

1 List decoding of Goppa codes

The task is to implement the list decoding algorithm in [1].

Fundamentals on Goppa codes [2, Chap 12.3][3, Chap 2], list decoding algorithm [4, Chap 12][5, Chap 9].

References

- [1] D. Augot, M. Barbier, and A. Couvreur, “List-decoding of binary goppa codes up to the binary johnson bound,” in *2011 IEEE Information Theory Workshop*, pp. 229–233, Oct 2011.
- [2] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*. 1978.
- [3] H. Liu, “Decoding of interleaved goppa codes and their applications in code-based cryptosystem,” Master’s thesis, Technical University of Munich, Dec. 2018.
- [4] J. Justesen and T. Høholdt, *A course in error-correcting codes*. Zürich: European Mathematical Society (EMS), 2004.
- [5] R. M. Roth, *Introduction to Coding Theory*. Cambridge University Press, 2006.