Parallel Reed-Solomon Codes

V.P. Semerenko

National Technical University, 95, Khmelnytske shose, Vinnytsia, Ukraine

vpsemerenko@mail.ru

Abstract. *The compound and integrated parallel Reed-Solomon (RS) codes for multichannel communication systems are suggested. The matrix model of errors for such codes is investigated. Methods of coding and decoding of parallel RS codes, and also methods of increase of their error correcting capability are developed.*

Keywords

Parallel codes, Reed-Solomon codes, decoder, multichannel communication, linear finite-state machines

1 Introduction

In many data transmission systems there are one single communication channel and one single source and one single receiver accordingly. Theoretical bases for such method of data transmission have been proposed already by K.Shennon [1]. The error-correcting codes developed since then are oriented only on the single communication channel.

However, data transmission can be organized simultaneously from ρ sources to ρ receivers on ρ channels [2,3]. Such situation is typical for digital terrestrial television broadcasting system, in broadband networks of wireless access (the project of WiMax), in optical fiber communication systems, in computer networks and ones.

The researches about the error correcting coding in multichannel communication are being proceeded a long time [4]. In [5] a parallel decoding method for cyclic burst error correcting codes is suggested. The paper [6] focuses primarily on information-theoretic aspects of low-density parity-check (LDPC) codes whose transmission takes place over a set of parallel channels. The paper [7] presents a high-speed parallel cyclic redundancy check (CRC) implementation based on unfolding, pipelining, and retiming algorithms.

Despite revolutionary developments in capacity-approaching codes in recent years, Reed-Solomon (RS) codes remain very relevant today, especially for high rate systems with relatively small data packets. RS codes have excellent error bursts correction capability. Reed-Solomon coding is very widely used in digital television, in xDSL systems and in mass storage systems.

Therefore it is important to investigate the possibilities of RS codes in multichannel communication.

In [8] authors propose a heuristic method based on RS codes in multiple channels, but this method is oriented to determine the erasures in data storage only. This and other known methods of error correction of by means of RS codes use traditional approaches which are characteristic to single-channel communication. For example, it is necessary to have separate encoders and decoders for each channel for this purpose.

The features of multichannel communication are being taken into consideration by means of theory multichannel linear finite-state machines (LFSM) [9] in the maximum degree.

Our purpose is to develop theoretical bases of error correction by means of RS codes in multichannel communication on the basis of mathematical tools of LFSM. The multichannel communication uses the parallel channels in which following conditions are satisfied:

- all codewords in channels are various and have length n;
- the j th code symbols in all channels are transferred simultaneously, i.e. in parallel ($j = 1 \div n$).

The proposed parallel RS codes are treated here as the generalization of traditional RS codes [10,11].

2 Main results

The theory of LFSM [12] for representation of parallel RS codes is used.

DEFINITION 1. ρ-channel LFSM $\Lambda_{(\rho)}$ over Galois field $GF(q)$ is a finite state automaton of linear type (the linear automaton) with ρ memory cells, ρ inputs and ρ outputs which is defined by transition function

$$S(t+1) = A_{(\rho)} \times S(t) + B_{(\rho)} \times U_{(\rho)}(t), \qquad GF(q),$$

and output function

$$Y_{(\rho)}(t) = C_{(\rho)} \times S(t) + D_{(\rho)} \times U_{(\rho)}(t), \qquad GF(q),$$

where t is index of discrete time;

$A_{(\rho)} = \|a_{ij}\|_{r\times r}$, $B_{(\rho)} = \|b_{ij}\|_{r\times\rho}$, $C_{(\rho)} = \|c_{ij}\|_{\rho\times r}$, $D_{(\rho)} = \|d_{ij}\|_{\rho\times\rho}$ are the LFSM characteristic matrices;

$S = \|s_i\|_r$, $U_{(\rho)}(t) = \|u_i\|_\rho$, $Y_{(\rho)} = \|y_i\|_\rho$ are the state, the input and the output vectors respectively.

Operation $\times$ denotes a vector multiplication modulo q, operation + denotes a vector addition modulo q.

