An Investigation on Reed-Solomon Codes as Erasure Coding Technique on Its Properties and Utilizations

Jianning Chen *

Department of Electrical and Computer Engineering, Northeastern University, Boston, the United States

* Corresponding Author Email: chen.jiann@northeastern.edu

Abstract. Erasure coding is an essential part of cloud computing, which is an important technology for effective data storage for recovering data that may be lost due to various reasons, there are various erasure coding techniques in the market. In this paper, linear MDS codes, which is a branch of erasure coding, will be investigated on their performance and usage. This paper will focus on the Reed-Solomon Code, which is the most implemented form of linear MDS codes, on three different aspects: 1) the methodologies of the encoding and decoding operations; 2) the pros and cons of different forms of Reed-Solomon Codes; 3) the different ways that different Reed-Solomon Codes are being employed. Moreover, the paper includes the definition of general Cloud Computing for the audience to understand its importance, how the erasure coding acts like a fault tolerance system of Cloud Computing, and how different kinds of Reed-Solomon code perform on tolerating erasures in cloud storage failures.

Keywords: Cloud computing; Erasure Coding; Reed-Solomon Code.

1. Introduction

In the era of information, the new developments resulting in the accelerated growth of the economy and technology are inseparable from the boost on the quantity of data storage units. Over the past decade, the amount of data being generated in the world grew exponentially, increasing from 2 zettabytes in 2010 to 120 zettabytes in 2023 [1]. With the advancement of the Internet of Things (IoT), it is estimated that there will be more than 79.4 zettabytes of data generated in the upcoming years, which may result in the doubling of the amount of data storage in 2025 compared to the amount of data present now [2]. While the speed of data generation is increasing dramatically, it becomes vital to have faster, more reliable, and efficient storage units. A well-known solution to this problem is Cloud Computing.

Traditionally, for digital data, solid state drives, or SSD, and hard disk drives, or HDD, are safe and simple ways to store data. Despite being a reliable unit for data storage, the problem of being heavy and hard to manage is the reason that traditional storage units are gradually being replaced by cloud storage. Cloud storage is a product from Cloud Computing that is built to handle a high capacity of data and a variety of IT services to internet users. With cloud storage, the physical drives are replaced with a storage unit in the "cloud". The term "cloud" means a platform with all kinds of software, hardware, and network resources that is designed and built by the service provider to the end user with data management and instruction execution [3]. Therefore, not only will the cloud storage system be able to store data, but the service provider will also manage the data and protect the data from cyberattacks or malfunctions of hardware.

Thus, fault tolerance becomes an essential part of cloud services. It is defined as a mechanism or algorithm that fixes errors or failures and ensures the correct execution of different instructions based on the demand from the end users [3]. There are a lot of different fault tolerance algorithms in the market now, however, no matter which algorithm a cloud service deploys, all algorithms tend to be outstanding in performance. To make it specific, an outstanding fault tolerance algorithm needs to use the shortest amount of time to access failure and fix it [3]. Erasure coding is one of the fault tolerance algorithms that are most commonly used. The implementation of erasure coding often involves multiple storage nodes. Depending on the input storage nodes, erasure coding generates

encoded storage nodes. Any of the storage nodes may fail, using different methodologies of erasure coding, the failed data should be recovered [4]. To determine the performance of erasure coding, there are 3 important indicators: 1) spatial efficiency: how much more spaces are required for data recovering; 2) encoding performance: how to encode the input data efficiently; 3) decoding performance: how to recover the failed data in an efficient way [3, 4]. There are a variety of erasure coding methodologies, however, this paper will mainly focus on Reed-Solomon Code, which is a branch of Maximum Distance Separable codes. These codes are designed to reach spatial optimality, which is strongly desired for erasure coding and is widely implemented.

