

Quantum guesswork: a combinatorial instance of quantum hypothesis testing

Michele Dall'Arno

1. Abstract

We consider a game-theoretical scenario involving two parties, say Alice and Bob. At each round, Alice chooses a quantum state from a given ensemble, known to both parties, and sends it to Bob. Bob is allowed to perform any quantum operation on the state and to query Alice multiple times, one state at a time, until he correctly guesses the state. The game is repeated many times, and Bob's aim is to minimize the average number of queries needed. This problem, known as quantum guesswork, can be reframed as an instance of quantum hypothesis testing, and has therefore long been conjectured not to admit analytical solutions except for the cases in which the hypothesis testing problem is solvable, that is, for binary and symmetric ensembles. Here, we disprove such a belief by deriving conditions under which the guesswork problem can be recast as a combinatorial problem, that is, an optimization over a finite set, and therefore can be solved analytically by exhaustive search. We further show that such conditions are verified by any qubit ensemble, thus conclusively settling the problem in dimension two, and we show that in that case the guesswork is equivalent to an NP-hard combinatorial problem known as quadratic assignment problem (QAP). Leveraging on known results on the QAP, we introduce the (infinite) class of so-called benevolent qubit ensembles, that includes symmetric, informationally complete (SIC) and mutually unbiased basis (MUBs) ensembles, and we explicitly solve the corresponding QAP for such a class. For non benevolent ensembles, we show that in the presence of symmetries the size of the exhaustive search can be reduced by a quadratic factor.