International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Reed Solomon Decoder with Parallel Syndrome Computation on FPGA: A Review

Saroj Bakale[1], Dhananjay Dabhade[2]

[1]Agnihotri College of Engineering, Nagpur University

[2]Assistant Professor, Agnihotri College of Engineering, Nagpur University

Abstract: ***In wireless, satellite, and space communication systems, reducing error rate is critical. High bit error rates of the wireless communication system require employing various coding methods on the data transferred. Channel coding for error detection and correction helps the communication system designers to reduce the effects of a noisy transmission channel. The purpose of this paper is to study and investigate the performance of Reed-Solomon decoder that is used to decode the data stream in digital communication. In this paper, the proposed work is to implement the decoder of Reed-Solomon (RS) coding scheme on the platform of VHDL using algorithm. Implementation will be done on VLSI Hardware Description Language (VHDL) and results can be seen on Field Programmable Gate Array (FPGA). This paper reviews the Reed Solomon decoder performance over Xilinx package.***

Keywords: Reed Solomon (RS), Galois Field, Generator polynomial, Syndrome calculator, Berlekamp-Massey, Chain search, VHDL, FPGA.

1. Introduction

Nowadays, we live in a world where communications play an important role both in our daily lives and in their involvement in the economic and technological fields. We constantly need to increase the flow of transmission while maintaining and improving their quality. But without a concern of reliability, all improvement efforts would be futile because it would necessarily mean that some data are to be rebroadcast An error correcting code allows the correcting of one or several errors in a code word by adding redundant symbols to the information, otherwise called, control symbols. Different possible codes exist but in this document we will only deal with Reed Solomon codes because for the moment being, they represent the best compromise between effectiveness (symbols of parity added to the information) and complexity (coding difficulty). Reed-Solomon coding is a very efficient and popular Forward Error Correction technique discovered by Reed and Solomon in 1960[1].Reed-Solomon (RS) codes are among the most widely used block error-correcting codes in digital communication and storage systems [2] and are very Effective in correcting random symbol errors and random burst errors. Therefore they are applied in many systems such as storage devices, mobile communications, and digital Television/DVB, high-speed modems etc. RS codes are adopted by various Standards like DVBT, DVBS, DVB DSNG, DVB C, and IEEE 802.16 WI-MAX.

The purpose of error correction coding can be expressed as increasing the reliability of data communications or data storage over a noisy channel, controlling errors so the reliable reproduction of data can be obtained, increasing the overall system's signal-to-noise energy ratio (SNR), reducing noise effects within a system. The reed-Solomon error correction codes were firstly introduced in the paper "Polynomial codes over certain finite fields" in 1960 for burst error correction. [1]. These codes are non-binary systematic cyclic linear block codes. These codes work with symbols that consist of several bits. The mostly used symbol size for non-binary codes is 8-bits, or a byte. A systematic code generates codeword that contain the message symbols in unaltered form. The encoder used mathematical function to the message symbols in order to generate the redundancy, or parity symbols. The basic block diagram for communication system is shown in Figure.*2*

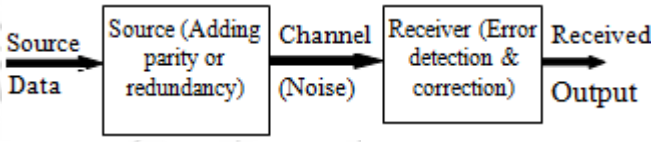

Figure 1: Block diagram for communication system

A. Types of error correction codes

The block and convolution coding are two important classes of error control or channel control coding. Block codes work on fixed-size blocks (packets) of bits or symbols of predetermined size. Practical block codes can generally be decoded in polynomial time to their block length. convolution codes work on bit or symbol streams of arbitrary. There are many types of block codes, but among the classical ones the most notable is Reed-Solomon coding because of its widespread use on the Compact disc, the DVD, and in hard disk drives. Other examples of block codes include BCH, Hamming, Turbo, Turbo Product, LDPC, fountain codes and BICM codes.

The rest of paper is organized as follows. This article is structured in six sections. Section II briefly review about Reed Solomon code. Section III gives literature review of reed Solomon code. Section IV provides conclusion.