2. Linear MDS Code and Reed-Solomon Code

Linear MDS code is defined as a linear code C with codeword length n, dimension k, and minimum distance between two codewords d that has the property $d = n - k + 1$, which is also named as the Singleton Bound [5, 6]. One of the most classical examples of linear MDS code is Reed-Solomon (RS) Code [6]. In Reed-Solomon code, a generator matrix G is used for encoding and decoding process. To symbolize the generator matrix, it is defined as:

$$G_{(n,k)} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ a_1 & a_2 & \cdots & a_n \\ a_1^2 & a_2^2 & \cdots & a_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{k-1} & a_2^{k-1} & \cdots & a_n^{k-1} \end{bmatrix} \quad (1)$$

In this generator matrix, the parameters in $\{a\}$, which are $a_1, a_2, \ldots, a_n$, are all distinct elements from a specific Galois Field. Suppose the input code is m, then the output code c is obtained by:

$$mG = c \quad (2)$$

Therefore, by performing matrix multiplication, the input message can be converted into encoded message in a short amount of time. Now suppose the codeword length is 5, and 2 of them failed in encoded message c, the codeword that didn't fail can be named as c'. Taking the remaining 3 codewords in c', as long as the corresponding parameters in G, which can be collectively named as G', the decoding process can be performed using the formula below:

$$c'G'^{-1} = m \quad (3)$$

It is calculated that Reed-Solomon can correct up to $\frac{1}{2}(n-k)$ erasures [6]. That indicates that Reed-Solomon code can adjust the number of erasures it can correct and has its limitations. Even though the encoding and decoding process is straightforward, the matrix multiplication over a specific Galois Field is much more complex than an XOR (exclusive-OR) operation [4], which is the most desirable operation for most MDS code encoding and decoding algorithm. Besides that, as the codeword length increase, the complexity of performing encoding and decoding process can grow exponentially. Thus, traditional RS code is not desirable for large codewords, however, the algorithm of RS code provide a strong basis for the advancement in MDS code, which leads to the transformation of RS code. In fact, the transformation of RS code is being utilized by a lot of companies as their cloud service fault tolerance mechanism.

3. Categories of Reed-Solomon Code

There are 2 categories of RS code: Generalized Reed-Solomon (GRS) Code and Twisted Reed-Solomon Code (TRS). Generalized Reed-Solomon (GRS) code, which is an extension of RS code, is not only associated with $\{a\}$, but is also associated with a vector $\{v\}$ with elements $\{v_1, v_2, \ldots, v_n\}$.

GRS code is defined as $GRS_{n,k}(a, v) = \{(v_1 f(a_1), v_2 f(a_2), \ldots, v_n f(a_n)) : \deg(f(x)) \leq k-1\}$ [7]. That means the RS code is just a special kind of GRS code that has all elements in vector $\{v\}$

equal to 1. However, the vector $\{v\}$ can be modified to change the weight of the specific encoded code block, thus, it provides more flexibility compared to the RS code. The generator matrix of the GRS code looks like the matrix below:

$$G_{(n,k)}[a,v] = \begin{bmatrix} v_1 & v_2 & \cdots & v_n \\ v_1a_1 & v_2a_2 & \cdots & v_na_n \\ v_1a_1^2 & v_2a_2^2 & \cdots & v_na_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ v_1a_1^{k-1} & v_2a_2^{k-1} & \cdots & v_na_n^{k-1} \end{bmatrix} \tag{4}$$

It is not hard to observe that the GRS code doesn't provide any improvement in efficiency because the encoding process, decoding process, and generator matrix structure of GRS code are the same as RS code. Therefore, the TRS Code is here to solve this issue.

It was not until recently that the TRS Code was investigated [8]. Due to its specialty, there are several types of TRS Code that jumps out from the category of MDS codes. This paper will not be discussing about such TRS Code specifically since there are a lot of branches of such TRS Code and research are still being performed to find an optimal way on the construction of it. In the following section, a branch of TRS Code, which is Cauchy Reed-Solomon Code, will be discussed.