If the generator polynomial of traditional RS code with the minimum distance d is

$$g(x) = \alpha_0^i + \alpha_1^i x + \alpha_2^i x^2 + \ldots + \alpha_{d-1}^i x^{d-1} + x^d,$$

then LFSM matrices over $GF(q)$ can be written down by following ($i = 0,1,2, \ldots, n-1$):

$$A_{(\rho)} = \begin{vmatrix} 0 & 0 & \cdots & 0 & \alpha_0^i \\ \alpha^0 & 0 & \cdots & 0 & \alpha_1^i \\ 0 & \alpha^0 & \cdots & 0 & \alpha_2^i \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & \alpha^0 & \alpha_{d-1}^i \end{vmatrix}, \quad B_{(\rho)} = \begin{bmatrix} \alpha^0 & 0 & \ldots & 0 \\ 0 & \alpha^0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & \alpha^0 \end{bmatrix}, \quad C_{(\rho)} = \begin{bmatrix} 0 & \ldots & 0 & \alpha^0 \\ 0 & \ldots & \alpha^0 & 0 \\ \ldots & \ldots & \ldots & \ldots \\ \alpha^0 & \ldots & 0 & 0 \end{bmatrix}.$$

Parallel RS code consists of ρ codewords Z_i ($i = 1 \div \rho$), united in a code matrix:

$$Z_{(\rho)} = \begin{bmatrix} Z_1 \\ Z_2 \\ \ldots \\ Z_\rho \end{bmatrix} = \begin{bmatrix} z_{11} & z_{12} & \ldots & z_{1n} \\ z_{21} & z_{22} & \ldots & z_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ z_{\rho 1} & z_{\rho 2} & \ldots & z_{\rho n} \end{bmatrix}, \quad GF(q), \qquad (1)$$

Let's distinguish two types of parallel RS codes: the compound and integrated ones.

DEFINITION 2. The compound parallel RS (n,k,ρ)-code over $GF(q)$ is the RS code whose code matrix consists of ρ codewords Z_i ($i = 1 \div p$), obtained accordingly to the rules of encoding of usual RS (n,k)-code.

To obtain the compound parallel RS code it is possible to use single-channel LFSM.

DEFINITION 3. The integrated parallel RS (n,k,ρ)-code over $GF(q)$ is RS code whose code matrix consists of the ρ codewords obtained accordingly to the rules of encoding based on ρ-channel LFSM.

The encoding procedure of parallel RS (n,k,ρ)-code consists in the fact that initial information $(\rho \times k)$-matrix $I_{(\rho)}$ is transformed to the code (ρ, n)-matrix $Z_{(\rho)}$ which is transferred on a communication channel.

Encoding of parallel RS code can be both systematic or unsystematic as it is for the traditional RS code. While doing systematic encoding from the information $(\rho \times k)$-matrix $I_{(\rho)}$ the control $(\rho \times r)$-matrix $R_{(\rho)}$ is computed. As a result the concatenation of the matrices $I_{(\rho)}$ and $R_{(\rho)}$ we'll obtain code (ρ, n)-matrix $Z_{(\rho)}$.

For compound parallel RS (n,k,ρ)-code the matrix $R_{(\rho)}$ consists of the ρ control words which are computed by the same method as it was for traditional RS (n,k,ρ)-code. Hence, to encode compound parallel RS (n,k,ρ)-code ρ coders based on single-channel LFSM are required.

For integrated parallel RS (n,k,ρ)-code the matrix $R_{(\rho)}$ is formed based on single ρ-channel LFSM, therefore a single coder is required, but it must be more complicated.

The encoding for integrated parallel RS (n,k,r)-code is based on the property of controllability of r-th channel LFSM [12]. This LFSM will be r-controlled for RS (n,k,r)-code, if the rank of $(r\times r)$-matrix $L_{(r),r}=\begin{bmatrix} l_1 & l_2 & \dots & l_r \end{bmatrix}$ is equal to r $(r=n-k)$.

where $l_j=\sum_1^r a_i$, $GF(q)$, a_i is i-th column of the matrix $A_{(r)}^{r-i}\times B_{(r)}$, $j=1\div r-1$.

