Products of subcodes of Reed–Solomon codes

Alain Couvreur and Thomas Debris–Alazard

In code–based cryptography, several attacks involve the following heuristic argument: *Let A be a random subspace of "low codimension" of the space $\mathbb{F}[X]_{\leq k}$ of polynomials of bounded degree, then the span A^2 of products of elements of A equals $\mathbb{F}[X]_{\leq 2k}$ with a high probability.* The objective of this project is to get precise statements by classifying subspaces A of $\mathbb{F}[X]_{\leq 2k}$ whose "square" A^2 does not fill in the whole $\mathbb{F}[X]_{\leq 2k}$.

The case of 1 codimensional subspaces is well understood even in a more general context which is that of one codimensional subspaces of a Riemann–Roch space[1]. On the other hand, for general subspaces, many examples are identified in a paper by Márquez–Corbella *et. al.*[2].

Starting from the understanding of one codimensional subspaces, we aim at classifying 2–codimensional subspaces of $\mathbb{F}[X]_{\leq k}$ whose squares have codimension 1 or 2 in $\mathbb{F}[X]_{\leq 2k}$. For this sake we wish to imply techniques developed by Márquez–Corbella *et. al.* together with techniques inspired from additive combinatorics.

[1] A. Alzati, F. Russo, *On the k–normality of projectied algebraic varieties.* Bulletin of the Brazilian Mathematical Society

[2] I. Márquez–Corbella, E. Martinez–Moro and Ruud Pellikaan. *The non-gap sequence of a subcode of a generalised Reed–Solomon code.* Des. Codes Cryptogr. 66, pp:317–333, 2013