A NEW PROCEDURE FOR DECODING CYCLIC AND BCH CODES UP TO ACTUAL MINIMUM DISTANCE

G. L. Feng and K. K. Tzeng

The Center for Advanced Computer Studies, University of Southwestern Louisiana, Lafayette, LA 70504 and the Department of Electrical Engineering and Computer Science, Lehigh University, Bethelehem, PA. 18015

Abstract

In this paper, a new procedure for decoding cyclic and BCH codes up to their actual minimum distance is presented. Previous algebraic decoding procedures for cyclic and BCH codes such as the Peterson decoding procedure and our procedure using nonrecurrent syndrome dependence relations can be regarded as special cases of this new decoding procedure. With the aid of a computer program, it has been verified that, using this new decoding procedure, all binary cyclic and BCH codes of length 63 or less can be decoded up to their actual minimum distance. The procedure incorporates an extension of our Fundamental Iterative Algorithm and the complexity of this decoding procedure is O(n^3).

Summary

For some years, algebraic decoding of cyclic and BCH codes has been restricted by the minimum distance bounds of the codes. Previous algebraic decoding algorithms (Berlekamp-Massey, Euclidean, and our generalizations) have aimed at solving Newton's identities which can be viewed as a set or sets of linear recurrences. We have recently introduced a procedure that frees the decoding of cyclic and BCH codes from the confinement of the bounds and can decode many cyclic and BCH codes up to their actual minimum distance [1]. In our recent procedure, the decoding is accomplished through the determination of nonrecurrent dependence relations among the syndromes. However, the application of this procedure depends on a condition that has to be satisfied for a code to be so decoded. Thus, that decoding procedure is still short of the desired final goal on achieving decoding of all cyclic and BCH codes up to their actual minimum distance. In this paper, we present a new decoding procedure that does not depend on the satisfaction of this condition. We show that, for a code with actual minimum distance d to correct up to $t = \lfloor (d-1)/2 \rfloor$ errors, all that is required is that a (2t+1)×(2t+1) syndrome matrix can be so formed that the syndromes above the minor diagonal are all known and those at the minor diagonal are some unknowns and their conjugates. With reference to the table of codes listed in van Lint and Wilson's paper [2] and with the aid of a computer program, the existence of at least one such matrix for each code has been verified for all binary codes of length 63 or less. Thus, to say the least, the procedure is capable of decoding all binary cyclic and BCH codes of length ≤ 63 up to their actual minimum distance. We have also demonstrated the existence of such syndrome matrices for some codes of length greater than 63. The procedure is a very general one and includes previously mentioned algebraic decoding procedures as special cases. It can be applied to the decoding of codes of any length for which such syndrome patterns exist.

More specifically, the syndrome matrix S referred to in this paper is of the following form:

$$\begin{bmatrix} S_b & S_{b+i_1} & S_{b+i_2} & \cdots & S_{b+i_{2t-2}} & S_{b+i_{2t-1}} & S_{b+i_{2t}} \\ S_{b+j_1} & S_{b+i_1+j_1} & S_{b+i_2+j_1} & \cdots & S_{b+i_{2t-2}+j_1} & S_{b+i_{2t-1}+j_1} & \\ S_{b+j_2} & S_{b+i_1+j_2} & S_{b+i_2+j_2} & \cdots & S_{b+i_{2t-2}+j_2} & & \\ | & | & | & & | & & \\ S_{b+j_{2t-1}} & S_{b+i_1+j_{2t-1}} & & & & & \\ S_{b+j_{2t}} & & & & & & S_{b+i_{2t}+j_{2t}} \end{bmatrix}$$

where the triangular portion of S above the minor diagonal consists of known syndromes and the syndromes at the minor diagonal of S are some unknowns and their conjugates.

Under the assumption that ν errors actually occurred where $\nu \leq t$, then there exist at most ν columns of S which are linearly independent. The other columns are then dependent on these columns. A major step for this decoding procedure is then to determine the unknown syndromes through the linear dependence relations among the columns of S. In this paper, we show that this can be accomplished through an extention of the Fundamental Iterative Algorithm we first introduced in [3].

Once $S_0, S_1, S_2, \cdots, S_{n-1}$ are computed, the error vector can be determined through an inverse Fourier transform of the syndrome vector $(S_0, S_1, S_2, \cdots, S_{n-1})$.

We note that the decoding of the (41,21,9) quadratic residue code [4] can be much more easily handled by this new procedure.

References

[1] G.L. Feng and K.K. Tzeng, "Decoding cyclic and BCH codes up to actual minimum distance using nonrecurrent syndrome dependence relations," *IEEE Trans., Inform. Theory,* vol. IT-37, pp. 1716-1723, Nov. 1991.

[2] J. van Lint and R.M. Wilson, "On the minimum distance of cyclic codes," *IEEE Trans., Inform. Theory,* vol. IT-32, pp. 23-40, Jan. 1986.

[3] G.L. Feng and K.K. Tzeng, "A Generalization of the Berlekamp-Massey Algorithm for Multisequence Shift-Register Synthesis with Applications to Decoding Cyclic Codes," *IEEE Trans., Inform. Theory,* vol. IT-37, pp. 1274-1287, Sept. 1991.

[4] I.S. Reed, T.K. Truong, X. Chen, and X. Yin, "The Algebraic Decoding of the (41,21,9) Quadratic Residue code," *IEEE Trans., Inform. Theory,* vol. IT-38, pp. 974-986, May 1992.

*This work was supported by the National Science Foundation under Grant NCR-9016095.