N94-18348

An Extended Reed Solomon Decoder Design

J. Chen
NASA Space Engineering Research Center for VLSI System Design
University of Idaho
Moscow, Idaho 83843

P. Owsley
Advanced Hardware Architectures
Moscow, Idaho 83843

J. Purviance
NASA Space Engineering Research Center for VLSI System Design
University of Idaho
Moscow, Idaho 83843

Abstract- **It has previously been shown that the Reed Solomon (RS) codes can correct errors beyond the Singleton and Rieger Bounds with arbitrarily small probability of a miscorrect [1]. That is an (n,k) RS code can correct more than (n-k)/2 errors. An implementation of such an RS decoder is presented in this paper. An existing RS decoder, the AHA4010, is utilized in this work. This decoder is specially useful for errors which are patterned with a long burst plus some random errors.**

1 Introduction

It is well known that an (n,k) RS code can correct up to (n-k)/2 random errors. When burst errors are involved, the error correcting ability of the RS code can be increased beyond (n-k)/2 with arbitrarily small probability of a miscorrect [1]. Errors considered in this paper, called composite errors, have a single burst plus random error pattern.

RS codes are powerful error correcting codes. There is a rich history of work developing decoding algorithms for RS codes. Virtually all of the work focuses on the general case of t unknown error locations. It is possible to extend the error correction capability of a RS code if error location information is available from some external source. This is called erasure decoding.

The extended decoding technique presented in this paper assumes that the locations of the burst are known and treats them as erasures. All possible burst error positions are given to the decoder sequentially as "guesses" to the burst error location. That is, the burst part of the error becomes an erasure and an erasure-locator polynomial is generated from the erasure locations for each burst location guess. By sending this erasure-locator polynomial along with a received code word to a general purpose RS decoder, such as AHA4010, the RS decoder will decode the received codeword. The result outputted by the

RS decoder is either a corrected data or a signal which indicates no correction can been made.

The erasure-locator polynomial is generated iteratively for all possible locations during the decoding procedure. It is possible that more than one error polynomial results from this iterative procedure. When more than one error is obtained, the error that has higher probability of occurrence should be chosen. It is assumed in this paper that an error with smaller weight has higher probability of occurrence. This is true for most channels.

If the chosen error is not the true error, a miscorrect occurs. The probability of miscorrect is a function of the size of the error that is detected and the channel statistics. It is usually very low as shown in reference 1.

The implementation presented in this paper is based on the AHA4010 RS decoder. The purpose is to increase the error correction capability with very little increase on the hardware and software.

2 Standard Decoding Description

The standard procedure for decoding the RS code is summarized below:

STEP 1: Compute syndromes
$S_j = v(\alpha^{j+j0-1})$ for $j = 1, 2, ..., 2t$.

STEP 2: From the syndromes, form the error-location polynomial $\Lambda(x)$, where $\Lambda(x) = (1 - xX_1)(1 - xX_2) \dots (1 - xX_i)$ and $X_1, X_2, \dots$ and X_i are the error locations.

STEP 3: Find error location X_j $(j = 1, ..., i)$ by finding zeros of $\Lambda(x)$.

STEP 4: Find error magnitude Y_j $(j = 1, ..., i)$ by calculating first i syndrome equations.

STEP 5: Correct the error.

Two polynomials are needed during the decoding and they are:

$$S(x) = \sum_{j=1}^{2t} S_j x^{j-1} \tag{1}$$

and

$$\Omega(x) = S(x)\Lambda(x) \quad (modx^{2t}) \tag{2}$$

This second equation is commonly known as the Key Equation, because solving it is the key to decoding the RS code. After obtaining the error locations, the error magnitudes can be found as:

$$Y_t = -\frac{X_r^j 0^{-1}\Omega(X_t^{-1})}{\Lambda'(X_t^{-1}} \tag{3}$$

For $j_0 = 1$,

$$Y_t = -\frac{\Omega(X_t^{-1})}{\Lambda'(X_r^{-1})} \tag{4}$$

It is now clear that the decoding procedure becomes one of finding the Λ and Ω polynomials from $S(x)$, and then finding the location and magnitude of the errors from those two polynomials.

When erasures are involved, an erasure-locator polynomial is created.

$$\Gamma(x) = \prod_{\mathrm{p}}(1 - xX_p)$$

where the X_p's are the erasure locations.

