Algebraic and combinatorial algorithms for equivalence problems

Monika Trimoska (Eindhoven University of Technology)

Abstract: Broadly, an equivalence problem considers two instances of the same mathematical object and asks if there exists a map between them that preserves some defined property. Two such problems will be looked at in detail in this talk. The matrix code equivalence problem takes as input two error-correcting codes in the rank metric and the map we are tasked to find is an isometry that preserves the rank of codewords. The second problem we are interested in is the alternating trilinear form equivalence, where we are given two alternating trilinear forms and the goal is to find an isomorphism between them. We first show how these two problems are similar, namely that an alternating trilinear form can be viewed as a matrix code with special properties, or that a matrix code can be viewed as a trilinear form without the alternating property. We then present a survey of recent advances in solving these two problems both with purely algebraic algorithms and with combinatorial algorithms that have algebraic system solving as subroutines. The rising interest in these problems is due to their aptness for building a zero-knowledge-based identification scheme. As such, these two problems, alongside the code equivalence problem in the Hamming metric, have been used as a hardness assumption in the design of the Fiat-Shamir-based digital signature schemes MEDS, ALTEQ, and LESS, which are candidates for standardization in the additional call for digital signatures by NIST.