MAR17-2017-020762

Abstract for an Invited Paper
for the MAR17 Meeting of
the American Physical Society

Reflections on Quantum Data Hiding

ANDREAS WINTER, Universitat Autonoma de Barcelona

Quantum data hiding, originally invented as a limitation on local operations and classical communications (LOCC) in distinguishing globally orthogonal states, is actually a phenomenon arising generically in statistics whenever comparing a 'strong' set of measurements (*i.e.*, decision rules) with a 'weak' one. The classical statistical analogue of this would be secret sharing, in which two perfectly distinguishable multi-partite hypotheses appear to be indistinguishable when accessing only a marginal. The quantum versions are richer in that for example LOCC allows for state tomography, so the states cannot be come perfectly indistinguishable but only nearly so, and hence the question is one of efficiency. I will discuss two concrete examples and associated sets of problems:
1. Gaussian operations and classical computation (GOCC): Not very surprisingly, GOCC cannot distinguish optimally even two coherent states of a single mode [Takeoka & Sasaki, PRA 78:022320, 2008]. Here we find states, each a mixture of multi-mode coherent states, which are almost perfectly distinguishable by suitable measurements, by when restricted to GOCC, i.e. linear optics and post-processing, the states appear almost identical. The construction is random and relies on coding arguments. Open questions include whether there one can give a constructive version of the argument, and whether for instance even thermal states can be used, or how efficient the hiding is.
2. Local operation and classical communication (LOCC): It is well-known that in a bipartite dxd-system, asymptotically $\log d$ bits can be hidden [Hayden *et al.*, CMP 250:371391, 2004]. Here we show for the first time, using the calculus of min-entropies, that this is asymptotically optimal. In fact, we get bounds on the data hiding capacity of any preparation system; these are however not always tight. While it is known that data hiding by separable states is possible (i.e. the state preparation can be done by LOCC), it is open whether the optimal information efficiency of (asymptotically) log d bits can be achieved by separable states.