The Key equation can be solved for Λ and Ω in several ways. One of them is Euclid's recursive algorithm. The Euclid's recursive algorithm is briefly described below. First let

$$\begin{aligned} \Omega^{(-1)}(x) &= x^{2t} \\ \Omega^{(0)}(x) &= S(x)\Gamma(x) \quad (mod x^{2t}) \\ \Lambda^{(-1)}(x) &= 0 \\ \Lambda^{(0)}(x) &= \Gamma(x) \end{aligned}$$

the recursive equations are

$$\Omega^i(x) = R_{\Omega^{(i-1)}(x)}[\Omega^{(i-2)}(x)], \tag{5}$$

or equivalently,

$$\Omega^(i-2)(x) = q^{(i)}(x)\Omega^{(i-1)}(x) + \Omega^{(i)}(x) \tag{6}$$

and

$$\Lambda^{(i)}(x) = q^{(1)}(x)\Lambda^{(i-1)}(x) + \Lambda^{(i-2)}(x) \tag{7}$$

The recursion is continued until the degree of Ω is less than $t + p/2$, where p is the number of erasures.

Erasures are the errors which have been located prior to decoding. Utilizing this information will improve the error correction capability of the decoder. Since the burst is a big part of a composite error, a burst erasure will make the error correction capability much greater. This idea leads to the following approach:

STEP 1 Set stop conditions, the maximum iteration time N and n=0.

STEP 2 Assume the burst begins at location a and n=n+1.

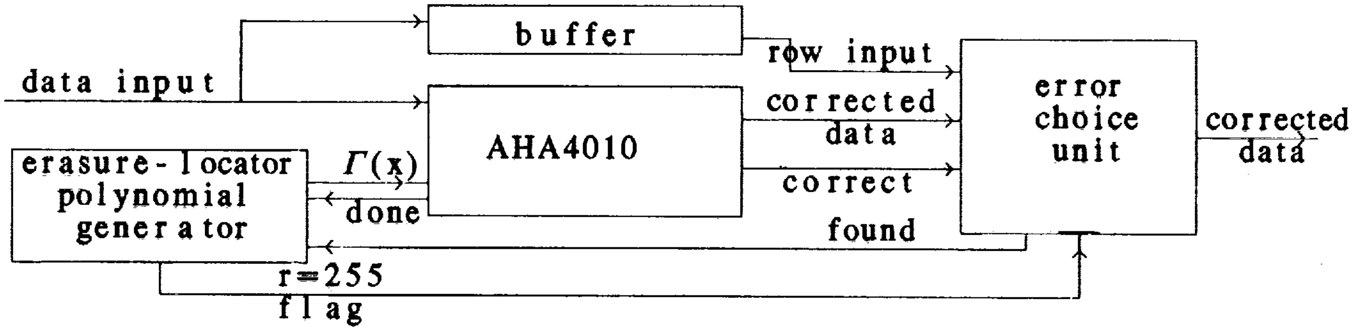


Figure 1: Block Diagram

STEP 3 Decode the error with the burst as erasures.

STEP 4 If the result satisfies the stop conditions or n¿N, go to STEP 5. Else, increase the beginning location of the burst, go to STEP 2.

STEP 5 Report the result.

In other words, the decoding method, used by the extended decoder, is to guess where the burst part of the error is and try to decode it.

3 Extended Decoder Design

The extended RS decoder has an AHA4010 decoder at its center. An erasure-locator polynomial generator, an error choice unit and a data buffer are attached to the AHA4010 decoder. The top level block diagram of this extended decoder is shown in Figure 1.

The erasure-locator polynomial generator generates $\Gamma(x)$. $\Gamma(x)$ could be generated for every possible error location. However, this may not be necessary. For example, let error, $e(x)$, be defined as:

$$e_1(x) = \alpha^6 + \alpha^9 x^1 + \alpha^6 x^2 + \alpha^0 x^3 + \alpha^4 x^{13} \qquad (8)$$

The error, $e(x)$, can be interpreted as

1. $e(x) = 0x^{-1} + \alpha^6 + \alpha^9 x^1 + \alpha^0 x^3 + \alpha^4 x^{13}$

   A burst length of 5 ($0x^{-1} + \alpha^6 + \alpha^9 x^1 + \alpha^6 x^2 + \alpha^0 x^3$) and one random error ($\alpha^4 x^{13}$).

2. $e(x) = 0x^{-2} + 0x^{-1} + \alpha^6 + \alpha^9 x^1 + \alpha^6 x^2 + x^3 + \alpha^4 x^{13}$.

