"FAST DECODING TECHNIQUES FOR EXTENDED SINGLE-AND-DOUBLE-ERROR-CORRECTING REED SOLOMON CODES"

BY

DANIEL J. COSTELLO JR.,*
Department of Electrical Engineering
University of Notre Dame
Notre Dame, IN 46556

HUIJIE DENG
Department of Electrical Engineering
Illinois Institute of Technology
Chicago, IL 60616

SHU LIN
Department of Electrical Engineering
University of Hawaii
Honolulu, HI 96822

(NASA-CR-173617) FAST DECODING TECHNIQUES FOR EXTENDED SINGLE-AND-DOUBLE-ERROR-CORRECTING REED SOLOMON CODES (Notre Dame Univ.) 4 p HC A02/MF A01 CSCL 09B G3/61

N84-26325

Unclas 19487

Submitted as a short paper to the 18th Annual Conference on Information Sciences and Systems - January, 1984.

This work was supported by NASA under Grant NAG 2-202.

*On leave from the Illinois Institute of Technology

ORIGINAL PAGE IS
OF POOR QUALITY

SUMMARY

A problem in designing semiconductor memories is to provide some measure of error control without requiring excessive coding overhead or decoding time. For example, some 256K-bit dynamic random access memories are organized as 32K x 8 bit-bytes. Byte-oriented codes such as Reed Solomon (RS) codes [1] can provide efficient low overhead error control for such memories. However, the standard iterative algorithm [2] for decoding RS codes is too slow for these applications.

In this paper we investigate some special high speed decoding techniques for extended single-and-double-error-correcting RS codes. These techniques are designed to find the error locations and the error values directly from the syndrome without having to form the error locator polynomial and solve for its roots. Two codes are considered:

I. A $d_{min} = 4$ SEC -DED Code

A $(2^m + 2, 2^m - 1)$ code is formed by adding a 3 x 3 identity matrix to the parity-check matrix of the RS code with generator polynomial

$$g(x) = (x + 1)(x + \alpha)(x + \alpha^2),$$

where α is a primitive element of GF (2^m). It is shown that this extended code with three additional information symbols has minimum distance $d_{min} = 4$, and hence is capable of single-error-correction (SEC) and double-error-detection (DED).

Decoding of the error vector $\underline{e}$ is based directly on the syndrome

$\underline{s} = \underline{e}\,\underline{H}^T = (s_0, s_1, s_2)$, where $\underline{H}$ is the parity-check matrix of the extended code. The decoding method can be summarized as follows:

1) A single error in the first three positions (corresponding to the identity positions of $\underline{H}$) results in a syndrome with only one nonzero element.

2) If a single error occurs in any other position, the syndrome elements satisfy

$$\alpha^{i-3} = \frac{s_1}{s_0} = \frac{s_2}{s_1},$$

and i gives the error location.

3) If a single syndrome element is zero, or if

$$\frac{s_1}{s_0} \neq \frac{s_2}{s_1},$$

a double-byte-error is detected.

In cases 1) and 2), the error value is easily determined from the syndrome.

II. A $d_{min} = 6$ DEC - TED Code

A $d_{min} = 6$ RS code is formed from the generator polynomial

$$g(x) = \sum_{i=-2}^{2} (x + \alpha^i),$$

where α is a primitive element of $GF(2^m)$. This code is capable of double-error-correction (DEC) and triple-error-detection (TED), and can be extended by adding two additional information symbols (see [1]).

The syndrome $\underline{s} = \underline{e}\,\underline{H}^T = (s_{-2}, s_{-1}, s_0, s_1, s_2)$. Decoding can be summarized as follows:

1) Calculate the following quantities:

$$\gamma_1 = s_1 s_{-2} + s_{-1} s_0$$

$$\gamma_2 = s_2 s_{-2} + s_0^2$$

$$\gamma_3 = s_0 s_1 + s_2 s_{-1}$$

If $\gamma_1 = \gamma_2 = \gamma_3 = 0$, a single-byte-error occured with value s_0 and location i, where $\alpha^i = \frac{s_1}{s_0}$.

2) If $\gamma_1 \neq 0$, $\gamma_2 \neq 0$, and $\gamma_3 \neq 0$, compute $k = \frac{c}{b^2}$ and $T_2(k)$, where $b \triangleq \frac{\gamma_2}{\gamma_1}$, $c \triangleq \frac{\gamma_3}{\gamma_1}$, and for a field element β,

$$T_2(\beta) \triangleq \sum_{i=0}^{m-1} \beta^{2^i}$$

is the trace of β. If $T_2(k) = 0$, solve the equation

$$y^2 + by + c = 0$$

using the high-speed method described in [3] to find the error locators α^i and α^j of a double-byte-error.

3) If $T_2(k) = 1$, or if at least one but not all of γ_1, γ_2, and γ_3 equals zero, or if more than two elements of $\underline{s}$ equal zero, a triple-byte-error is detected.

In case 2), the error values can be found directly from the syndrome and the quantities calculated.

REFERENCES

1. S.Lin and D.J.Costello, Jr., Error Control Coding: Fundamentals and Applications, Prentice-Hall, New Jersey, 1983.

2. E.R.Berlekamp, Algebraic Coding Theory, McGraw-Hill, New York, 1968.

3. C.L.Chen, "Formulas for the Solutions of Quadratic Equations", IEEE Trans. Infor. Th., IT-28, pp. 792-794, Sept. 1982.