Abstract

We first present a new decoding algorithm for Reed-Solomon codes. The algorithm attempts to decode $M - 1$ transmitted codewords together, using $M$-variate polynomial interpolation. It is shown that if the channel errors are synchronized — occur in the same positions in all the $M - 1$ codewords — this algorithm can, in principle, correct up to $n(1 - R^{(M-1)/M})$ errors in a Reed-Solomon code of length $n$ and rate $R$, which is significantly higher than the Guruswami-Sudan decoding radius.

The second part of the presentation is about constructing family of algebraic codes that are provably decodable beyond the Guruswami-Sudan radius in the worst-case. The key idea is to combine multivariate interpolation decoding with a kind of ”inverted” algebraic-geometric construction. That is, instead of evaluating certain functions at the rational points of a curve, we evaluate the rational points themselves, viewed as pairs of polynomials over a subfield, at certain elements of the subfield.