4. Cauchy Reed-Solomon Code

Cauchy Reed-Solomon (CRS) Code is a modification to RS code that is aimed to improve efficiency in encoding and decoding of data. The general approach is to reduce the matrix multiplication to solely XOR operations. Similar to the RS code methodologies mentioned above, the CRS code utilizes the Cauchy distribution matrix to perform encoding and decoding [4]. The Cauchy distribution matrix is generated using the following method:

Suppose the codeword length is n, and the code is encoded and decoded in the Galois Field GF (2^w), then specify a number m that has the property $n + m \leq 2^w$. The size of the Cauchy distribution matrix will be $m \times n$. Then, the Cauchy matrix is a combination of an $n \times n$ identity matrix and the Cauchy distribution matrix, which sums to a $(n + m) \times n$ sized matrix. Since the input data is an $n \times 1$ sized vector, the encoded data will be a $(n + m) \times 1$ sized vector [4].

After the size is determined, the elements inside the Cauchy matrix should be determined as well. To do this, specify two arrays named X and Y, with X contain m numbers and Y contain n numbers, most importantly, all numbers in X and Y should be distinct numbers from GF (2^w), and there are no intersections between X and Y. Suppose the Cauchy matrix is represented by C, the number in i-th row and j-th column of C is determined by [9]:

$$C_{i,j} = \frac{1}{x_i + y_j} \tag{5}$$

Then C will look like this:

$$C = \begin{bmatrix} \frac{1}{x_1+y_1} & \frac{1}{x_1+y_2} & \cdots & \frac{1}{x_1+y_n} \\ \frac{1}{x_2+y_1} & \frac{1}{x_2+y_2} & \cdots & \frac{1}{x_2+y_n} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{x_m+y_1} & \frac{1}{x_m+y_2} & \cdots & \frac{1}{x_m+y_n} \end{bmatrix} \tag{6}$$

Compared to RS code, CRS code doesn't require the calculation of power over a specific Galois Field, which is an improvement in calculation efficiency. To perform decoding, the algorithm is the same as the RS code, an inversion of a submatrix of the Cauchy distribution matrix is needed, and that is the reason for the identity matrix to be combined with the Cauchy matrix, since the Cauchy matrix has a size that is insufficient to perform matrix inversion.

However, since the Cauchy distribution matrix contains an identity matrix, that will make the first n parameters in encoded data to be the same as the input data, which is the most redundant part of this approach. Therefore, an improvement to the CRS code is introduced, which is the binary projection method of the CRS code. This method abolishes the use of the identity matrix and projects the Cauchy matrix into a binary field.

Suppose the CRS code is still in GF (2^w), then use e to represent all distinct numbers in that Galois Field, and 2 projection method: $V(e)$ and $M(e)$ are introduced. $V(e)$ is the method that projects the number into a $w \times 1$ vertical vector, the top element represents the least significant number, and the bottom element represents the most significant number. In another word, $V(e)$ simply transforms the binary representation of e into vector form. $M(e)$ is the method that project the number into a $w \times w$ square matrix, where the i-th column of $M(e)$ is determined by $V(e \cdot 2^{i-1})$. The table 1 below provides an example of the binary projection method of CRS code when it is operating in GF (8) ($w = 3$) [4].

Table 1. The binary projection method for numbers in GF (8) from [4]

e	0	1	2	3	4	5	6	7
$V(e)$								
$M(e)$								

In this method, the Cauchy matrix will be projected using $M(e)$ and both the input data and the output (encoded) data will be projected using $V(e)$. Using this method, all of the matrix multiplication will be reduced to multiplications in GF (2), which means all of the multiplications will be transformed into XORs. That means the CRS binary projection method eliminates the power and matrix multiplication, and reduces the size of the generator matrix, which improves spatial and time efficiency [9].

Even though the CRS code has a significant improvement in reducing computing complexity and spatial occupancy, it has several limitations. For instance, the CRS code can only be implemented in the case when the encoding and decoding operations happen in the Galois Field of the power of 2. In addition, even though the binary projection method reduced the numbers involved in the generator matrix, it projects numbers into vectors or matrices, which means as w increases, the size of vectors and matrices will increase, and the problem of complex computation will persist. Since the complexity of computation rely on XOR operations, which also relies on the number of 1s inside projected vectors/matrices, therefore, it is important to select a Cauchy matrix that can reduce the computation complexity to the maximum extent [9].

