \leq c \cdot \tau^{\text{approx-quant}}_{\boldsymbol{AB|XY}} \quad ; \quad \mathrm{P}^{\text{ns}}_{\boldsymbol{AB|XY}} \leq c \cdot \tau^{\text{approx-ns}}_{\boldsymbol{AB|XY}} \ , \tag{8.7}$$

where $\tau^{\text{approx-quant}}_{\boldsymbol{AB|XY}}$ is an *approximately*-quantum de Finetti box and $\tau^{\text{approx-ns}}_{\boldsymbol{AB|XY}}$ is an *approximately*-non-signalling one. By approximately-quantum (and analogously for the non-signalling case) we mean that the de Finetti box can be written as

$$\tau^{\text{approx-quant}}_{\boldsymbol{AB|XY}} = \int \left(\mathrm{O}^{\text{quant}}_{AB|XY}\right)^{\otimes n} \mathrm{dO}^{\text{quant}}_{AB|XY} + \int \left(\mathrm{O}^{\text{non-quant}}_{AB|XY}\right)^{\otimes n} \mathrm{dO}^{\text{non-quant}}_{AB|XY} \ ,$$

where $\mathrm{dO}^{\text{quant}}_{AB|XY}$ and $\mathrm{dO}^{\text{non-quant}}_{AB|XY}$ are measures over quantum and non-quantum single-round boxes, respectively, and $\int \mathrm{dO}^{\text{non-quant}}_{AB|XY}$ is, say, exponentially small in n and/or assigns weight only to boxes $\mathrm{O}^{\text{non-quant}}_{AB|XY}$ which are close to quantum boxes, under some distance measure.[16]

Parallel repetition results can, again, be used to show that such reductions cannot hold in general, at least in the non-signalling case. Here the reason lies in the observation that the reductions in Eq. (8.7) are independent of the choice of *distribution* over the inputs $\mathcal{X}^n$ and $\mathcal{Y}^n$ (while they may depend on the *alphabet* of the inputs). Thus, they would imply general parallel repetition results which hold for any distribution over the inputs to the parallel boxes. As there are games for which such non-signalling parallel repetition results do not hold [18], at best $\mathrm{P}^{\text{ns}}_{\boldsymbol{AB|XY}} \leq c \cdot \tau^{\text{approx-ns}}_{\boldsymbol{AB|XY}}$ cannot be true in general.

[16] The hope here is that by adding the additional weight on non-quantum or signalling boxes one could account for the "gap" between Eq. (8.6) and the known parallel repetition results.

By this we learn that we ought to consider reductions that also include the input distribution $\mathrm{P}_{\boldsymbol{XY}}$:

$$\mathrm{P}_{\boldsymbol{XY}}\mathrm{P}^{\text{quant}}_{\boldsymbol{AB|XY}} \leq c \cdot \mathrm{P}_{\boldsymbol{XY}}\tau^{\text{approx-quant}}_{\boldsymbol{AB|XY}} \ , \tag{8.8}$$

$$\mathrm{P}_{\boldsymbol{XY}}\mathrm{P}^{\text{ns}}_{\boldsymbol{AB|XY}} \leq c \cdot \mathrm{P}_{\boldsymbol{XY}}\tau^{\text{approx-ns}}_{\boldsymbol{AB|XY}} \ . \tag{8.9}$$

The case of $\mathrm{P}_{\boldsymbol{XY}} = \mathrm{Q}_{XY}^{\otimes n}$ is of special interest. For such distributions, two results are known. In Sect. 10.2 we prove a result in the *flavour* of Eq. (8.9) using the de Finetti reduction given as Theorem 8.3. The result, which originally appeared as part of [19], is stated informally as Theorem 10.2. Roughly speaking, it says that observed data that is sampled using a permutation invariant non-signalling parallel box looks *as if* it was sampled using an approximately non-signalling IID box.