   A burst length of 5 ($0x^{-2} + 0x^{-1} + \alpha^6 + \alpha^9 x^1 + \alpha^6 x^2$) and two random errors ($\alpha^0 x^3, \alpha^4 x^{13}$).

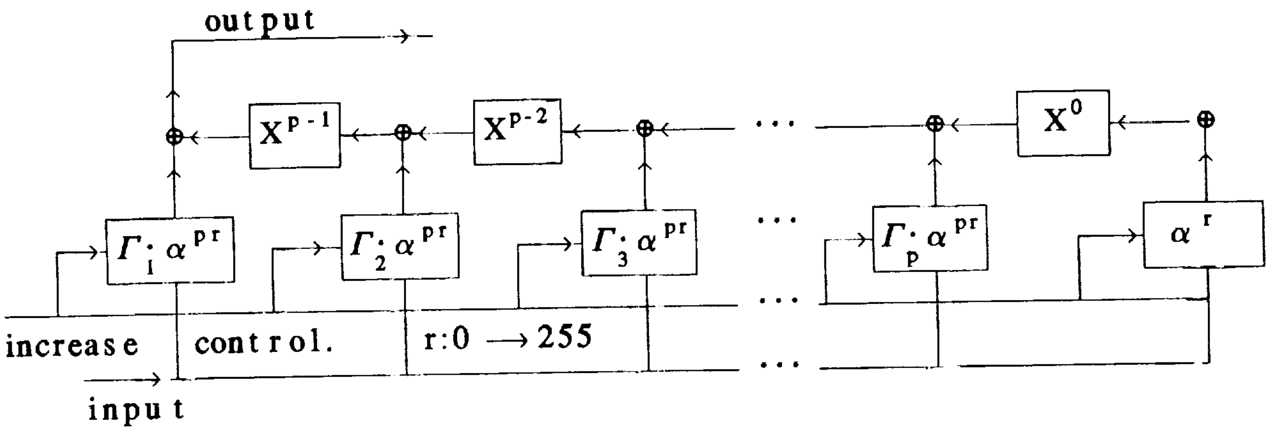
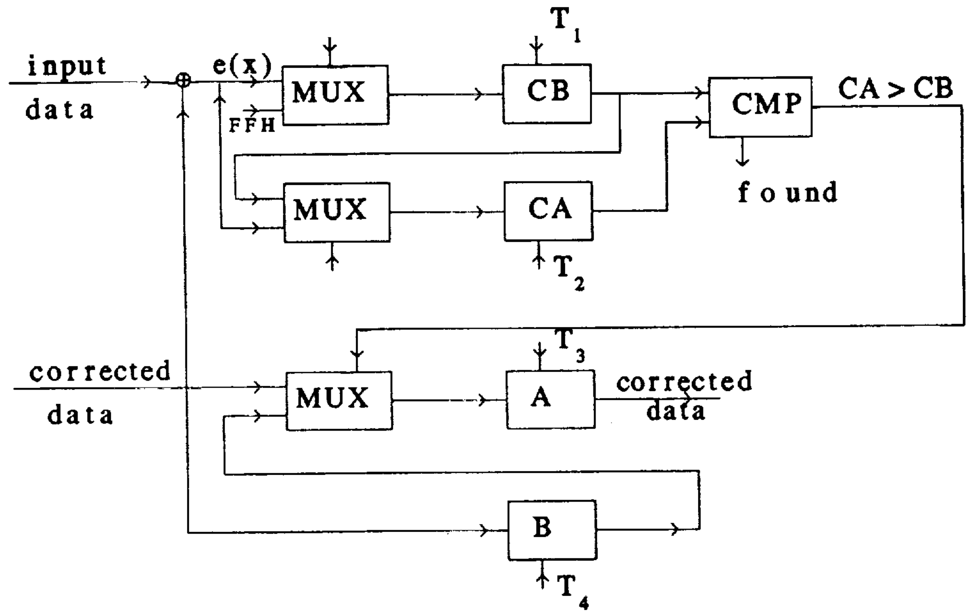

output
X^{p-1}
X^{p-2}
X^0
...
$\Gamma_1 \cdot \alpha^{pr}$
$\Gamma_2 \cdot \alpha^{pr}$
$\Gamma_3 \cdot \alpha^{pr}$
$\Gamma_p \cdot \alpha^{pr}$
α^r
increase
control.
r:0 ⟶ 255
input

Figure 2: Erasure-locator Polynomial Generator



CONTROLS:

$T_1 = P_0 + P_1 * \text{CORRECT} * (C \neq 1)$,

$T_2 = P_1 * \text{CORRECT} * (C = 1) + P_2 * (CA > CB)$,

$T_3 = P_0 + P_1 * \text{CORRECT} * (C = 1) + P_2 * (CA > CB)$,

$T_4 = P_0 + P_1 * \text{CORRECT} * (C \neq 1)$.

