Error-correcting Codes For Multipermutations

Read/Download
implemented a parity-based error detection architecture for the Datapath and one for the Key Schedule mechanism of IDEA NXT. The solution we use is a linear multipermutation defined by a Galois field. This check code is a code in which the parity of multiple elements needs to be checked periodically for correct functioning. There is research on optimization techniques for error correction codes.

Keywords: MDS map, MDS matrix, MDS code, Multipermutation. (7) F. J. MacWilliams and N.J.A. Sloane, The Theory of Error-Correcting Codes.