



Technology Opportunity, Ref. No. UZ-12/733

Evaluation of polynomials over finite fields and Decoding of cyclic codes

A method has been developed which allows to efficiently evaluate a polynomial in finite fields, which is a computational task to be performed in many applications, such as transmission, storage and reading of data as well as cryptography.

Keywords Polynomial evaluation, Decoding, Error Correcting Codes, BCH, Reed-Solomon codes, Syndrome Computation, Cryptography, Data Transmission, Multicast protocols, CD-ROM.

Inventors Davide Schipani and Joachim Rosenthal, University of Zurich; Michele Elia, Politecnico di Torino

Reference D.Schipani et al. Proceedings Australian Communications Theory Workshop (AusCTW), 2011, pp. 154-15.
D.Schipani et al. Proceedings IEEE International Symposium on Information Theory (ISIT), 2011, pp. 835 - 839.

Background Cyclic codes, such as the BCH and Reed-Solomon codes are widely used to correct errors in data transmission, storage and reading. More and more often codes of large length are required, given the huge and increasing amount of data to be handled. The standard decoding of cyclic codes becomes however very time-consuming when the lengths of the code words are large.

Invention The invention allows to reduce the computational cost of decoding cyclic codes dramatically, by means of a smart way of evaluating polynomials and a new technique to find the error positions.

Fields of Use Decoding of standard algebraic codes in any situation (e.g. CD-ROM's), Polynomial evaluation in finite fields, which, besides the decoding error correcting codes, occurs in many other applications such as Cryptography and Data Transmission (e.g. Secret Sharing Scheme, Multicast Key Distribution).

Patent Status Patent application filed

Contact *Unitecra, Technology Transfer of University Zurich, Dr. W. Henggeler, Möhrlistrasse 23, CH-8006 Zürich, +41 44 634 44 01, mail@unitecra.ch*