2. Reed Solomon Code

RS code is short for Reed-Solomon encoder, which is a kind of non-binary BCH codes, and is particularly applicable in correcting burst errors. Reed Solomon codes have higher error correcting capability that any other codes have. The parameters of RS code are:

m= the number of bits per symbol
n= the block length
k = the uncoded message length in symbols
(n- k) = the parity check symbols (check bytes)
t= the number of correctable symbol errors.

Reed Solomon (RS) codes are a subset of BCH codes and also in a class of linear block codes. A RS code is specified as RS (*n*, *k*) with *s*-bit symbols. This means that the encoder takes *k* data symbols of *s* bits each and adds parity symbols to make an *n* symbol codeword. There are $n - k$ parity symbols of *s* bit each. A RS decoder can correct up to *t* symbols that contain errors in a codeword, where $2t = n - k$. Figure.1 shows a typical RS codeword which is also known as a systematic code.

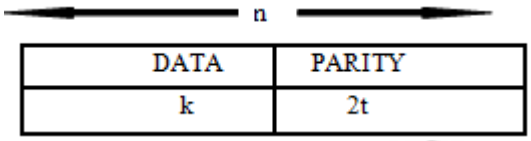

Figure 1: Typical RS Codeword

RS codes are particularly suitable to correct burst errors whereas series of bits in the codeword are received in error. The RS algebraic decoding procedure can correct errors as well as erasures. An erasure occurs when the position of an error symbol is identified at the decoder by the external circuitry. In general, an RS decoder can detect and correct up to (t = r/2) incorrect symbols if there are (r = n-k) redundant symbols in the encoded message. One redundant symbol is used in identifying the precise value of that error. If the RS decoder has been instructed that a specific message symbol is in error, it only has to use one redundant symbol to correct that error and does not have to use an additional redundant symbol to determine the location of the error 2t erasures can be corrected if the locations of all the errors are given to the RS codec by the control logic of the system.

3. Literature Review

Channel coding is a widely used technique for the reliable transmission and reception of data. Generally systematic linear cyclic codes are used for channel coding. In 1948, Shannon introduced the linear block codes for complete correction of errors. Cyclic codes were first discussed in a series of technical notes and reports written between 1957 and 1959 by Prange. This led directly to the work published in March and September of 1960 by Bose and Ray-Chaudhuri the BCH codes [3]. In 1959, Irving Reed and Gus Solomon described a new class of error-correcting codes called Reed-Solomon codes. Originally Reed-Solomon codes were constructed and decoded through the use of finite field arithmetic [4], [5] which used nonsingular Vandermonde matrices. In 1964 Singleton showed that this was the best possible error correction capability for any code of the same length and dimension [6]. Codes that achieve this "optimal" error correction capability are called Maximum Distance Separable (MDS). Reed-Solomon codes are by far the dominant members, both in number and utility, of the class of MDS codes. MDS codes have a number of interesting properties that lead to many practical consequences. The generator polynomial construction for Reed-Solomon codes is the approach most commonly used today in the error control literature. This approach initially evolved independently from Reed-Solomon codes as a means for describing cyclic codes. Gorenstein and Zierler then generalized Bose and Ray-Chaudhuri's work to arbitrary Galois fields of size p m , thus developing a new means for describing Reed and Solomon's "polynomial codes" [7]. It was described that vector c is a code word in the code defined by g(x) if and only if its corresponding code polynomial c(x) is a multiple of g(x). So the information symbols could be easily mapped onto code words. All valid code polynomials are multiples of the generator polynomial. It follows that any valid code polynomial must have as roots the same 2t consecutive powers of α that form the roots of g(x). This approach leads to a powerful and efficient set of decoding algorithms. After the discovery of Reed-Solomon codes, a search began for an efficient decoding algorithm. In 1960, Reed and Solomon proposed a decoding algorithm based on the solution of sets of simultaneous equations. Though much more efficient than a look-up table, Reed and Solomon's algorithm is still useful only for the smallest Reed-Solomon codes. In 1960 Peterson provided the first explicit description of a decoding algorithm for binary BCH codes [8], His "direct solution" algorithm is quite useful for correcting small numbers of errors but becomes computationally intractable as the number of errors increases. Peterson's algorithm was improved and extended to non - binary codes by Gorenstein and Zierler (1961) [7], Chien (1964) [9], and Forney (1965) [10]. These efforts were productive, but Reed-Solomon codes capable of correcting more than six or seven errors still could not be used in an efficient manner. In 1967, Berlekamp demonstrated his efficient decoding algorithm for both non - binary BCH and Reed-Solomon codes [11]. Berlekamp's algorithm allows for the efficient decoding of dozens of errors at a time using very powerful Reed-Solomon codes. The operation needed for original Berlekamp-Massey algorithm and modified Berlekamp-Massey algorithm are similar except for the extra multiplications in the modified method and the division operation needed in the original method. The division operation needed in the original method required a table-lookup to find an inverse element, which can be a tedious and time consuming process. In modified Berlekamp-Massey algorithm, one extra reloaded register is used that stores syndromes codeword following the modified structure. So, VLSI structure of modified Berlekamp-Massey algorithm is simple and regular and suitable for decoding of Reed-Solomon codes. In 1968 Massey showed that the BCH decoding problem is equivalent to the problem of synthesizing the shortest Linear Feedback Shift Register capable of generating a given sequence [12]. Massey then demonstrated a fast shift register-based decoding algorithm for BCH and Reed-Solomon codes that is equivalent to Berlekamp's algorithm. This shift register-based approach is now referred to as the Berlekamp-Massey algorithm. In 1975 Sugiyama, Kasahara, Hirasawa, and Namekawa showed that Euclid's algorithm can also be used to efficiently decode BCH and Reed- Solomon codes [13]. Euclid's algorithm is a means for finding the greatest common divisor of a pair of integers. It can also be extended to more complex collections of objects, including certain sets of polynomials with coefficients from finite fields.

