About Skew Reed-Solomon Codes

D. Boucher

IRMAR (UMR 6625), Université de Rennes 1, Campus de Beaulieu, F-35042 Rennes Cedex

Abstract

Skew Reed-Solomon codes over a division ring A are a generalization of Reed-Solomon codes ([2], [3]). They are obtained by evaluating skew polynomials at some particular points. These codes are optimal for the skew polynomial metric ([2], [4]) which is a generalization of the Hamming metric.

The ring R of skew polynomials over A is the set of polynomials $\sum a_i X^i$ over A endowed with the classical additive law and the multiplicative law given by : $\forall a \in A, X \cdot a = \theta(a)X + \delta(a)$ where θ is an endomorphism of A and δ is a derivation on A. This ring is Euclidean on the right: Euclidean division on the right, least common left multiples (lclm) and greatest common right divisors (gcrd) are well defined. For f in R and a in A the evaluation of f on a is defined as the remainder in the right division of f by $X - a$ (see [1]). When θ is the identity and δ is the zero derivation, the skew polynomial ring R is the classical ring, the skew evaluation is the classical evaluation, skew Reed-Solomon codes are classical Reed-Solomon codes and the skew polynomial metric is the Hamming metric.

This talk aims at presenting the family of skew Reed Solomon codes and the skew polynomial metric by using a simple formalism (mainly based on gcrd and lclm). This interpretation enables first to make the bridge with the classical Reed-Solomon codes and the Hamming metric in a simple way and secondly to design decoding algorithms which generalize the classical decoding algorithms for Reed-Solomon codes.

Keywords

skew polynomial ring, coding theory

References

[1] T. Y. Lam; A. Leroy : *Vandermonde and Wronskian matrices over division rings.* Bull. Soc. Math. Belg. Sér. A 40 (2), 281–286 (1987).

[2] U. Martínez-Peñas : *Skew and linearized Reed-Solomon codes and maximum sum rank distance codes over any division ring.* J. Algebra 504, 587–612 (2018).

[3] D. Boucher; F. Ulmer : *Linear codes using skew polynomials with automorphisms and derivations.* Des. Codes Cryptogr. 70 (3), 405–431 (2014).

[4] D. Boucher : *An algorithm for decoding skew Reed-Solomon codes with respect to the skew metric.* Des. Codes Cryptogr. 88 (9), 1991–2005 (2020).