In [20] a reduction similar to that of Eq. (8.9) was proven by combining the de Finetti reduction in Theorem 8.3 together with another de Finetti-type theorem, presented in [21]. Their theorem can be written as follows[17]:

Theorem 8.17 (Theorem 4.3 in [20]) *For any non-signalling permutation invariant parallel box* $\mathrm{P}_{\boldsymbol{AB|XY}}$ *and distribution* Q_{XY}

$$\mathrm{Q}_{XY}^{\otimes n}\mathrm{P}_{\boldsymbol{AB|XY}} \leq \int \tilde{\mathrm{F}}\left(\mathrm{O}_{ABXY}\right)^{2n} \mathrm{O}_{ABXY}^{\otimes n} \mathrm{d}\mathrm{O}_{ABXY} \ , \tag{8.10}$$

where

$$\tilde{\mathrm{F}}\left(\mathrm{O}_{ABXY}\right) = \min\left\{\max_{\mathrm{R}_{A|X}} \mathrm{F}\left(\mathrm{Q}_{XY}\mathrm{R}_{A|X}, \mathrm{O}_{AXY}\right), \ \max_{\mathrm{R}_{B|Y}} \mathrm{F}\left(\mathrm{Q}_{XY}\mathrm{R}_{B|Y}, \mathrm{O}_{BXY}\right)\right\}$$

for F *the fidelity.*

To see that Eq. (8.10) is in the spirit of Eq. (8.9) note that $\tilde{\mathrm{F}}\left(\mathrm{O}_{ABXY}\right)$ is some measure of how far O_{ABXY} is from $\mathrm{Q}_{XY}\tilde{\mathrm{O}}_{AB|XY}$ for a non-signalling box $\tilde{\mathrm{O}}_{AB|XY}$. Recall that the fidelity is small when the distributions are far from one another; thus, $\tilde{\mathrm{F}}\left(\mathrm{O}_{ABXY}\right)^{2n}$ assures that only negligible weight is assigned to distributions O_{ABXY} originating from highly signalling boxes (or with marginals O_{XY} far from Q_{XY}).

We conjecture that reductions similar to Eq. (8.8), relevant for quantum boxes, should also hold. Yet, up to date there are no proofs in this direction (the difficulty in deriving such a statement is discussed in Chap. 10).

8.4.2 Extension to an Adversary

Another direction in which one may wish to extend our de Finetti reductions is relevant for device-independent cryptographic protocols. To explain what we aim

[17] We present only the bipartite case; [20, Theorem 4.3] is stated for an arbitrary number of parties.

for, let us first discuss the quantum variant of Theorem 8.15, also called the post-selection technique, developed in [7].[18] The post-selection theorem implies that for any two permutation invariant quantum channels, $\mathcal{E}$ and $\mathcal{F}$, acting on quantum states $\rho_{\boldsymbol{Q_A Q_B}} \in \mathcal{S}(\mathscr{H}_{Q_A Q_B}^{\otimes n})$ for some bipartite Hilbert space $\mathscr{H}_{Q_A Q_B}$ of dimension d,

$$\|\mathcal{E} - \mathcal{F}\|_\diamond \leq (n+1)^{d^2-1} \| (\mathcal{E} - \mathcal{F}) \otimes \mathbb{I}(\tau_{\boldsymbol{Q_A Q_B} E}) \|_1 \tag{8.11}$$

where $\tau_{\boldsymbol{Q_A Q_B} E}$ is a purification of a given de Finetti state. Equation (8.11) should be compared to Eq. (8.4); while Eq. (8.4) includes a maximisation over all possible non-signalling extensions of the de Finetti box, in Eq. (8.11) we consider only a single purification. The reason is simple—in the quantum case all purifications of a state are equivalent up to local unitaries. Furthermore (and crucially for applications), there exists a purification of a de Finetti state that has a very special form. To purify

$$\tau_{\boldsymbol{Q_A Q_B}} = \int \left(\sigma_{Q_A Q_B}\right)^{\otimes n} \mathrm{d}\sigma_{Q_A Q_B}$$

we can first purify the states $\sigma_{Q_A Q_B}$ to get

$$\tau_{\boldsymbol{Q_A Q_B} E'} = \int \left(\sigma_{Q_A Q_B E'}\right)^{\otimes n} \mathrm{d}\sigma_{Q_A Q_B E'}$$

and then purify the state $\tau_{\boldsymbol{Q_A Q_B} E'}$ using an additional system E'' to account for the convex combination of the pure states $\left(\sigma_{Q_A Q_B E'}\right)^{\otimes n}$. This defines us the pure state $\tau_{\boldsymbol{Q_A Q_B} E' E''}$. Denoting $E = E' E''$ we get our pure $\tau_{\boldsymbol{Q_A Q_B} E}$.

