Cone programs and generalised probabilistic theories

Abstract

The following is an extended abstract for the two papers [Sikora, J. and Selby, J.H. *"A simple proof of the impossibility of bit-commitment in generalised probabilistic theories using cone programming."* arXiv:1711.02662 (2017)] and [Selby, J.H. and Sikora, J. *"How to make unforgeable money in generalised probabilistic theories."* arXiv:1803.10279 (2018)].

1 From GPTs to GITs

The framework of generalised probabilistic theories (GPTs) has been a powerful way to study classical and quantum theory "from the outside". More precisely, GPTs are a landscape of potential theories which are broad enough to encompass any conceivable theory of nature which admit an *operational* description. This generality however comes with a challenge. Many of the tools that we use in quantum and classical theory do not obviously extend to the generalised setting. Hence, our understanding of these alternative theories is limited. Specifically, the information theoretic consequences of these alternative theories is not entirely clear. For example, what is their computational power, and what kinds of cryptographic protocols are possible?

There is a broad and growing literature on this, but it remains piecemeal and fragmented. This should not be surprising: the development of classical and quantum information theory was not a single coherent and systematic study, indeed both are still being developed to this day. We should therefore not expect the implications of studying these generalised theories be so easily forthcoming. Having said that, we should be able to learn from the development of these two information theories and our understanding of GPTs to hopefully have a systematic approach to the development of *generalised information theories* (GITs).

2 Optimisation problems

Optimisation problems are central to the study of both quantum and classical information theory. For example we may want to find some protocol that minimises the amount of information that can be learnt by an eavesdropper in some crytographic set up, or we may wish to maximise the amount of information that can transmitted by a particular channel. Moreover, various primitive information theoretic notions can be expressed as particular optimisation problems (which may or may not have a specific operational interpretation), for example, entropies, fidelities and trace-distances.

In classical information theory, these optimisation problems typically are of the form of *linear programs* whilst their quantum generalisation are typically expressed as *semidefinite programs* (SDPs). Indeed, much of the recent development in quantum information theory relies on formulating problems as SDPs which have both useful analytic properties as well as efficient numerical algortithms. The natural question to then pose is, what is the analogous optimisation problem for GPTs?

Conveniently, there is a generalisation of both linear and semidefinite programs which is precisely what we need. These are known as *cone programs* a.k.a. linear conic optimisation problems. These are well-studied in the optimization community, see for example [1]. The sorts of problems that they describe are of the form:

$$\sup\{\langle C, X\rangle \mid \phi(X) = b, X \in K\}$$

where we are trying to maximise $\langle C, X \rangle$ with C some fixed vector, $\phi(X) = b$ is an affine constraint on the possible choices of X and K is some convex cone to which X must belong.

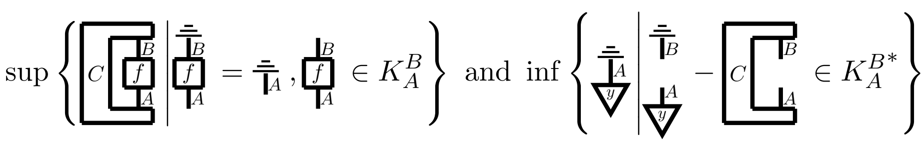
If we restrict to the case that K is a simplicial based cone we obtain linear programming and in the case that K is the cone of positive semidefinite matrices we obtain semidefinite programming. Such cones naturally arise in classical (resp. quantum) theory as the cone of processes with fixed input and output, and so it is easy to see how these become ubiquitous whilst studying such theories.

In the case of linear programs and SDPs we mentioned that there are both useful analytic properties and efficient numerical algorithms for these optimisation problems. Unfortunately, the latter of these does not remain true when considering arbitrary cones. In particular, there are particular cones for which these problems can be in NP or even uncomputable. However, luckily many of the analytic tools for SDPs do remain valid in the general case. In particular, we can always define a *dual* program which, under certain weak assumptions, is equivalent to the original problem. This is defined as:

$$\inf \{ \langle b, y \rangle \mid \phi^*(y) - C \in K^* \}$$

where we are now optimising over vectors y with ϕ^* the adjoint of ϕ and K^* the dual cone of K.

To gain some more intuition for these optimisation problems it is convenient to switch to a diagrammatic representation. For example, if we want to find the optimal causal process with input A and output B, which lives inside some cone denoted K_A^B then this, and its dual, can be denoted as:



respectively.

The dual often provides a new perspective on the original (primal) problem. The primal typically being defined in operational terms whilst the dual typically lacks such an interpretation. Giving such a diagrammatic perspective however allows us to at least identify some of the components of the dual with some operational process, and so we get a new operational perspective on the same problem. It is optimisation problems of this form that we have considered in [6] and [7], and in both cases the change in perspective offered by the dual program was vital to the solution.

3 Examples

We consider two cryptographic primitives, bit (or integer) commitment and the construction of unforgeable money, in the setting of GPTs. For a full description of these protocols, the definition of the GPT framework, and proofs see [7] and [6] respectively. Here we will simply state the results and provide a diagrammatic presentation of the relevant cone programs used to prove the result.