Figure 3: Error Choice Unit

3. $e(x) = \alpha^6 + \alpha^9 x^1 + \alpha^6 x^2 + \alpha^0 x^3 + 0x^4 + 0x^5 + \alpha^4 x^{13}$.
   A burst length of 5 $(\alpha^6 + \alpha^9\alpha^1 + \alpha^6\alpha^2 + \alpha^0\alpha^3 + 0\alpha^4)$ and one random error $(0x^5, \alpha^4 x^{13}$.

4. $e(x) = 0x^{-1} + \alpha^6 + \alpha^9 x^1 + \alpha^6 x^2 + \alpha^0 x^3 + 0x^4)$.
   A burst length of 5 $(0x^{-1} + \alpha^6 + \alpha^9 x^1 + \alpha^6 x^2 + \alpha^0 x^3 + 0x^4\ )$ and two random error $(0x^5, \alpha^4 x^{13})$.

A RS code with the ability of correcting a burst of length 5 and 2 random errors will correct all the errors above. Using this logic, $\Gamma(x)$ can be generated every m error location bits. The user must decide the value of m under the consideration of the number of iteration times and the size of the correctable error.

Meanwhile, the error choice unit stores the data corrected by the AHA4010 decoder and reverses it back to the error polynomial. If the size of the error is less than t' (i.e. This error has the highest probability of occurrence), the error choice unit interrupts the iteration and outputs the corrected data. Otherwise the iteration continues. If more than one error is found, the error choice unit compares these errors and the smallest error is chosen (It is assumed that the smallest error has the highest probability of occurrence).

4 Erasure-Locator Polynomial Generator

Assume the received code words have a composite error patterned with i random errors and one burst error of length v. The burst locations may be $\alpha^{r+1}, \alpha^{r+2}, ..., \alpha^{r+v}$, where r is from 0 to 255. The erasure-locator polynomial, $\Gamma(x)$, has a form:

$$\Gamma(x) = \prod_{j=1}^{v}(1 + x\alpha^{j+r})$$

$$= \prod_{j=1}^{v}(\alpha^{-r} + x\alpha^{j})\alpha^{r}$$

$$= \alpha^{vr}(\Gamma_1 x^v + \Gamma_2 x^{v-1} + ... + \Gamma_v x + \alpha^{-v})$$

where $\Gamma_1, \Gamma_2, \text{and} \Gamma_v$ are constant and r is form 1 to 255.

For each received code word, the corresponding decoding process is performed N/m times with N/m different $\Gamma(x)$, where N is the length of the RS code and m is the bits that $\Gamma(x)$ skips. At each end of the decoding process, a DONE signal is sent to the erasure-locator polynomial generator. The DONE signal causes erasures to shift to the right m bits. Therefore, a new $\Gamma(x)$ is generated. This operation repeats until a FOUND signal is received or r > 255.

The erasure-locator polynomial generator is depicted in Figure 2. The coefficients of this polynomial, $\Gamma_j\alpha^{pr}$ (j from 0 to v), are not constant. $\Gamma_j\alpha^{pr}$ multiply by α whenever INCREASE CONTROL (i.e. DONE signal) is assertive.

The operations can be described in a register transfer language where each P_i is a control state that defines the data transfers that take place when P_i is active. A register transfer language description for the erasure-locator polynomial generator is shown below:

- P_0 : r=0, if GO=1, then go to P_1.
- P_1 : if FOUND=1 or r=255, then go to P_0 , else $\Gamma_0 = \alpha^r, \Gamma_1 = \Gamma_1\alpha^{pr}, \Gamma_2 = \Gamma_2\alpha^{pr}, ..., \Gamma_p = \Gamma_p\alpha^{pr}$ and $r = r + 1$.
- $P_2 : \Gamma(x) = \prod(1 - x\alpha^r)$, if DONE=1, go to P_1 .

5 Error Choice Unit

During the decoding iteration, it is possible that more than one error results. The error with the highest probability of occurrence should be chosen. It is assumed that will be the smallest error. The diagram of the error choice unit is shown in Figure 3.