In the cryptographic setting the quantum register E is considered to belong to the adversary. Hence, any information about the structure of the system kept in it could be useful when analysing security. Equation (8.11) in combination with the observation regarding the structure of the purification, $\tau_{\boldsymbol{Q_A Q_B} E' E''}$, we learn that the main task when proving security is to analyse the IID case, as in Chap. 7 (see [7, 16] for the detailed explanation). That is, the quantum de Finetti reduction can be used as a reduction to IID in quantum cryptography.

In contrast, in general, it is impossible to prove a modified version of Theorem 8.15 in which the extension $\tau_{\boldsymbol{ABC}|\boldsymbol{XYZ}}$ of our de Finetti box $\tau_{\boldsymbol{AB}|\boldsymbol{XY}}$ will be as structured as the quantum state $\tau_{\boldsymbol{Q_A Q_B} E}$. In particular, even if we can start with a de Finetti reduction where both $\mathrm{P}_{\boldsymbol{AB}|\boldsymbol{XY}}$ and $\tau_{\boldsymbol{AB}|\boldsymbol{XY}}$ are non-signalling,[19] it is impossible to derive a theorem which would imply that the analysis of device-independent cryptography in the presence of a non-signalling adversary can be reduced to the analysis under the

[18] Reference [7] presented the first de Finetti reduction, i.e., an inequality relation between permutation invariant systems and de Finetti systems (all previous de Finetti-type theorems gave other types of relations between the two systems). The term "de Finetti reduction" was not used at that time and the authors chose the name "post-selection technique" as they first proved the quantum analogue of Lemma 8.6.

[19] In the presence of certain types of symmetries (in addition to permutation invariance) one can derive such de Finetti reductions; see [13].

IID assumption. This is due to the impossibility result of [22], which asserts that, while exponential privacy amplification in the presence of a non-signalling adversary is possible under the IID assumption [23], it is impossible when the IID assumption is dropped.

8.4.3 Other de Finetti-Type Theorems

A final remark is with regards to the more common type of de Finetti theorem, in which one bounds the trace distance between an *n-exchangeable* system and a de Finetti one. More specifically, let us first consider the classical case, i.e., a system is a probability distribution. $\mathrm{P}_{A_1,\ldots,A_k}$ is permutation invariant if it is invariant under any permutation of $A_1, \ldots, A_k$ (as before). We say that $\mathrm{P}_{A_1,\ldots,A_k}$ is n-exchangeable, for $n \geq k$, if it is a marginal of some permutation invariant $\mathrm{P}_{A_1,\ldots,A_n}$. In [24] a bound on the *distance* between an n-exchangeable probability distribution and a de Finetti distribution was proven.[20] Results of this type were also proven for quantum states [6, 25] and non-signalling boxes [8].

Let us focus on the non-signalling case [8]. There, a conditional probability distribution $\mathrm{P}_{A_1,\ldots,A_n|X_1,\ldots,X_n}$ is said to be non-signalling if the box cannot be used to signal from any subset of parties $I \subset [n]$ to the rest of the parties $[n] \setminus I$. Permutation invariance is defined with respect to permutations $\pi : [n] \to [n]$. Similarly to the classical case described above, $\mathrm{P}_{A_1,\ldots,A_k|X_1,\ldots,X_k}$ is n-exchangeable, for $n \geq k$, when it is the marginal of a permutation invariant non-signalling box $\mathrm{P}_{A_1,\ldots,A_n|X_1,\ldots,X_n}$. We then have the following bound [8, Theorem 3] (using the above notation):

Theorem 8.18 ([8]) *For any permutation invariant non-signalling box* $\mathrm{P}_{A_1,\ldots,A_n|X_1,\ldots,X_n}$ *and any* $k < n$ *there exists a de Finetti box* $\tau_{A_1,\ldots,A_k|X_1,\ldots,X_k}$ *such that*

$$\left|\mathrm{P}_{A_1,\ldots,A_k|X_1,\ldots,X_k} - \tau_{A_1,\ldots,A_k|X_1,\ldots,X_k}\right| \leq \min\left\{\frac{2k|\mathcal{X}||\mathcal{A}|^{|\mathcal{X}|}}{n}, \frac{k(k-1)|\mathcal{X}|}{n}\right\}.$$

The crucial thing to note here is that the boxes $\mathrm{P}_{A_1,\ldots,A_k|X_1,\ldots,X_k}$ and $\mathrm{P}_{A_1,\ldots,A_n|X_1,\ldots,X_n}$ are a very special type of parallel boxes: the non-signalling conditions must hold for any division of the indices in $[n]$. This implies that the for any $i, j \in [n]$, A_i is independent of the inputs X_j for $j \neq i$. Theorems such as Theorem 8.18 cannot be proven for general parallel boxes since they study exchangeable boxes, which inherently require the ability to consider the marginals of the boxes.

