Chapter 12
Outlook

The development and application of the concept of reductions to IID, taking the form of de Finetti theorems, flourished in "standard" quantum information processing in the last decade and more. The tools used, unfortunately, were not applicable when considering device-independent information processing tasks, where the devices being analysed are uncharacterised. The reductions presented in the thesis, namely the de Finetti reduction (Chap. 8) and the entropy accumulation theorem (Chap. 9), are the first to be applicable in the device-independent setting. As such, they have opened the possibility of a significantly simpler analysis of device-independent information processing tasks.

Among the advantages of applying the approach of reductions to IID in the device-independent setting, compared to directly analysing the most general case, are tighter quantitive results and modular proofs. The thesis' showcases, used to exemplify the usage of the reductions, indeed report such benefits. Our proof of non-signalling parallel repetition (Chap. 10) is automatically valid for any complete-support game with any number of players and achieves an exponential decrease that matches that of IID strategies. Our security proof for device-independent quantum key distribution (Chap. 11) achieves tight key rates, as under the IID assumption, that are significantly better than all prior results and can be easily adapted to other related protocols.

With this in mind, it is interesting to investigate how the presented reductions or variants thereof can be used in the analysis of other tasks. Let us discuss a partial list of questions and possible future work that we find intriguing.[1]

[1] We list here questions that are not directly related to the showcases considered in the thesis. For concrete open questions regarding parallel repetition (e.g., extensions of the results) and device-independent quantum key distribution (such as possible improvements and experimental implementations) see Sects. 10.4 and 11.4, respectively.

R. Arnon-Friedman, *Device-Independent Quantum Information Processing*,
Springer Theses, https://doi.org/10.1007/978-3-030-60231-4_12

12.1 Two-Party Device-Independent Quantum Cryptography

In the cryptographic protocols discussed in the thesis we considered two honest and cooperating parties, Alice and Bob. Two-party cryptography, on the other hand, refers to cryptographic protocols in which Alice and Bob do not trust each other. When considering device-independent two-party cryptography the dishonest party (which can be either Alice or Bob) takes the role of the adversary and hence is allowed to prepare the device used to implement the protocol. References [1, 2] present examples for such protocols.

The above mentioned works study the security of the protocols under the IID assumption (or a closely related assumption). Clearly, it is interesting to see if the analysis can be extended to capture the most general adversarial scenario, which, in the case of these protocols, includes the use of sequential boxes. Applying a reduction to IID can be beneficial here. Unfortunately, it is not clear whether the entropy accumulation theorem, in its current form, can be of use in such protocols. The reason is that the Markov-chain conditions stated in Eq. (9.4) do not hold, at least when considering the most obvious choices of random variables.[2]

In some cases, one can overcome the problem by considering "imaginary" protocols, closely related to the "real" protocol, in which the Markov-chain conditions do hold. The idea is then to reduce the problem of proving the security of the real protocol to that of the imaginary one and perform the analysis of the imaginary protocol using the entropy accumulation theorem.

Such a proof technique is used in [3]. There, the protocol of interest is a device-independent entanglement certification protocol and its analysis requires an upper bound on the smooth max-entropy, rather than a lower bound on the smooth min-entropy as in cryptographic scenarios.[3] Thus, the steps used in [3] are not directly applicable to two-party device-independent cryptography. It is interesting to see if similar ideas can be useful in cryptographic scenarios as well.

Alternatively, one could also try to prove a different variant of the entropy accumulation theorem in which the Markov-chain conditions are replaced by some other restrictions on the sequential process, which are fulfilled by two-party cryptographic protocols. (Finding such conditions is interesting by itself). As discussed in Sect. 9.2.1, some conditions on the process must appear in the theorem, since entropy does not accumulate in any sequential process. While the Markov-chain conditions are sufficient, we currently have no reason to believe that they are necessary; it might as well be that some weaker or incomparable conditions also suffice.