The first data corrected by the AHA4010 decoder is stored in register A, its corresponding error is also calculated and the size of the error is stored in CA. If the size of the error is less than t', the CMP asserts the FOUND signal and outputs the data in register A. The decoding process otherwise continues. The second corrected data is stored in register B, the size of the second error is stored in CB. The CMP compares the values of CA and CB. If CA > CB, A is replaced by B and CA is replaced by CB. If the value of CB is less than t', the CMP asserts the FOUND signal and outputs the data in register A. If CA $\leq$ CB, nothing changes. This comparison is performed every time a corrected data is output from the AHA4010 decoder. It guarantees that the register A always has the data which is corrected from the smallest error.

A signal from the erasure-locator polynomial generator tells the error choice unit that the iteration is finished. The data in register A is the output.

A register transfer language description for the error choice unit is:

- $P_0 : 0 \rightarrow \text{A}, 0 \rightarrow \text{B}, 1 \rightarrow \text{C}, \text{FFH} \rightarrow \text{CB}$, if GO = 1, go to P_1 .
- P_1 : if CA < t' or CB < t' or FLAG=1 (i.e. r=255), output data, set FOUND=1, go to P_0 .
- if CORRECT=1 & C=1, correctedData → A, size (correctedData) → CA, c = c+1;
- if CORRECT=1 & C ‡ 1, correctedData → B, size (correctedData) → CB;
- P_2 : if $\text{CA} > \text{CB}, \text{B} \rightarrow \text{A}, \text{CB} \rightarrow \text{CA}$, go to P_1.

CORRECT is a signal from the AHA4010 decoder which indicates a correction has or has not been made. C is a counter. It counts the number of correction times for one received code word.

6 An Example

Consider a (255,235) RS code over GF(2^8) defined by the primitive polynomial $p(x) = x^8 + x^7 + x^2 + x^1 + 1$ with the primitive element $\alpha = x$. This code can normally correct ten random errors. Assume received errors have a burst of length 8 and 5 random errors. After considering the number of iteration times and the size of the correctable error, let's set the m=4 and t'=11.

SOLUTION:
The received polynomial is:

$$v(x) = x^{14}+\alpha^3x^{15}+\alpha^{200}x^{16}+\alpha^8x^{17}+\alpha^{40}x^{18}+\alpha^{23}x^{19}+\alpha^6x^{20}+x^{21}+\alpha^{54}x^{183}+\alpha^{71}x^{198}+\alpha x^{233}. \tag{9}$$

When the extended RS decoder is turned on, the erasure-locator polynomial is:

$$\Gamma(x) = \prod_{j=1}^{8}(1 + x\alpha^1). \tag{10}$$

This $\Gamma(x)$ is sent to the AHA4010 decoder, the FOUND signal is zero. Multiply the coefficients of $\Gamma(x)$ by α^{32} (i.e. $\alpha^{vr} = \alpha^{4\cdot 8} = \alpha^{32}$). The erasure-locator polynomial becomes:

$$\Gamma(x) = \prod_{j=1}^{8}(1 + x\alpha^1\alpha^4)$$

and this new $\Gamma(x)$ is sent to the AHA4010, the FOUND signal is still zero. This decoding process performs repeatedly until the FOUND signal is one. That gives the corrected data:

$$\{0, 0, 0, ..., 0\}$$

The corresponding erasure-locator polynomial is:

$$T(x) = \prod_{j=1}^{8}(1 + x\alpha^j\alpha^{12}) \tag{11}$$

and the corresponding error polynomial is:

$$v(x) = x^{14} + \alpha^3x^{15} + \alpha^{200}x^{16} + \alpha^8x^{17} + \alpha^{40}x^{18} + \alpha^{23}x^{19} + \alpha^6x^{20} + x^{21} + \alpha^{54}x^{183} + \alpha^{71}x^{198} + \alpha^{233}.$$

7 Summary

An extended RS decoder has been presented in this paper. With two extra circuits, the error correction capability of a general purpose RS decoder can be increased. This design shows a way to improve the error correction capability of existing RS decoders.

References

[1] P. Owsley, "Burst Error Correction Extensions for Reed Solomon Codes," PH.D Dissertation, E.E. Dept. University of Idaho, July 1988.

[2] W. W. Peterson, "Encoding and Error-Correction Procedures for the Bose-Chaudhuri Codes," IEEE Trans. Inf. Theor. IT-6 (1960), pp. 459-470.

[3] R. E. Blahut, *Theory and Practice of Error Control Codes*, Addison-Wesley Publishing Company, 1983.