Associate Professorship of Coding and Cryptography
TUM Department of Electrical and Computer Engineering
Technical University of Munich

Seminar

Rank-Metric Codes and Their Applications

Rank-matric codes are codes that live in a vector space that is endowed with a different metric than the Hamming metric: in the rank-metric the distance between two codewords, represented as matrices over a smaller field, is defined as the rank of their difference.

The theory of rank-metric codes has interesting connections to many topics in discrete mathematics and promissing applications to code-based cryptography and network coding.

In this seminar work, the student will study properties and constructions of rank-metric codes and one or more applications. The goal is to understand and summarize parts of the following papers:

[1] H. Bartz, L. Holzbaur, H. Liu, S. Puchinger, J. Renner, A. Wachter-Zeh (2022). “Rank-Metric Codes and Their Applications”. arXiv: 2203.12384 https://arxiv.org/pdf/2203.12384.pdf

[2] K. Marshall, (2016). “A study of cryptographic systems based on Rank metric codes”, Dissertation, University of Zurich https://www.zora.uzh.ch/id/eprint/127105/1/Diss%20Kyle.pdf

[3] T. Randrianarisoa, (2018). “Rank metric codes, codes using linear complexity and applications to public key cryptosystems”, Dissertation, University of Zurich
https://www.zora.uzh.ch/id/eprint/153545/1/153545.pdf

[4] E. Gorla (2019). “Rank-metric codes”. arXiv: 1902.02650 https://arxiv.org/pdf/1902.02650.pdf

[5] E. Gorla and A. Ravagnani. (2018). “Codes endowed with the rank metric”. In: Network Coding and Subspace Designs. Springer. 3–23.
https://link.springer.com/content/pdf/10.1007/978-3-319-70293-3.pdf

Advisors

Hugo Sauerbier Couvée