To generate such a Cauchy matrix, the number of XOR operations needs to be calculated. Suppose o is the average number of ones per row in a Cauchy matrix, then the number of XOR operations required by each encoded coding word is given by $o - 1$ [4]. Thus, the Cauchy matrix that produces the smallest o can be identified to be "optimal". The research study has calculated all possible combinations of the Cauchy matrix for $w \leq 4$, and found that as n increases, the number of XOR operations per encoded word inevitably increases, but the optimal Cauchy Matrix is able to control the complexity to a certain boundary [4]. In addition, the worst and optimal Cauchy matrix gradually approaches the same computing complexity as n increases. Thus, it can be concluded that as the codeword length increases, the time and spatial efficiency of the CRS code will decrease, but the CRS code will still outperform the original RS code for the case when n increases.

5. Usages of Reed-Solomon Code

One of the well-known examples that utilizes RS code is the Quick Response (QR) code. It is widely used because it is extremely fast and secure in decoding. When people try to scan the QR codes, the decoding can be affected by multiple factors, such as geometric distortions, blurriness, camera noise, uneven brightness, or scratch on the QR code, these problems can all be solved by RS code implementations [10]. For an RS code with codeword length n and dimension k, the generator matrix is defined as:

$$G = (I_k | A_{n-k}) \tag{7}$$

Where I_k is a $(k \times k)$ sized identity matrix, and A_{n-k} is a $\big(k \times (n-k)\big)$ sized matrix with elements $\{a_{1,1}, a_{1,2}, \dots, a_{k,(n-k)}\}$, the generation method is mentioned in sections above. After that, the encoding process analyzes the message to be encoded according to 4 different categories (numeric, alphanumeric, byte, or Kanji) and encode the data with a specific generator matrix according to 4 fixed error correction capacity (low, medium, quality, or high) [10]. To be specific, the number of error correction bits is defined by $u = n - k$. If there are m bits that need to be encoded, then there will be a padding bit p added between m and u that adds up to n bits. Since the encoded data might large, all data will be separated into smaller chunks, and each chunk of data will have its own n bit data that need to be encoded. After the RS code encoding process, all encoded data will be mapped to the QR code. In that way, the QR code will contain the encoded data, the encoded padding bits, and the error-correcting bits, making the QR code robust against data erasures [10].

Similarly, the error correction method is also implemented in flash memory error corrections. Even though BCH codes are popular approaches that correct erasures in flash memories, according to the research done in [11], it has proven that RS code can perform decoding tasks as same as BCH codes that have a much larger codeword length compared to that of RS codes. This is because RS code that is encoded/decoded in a Galois Field can build the same codeword length as the BCH code that encodes/decodes in a significantly larger Galois Field size [11]. As the spatial optimality of RS code is achieved, it can create more throughputs, because of that, RS Code is a desired method for recovering erasures in flash memories [11].

Besides that, the RS Code is commonly used in RAID architectures for cloud storage systems. With the RS Code being utilized in RAID architectures, in addition to the data disks RAID architectires originally possess, parity disks will be added with data in it compouted with RS Code encoding algorithm. Depending on different RS Code being utilized, the size of the parity disks varies. In fact, there are other methodologies that are used in RAID architectures and can be inspected in future research, such as implementing cryptographic hash codes as parity or combining turbo code and RS code, which can be implemented to achieve a better performance compared to a solely RS Code approach [12,13].

There are a lot of other uses of RS Code, such as underwater acoustic communication systems, file transfer protocols, and a lot of applications that are used in different cloud computing systems [14]. That shows the property of RS Code is favored by different applications because of its property on an efficient encoding/decoding algorithm and the ability to fix unexpected erasures.

6. Conclusion

In this paper, the importance of Cloud Computing has been investigated. Without cloud computing, the capability of data storage will not be able to sustain the amount of data being generated in recent years. As of now, the statistic has shown that more than 41 million messages in WhatsApp are being shared and 1.4 million calls are being made worldwide per minute, that is a countless amount of data being generated, which didn't even include messages sharing from other chatting applications, the data generated by different data centers, and video downloads from web users. As the cost of data generation gets cheaper and cheaper, and as internet users continue to increase, it is imaginable how will the speed of data generation accelerate. Since more and more people rely on cloud computing, it

is essential to ensure the correctness of data storage when a massive amount of data flows into the database.

