

An extension of the Error Correcting Pairs algorithm

ISABELLA PANACCIONE AND ALAIN COUVREUR

INRIA & CNRS UMR 7161, Laboratoire LIX, Université Paris-Saclay

isabella.panaccione@inria.fr, alain.couvreur@lix.polytechnique.fr

Abstract. In this talk we present a “power” extension of the Error Correcting Pairs algorithm for Reed-Solomon codes. If ℓ is the power we choose, we get for $\ell = 2$ an algorithm whose decoding radius equals that of the Power Decoding algorithm.

It is known that several algorithms have been designed in order to decode Reed-Solomon codes. In particular Berlekamp-Welch algorithm and the Error Correcting Pairs algorithm are two classical algorithms which correct up to $\frac{d-1}{2}$ errors.

Berlekamp-Welch algorithm can be extended to algorithms correcting beyond half the minimum distance. On the one hand Sudan algorithm and Guruswami-Sudan algorithm are deterministic and return the list L of all possible solutions (note that in the typical situation $|L| = 1$). On the other hand, the Power Decoding algorithm has the same decoding radius as Sudan algorithm, is quicker but may fail (it gives one solution or zero).

The Error Correcting Pairs algorithm behave slightly differently, since it mainly consists in localizing errors. After that, decoding boils down to elementary linear algebra. The advantage of this algorithm is that it can also be applied to some cyclic codes. It would be then interesting to have an extension of the Error Correcting Pairs algorithm correcting more than half the minimum distance.

We propose then a “power” generalisation of the Error Correcting Pairs algorithm. In order to do that, as for the Power Decoding algorithm, we start by considering more subproblems (each of them given by a power of the main one) at the same time. Though, while for the Power Decoding algorithm the condition to have a solution depends on the dimension of a linear system solution space, for the Power Error Correcting Pairs algorithm, it depends on the nullity of the intersection of some spaces.