Proceedings of the 5th WSEAS Int. Conf. on Signal Processing, Computational Geometry & Artificial Vision, Malta, September 15-17, 2005 (pp182-187)

SYNTHESIS OF CYCLIC ENCODER AND DECODER FOR HIGH SPEED NETWORKS

MARIA RIZZI, MICHELE MAURANTONIO, BENIAMINO CASTAGNOLO

Dipartimento di Elettrotecnica ed Elettronica,
Politecnico di Bari
v. E. Orabona, 4 - 70125 Bari
ITALY

Abstract: In this paper a parallel implementation of an encoder and of a decoder for cyclic codes to increase the bit rate is proposed. The structures are composed of a cascade of iterative combinational cells able to obtain a finite output sequence spatially. The proposed solution allows high bit rates and high degree of modularity, so an easy integration of the circuits is possible. These characteristics make the method suitable to be adopted in a photonic environment in which clocked digital memory elements are still a critical aspect

Key words: Sequential logic circuit, finite state machine, logic design, combinational logic circuits, Hamming code

1 Introduction

Channel encoding for error detection and correction is achieved by adding to the source binary sequence a controlled amount of redundancy. This solution protects the information against possible transmission errors. However, the occurrence of errors in the message gives rise to increase message loss and consequently to reduce the network quality of service.

The adopted encoding rule will heavily affect the decoding algorithm complexity, that is the process to be performed on the received sequence to recover the transmitted information.

Cyclic codes are widely used for the detection and correction of errors in modern networks. They possess a great deal of well-understood mathematical structure and are effective particularly in controlling errors with a minimal amount of hardware [1], [2] [3], [4], [5]. Moreover, the transmitter and the receiver have an equal logical structure. The encoding and the decoding process of cyclic codes is achieved using a division algorithm. For this reason the classical hardware implementation adopts shift registers with feedback connections related to the used code. Due to its sequential logic nature, the circuit is time variant so the output depends on the input and the current state of memory elements. Therefore, the output may be viewed as a sequence because it varies with time and is dependent on the past.

However, the grow of speed in modern transmission systems makes necessary the research of hardware solutions able to work at frequencies of Gbit/s.

In a previous paper a solution based on the transformation of an FSM in a fully parallel circuit was presented [6].

In this paper in order to determine the speed limit of the parallel solution taking into account the current technological implementation, an encoder and a decoder for the systematic Hamming code are presented. They are based on a fully parallel and feed-forward operating mode, but it is possible to adopt any parallelism that is necessary. The modularity of the circuits makes an easy hardware implementation possible. These characteristics make the method suitable to be adopted in a photonic environment, too.

In section 2, the principles of the encoding and decoding of cyclic codes are summarized and the design of the classical encoder and decoder for the Hamming code (15,11) are indicated. Section 3 deals with the method to transform generic Synchronous Finite State Machines (S-FSMs) in combinational circuits In section 4, the designs of the parallel solutions are presented and in section 5 their performance are evaluated. The general validity of the method is outlined and some conclusions are drawn.

2 Cyclic code encoding and decoding procedure

The cyclic codes are a particular class of block codes. Suppose that a block of *n* bits (message word) is generated by a source. In order to achieve a given bit error probability, the word has to be encoded before transmission. The basic feature of block codes is that another block of *r* redundant bits is added to the information packet. These bits derive from *r* parity checks performed on the original message word.

If the first *n* bits of the code word are the message bits and the last *r* bits are the parity check bits, the block code is called systematic.

An $(n + r,\ n)$ block code is a cyclic code if and only if any cyclic shift of an $(n + r)$ bits code word produces another code word. In dealing with cyclic codes, it is useful to represent any binary sequence with the coefficients of a polynomial in the indeterminate D.

