Quantum Protocols within Spekkens' Toy Model

Leonardo Disilvestro
CNRS LTCI, Departement Informatique et Reseaux,
Telecom ParisTech,
23 Avenue d'Italie, 75214 Paris, France
leonardo.disilvestro@telecom-paristech.fr

Damian Markham
CNRS LTCI, Departement Informatique et Reseaux,
Telecom ParisTech,
23 Avenue d'Italie, 75214 Paris, France
markham@enst.fr

Full paper can be found `http://perso.telecom-paristech.fr/~disilves/QPL.html`

1 Intro and motivation

Quantum theory is known to provide advantages with respect to classical information processing tasks and protocols. In broader terms, it can even be argued that it provides a whole new framework to access and manipulate information, where rules are different and gains are often higher than in classical information theory. These gains are often broadly referred to as '*quantum supremacy*'. While some of the most celebrated cases of quantum supremacy relate to computational tasks (e.g. Shor and Groover's algorithms), there are many other examples where the advantages are not computational. These improvements touch upon other aspects of information theory and range from communication complexity to the security properties of quantum key distribution (QKD). Although the first quantum protocols date back to the early 80s, there is not yet a communal agreement regarding which features of quantum theory are truly responsible for these improvements. Over the years several candidates have been proposed and, among the many, Bell non-locality and contextuality are often considered as the 'quantum signatures' of those advantages (for example [4, 6]) . That is, they are believed to be responsible for quantum *computational* improvements. At the same time, less clear is the link between these two distinctive quantum phenomena and non-computational protocols — for example, non-locality and contextuality do not explicitly play any role in standard QKD protocols. In particular there are many interesting quantum protocols, such as blind and verified computation [3], secret sharing [2], error correcting codes, and continuous variable QKD which present some form of quantum supremacy without any explicit use of Bell non-locality nor contextuality. These are the tasks we are interested in studying within a simple, fully classical, and local theory commonly known as the Spekkens toy model [7]. Given some figures of merit encoding the advantage of the quantum protocol at hand and due to the local nature of the toy model, being able to show the existence of a toy protocol with matching figures of merit will indicate that non-locality should not be a necessary ingredient to obtain the given quantum advantage.

More explicitly, the toy model is a local hidden variable (LHV) theory phenomenologically very close to quantum mechanics as it reproduces many distinctly quantum phenomena such as the incompatibility of measurements, interference, no cloning, remote steering, teleportation, etc [7]. However, due to its LHV nature it cannot reproduce any non-local or contextual behaviour. On the one hand translating quantum protocols to the toy model cannot reproduce quantum computational speeds up, on the other hand it directly suggests that the original quantum protocol does not relay on non-locality or contextuality. In particular, recalling that correlations between multipartite systems can be expressed in a hierarchy of non-local behaviours, our work can be considered a study or quantum protocols within a local but steerable theory [9].

Submitted to:
QPL 2016

The motivation of this work is hence double-folded. Firstly, it analyzes which kind of protocols and tasks are fundamentally compatible with the toy model. The toy model fits within a framework of epistemically restricted theories [8]: these theories distinguish between the underlying ontic states[1], which represent the 'real' state of the system and is completely hidden to an observer, and the epistemic states[2] which represent an observer's statistical description of the ontic states. Only epistemic states can be directly accessed, prepared, and measured. Crucially, in order to represent valid states they also need to respect a knowledge-restraining principle which, *de facto*, limits how much an observer is allowed to know about the underlying hidden ontic distribution. Casting quantum protocols within the toy model further expands Spekkens' work by studying which quantum tasks are compatible with such class of theories and the relations of these protocols to LHV theories. However, this work also helps to pinpoint the core features behind the existence of many quantum protocols with better than classical figures of merit. Due to the inherit local but steerable nature of these toy models our results suggest that in many cases steering correlations, rather than the stronger Bell non-local ones, should indeed be enough for the realization of the studied protocols. As a further motivation, some toy models are also related to physically well-motivated restrictions of quantum theory, such as Gaussian quantum optics [8], suggesting more experimentally accessible realization of quantum protocols.