$l_r=\sum_1^r a_i$, $GF(q)$, a_i is i-th column of the matrix $B_{(r)}$.

$$A^r\times S(k)=L_{(r),r}\times U_{(r)},\qquad GF(q).$$

It is necessary to find some unknown values of components of the vector $U_{(r)}$ from the system of equations for calculation of control matrix $R_{(r)}$ at systematic encoding.

If $\rho<r$ then it is possible to consider that zero codewords are transferred on $(r-\rho)$ channels and all above-stated reasonings will be correct for such an instances.

For compound parallel RS (n,k,ρ)-code two variants control $(\rho\times r)$-matrix $R_{(\rho)}$ and, accordingly, two variants of code $(\rho\times n)$-matrix $Z_{(\rho)}$ can be obtained.

EXAMPLE. For integrated parallel RS (7,3,4)-code with the generator polynomial

$$g(x)=\alpha^3+\alpha^1x+\alpha^0x^2+\alpha^3x^3+x^4,\ GF(8)$$

the information matrix $I_{(4)}$ is following

$$I_{(4)}=\begin{bmatrix} \alpha^5 & \alpha^3 & \alpha^1 \\ \alpha^2 & \alpha^4 & \alpha^1 \\ \alpha^5 & \alpha^3 & \alpha^0 \\ \alpha^6 & \alpha^1 & \alpha^5 \end{bmatrix}.$$

As the result of the systematic coding it is possible to compute two variants of the code matrix:

$$Z'_{(4)}=\begin{bmatrix} \alpha^5 & \alpha^3 & \alpha^1 & \alpha^3 & \alpha^5 & \alpha^1 & \alpha^1 \\ \alpha^2 & \alpha^4 & \alpha^1 & \alpha^3 & \alpha^5 & \alpha^1 & \alpha^1 \\ \alpha^5 & \alpha^3 & \alpha^0 & \alpha^3 & \alpha^5 & \alpha^1 & \alpha^1 \\ \alpha^6 & \alpha^1 & \alpha^5 & \alpha^3 & \alpha^5 & \alpha^1 & \alpha^1 \end{bmatrix},\quad Z''_{(4)}=\begin{bmatrix} \alpha^5 & \alpha^3 & \alpha^1 & \alpha^3 & \alpha^3 & \alpha^3 & \alpha^3 \\ \alpha^2 & \alpha^4 & \alpha^1 & \alpha^5 & \alpha^5 & \alpha^5 & \alpha^5 \\ \alpha^5 & \alpha^3 & \alpha^0 & \alpha^1 & \alpha^1 & \alpha^1 & \alpha^1 \\ \alpha^6 & \alpha^1 & \alpha^5 & \alpha^1 & \alpha^1 & \alpha^1 & \alpha^1 \end{bmatrix}.$$

Let's consider mathematical models of errors in parallel RS codes.

In wireless parallel channels the majority of errors can be the consequence of either external random narrow-band noises (or fading), or of impulse noises. Narrow-band noises can be active in one of the channels and the result will be the distortion of some positions in one of lines of a code matrix. Impulse noises can be active simultaneously what will lead to the distortions of identical positions in several channels (cross errors), i.e. in one of columns of a code matrix.

Thus, the errors in parallel RS codes have a trellised configuration and the errors matrix $E_{(\rho)}$ in which nonzero elements correspond to the distorted positions can be as mathematical model of errors. As the result of various noises influence in parallel channels the code matrix with errors will be received.

The main principles of decoding of parallel RS (n,k,ρ)-code are similar to the principles of decoding traditional RS (n,k)-code, but with using the single generalised decoder based on ρ-channel LFSM. Distinctive property of parallel RS code consist in the fact that single error syndrome corresponds to several one-type errors.

The compound and integrated parallel RS codes considered above we will name as basic. Relative to their capabilities to detect and correct random errors and burst errors we can make the following conclusions.

1. Error detecting capability of the basic parallel RS (n,k,ρ)-code is high enough: all errors are detected, which the generated them RS (n,k)-code detects except for the parity errors which are located on the diagonals of the code matrix.

