# HIGH DATA RATE REED-SOLOMON ENCODING AND DECODING USING VLSI TECHNOLOGY

Warner Miller
Instrument Division, Code 728
Goddard Space Flight Center
Greenbelt, Maryland 20771

Dr. James Morakis
Applied Engineering Division, Code 730
Goddard Space Flight Center
Greenbelt, Maryland 20771

## ABSTRACT

Presented as an implementation of a Reed-Solomon encoder and decoder, which is 16-symbol error correcting, each symbol is 8 bits. This Reed-Solomon (RS) code is an efficient error correcting code that the National Aeronautics and Space Administration (NASA) will use in future space communications missions. A Very Large Scale Integration (VLSI) implementation of the encoder and decoder accepts data rates up to 80 Mbps. A total of seven chips are needed for the decoder (four of the seven decoding chips are customized using 3$\mu$m Complementary Metal Oxide Semiconduction (CMOS) technology) and one chip is required for the encoder. The decoder operates with the symbol clock being the system clock for the chip set. Approximately 1.65 billion Galois Field (GF) operations per second are achieved with the decoder chip set and 640 MOPS are achieved with the encoder chip.

## INTRODUCTION

An RS code is a cyclic symbol error correcting code that is useful in burst error channels. This code has potential applications in communications systems and in digital systems where burst error conditions exist. In each of these areas, VLSI implementations of the encoder and decoder systems are of great interest since Transistor Transistor Logic (TTL) implementations could require 1,000 to 2,000 chips, using conventional Medium Scale Integration (MSI) devices.

The Microelectronic Research Center at the University of Idaho has designed a chip set for NASA to implement a (255, 223) RS code according to the Consultative Committee for Space Data Systems (CCSDS) specifications (1) which have been promoted by NASA and the European Space Agency (ESA). The chip set has been fabricated and is functional. The encoder was built following a conventional architecture (2) and the decoder has been designed around Euclid's algorithm (3).

The RS code has been well described in the references and no attempt will be made to define all of its parameters.

## PARAMETERS

The RS code can be described with the following parameters and notation:

| | |
|---|---|
| q | = the number of bits in each symbol |
| $n \leq 2^q - 1$ | = thenumber of symbols in each code block |
| t | = the number of correctable symbol errors in a block of n symbols |
| 2t | = the number of check symbols |
| k = n-2t | = the number of information symbols |
| C(x) | = the code block represented as an order n-1 polynomial |
| M(x) | = the k information symbols represented as an order k-1 polynomial |

For the code designed,

$$q = 8 \text{ and } t = 16$$

## CODE DESCRIPTION

The RS code block is defined to be

$$C(x) = x^{32} \bullet M(x) + M(x) \bmod G(x). \tag{1}$$

Every valid code block is a multiple of the generator polynomial G(x). In its simplest form, the generator polynomial is defined as

$$G(x) = \prod_{i=0}^{2t-1} (x - \alpha^i) = \sum_{j=0}^{2t} G_j x^j \tag{2}$$

where α is a primitive element of the field.

A more general form of the generator polynomial is described as

$$G(x) = \prod_{i=s}^{s+2t-1} (x - \beta^i) = \sum_{j=0}^{2t} G_j x^j \tag{3}$$

where s is an offset and β is another primitive element of the field equal to $\alpha^i$. The second form is used by NASA and ESA; specifically, $\beta = \alpha^{11}$ and s = 112. Symmetrical coefficients of G(x) are a consequence of an offset of 112 (4).

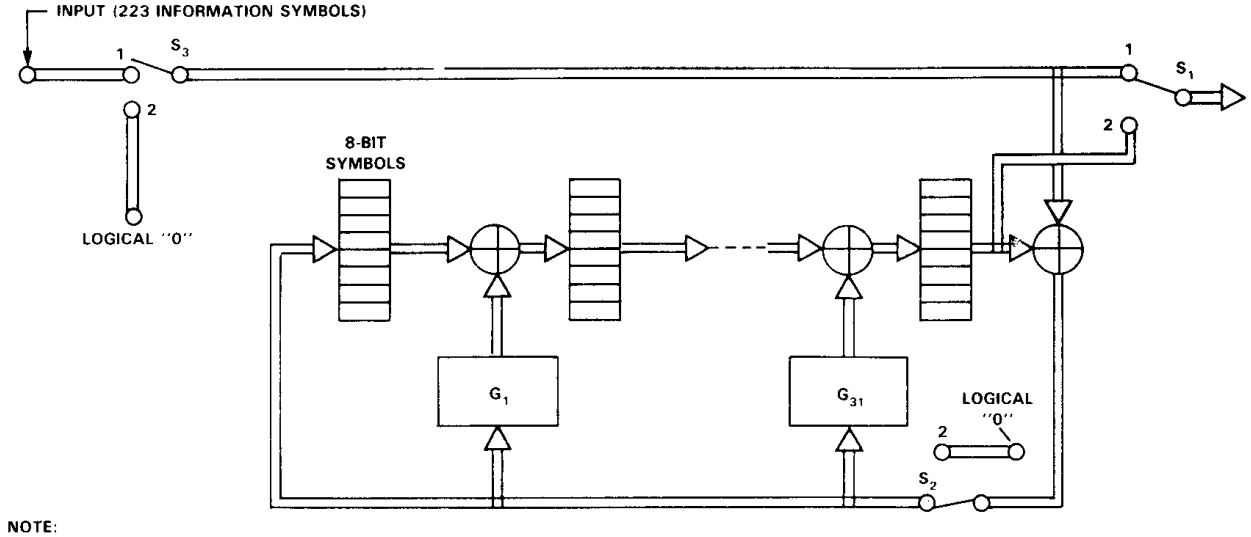
Each of the 255 8-bit symbols of the code polynomial are members of the finite Galois Field GF($2^8$). A Galois Field can be defined by an irreducible polynomial p(x) (5). For the field under consideration, $p(x) = x^8+x^7+x^2+x+1$.