2 Contributions and results

Starting from the work of Pusey [5] — where a notation for the toy model reminiscent of the quantum stabilizer formalism is defined — we develop and analyze toy protocols based on quantum stabilizers. We begin by explicitly introducing a partial trace operation, purifications and their equivalence up to local transformation on the reference system, as well as irreversible transformations. These additions allow us to formally define quantum stabilizer protocols and obtain the following three results. Firstly, we prove the existence of a model for universal toy computation based on single system measurements and toy graph states. We call it 'measurement based toy computation' model to highlight its similarity with measurement based quantum computation model (MBQC). This in turn allows us to translate to the toy model the protocol for blind and verified computation defined for MBQC [3]. Explaining the terminology, a blind and verified protocol can be seen as a delegated computation between a client and a server: the server, despite physically running the computation, gains no information whatsoever on the protocol that it is performing (blind), while any possible attempt by the server to deviate from the scheduled protocol has a non-zero probability of being detected (verified). Secondly, we prove that to any quantum stabilizer error correcting code there exists a toy error correcting code bearing the same correcting properties. We further show the existence of a no-deletion theorem and how any k-threshold secret sharing code is also an error correcting code just as in the quantum case. Finally, we prove the impossibility of both perfect and imperfect bit-commitment schemes in the toy model.

3 Discussion

Our toy protocols can be seen as explicit constructions which reinforce the known link between theories that feature purifications and the existence of many quantum-like phenomena [1]. Indeed in reference [1] this connection was originally introduced, already including proofs of existence of toy error correction

[1] Ontic is a greek rooted word which means *of existence*.

[2] Again from greek, *of knowledge*.

and impossibility of perfect bit commitment. While for these two protocols our contribution simply has the merit of providing an explicit toy construction, our other results can be seen as entirely original toy extension of the precedent work. Furthermore, we conjecture that the existence of a blind and verified protocol is not particular to toy models alone and should in theory be accessible to the generalized theories with purifications of [1].

However, it is also interesting to analyse the consequences arising from the existence of a toy blind and verified protocol. In particular, it is worth remebering that quantum verified protocols guarantee informationally theoretic security instead of the computational security provided by their classical counterparts [3]. Here, by implementing a toy protocol with matching security properties we suggest that the security of the quantum protocol is also based on steering properties rather than any form of Bell nonlocality. This is important as all known quantum verified protocols either directly feature non-locality or do not explicitly knowledge its use. Our result then strongly suggest that non-locality is not a necessary ingredient for verification protocols like [3], which do not make explicit use of it. It must also be added that our toy verified protocol verifies only toy computations (which are classically efficiently simulable). Therefore, our result does not provide a proof of the non-necessity of non-locality when the task is to verify universal quantum computation, as it is still possible that quantum non-locality or contextuality may be needed in such a scenario. However, as our result decouples non-locality to the 'mechanical' properties of the verification protocol, it shows that if non-locality is necessary for verification of quantum computations this necessity should arise in an highly non-trivial fashion. Conversely, if as suggested by our result non-locality is not a necessary ingredient, then we conjecture that a Gaussian client should be able to verify a full quantum computation.

References

[1] Giulio Chiribella, Giacomo Mauro D'Ariano & Paolo Perinotti (2010): *Probabilistic theories with purification*. *Physical Review A* 81(6), p. 062348, doi:10.1103/PhysRevA.81.062348.

[2] Richard Cleve, Daniel Gottesman & Hoi-Kwong Lo (1999): *How to Share a Quantum Secret*. *Physical Review Letters* 83(3), pp. 648–651, doi:10.1103/PhysRevLett.83.648.

[3] Joseph F. Fitzsimons & Elham Kashefi (2012): *Unconditionally verifiable blind computation*. Available at http://arxiv.org/abs/1203.5217.

[4] Mark Howard, Joel Wallman, Victor Veitch & Joseph Emerson (2014): *Contextuality supplies the magic' for quantum computation*. *Nature*, p. 5, doi:10.1038/nature13460.

[5] Matthew F. Pusey (2012): *Stabilizer Notation for Spekkens' Toy Theory*. *Foundations of Physics* 42(5), pp. 688–708, doi:10.1007/s10701-012-9639-7.

[6] Robert Raussendorf (2013): *Contextuality in measurement-based quantum computation*. *Physical Review A* 88(2), p. 022322, doi:10.1103/PhysRevA.88.022322.

[7] Robert Spekkens (2007): *Evidence for the epistemic view of quantum states: A toy theory*. *Physical Review A* 75(3), p. 032110, doi:10.1103/PhysRevA.75.032110.

[8] Robert W Spekkens (2016): *Quasi-quantization: classical statistical theories with an epistemic restriction*. In: *Quantum Theory: Informational Foundations and Foils*, Springer, pp. 83–135.

[9] H. M. Wiseman, S. J. Jones & A. C. Doherty (2007): *Steering, Entanglement, Nonlocality, and the Einstein-Podolsky-Rosen Paradox*. *Phys. Rev. Lett.* 98, p. 140402, doi:10.1103/PhysRevLett.98.140402. Available at http://link.aps.org/doi/10.1103/PhysRevLett.98.140402.