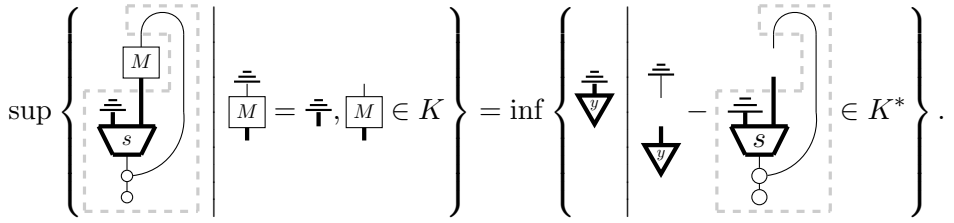
Bit-commitment [7] **Thm. 1** *For GPTs satisfying the No-restriction Hypothesis [2] and the Purification Principle [2], in any integer-commitment protocol, Alice and Bob's cheating probabilities satisfy*

$$P_A \cdot P_B \geq \frac{1}{n}$$

This proves that integer-commitment is impossible since if Bob cannot cheat, i.e., $P_B \approx 1/n$, we have that Alice can cheat almost perfectly, making it insecure.

This statement generalises the fact that quantum bit-commitment is impossible [4, 3], and gives an alternative proof that bit-commitment in GPTs is impossible, see [2].

The cone program (and dual) of interest capture Bob's cheating probability as:

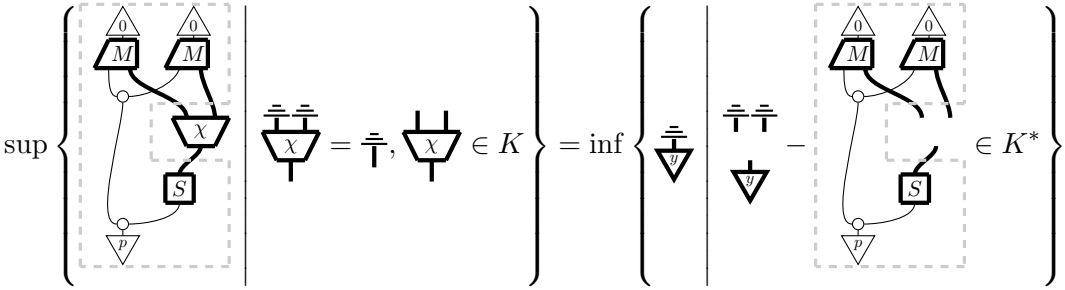


That is, it is the maximum probability that Bob can succesfully guess a randomly generated integer only given access to one half of a bipartite state. Here we optimise over the possible measurements M that Bob can perform.

Aside from using this as a proof of principle that cone programming is useful, the most exciting part of this result, at least for the study of GPTs, is that it provides us with a lower bound on cheating which is independent of the theory that we are considering. This contrasts with typical results in GPTs in which to obtain numerical values we typically must restrict to a specific theory. This is therefore a surprising result for the study of GPTs and demonstrates the power of the use of cone programs for studying GITs.

Unforgeable money [6] **Thm. 2** *For any GPT we have a dichotomy. Either practically unforgeable money is possible (as is the case in quantum theory, see e.g. [8, 5]) or perfect counterfeiting is possible (as is the case in classical theory). Interestingly, there is no middle ground.*

The cone program (and dual) of interest which captures the maximum probability of successfully counterfeiting is:



Moreover, under fairly weak assumptions one can show that the only GPT that does not support unforgeable money is classical theory. Therefore our work provides much stronger evidence for the possibility of secure money than the standard proofs relying on the validity of quantum theory.

4 Conclusion

The application of cone programming to the study of GPTs offers the potential for a systematic way to investigate information theoretic properties of these alternative theories. We have illustrated this with the two examples above with hopes that this tool will find many future uses in different scenarios. Some potential scenarios for future research include fully fledged GITs, GPT combs, higher order transformations and indefinite causal structures.

References

[1] Stephen Boyd and Lieven Vandenberghe. *Convex Optimization*. Cambridge University Press, 2004.

[2] Giulio Chiribella, Giacomo Mauro D'Ariano, and Paolo Perinotti. Probabilistic theories with purification. *Physical Review A*, 81(6):062348, 2010.

[3] Hoi-Kwong Lo and Hoi Fung Chau. Why quantum bit commitment and ideal quantum coin tossing are impossible. *Physica D: Nonlinear Phenomena*, 120(1–2):177–187, 1998.

[4] Dominic Mayers. Unconditionally secure quantum bit commitment is impossible. *Phys. Rev. Lett.*, 78(17):3414–3417, 1997.

[5] Abel Molina, Thomas Vidick, and John Watrous. Optimal counterfeiting attacks and generalizations for Wiesner's quantum money. In *Proceedings of the 7th Conference on Theory of Quantum Computation, Communication, and Cryptography*, volume 7582 of *Lecture Notes in Computer Science*, pages 45–64, 2013.

[6] John H. Selby and Jamie Sikora. How to make unforgeable money in generalised probabilistic theories, 2018. arXiv:1803.10279v1.

[7] Jamie Sikora and John Selby. A simple proof of the impossibility of bit-commitment in generalised probabilistic theories using cone programming. *arXiv preprint arXiv:1711.02662*, 2017.

[8] Stephen Wiesner. Conjugate coding. *SIGACT News*, 15(1):78–88, 1983.