Contemporary algebraic and geometric techniques
in coding theory and cryptography
Summer school — July 18-22, 2022
Università degli Studi della Campania "Luigi Vanvitelli"

On decoding of restricted optimal rank metric codes

Wrya K. Kadir

Affiliation: Simula - UiB
Bergen, Norway

Abstract

Gabidulin codes are the most well known family of rank metric codes. They are obtained via evaluation of a set of linearized polynomials on linearly independent points. Those codes that achieve their Singleton-like bounds, are called optimal evaluation rank metric codes. Optimal evaluation rank metric codes that are not $\mathbb{F}_{q^n}$-linear can be divided into two groups. The first group contains rank metric codes that are maximum rank distance (MRD) codes and they are generalized versions of Gabidulin codes [2]. Their constructions are based on Sheekey's idea [11] and all of them have a twisted term in their linearized polynomial representations. The codes in this group are twisted Gabidulin (TG) codes [11], generalized twisted Gabidulin (GTG) codes [6], additive generalized twisted Gabidulin (AGTG) codes [7] and Tromebetti-Zhou (TZ) codes [12]. The second group are rank metric codes that are subsets of restricted matrices and equipped with rank metric. The codes in this group are symmetric [9], alternating [1] and Hermitian [10] rank metric codes. The codes in the first group were proposed without any decoding algorithm and the codes in the second group were proposed with no encoding and decoding procedures. Hence efficient decoding algorithms for the first group and both encoding and decoding algorithms for the second group are necessary.

Rank syndrome-based decoding algorithm [2] which was applied to decode Gabidulin codes requires the code to be $\mathbb{F}_{q^n}$-linear. In this talk encoding and decoding procedures for the codes in the second group are considered. The encoding algorithms are the main challenges which they require more steps in compare to the known encoding methods for evaluation rank metric codes. In the decoding process of the first group of codes, when the rank of the error vector attains the unique decoding radius, the decoding problem is reduced to the problem of solve some specific polynomial equations [8, 3, 4] while for the codes in the second group it is possible to apply known decoding algorithms for Gabidulin codes. For this purpose we recall Berlekamp-Massey algorithm and also the properties of the Dickson matrix associated with linearized polynomials, [5].

Keywords: Rank metric, Gabidulin codes, Interpolation-based, encoding, decoding algorithm

References

[1] Philippe Delsarte and Jean-Marie Goethals. Alternating bilinear forms over GF(q). *Journal of Combinatorial Theory, Series A*, 19(1):26–50, 1975.

[2] Ernest Mukhamedovich Gabidulin. Theory of codes with maximum rank distance. *Problemy Peredachi Informatsii*, 21(1):3–16, 1985.

[3] Wrya K. Kadir and Chunlei Li. On decoding additive generalized twisted Gabidulin codes. *Cryptography and Communications*, 12:987 – 1009, 2020.

[4] Wrya K. Kadir, Chunlei Li, and Ferdinando Zullo. On interpolation-based decoding of a class of maximum rank distance codes. In *2021 IEEE International Symposium on Information Theory (ISIT)*, pages 31–36, 2021.

[5] Wrya K Kadir, Chunlei Li, and Ferdinando Zullo. Encoding and decoding of several optimal rank metric codes. *Cryptography and Communications*, pages 1–20, 2022.

[6] Guglielmo Lunardon, Rocco Trombetti, and Yue Zhou. Generalized twisted Gabidulin codes. *Journal of Combinatorial Theory, Series A*, 159:79–106, 2018.

[7] Kamil Otal and Ferruh Özbudak. Additive rank metric codes. *IEEE Transactions on Information Theory*, 63(1):164–168, 2017.

[8] Tovohery Hajatiana Randrianarisoa. A decoding algorithm for rank metric codes. *arXiv.org.*, abs/1712.07060, 2017.

[9] Kai-Uwe Schmidt. Symmetric bilinear forms over finite fields of even characteristic. *Journal of Combinatorial Theory, Series A*, 117(8):1011–1026, 2010.

[10] Kai-Uwe Schmidt. Hermitian rank distance codes. *Designs, Codes and Cryptography*, 86(7):1469–1481, 2018.

[11] John Sheekey. A new family of linear maximum rank distance codes. *Advances in Mathematics of Communications*, 10:475, 2016.

[12] R. Trombetti and Y. Zhou. A new family of MRD codes in $\mathbb{F}_q^{2n\times 2n}$ with right and middle nuclei $\mathbb{F}_{q^n}$. *IEEE Transactions on Information Theory*, 65(2):1054–1062, 2019.