A. Forward Error Correction Code

In communication, information and coding theory, error control technique is used for controlling errors in data transmission over unreliable or noisy communication channels to provide robust data transmission through imperfect channel by adding redundancy to the data according to predetermined algorithm. The redundancy allows the receiver to detect a limited number of errors that may occur anywhere in the message, and often to correct these errors without retransmission. Forward Error correction (FEC) is the key ingredient for improving reliability of modern digital communication and storage systems and to guarantee data integrity. FEC gives the receiver the ability to correct errors without needing a reverse channel to request retransmission of data, but at the cost of a fixed, higher forward channel bandwidth. FEC is therefore applied in situations where retransmissions are costly or impossible, such as when broadcasting to multiple receivers in multicast. Design of the FEC code determine maximum fractions of errors or of missing bits that can be corrected, so different forward error correcting codes are suitable for different applications. Designers have tradeoffs to consider when choosing a FEC code for a transmission system such as power, FEC complexity, and FEC performance, etc. The error correction codes, also known as Forward Error Correction (FEC) codes, allow the recovery of a certain amount of error during data transmission without having to resend the data itself, thus increasing the system transmission capacity [14]. The high transmission rate communication systems need high performance and low cost hardware implementations of error correction codes. The block code, one of the FEC code, adds a constant size redundancy and it is capable of correcting multiple errors [15]. Error correction codes provide various benefits such as larger communication links, power gain and inter-channel interference correction.

In [16] authors, Reed-Solomon (RS) codes are widely used as forward correction codes (FEC) in digital communication and storage systems. Correcting errors of RS codes have been extensively studied in both academia and industry. However, for burst-error correction, the research is still quite limited due to its ultra-high computation complexity. In this brief, starting from a recent theoretical work, a low-complexity reformulated inversion less burst-error correcting (RiBC) algorithm is developed for practical applications. Then, based on the proposed algorithm, a unified VLSI architecture that is capable of correcting burst errors, as well as random errors and erasures, is firstly presented for multi-mode decoding requirements. This new architecture is denoted as unified hybrid decoding (UHD) architecture. It will be shown that, being the first RS decoder owning enhanced burst-error correcting capability, it can achieve significantly improved error correcting capability than traditional hard-decision decoding (HDD) design. Which concludes that In this brief, a high-speed RiBC algorithm for RS code burst-error correcting, and a UHD architecture that can support three different decoding modes are proposed. Comparison results show that the UHD decoder can achieve enhanced capability of correcting long burst of errors with good hardware efficiency.

