The Use of Matlab for the Simulation of the Burst Error Correction

Ing. Vítězslav Křivánek,

Department of Telecommunications, Brno University of Technology, Purkynova 118, 612 00 Brno, Czech Republic

Summary

During the message transmission, an impairment occurs from time to time i.e. an error arises which is caused by interfering signals during the transmission. The situation requires that the respective coding is adapted as much as possible to the given conditions of the transmission. The convolutional coding is suitable for the correction of burst errors. However, the procedure of the majority of burst error correction solutions is very demanding. This article therefore explains a complex procedure of design and simulation in Matlab on a specific case which is suitable for its simplicity and makes the explanation of the lesson easier.

Key words:

Forward error correction, convolution coding, burst error.

Introduction

Nowadays security codes are used systematically as a standard for the message transmission in digital networks. They are used on the basis of adding redundant information by means of an encoder. The respective code security is obtained by the artificial increasing of the redundancy of the transmitted sequence of signal elements which, however, reduces the value of the transmitted information. The purpose of this step consists in the eventual correction of the error caused during the transmission through a real channel. The decoder on the receiver's side attempts to recover the message. If the original message is at your disposal as well, you can compare the efficiency of various security modes (see Fig. 1).

There are three basic types of security codes: block codes, cyclic codes and convolutional codes. In the communication technology various suitable combinations of security codes, in particular cyclic and convolutional codes, are used. To generate a convolutional code, there are two basic generating methods available. The code can be entered by means of a generator polynomial or by means of a generator matrix. Each of these methods is suitable for a diverse coding procedure.

In the case of convolutional codes, Viterbi algorithm is used most frequently to find the most probable sequence.

The algorithm principle is based on the detection of the shortest Hamming distance of the decoded sequence from the received sequence. The substantial disadvantage of the above-mentioned method consists in the fact that it is significantly demanding as for the number of numerical operations. This method is used only for the decoding of codes with relatively short constraint lengths because the dependency of the number of operations on the constraint length has an exponential character. Another method which can be used for error detection is the threshold decoding principle. The threshold decoding is based on finding a sufficient number of check operations among the elements of message sections which are in the so-called orthogonality relation towards the element whose correctness is checked after the transmission. The latter method shall be outlined in this document.



Fig. 1 Message transmission process

2. General implementation of convolutional coding

In the case of convolutional coding, the check (security) bits are generated both with respect to the information bits

Manuscript received June 5, 2006.

Manuscript revised June 25, 2006.

of the block being transmitted and with respect to the information bits of previous blocks (see Fig. 2). In the course of coding, the security bits of the block being transmitted are generated in relation to the information bits of all blocks contained in the group. Therefore each output codeword n_0 has extra check bit(s). The above-mentioned bit is generated from selected information bits of the block in the encoder (see Fig. 3). The division of the message into the information part and the security part is performed so that the technical solutions of the encoder and decoder will be less complicated.



Fig. 3 General convolutional encoder

The message in the decoder input consists of useful information and security bits with no information value for the receiver in the output. In the course of decoding, the decoded word is obtained from information bits of the word just being transmitted and from check bits of the whole group which are compared with one another (see Fig. 4). It is obvious that the decoded information cannot be available, but after the completion of the transmission of the whole group of bits from which the security bits are generated. The respective decoded word can therefore be obtained only after the distance velocity lag has elapsed. This lag occurs because of the use of the serial transmission of the message (see Fig. 5).



Fig. 4 Decoding principle

The number of convolutional codes whose encoders and decoders allow the burst error correction and whose circuit solutions are simple is not large. Most solutions need a significantly demanding procedure. However, Iwadare code can be used without great difficulties for the modelling since it is suitable because of its simplicity. This code can also serve for the studies of other more complex codes which enable more perfect error-control coding, especially in individual systems.



Fig. 5 General convolutional decoder

3. Iwadare code

Iwadare code can be ranked among the systematic convolutional codes. It does not therefore need to be divided into blocks for security reasons. The resulting transmitted code combination can be divided into information elements and security elements. If the threshold security capability is exceeded, the infinite error intrusion into the information itself does not occur. Iwadare code is capable of correcting error bursts b if there is security interval A among these bursts where the respective information is transmitted error-free.

142

There are basic version and extended version which has higher security capability, but lower information rate. The extension level is marked with letter *i*. If i = 1, then it is a basic code. Iwadare code is described with the generator block matrix for which the following relationships are given (derivation in [1]):

$$\mathbf{B}_{\mathbf{0}} = \begin{bmatrix} m \cdot n_0; m \cdot k_0 \end{bmatrix},\tag{1}$$

m and k_0 are defined as follows:

$$m = \frac{n_0 \cdot (n_0 - 1)}{2} + (2n_0 - 1) \cdot i , \qquad (2)$$

$$k_0 = n_0 - 1 , (3)$$

where k_0 and n_0 means the number of partial input or output parallel flows. Consequently, correction capability *b* and security interval *A* are defined:

$$b \le n_0 \cdot i \quad , \tag{4}$$

$$A \ge n_0 \cdot m - 1. \tag{5}$$

$$B_{o} = \begin{bmatrix} 0 & 0 & \cdots & 0 & 0 & 1 \\ 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 & 0 \\ 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 0$$

