The true dimension of Goppa Codes

Sabira El Khalfaoui, Gábor P. Nagy

University of Szeged, Szeged, Hungary

In my talk, I will investigate the problem of finding the true dimension of Goppa Codes. It has been studied with two strategies presented in a series of papers dealing with this problem. The first one is using the kernel of an associated trace map, and the second one is using the link between the parity check matrix of Goppa codes and the parity check matrix of generalized Reed-Solomon codes. We describe results with some computations in chronological order on Goppa Codes with specific parameters whose dimension exceeds the classical lower bound.

[1] VÉRON, P., Proof of Conjectures on the True Dimension of Some Binary Goppa codes, *Designs, Codes and Cryptography. An International Journal* **36** (2005), 317–325.

[2] BEZZATEEV, SERGEI V. AND SHEKHUNOVA, NATALIA A., Subclass of binary Goppa codes with minimal distance equal to the design distance, *IEEE Trans. Information Theory* **41** (1995), 554–555.

[3] DELSARTE, PHILIPPE, On subfield subcodes of modified Reed-Solomon codes, *IEEE Trans. Inform. Theory* **IT-21** (1975), 575–576 .

[4] ROSEIRO, ALBERT M. AND HALL, JONATHAN I. AND ADNEY, JOSEPH E. AND SIEGEL, MARVIN, The trace operator and redundancy of Goppa codes, *IEEE Trans. Inform. Theory* **38** (1992), 1130–1133.

[5] VÉRON, P., Goppa codes and trace operator, *IEEE Trans. Inform. Theory* **44** (1998), 290–294.

[6] VÉRON, P., True dimension of some binary quadratic trace Goppa codes, *Des. Codes Cryptogr.* **24** (2001), 81–97.

[7] MACWILLIAMS, F. J. AND SLOANE, N. J. A., *The theory of error-correcting codes. I*, North-Holland Mathematical Library, Vol. 16, North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977.