## ENCODER ARCHITECTURE

The encoder consists of one VLSI chip and uses the classical architecture as shown in Figure 1 and implements a feedback shift register (6). The feedback multipliers are the coefficients of the generator polynomial G(x). The operation can be defined as follows for a (n,k) code: with the shift register initially empty, the k information symbols are shifted into the encoder one symbol at a time; each symbol is input in a parallel (bit-wise) fashion. After k clock pulses, the feedback shift register contains the check symbols; the input is disabled and the n-k check symbols are shifted out. All operations occur in a bit-wise parallel fashion. The hardware necessary to implement this circuit is summarized below:

n-k, j-bit registers
n-k, j-bit in, j-bit out GF multipliers
n-k, j-bit exclusive or gates.

With a symmetric generator polynomial, the number of multipliers is reduced by a factor of two.

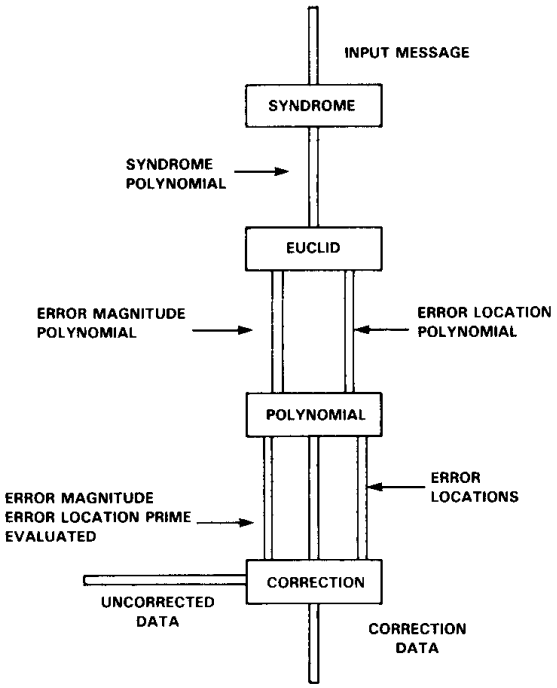



NOTE:
1. ALL ARE 8-BIT PARALLEL BUSES.
2. ADDITION AND MULTIPLICATION ARE IN GF ($2^8$) MODULE F(X).
3. ALL REGISTERS INITIALLY SET TO ZERO.
4. SWITCHES $S_1$ THROUGH $S_3$ IN POSITION 1 FOR FIRST 223 SYMBOL SHIFTS, THEN IN POSITION 2 FOR LAST 32 SYMBOL SHIFTS.

**Figure 1. Reed-Solomon Encoder RS (255, 223)**

## DECODER ARCHITECTURE

The decoder consists of four VLSI chips as shown in Figure 2. The system is configured to perform in a pipeline manner where several messages are being processed simultaneously.




| TRANSISTORS | MOPS | CALCULATIONS |
|---|---|---|
| 19,400 | 640 | 16,320 |
| 66,000 | 122 | 3,110 |
| 33,000 | 840 | 20,910 |
| 19,200 | 40 | 1,020 |
| 137,600 | 1,642 | 41,360 |

NOTE:
1. EIGHT-BIT, 16-SYMBOL CORRECTION.
2. DATA RATE 80 MBPS.
3. CMOS ¼ WATT MODULE.

**Figure 2. Reed-Solomon Decoder, RS (255, 223)**

During transmission, the code changes due to noise in the channel which amounts to an error polynomial being added to the code polynomial C(x). Let the received polynomial be

$$R(x) = C(x) + E(x) = r_{n-1} X^{n-1}\text{-}1\text{+} \ldots r_1 + r_0 \qquad (4)$$

where E(x) is the error polynomial and each $r_i$ is a field element. Symbols $r_i$, i goes from 0 to n-1 and are the check symbols. The first step in the decoding algorithm is to calculate the syndromes. The syndrome polynomial is defined as

$$S(x) = R(x) \bmod G(x). \qquad (5)$$

An equivalent definition of the syndrome polynomial is:

$$S_k = \sum_{i=0}^{n-1} r_i b^{i(k+s)} \tag{6}$$

where $0 \le k \le 2t-1$. The syndrome polynomial can be defined as

$$S(x) = \sum_{k=0}^{2t-1} s_k x^k \tag{7}$$

The next step is to obtain the error location polynomial, $\Delta(x)$ and the error magnitude polynomial $\Omega(x)$. These polynomials have the following relationship with the syndrome polynomial

$$S(x)\Delta(x) = \Omega(x) \bmod x^{2t} \tag{8}$$

The error location and error magnitude polynomials can be obtained by using Euclid's greatest common divisor algorithm (5), which is a recursive operation.

