PRADEEP SARVEPALLI, University of British Columbia
Quantum Secret Sharing, Matroids and Stabilizer Codes

Quantum secret sharing schemes deal with the distribution of a quantum state among a set of n players, so that only authorized subsets can reconstruct the secret. While the connections between codes, secret sharing schemes and matroids have been subject of extensive investigations, their analogues in the context of quantum secret sharing schemes have not been studied as much, in particular no associations have been made with matroids. In this talk we give the first steps toward establishing the connections between matroids and quantum secret sharing schemes. In addition to providing a new perspective on quantum secret sharing schemes, this characterization has important benefits; they enable us to construct efficient quantum secret sharing schemes for many general access structures. We show that an identically self-dual matroid that is representable over a finite field induces a quantum secret sharing scheme with information rate one. Using the theory of quantum stabilizer codes, we make this association constructive which additionally elaborates on the correspondence between quantum codes and secret sharing schemes.

This is a joint work with Robert Raussendorf (University of British Columbia).