[20] In this language, the original result of de Finetti [1] stated that all infinitely-exchangeable distributions (i.e., distributions that are n-exchangeable for *any* $n \geq k$) are equal to distributions of the form of a convex combination of IID distributions.

References

1. de Finetti B (1969) Sulla proseguibilità di processi aleatori scambiabili. Rend Matem Trieste 53–67
2. Diaconis P, Freedman D (1980) Finite exchangeable sequences. Annal Probab 745–764
3. Raggio G, Werner R (1989) Quantum statistical mechanics of general mean field systems. Helv Phys Acta 62(8):980–1003
4. Caves CM, Fuchs CA, Schack R (2002) Unknown quantum states: the quantum de-Finetti representation. J Math Phys 43:4537
5. Renner R (2007) Symmetry of large physical systems implies independence of subsystems. Nat Phys 3(9):645–649
6. Christandl M, König R, Mitchison G, Renner R (2007) One-and-a-half quantum de Finetti theorems. Commun Math Phys 273(2):473–498
7. Christandl M, König R, Renner R (2009) Postselection technique for quantum channels with applications to quantum cryptography. Phys Rev Lett 102(2):020504
8. Christandl M, Toner B (2009) Finite de Finetti theorem for conditional probability distributions describing physical theories. J Math Phys 50:042104
9. Brandao FG, Harrow AW (2013) Quantum de Finetti theorems under local measurements with applications. In: Proceedings of the forty-fifth annual ACM symposium on Theory of computing, pp. 861–870. ACM
10. Leverrier A (2014) Composable security proof for continuous-variable quantum key distribution with coherent states. arXiv:1408.5689
11. Christandl M, Renner R (2012) Reliable quantum state tomography. Phys Rev Lett 109(12):120403
12. Berta M, Christandl M, Renner R (2011) The quantum reverse Shannon Theorem based on one-shot information theory. Commun Math Phys 306(3):579–615
13. Arnon-Friedman R, Renner R (2015) de Finetti reductions for correlations. J Math Phys 56(5):052203
14. Hänggi E, Renner R, Wolf S (2010) Efficient device-independent quantum key distribution. In: Advances in cryptology–EUROCRYPT 2010, pp 216–234. Springer
15. Hänggi E, Renner R (2010) Device-independent quantum key distribution with commuting measurements. arXiv:1009.1833
16. Renner R (2010) Simplifying information-theoretic arguments by post-selection. In: NATO advanced research workshop quantum cryptography and computing: theory and implementation, vol 26, pp 66–75. IOS Press
17. Kitaev AY (1997) Quantum computations: algorithms and error correction. Russ Math Surv 52(6):1191–1249
18. Holmgren J, Yang L (2017) (a counterexample to) parallel repetition for non-signaling multiplayer games. In: Electronic colloquium on computational complexity (ECCC), vol 24, p 178
19. Arnon-Friedman R, Renner R, Vidick T (2016) Non-signaling parallel repetition using de finetti reductions. IEEE Trans Inf Theory 62(3):1440–1457
20. Lancien C, Winter A (2016) Parallel repetition and concentration for (sub-)no-signalling games via a flexible constrained de finetti reduction. Chic J Theor Comput Sci (11)
21. Lancien C, Winter A (2017) Flexible constrained de finetti reductions and applications. J Math Phys 58(9):092203
22. Arnon-Friedman R, Ta-Shma A (2012) Limits of privacy amplification against nonsignaling memory attacks. Phys Rev A 86(6):062333
23. Hänggi E, Renner R, Wolf S (2009) Quantum cryptography based solely on bell's theorem. arXiv:0911.4171
24. Diaconis P, Freedman D (1980) Finite exchangeable sequences. Ann Probab 745–764
25. König R, Renner R (2005) A de finetti representation for finite symmetric quantum states. J Math Phys 46(12):122108