SEARCH FOR POLYNOMIAL ROOTS OF ERROR LOCATORS WHEN DECODING REED-SOLOMON CODES

Krylova V.A., Tverytnykova E.E, Tarasenko M.V.
National Technical University
«Kharkiv Polytechnic Institute», Kharkiv

In telecommunications and information systems with an increased noise component the noise-resistant Reed-Solomon codes are used. The adjustment and correcting errors in a message require some effective decoding methods. One of the stages in the procedure of decoding RS codes to determine the position of distortions is the search for the roots of the error locator polynomial. The calculation of polynomial roots, especially for codes with significant correction capacity is a laborious task requiring high computational complexity. That is why the improvement of RS codes decoding methods providing to reduce the computational complexity is an urgent task. The Chan's procedure for searching the roots of the polynomial error becomes quite complicated for calculations in large finite fields (m>8) and for error locators polynomials of a large degree, because it requires a significant number of operations. Therefore, the task is to improve the method for determining the positions of distortions in the code word and to reduce the computational complexity of the algorithm for finding the roots of the error polynomial in the finite fields of GF(2^m) when decoding RS codes.

The application of the modified algorithm for searching the roots of error locator polynomials, presented as the linearized polynomials, makes it possible to achieve a speed gain of 1.5 times in comparison with the Chan's method. For the GF(2^8) finite field, the average number of operations to search for the of polynomial roots of 8 degree is 4100 for the Chan's procedure and 1532 for the proposed modified root search method. For 16 degree of polynomial, the average number of operations is 8240 and 3562 respectively.

An improved algorithm for computing the roots of a polynomial of errors with coefficients in a finite field based on the Berlekamp-Massey algorithm for linearized polynomials, which provides the minimum number of arithmetic operations due to the use of data obtained in the previous stages of calculations. The proposed method reduces the complexity of calculating the roots at one point of the finite field due to the use of a special arrangement of all elements of the finite field.

References:

1. Blahut Richard E. Algebraic Codes for Data Transmission / E. Richard Blahut. Cambridge : Cambridge University Press, 2003. – 482 p.

2. Nabipour S. Error Detection Mechanism Based on Bch Decoder and Root Finding of Polynomial Over Finite Fields / S. Nabipour, J. Javidan, F. Zare Gholamreza // Journal of Mathematics and Computer Science. – 2014, Issue 4. – P. 271–281. DOI: http://dx.doi.org/10.22436/jmcs.012.04.03.

.