[2] In the case of two-party cryptography, the natural choice to make when trying to use the entropy accumulation theorem is one in which the $\boldsymbol{O}$ systems belong to the honest party and the $\boldsymbol{S}$ systems to the dishonest party. One can easily come up with boxes that do not fulfil Eq. (9.4) with these choices.

[3] In the considered scenarios the two quantities are not dual to one another; see [3] for the details.

12.2 Parallel Device-Independent Quantum Cryptography

Another type of cryptographic protocols to which the presented reductions to IID are not applicable in a trivial manner are ones in which the most general analysis should be done with quantum parallel boxes. An example is the parallel device-independent quantum key distribution protocol of [4], in which all the non-local games are played in parallel with the device (as in the parallel repetition question). While [4] includes a security proof that goes beyond the IID scenario, it achieves quantitively weak results. This raises the fundamental question of whether parallel adversaries, i.e., adversaries that can create parallel boxes, are stronger than sequential and IID adversaries (which are proven to have the same strength by our work). To learn the answer to this question there is a need to supply tight key rates for parallel device-independent quantum key distribution protocols.

Utilising a reduction to IID instead of analysing the general case directly, as in [4], will almost surely lead to stronger, perhaps even tight, results. Alas, the known reductions are not directly applicable here. The entropy accumulation theorem is not useful in this case since it is restricted to sequential boxes and here one ought to analyse parallel boxes. The de Finetti reduction, while suitable for parallel boxes, is a priori not applicable here since the de Finetti box does not include the adversary and is not a quantum box; see Sect. 8.4. It is therefore interesting to investigate whether the analysis can somehow be manipulated so that the known techniques can be utilised to prove security of parallel device-independent quantum cryptography or, otherwise, whether other types of reductions, more adequate for such scenarios, can be developed.

12.3 Device-Independent Tomography

One of the applications of the "original" quantum de Finetti reduction (also called the post-selection technique) [5] is a technique for a reliable quantum state tomography [6]. The technique is said to be reliable since it reports not just an estimation of the quantum state but also a confidence region around the estimated state, which acts as a meaningful "error bar". This is of crucial importance as the other more standard approaches, such as the maximum-likelihood optimisation and least-square-error estimation, suffer from systematic errors [7].

Recently, the device-independent equivalents of the maximum-likelihood optimisation and least-square-error estimation were considered in [8]. The goal of such device-independent tomographic techniques is to report an estimated quantum box from the observed finite statistics. Apart from systematic errors, device-independent tomographic procedures as above are also at risk of providing a non-quantum box, since up to date it is unknown how to perform optimisation problems over the set of quantum boxes. In analogy to [6], applying our de Finetti reductions to achieve reliable device-independent tomography can therefore be of interest.

References

1. Fu H, Miller CA (2018) Local randomness: examples and application. Phys Rev A 97(3):032324
2. Ribeiro J, Kaniewski J, Helsen J, Wehner S et al (2018) Device independence for two-party cryptography and position verification with memoryless devices. Phys Rev A 97(6):062307
3. Arnon-Friedman R, Bancal J-D (2019) Device-independent certification of one-shot distillable entanglement. New J Phys 21(3):033010
4. Jain R, Miller CA, Shi Y (2017) Parallel device-independent quantum key distribution. arXiv:1703.05426
5. Christandl M, König R, Renner R (2009) Postselection technique for quantum channels with applications to quantum cryptography. Phys Rev Lett 102(2):020504
6. Christandl M, Renner R (2012) Reliable quantum state tomography. Phys Rev Lett 109(12):120403
7. Schwemmer C, Knips L, Richart D, Weinfurter H, Moroder T, Kleinmann M, Gühne O (2015) Systematic errors in current quantum state tomography tools. Phys Rev Lett 114(8):080403
8. Lin P-S, Rosset D, Zhang Y, Bancal J-D, Liang Y-C (2018) Device-independent point estimation from finite data and its application to device-independent property estimation. Phys Rev A 97(3):032309