In [17] authors, to reduce the complexity of algebraic soft-decision decoding (ASD) of Reed–Solomon (RS) codes, re-encoding and coordinate transformation can be applied. For an (n, k) code, the re-encoding was implemented as applying erasure decoding to the k most reliable code positions previously. Such re-encoding can occupy a significant part of the overall decoder area. In this brief, we propose to choose the first k positions and implement the re-encoding in the low-complexity Chase (LCC) ASD algorithm by systematic encoding, which can be done by simple constant multipliers. Moreover, novel schemes are developed to modify the following interpolation and code word recovery steps in the case that systematic symbols need to be flipped to form the test vectors in the LCC decoding. Without any performance loss, the proposed schemes can lead to 15.5% higher efficiency in terms of throughput-over-area ratio in the LCC decoder with eight test vectors for a (255, 239) RS code over GF(28) which conclude that to use systematic re-encoding in the LCC decoder and developed novel schemes to accommodate the flipping of systematic code positions? Systematic re-encoding is much simpler than erasure re-encoding, and the required modifications on the following decoding steps have small overhead. As a result, the proposed decoder can achieve much higher efficiency than prior designs. Our future work will exploit if systematic re-encoding can be employed in general ASD decoders.

In [18] authors, present an iterative soft-decision decoding algorithm for Reed–Solomon (RS) codes offering both complexity and performance advantages over previously known decoding algorithms. algorithm is a list decoding algorithm which combines two powerful soft-decision decoding techniques which were previously regarded in the literature as competitive, namely, the Koetter–Vardy algebraic soft-decision decoding algorithm and belief-propagation based on adaptive parity-check matrices, recently proposed by Jiang and Narayanan. Building on the Jiang–Narayanan algorithm, he presents a belief-propagation- based algorithm with a significant reduction in computational complexity. He introduces the concept of using a belief-propagation- based decoder to enhance the soft-input information prior to decoding with an algebraic soft-decision decoder. Which concludes that algorithm is based on enhancing the soft reliability channel information before passing them to an algebraic soft-decision decoding algorithm. This was achieved by deploying the Jiang and Narayanan algorithm, which runs belief-propagation on an adapted parity-check matrix. Using the Koetter–Vardy algorithm as the algebraic soft-decision decoding algorithm, algorithm has impressive coding gains over previously known soft-decision decoding algorithms for RS codes. By comparing with averaged bounds on the performance of ML decoding of RS codes, we observe that our algorithm achieves a near optimal performance for relatively short, high-rate codes. He introduced some modifications over the JN algorithm that resulted in better coding gains. He presented a low complexity adaptive belief-propagation algorithm, which results in a significant reduction in the computational complexity. The performance of our algorithm was studied for the cases when the interpolation cost of the algebraic soft-decision decoding algorithm is both finite and infinite. A small loss in coding gain results when using manageable interpolation costs. The coding gain

of the presented algorithm is larger for channels with memory. Algorithm could also be viewed as an interpolation multiplicity assignment algorithm for algebraic- soft decoding.

In [19] authors, proposed a new area-efficient truncated inversion less Berlekamp-Massey architecture for the Reed-Solomon (RS) decoder, where RS decoder is one of the forward error correction techniques. The area-efficient feature of the proposed architecture is obtained by truncating redundant processing elements in the key equation solver (KES) block using the BM algorithm. This increases the hardware utilization of the processing elements used to solve the key equation and reduces the hardware complexity of the KES block. The proposed TiBM architecture has the lowest hardware complexity compared with conventional KES architecture which concludes that area-efficient TiBM architecture and evaluated its performance for the RS (255,239) decoder design, which can correct up to eight bit error in one block. The TiBM architecture has very low complexity in comparison with the conventional KES architectures. TiBM architecture is well suited for high-speed low-complexity RS decoder design.

