Open problems in code-based cryptography

Violetta Weger

Technical University of Munich, Germany

Algebraic coding theory enjoys many connections to finite geometry, graph theory, combinatorics and many more research directions. Exploring such connections has been proven to be very fruitful in the past for constructing codes or answering open questions.

As algebraic coding theory also finds applications in cryptography, I would like to take this talk as an opportunity to bring the exciting topic of code-based cryptography closer to its related fields.

For this we will start with a gentle introduction to code-based cryptography and then delve into the most pressing challenges therein. In particular, we will see the distinguishing problem for Goppa codes, the rank-metric decoding problem, how to construct codes with many decodable syndromes and many more.

All of the discussed problems are long open-standing, have a high impact for the post-quantum standardization process and could possibly use a new point of view to be tackled.

Department of Electrical and Computer Engineering, Technical University of Munich, Theresienstrasse 90, 80333 Munich, Germany
violetta.weger@tum.de