How hard is code equivalence?

Violetta Weger

Technical University of Munich, Germany

Linear codes over finite fields possess rich algebraic structure, giving rise to natural equivalence questions: when should two codes be considered the same, and can an equivalence between them be recovered efficiently? These questions lead to the code equivalence problem, whose precise computational complexity remains unknown. Beyond its intrinsic mathematical interest, code equivalence has recently become important in post-quantum cryptography, where it serves as a hardness assumption for several constructions.

In this talk, we survey different variants of code equivalence, discuss algebraic and combinatorial invariants and present an overview of known algorithmic approaches and their complexity. We conclude with several open directions that may eventually determine how hard code equivalence really is.