Fine-Grained Unambiguous Measurements

Quentin Buzet*[1]

[1]Centre Inria de Paris – Institut National de Recherche en Informatique et en Automatique – France

Résumé

Unambiguous measurements play an important role in quantum information, with applications ranging from quantum key distribution to quantum state reconstruction. Recently, such measurements have also been used in quantum algorithms based on Regev's reduction.The key problem for these algorithms is the S-—LWE⟩ problem in the lattice setting and the Quantum Decoding Problem in the code setting. A key idea for addressing this problem is to use unambiguous measurements to recover k coordinates of a code (or lattice) element x from a quantum state —ψx⟩, which corresponds to a noisy word x with errors in quantum superposition. However, a general theoretical framework to analyze this approach has been lacking.
In this work, we introduce the notion of fine-grained unambiguous measurements. Given a family of states {—ψx⟩, x∈F2n} , we ask whether there exist measurements that can return, with certainty, k parities about x. We study this question in the setting of symmetric states, which naturally arises in the Quantum Decoding Problem. We show that determining the maximal number of parities that a measurement can output can be formulated as a linear program, and we use its dual formulation to derive several upper bounds. In particular, we establish necessary and sufficient conditions for the existence of fine-grained unambiguous measurements and prove impossibility results showing in particular that such measurements cannot improve upon the approach of (CT24). Finally, we discuss the implications of these findings for the Quantum Decoding Problem.
Collaboration avec André Chailloux.

*Intervenant