Fig. 6 General scheme of the block matrix of the basic Iwadare code

4. Iwadare encoder

The basic code determines the general scheme of the block matrix \mathbf{B}_0 (see Fig. 6). The code matrix can be expanded so that its security capabilities can be increased or security interval can be reduced. In the case of *i*-multiple

expansion, the number of (i - 1) zero lines are substituted for all non-zero lines. The modelling of encoder and decoder shall be also demonstrated in the basic Iwadare code which is capable of the correction of the burst of 4 errors. From equations (2 - 5):

$$n_0 = b = 4 ,$$

$$m = \frac{4 \cdot 3}{2} + (2 \cdot 4 - 1) \cdot 1 = 13$$

$$k_0 = 4 - 1 = 3 ,$$

$$A \ge 4 \cdot 13 - 1 \ge 51.$$

It is based on the generator block matrix $\mathbf{B}_{0(52,39)}$ defined in the formula (1). To generate a connection design, you shall need the basic syndrome equation of the code matrix from which individual elements of encoder can be derived:

$$s_{13} = a_1 + a_4 + b_5 + b_7 + c_8 + c_9 + d_{13}.$$
 (6)

The designed encoder connection is based on the syndrome equation (6). On condition no errors occur it the encoder system itself, the following relationship is valid:

$$s_{13} = 0$$
, (7)

consequently, the relationship shall be simplified as follows to derive the security element d_{13} :

$$d_{13} = a_1 + a_4 + b_5 + b_7 + c_8 + c_9 .$$
(8)

The connection diagram of the basic encoder (see Fig. 7) can be uniquely determined from the equation (8). In the figure of the encoder and decoder, only the first and the last memory cell of the respective section are marked for the reason of clarity.



Fig. 7 Encoder Iwadare code (52, 39)

5. Iwadare decoder

The basic principle of the decoder consists in the use of the threshold decoding principle. It is necessary to find the orthogonality relation towards the element whose correctness after the transmission is just being checked. To derive the decoder connection, you shall need the syndrome equation system. The number of necessary equations is determined by the requirement of the existence of at least two orthogonality sums for one corrected bit. The basic substance and condition are as follows: The corrected bit occurs in both of these equations while the other bits do not and shall not occur in both the equations.

The above-mentioned example of Iwadare code corrects the erroneous bursts $b \le 4$. Yet, it does not deal with the correction of the security bit d_i because its correction is of no significance for the transmitted information. The following three information bits a_i , b_i , c_i are only corrected. To design the Iwadare decoder, one can use the fact that it is a systematic code which is organized as follows: security bits follow only after information bits of the respective transmission. One more syndrome equation in relation to the basic syndrome equation (6) shall be therefore found. If you define the syndrome equation for specific time, you shall find bits participating in security in previous time in relation to the bits contained in this equation. The second syndrome equation:

$$s_{12} = a_0 + a_3 + b_4 + b_6 + c_7 + c_8 + d_{12} .$$
⁽⁹⁾

Using these two syndrome equations (6) and (9), the correction of bit c_8 can be made:

$$s_{13} \cdot s_{12} = 0 \land s_{13} \cdot s_{12} = 1 , \qquad (10)$$

where the result equals zero if bit c_8 is correct, and the syndrome product equals one if there is an error. If you want to correct other bits, you have to go "deeper in the history" and determine other necessary syndrome equations for the correction of bits b_5 , a_1 .

On the basis of knowledge of other syndrome equations, it is possible to model a decoder (see Fig. 8).



Fig. 8 Decoder Iwadare code (52, 39)

Iwadare code can be ranked among the systematic convolutional codes. It does not therefore need to be divided into blocks for security reasons. The resulting transmitted code combination can be divided into information elements and security elements. If the threshold security capability is exceeded, the infinite error intrusion into the information itself does not occur. Iwadare code is capable of correcting error bursts b if there is security interval *A* among these bursts where the respective information is transmitted error-free.

6. Simulation of the above-mentioned solution

Simulation is a good method for verifying and presenting the processed models. It can be based on the mathematical program Matlab where you can use in particular the specialized Simulink library which mostly serves for modelling and simulation of dynamic systems. The substantial advantage in this environment is the possibility to construct the designed model from individual blocks directly from the library. The model of encoder and decoder (see Fig. 9 and Fig. 10) suitable for simulation can be made in a simple way. The result can also improve the view of the respective issue and makes the explanation of the lesson easier.



Fig. 9 Iwadare encoder in Matlab



Fig. 10 Iwadare decoder in Matlab

The message transmission which is mostly binary both in the input and output of the transmission system has been made in particular by means of discrete signal lately. The respective sequence of signal elements representing the transmitted message uses values 0 and 1 for the binary discrete signal. In consequence of the operation of various and frequently variable interferences, the message transmission is accompanied by error occurrence in the transmission channel. The error proves by the change of the respective signal element in the other value. The element 0 is changed into the element 1 and vice versa. Interfering influences can be easily simulated by means of the mod2 adder (see Fig. 11).



Fig. 11 Transmission channel simulation

The whole system of the detection and correction of occurred errors is based on the work in binary system. The correct function of the decoder can be easily verified by means of the error sequence. The security capabilities of the respective code can be fully checked by the simulation of various error sizes and locations.

7. Conclusion

In the majority of cases there is a greater number of possible solutions of the encoder and decoder implementation under the set conditions. It aims at using the simplicity of the modelling by means of Iwadare code to generate an input set of criteria for the analysis of error-control systems which use convolutional coding. It can also enhance the quality and attractiveness of the explanation of a lesson. The obtained knowledge can be used as the starting point for studying other codes. Consequently, it can be employed with systems used in the present digital signal transmission systems.

References

- Kasami, T., Tokura, N., Iwadari, J., Inagaki, J.: *Těorija kodirovanija*. Mír, Moscow 1978
- [2] Vlček, K.: Komprese a kódové zabezpečení v multimediálních komunikacích. BEN – technická literatura, Praha 2004
- [3] RFC 3452 Forward Error Correction (FEC) Building Block, http://www.faqs.org/rfcs/rfc3452.html