2. Error correcting capability of the basic parallel RS codes is low, because of the fact that single error syndrome corresponds to a several one-type errors. However correcting capability can be easily raised if some transformations of these codes will be executed.

To make distinction among horizontal configurations of random errors and horizontal burst errors the additional $(\rho+1)$-th channel is introduced. In this channel the parity check bits will be transferred. The value of j th symbol of this code is equal to the sum of all symbols of j th column of a code matrix over $GF(q)$.

For distinction among vertical configurations of random errors and vertical burst errors the additional $(n+1)$th column is entered into code matrix $Z_{(\rho)}$. In this column the parity check bits will be transferred. The value of i th check character is equal to the sum of all symbols of i th row of a code matrix $Z_{(\rho)}$ over $GF(q)$. We name such parallel RS (n,k,ρ)-code expanded.

The method of increase of error correcting capability of the parallel RS code is possible which requires the use of several decoders. The basic decoder serves for the establishment of the presence of an error and for the definition of a basic configuration of the errors. The "horizontal" decoder is used to more precisely define the row number with a multiple error, and the “vertical" decoder – the column number with a multiple error. We name such parallel code as modified.

The expanded and modified parallel RS (n,k,ρ)-codes have the same error detecting and correcting capability as RS (n,k)-code has which generated them.

3 Conclusion

There are three ways using of RS codes in ρ-channel communication:

- by carrying out separate coding and separate decoding of information messages in each channel; then it will required ρ coders and ρ decoders,

- by carrying out separate coding of information messages for each channel and the general decoding for all channels; then it will be required ρ coders and one multichannel decoder,

- by carrying the general coding and the general decoding of information messages for all channels; then it will be required one multichannel coder and one multichannel decoder is required.

In the first case the traditional RS code is used, in the second case the compound parallel RS code is used, and in the third case the integrated parallel RS code is used.

References

[1] Шеннон К. Работы по теории информации и кибернетике / К. Шеннон – М.: Изд-во иностр. лит., 1963. – 829 с.
[2] Мелентьев О.Г. Теоретические аспекты передачи данных по каналам с группирующимися ошибками / Под ред. В.П. Шувалова. – М., Горячая линия-Телеком, 2007. – 232 с.
[3] Габидулин Э.М. Кодирование в радиоэлектронике / Э.М. Габидулин, В.Б. Афанасьев – М.: Радио и связь, 1986. – 176 с.
[4] R. Ahlswede: Multi–way communication channels. In: 2nd Int. Symp. Inform. Theory, 23–52, Publishing House of the Hungarian Academy of Sciences,Tsahkadzor, Armenian SSR, 1973.
[5] G. Umanesan and E. Fujiware: Parallel Decoding Cyclic Burst Error Correcting Codes. *IEEE Trans. on Computers*, vol. 54, NO 1, pp. 87–92, Jan. 2005.
[6] I. Sason and G. Wiechman: On Achievable Rates and Complexity of LDPC Codes over Parallel Channels: Bounds and Applications. *IEEE Trans. on Information Theory*, vol. 53, NO 2, pp. 580 - 598, Feb. 2007.
[7] P. Harika, B. V. V. Satyanarayana: Fpga Based High Speed Parallel Cyclic Redundancy Check. *International Journal of Engineering Research & Technology*, Vol. 2 Issue 3, pp. 1–8, March 2013
[8] M. Varsamou and T. Antonakopoulos: A new data allocation method for parallel probe-based storage devices. *IEEE Transactions on Magnetics*, vol. 44, NO. 4, pp. 547–554, Apr. 2008.
[9] M.Y. Hsiao: Single-Channel Error Correction in an f-Channel System. *IEEE Trans. On Computers*, vol. C17, pp. 935-943, Oct. 1968.
[10] B. Sklar; Digital Communications. Fundamentals and Applications. Second Edition, Prentice Hall, Los Angeles, 2001.
[11] Семеренко В.П. Декодирование кодов Рида-Соломона на основе графовой и автоматной моделей // *Электронное моделирование*, 2011. — №. 1. — С. 57-72.
[12] Gill A. “Linear Sequential Circuits. Analysis, Synthesis and Application”, McGraw-Hill Book Company, New York, London, 1967.