Once the two polynomials are known, the location and magnitude of a given error is found as follows: let $\beta^i$ be a zero of $\Delta(x)$ (i.e., $\Delta(\beta^i) = 0$), then the error magnitude at location $-i \bmod 2^q-1$ is

$$\Delta(\beta^i) / \Delta'(\beta^i) \bullet (\beta^{112i}) \tag{9}$$

where $\Delta'(x)$ is the first derivative of $\Delta(x)$ with respect to x. For more details and examples, refer to Clark and Cain (5).

The general operation can be described as follows: the received polynomial, R(x), is input from a fast serial to parallel module to both the First In First Out (FIFO) for storage and to the syndrome calculator. The 32 syndromes are passed to the Euclid Divide/Multiply module that generates $\Omega(x)$ and $\Delta(x)$. These polynomials are passed to the Polynomial Solver. The Polynomial Solver evaluates $\Omega(x)$, $\Delta(x)$, and $\Delta'(x)$ at $x = B^i$ where i takes on the values (255, 254, . . ., (255-N)) where 255-N is the amount that the code has been shortened. If $\beta^i$ is a root of $\Delta(x)$, then a zero is passed to the Error Correction Module. Both $\Delta'(x)$ and $\Omega(x)$ are evaluated for $x = \beta^i$ and these results are also presented to the Error Correction Module. The Error Correction Module determines the error magnitudes: if $x = \beta^i$ is zero, then the magnitude for location $-i \bmod(2^q-1)$ is given by Equation 8; otherwise, there is no error at that location. The polynomial solver calculates both $\Delta(x)$ and $\Omega(x)$; to error correct, it divides these two values and in doing so generates a new

polynomial. This new polynomial is then exclusively-ored with the delayed original information signal, and the resultant is the corrected message which is passed on to the user.

The system clock is the symbol clock which is a very important feature. Therefore, this decoder can decode symbols at the same rate message symbols are received. Decoders that cannot use the symbol clock as the system clock must utilize a more complex clock system where the decoder operates at a higher clock rate than the symbol clock. Therefore, for a given technology, this decoder can operate faster than other designs that require a system clock that operates at a higher rate than the symbol clock. Moreover, operating at the symbol clock rate reduces the amount of message buffering.

## CONCLUSION

A decoder has been described that corrects up to 16 symbol errors for an RS code at an 80-Mbps data rate. The output consists of the corrected information symbols and a status word. The status word, which is inserted in symbol location 31 (location of the first check symbol), contains the number of errors found and an uncorrectable error flag. If the message is uncorrectable, the information symbols are unchanged. The operation rate of the decoder chip set as a whole exceeds 1.65 BOPS.

The decoder is configured to perform in a pipeline manner where several messages are being processed simultaneously. The processing delay has a latency of four messages, one message delay per module. The decoder, as designed, consists of four customized chips and are implemented using 3 $\mu$m CMOS technology. The decoder requires three support chips, one three-message buffer (FIFO), and two Read Only Memory (ROM) devices.

The encoder requires one customized chip and was also implemented using 3 $\mu$m CMOS technology. Both the encoder and decoder chip set has been fabricated, tested, and operates at the real time of 80 Mbps as presented in the paper. This code is currently designed into the next generation spacecraft systems by both NASA and ESA.

## REFERENCES


1 . Consultative Committee for Space Data Systems, “Telemetry Channel Coding”, NASA, May 1984.

2. Maki, G., Owsley, P., Cameron, K., and Shovic, J., “A VLSI Reed-Solomon Encoder: An Engineering Approach”, Custom Integrated Circuits Conference, pp. 177-181, May 1986.

3. Maki, G., Owsley, P., Cameron, K., and Venbrux, J., “VLSI Reed-Solomon Decoder Design”, IEEE Military Communications Conference, October 1986.

4. Reefs, H. F. A. and Best, A. R., “Concatenated Coding on a Spacecraft-to-Ground Telemetry Channel Performance”, Proceedings ICC-81, 1981.

5. Clark, George C., and Cain, J. Bibb, *Error-Correcting Coding for Digital Communication* Plenum Press, New York, NY, 1981.

6. Perlman, Marvin and Lee, Jun-Ji, “Reed-Solomon Encoders - Conventional versus Berlekamp’s Architecture”, Jet Propulsion Laboratory, 82-71, December 1982.