On Decoding Algebraic Codes

Sergei V. Fedorenko

Information systems security department
St.Petersburg State University of Aerospace Instrumentation
190000, Bolshaya Morskaia, 67, St.Petersburg, Russia
Email: sfedorenko@ieee.org

Abstract

The algebraic codes are a very important class of codes including Bose-Chaudhuri-Hocquenghem, Reed-Solomon, Goppa, and alternant codes. Those codes have wide application in standards. A few algorithms for decoding algebraic codes are considered. The steps of decoding algorithms are described in details. The original methods of improving those steps (methods of finding roots of polynomials and calculation of the cyclotomic Fast Fourier Transform algorithm over finite fields) are proposed.

REFERENCES

[1] S. V. Fedorenko, P. V. Trifonov. Finding roots of polynomials over finite fields. *IEEE Transactions on Communications*, vol. 50, no. 11, pp. 1709–1711, 2002.

[2] P. V. Trifonov, S. V. Fedorenko. A method for fast computation of the Fourier transform over a finite field. *Problems of Information Transmission*, vol. 39, no. 3, pp. 231–238, 2003. Translation of *Problemy Peredachi Informatsii*.

[3] S. V. Fedorenko, P. V. Trifonov, E. Costa. Improved hybrid algorithm for finding roots of error-locator polynomials. *European Transactions on Telecommunications*, vol. 14, no. 5, pp. 411–416, 2003.

[4] E. Costa, S. V. Fedorenko, P. V. Trifonov. On computing the syndrome polynomial in Reed-Solomon decoder. *European Transactions on Telecommunications*, vol. 15, no. 4, pp. 337–342, 2004.

[5] S. V. Fedorenko. A simple algorithm for decoding Reed-Solomon codes and its relation to the Welch-Berlekamp algorithm. *IEEE Transactions on Information Theory*, vol. 51, no. 3, pp. 1196–1198, 2005.

[6] S. V. Fedorenko. A method for computation of the discrete Fourier transform over a finite field. *Problems of Information Transmission*, vol. 42, no. 2, pp. 139–151, 2006. Translation of *Problemy Peredachi Informatsii*.