Therefore, the paper examined one of the most practiced methods for fixing data erasures which is erasure coding, or Reed-Solomon Code specifically. This paper discussed about different types of RS code, illustrated how the encoding and decoding are performed by these different methods, and in which circumstances are these methods effective/ineffective. In general, because RS Code are strongly associated with their corresponding generator matrices and a specific Galois Field, all RS Code methodologies will have a significant drop in their performance as the data length increases, however, as the Cauchy Reed-Solomon codes are being discussed, the problem of encoding/decoding complexity is proved to be solvable and can be maintained within a boundary. It can be convinced that as the research of TRS Code continues, the RS Code will have a great potential on achieving an even better encoding/decoding method on cloud storage systems.

In the end, the different uses of RS codes are also investigated, which are some of the most popular applications. In general, RS code is a desirable approach that is spatial and computationally efficient which are used widely, because of that, RS Code has been a frequently researched field on erasure coding. As more and more research is being conducted, it can be expected that more types of RS code will be utilized in a variety of applications in cloud computing and distributed storage system.

References

[1] Djuraskovic O. 30+ big data statistics - amount of data generated in the world. FirstSiteGuide, 2023.

[2] Yang P, Xiong N, Ren J. Data security and privacy protection for cloud storage: a survey. IEEE Access, 2020, 8: 131723–131740 DOI:10.1109/access.2020.3009876.

[3] Mishra D, Buyya R, Mohapatra P, Patnaik S. A systematic overview of fault tolerance in cloud computing. Intelligent and Cloud Computing Proceedings of ICICC 2019, 2021, 2: 13-21.

[4] Plank J S, Xu L. Optimizing cauchy reed-solomon codes for fault-tolerant network storage applic ations. Fifth IEEE International Symposium on Network Computing and Applications, 2005, DOI:10.1109/nca.2006.43.

[5] Zhang J, Zhou Z, Tang C. A class of twisted generalized reed–solomon codes. Designs, Codes and Cryptography, 2022, 90(7): 1649–1658, DOI:10.1007/s10623-022-01064-w.

[6] Ball S. Maximum distance separable codes. A course in algebraic error-correcting codes, 2020: 83–101.

[7] G Luo, Cao X. Two new families of entanglement-assisted quantum MDS codes from generalized reed–solomon codes. Quantum Information Processing, 2019, 18(3), DOI:10.1007/s11128-019-2207-8.

[8] Liu H, Liu S. Construction of MDS twisted reed–solomon codes and LCD MDS codes. Designs, Codes and Cryptography, 2021, 89(9): 2051–2065, DOI:10.1007/s10623-021-00899-z.

[9] Makovenko M, Cheng M, Tian C. Revisiting the optimization of cauchy reed-solomon coding matrix for fault-tolerant data storage. IEEE Transactions on Computers, 2022, 1839–1846, DOI:10.1109/tc.2021.3110131.

[10] Pena-Pena K, Arce G R. Channel coding optimization for visually pleasant QR codes: invited presentation. Annual Conference on Information Sciences and Systems (CISS), 2019, DOI:10.1109/ciss.2019.8692837.

[11] Chen Bainan, Zhang Xinmiao, Wang Zhongfeng. Error correction for multi-level NAND flash memory using reed-solomon codes. 2008 IEEE Workshop on Signal Processing Systems, 2008, DOI:10.1109/sips.2008.4671744.

[12] Rehman O U, Zivic N. Successive iterative decoding of reed solomon codes using cryptographic hash codes as parity. International Conference on Innovations in Information Technology, 2011, DOI:10.1109/innovations.2011.5893817.

[13] Zhou G et al. On the concatenation of turbo codes and reed-solomon codes. IEEE International Conference on Communications, 2003, DOI:10.1109/icc.2003.1204021.

[14] Goalic A, Trubuil J, Laot C, Beuzelin N. Underwater acoustic communication using reed solomon block turbo codes channel coding to transmit images and speech. OCEANS 2010 MTS/IEEE SEATTLE, 2010, DOI:10.1109/oceans.2010.5664507.