A characterization of MDS codes that have an error correcting pair

Irene Márquez-Corbella[1], Ruud Pellikaan[2]

[1] *SECRET of INRIA, Rocquencourt, France. E-mail: irene.marquez-corbella@inria.fr*
[2] *Dept. of Mathematics, Eindhoven University of Technology. E-mail: g.r.pellikaan@tue.nl*

1 abstract

Error-correcting pairs (ECP) were introduced in [6, 8] and independently in [3] as a general algebraic method of decoding linear codes. These pairs exist for several classes of codes such as for generalized Reed-Solomon, cyclic, alternant and algebraic geometry codes [1, 2, 3, 4, 7, 8, 9]. However little or no study has been made for characterizing those codes. This article is an attempt to fill the vacuum left by the literature concerning this subject. The aim of this paper is to characterize those t-error correcting MDS codes that have a t-error correcting pair. Since every linear code is contained in an MDS code of the same minimum distance over some finite field extension, see [9], we have focused our study on the class of $[n, n-2t, 2t+1]$ codes with a t-ECP. It turns out to be the class of generalized Reed-Solomon codes. This was shown for $t \leq 2$ in [9].

We will give the back round of MDS codes. Generalized Reed-Solomon codes and an equivalent way to describe such a code as a projective system on a rational normal curve in projective space is reviewed. A classical result is stated that a rational rational curve in projective r space is uniquely determined by n of its points in case $n \geq r+2$. This classical result will be vital in our main result.

For further details on the notion of an error correcting pair we formally review this definition, detailing the state-of-art and the existence of error correcting pair for some families of codes. Also a survey of well-known results related to generalized Reed-Solomon codes which would be used to set the notation and recall some properties that are relevant for the proof of the main result.

Finally, we present the main result of this paper that states that every MDS code with minimum distance $2t+1$ and having a t-ECP belongs to the class of generalized Reed-Solomon codes. A second proof is given using a recent results [5, 10] on the Schur product of codes.

References

[1] I.M. Duursma, *Decoding codes from curves and cyclic codes*, PhD Thesis, Eindhoven University of Technology (1993).

[2] I.M. Duursma and R. Kötter, *Error-locating pairs for cyclic codes*, IEEE Trans. Inform. Theory **40**, pp. 1108–1121 (1994).

[3] R. Kötter, *A unified description of an error locating procedure for linear codes*, Proceedings of Algebraic and Combinatorial Coding Theory, Voneshta Voda, pp. 113–117 (1992).

[4] R. Kötter, *On algebraic decoding of algebraic-geometric and cyclic codes*, PhD Thesis, Linköping Studies in Science and Technology, Dissertation no. **419**, (1996).

[5] D. Mirandola and Z. Gilles,*Critical pairs for the product singleton bound*, arXiv:1501.06419 (2015).

[6] R. Pellikaan,*On decoding linear codes by error correcting pairs* Preprint Eindhoven University of Technology, 1988.

[7] R. Pellikaan, *On a decoding algorithm of codes on maximal curves*, IEEE Trans. Inform. Theory **35**, pp. 1228–1232 (1989).

[8] R. Pellikaan, *On decoding by error location and dependent sets of error positions*, Discrete Math. **106–107**, pp. 369–381 (1992).

[9] R. Pellikaan, *On the existence of error-correcting pairs*, Statistical Planning and Inference **51**, pp. 229–242 (1996).

[10] H. Randriambololona, *An upper bound of singleton type for componentwise products of linear codes*, IEEE Trans. Inform. Theory **59**, 12, pp. 7936–7939 (2013).