4. Conclusion

A simple encoding and decoding algorithm for RS code is presented in this paper is based on the fact that the code word used in Euclid's algorithm is a non-systematic RS code. It uses the recursive extension to compute the remaining unknown syndromes. Finally, the message symbols are thus obtained by only subtracting all known syndromes from the coefficients of the corrupted information polynomial. Reed-Solomon codes are used for error detection and correction for reliable communication. The encoder splits the incoming data stream into blocks and processes each block individually by adding redundancy and the decoder processes each block individually and it corrects errors by exploiting the redundancy present in the received data. This code can be implemented using VHDL language on Xilinx 13.1 and simulated on ISE simulator. The code is synthesized on Spartan 3 to compare the parameters related to parallel syndrome. Proposed Reed-Solomon encoder and decoder implemented on Spartan3 with parallel syndrome can save a lot of area and improves the speed. The performance of Reed-Solomon codes can be improved by using Euclidean Algorithm to solve Key equation.

References

[1] I. S. Reed and G. Solomon, "Polynomial Codes over Certain Finite Fields", Journal of the Society of Industrial and Applied Mathematics, pp. 300–304, 1960
[2] M. Sudan, "Decoding of Reed-Solomon codes beyond the error correction bound," J. Complexity, vol. 12, pp. 180-193, 1997
[3] R. C. Bose and D. K. Ray-Chaudhuri, "On a Class of Error Correcting Binary Group Codes," Information and Control, Volume 3, pp. 68-79, March 1960.
[4] R. J. McEliece, Finite Fields for Computer Scientists and Engineers, Boston: Kluwer Academic, 1987.
[5] S. B. Wicker, Error Control Systems for Digital Communication and Storage, N.J.Prentice-Hall, 1994.
[6] R. C. Singleton, "Maximum Distance Q-nary Codes," IEEE Transactions on Information Theory, Volume IT-10, pp. 116-118,1964.
[7] D. Gorenstein and N. Zierler, "A Class of Error Correcting Codes in pm Symbols," Journal of the Society of Industrial and Applied Mathematics, Volume 9, pp. 207-214, June 1961.
[8] W. W. Peterson, "Encoding and Error-Correction Procedures for the Bose-Chaudhuri Codes," IRE Transactions on Information Theory, Volume IT-6, pp. 459-470, September 1960.
[9] R. T. Chien, "Cyclic Decoding Procedure for the Bose-Chaudhuri- Hocquenghem Codes," IEEE Transactions on Information Theory, Volume IT-10, pp. 357-363, October 1964.
[10] G. D. Forney, "On Decoding BCH Codes " IEEE Transactions on Information Theory, Volume IT-11, pp. 549-557, October 1965.
[11] E. R. Berlekamp, "Nonbinary BCH Decoding," paper presented at the 1967 International Symposium on Information Theory, San Remo, Italy.
[12] J. L. Massey, "Shift Register Synthesis and BCH Decoding," IEEE Transactions on Information Theory, Volume IT-15, Number 1, pp. 122- 127, January 1969.
[13] Y. Sugiyama, Y. Kasahara, S. Hirasawa, and T. Namekawa, "A Method for Solving Key Equation for Goppa Codes," Information and Control, Volume 27, pp. 87-99, 1975.
[14] A. Betten, "Error-Correcting Linear Codes: Classification by Isometric and Applications", Springer, Berlin (2006).
[15] J. C. Moreira and P. G. Farrell, "Essentials of Error-Control Coding", John Wiley & Sons Ltd, Chichester (2006).
[16] Li Li et. al. "Unified Architecture for Reed-Solomon Decoder Combined With Burst-Error Correction" IEEE Vol. 20, No. 7, July 2012
[17] Xinmiao Zhang, Yu Zheng "Systematically Re-encoded Algebraic Soft-Decision Reed–Solomon Decoder" IEEE Vol. 59, No. 6, June 2012.
[18] Yingquan Wu "Novel Burst Error Correction Algorithms for Reed-Solomon Codes" IEEE Vol. 58, No. 2, February 2012.
[19] J.-I. Park, H. Lee "Area-efficient truncated Berlekamp-Massey architecture for Reed-Solomon decoder" 17th February 2011.

Author Profile

Saroj Bakale is pursuing M.Tech. (Electronics) from Nagpur University and B.E. (Electronics & Tele.) from Nagpur University.

Dhananjay Dabhade is working as **Assistant Professor.** He has completed M.Tech. degree in (VLSI) from Nagpur University in 2011 and B.E. (Electronics & Tele.) from Nagpur University in 2007.