A cyclic code is generated using a generator polynomial *g*(D) which for an $(n+ r,\ n)$ cyclic code is unique and is of the form:

$$D^r + g_{r-1} D^{r-1} + \ldots + g_1 D + 1 \quad (\text{with } g_k=0,1)$$

All the code words of every cyclic code are multiples of the polynomial g(D). Therefore, one cyclic code is obtained as follows:

$$t(D) = x(D)\, g(D)$$

where *x*(D) is the information sequence. To generate a systematic code another algorithm is employed, by which message words are multiplied by D^r and then divided by g(D).

Denoting with *q*(D) and *r*(D) the quotient and the remainder of the division, the following expression is obtained:

$$D^r x(D) = q(D)\, g(D) + r(D)$$

The previous formula can be rewritten as:

$$D^r x(D) + r(D) = q(D)\, g(D) = u(D)$$

The polynomials u(D), being multiples of g(D), are code words of a systematic cyclic code. In fact *r*(D) constitutes the parity check word whose bits occupy the last *r* positions of u(D).

The cyclic encoder is based on a shift register with linear feedback (Fig.1a), by which the division of the message word by the generator polynomial is performed.

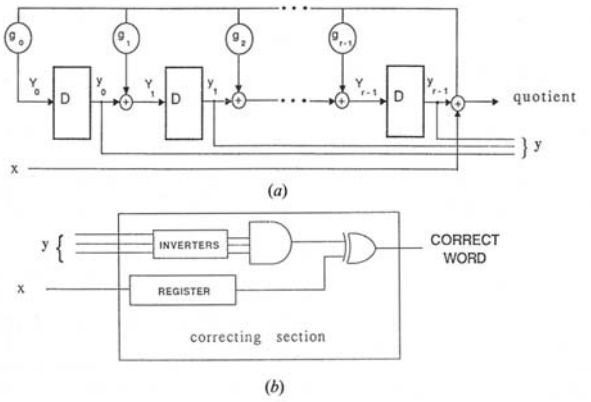

Fig.1 (a) The cyclic code encoder.
(b) The cyclic code correcting section

The shift register is initially set to all zero values. The message word enters one bit at a time in the register at its right end: this is equivalent to multiplying the message word by D^r. After *n* clock pulses, the remainder is stored into the shift register. The code word appears serially in $(n + r)$ clock pulses.

Adding to the previous circuit the correction section indicated in Fig.1b, it is possible to perform the decoding operation with error detection and correction. If some errors occur during the transmission, the received polynomial *w*(D) can be expressed as follows:

$$w(D) = u(D) + e(D)$$

where *e(D)* is an error polynomial. Dividing *w(D)* by g(D), we obtain

$$w(D) = p(D)\, g(D) + s(D)$$

where *s(D)* is the remainder of the division, called the syndrome. If *s(D)* is equal to zero, *w(D)* is a multiple of *g(D)* and therefore it is a code word. In this case, either the processed word is correct or *e(D)* transforms the true word in a different code word and so errors are not detectable.

The error correction process is more complicated: the decoder consists of a detecting section (which has the same structure as the encoder), a shift register in which the received word is stored and a correcting combinational network (Fig.1b). The binary digits y_i represent the bits of the syndrome.

After the error detection, the syndrome is cyclically shifted into the shift register while the serial input is kept to zero, so that (2^r-1) different syndrome values could be obtained. If one error occurs in the *i*th position (for $1 \le i \le n+r$), the syndrome value obtained at the *i*th pulse clock is the same, whatever the

value of *i*.
Therefore, the correcting section of the circuit is able to correct a single error, independently from its position into the received word. The syndrome words, together with the code word, are fed step-by-step into the correcting gates. If there is a single error, the incorrect bit is complemented.

3. The iterative cells architecture

Every S-FSM which transforms a finite input sequence x(i) into a finite output sequence z(i), can be transformed into a combinational circuit [7]. Therefore, every p bits long output sequence obtained by an FSM, can also be generated spatially by a combinational iterative network, consisting of a cascade of p identical cells, one of which is shown schematically in Fig. 2. $\mathbf{x}_i$ is the input vector, $\mathbf{z}_i$ is the output vector, $\mathbf{y}_i$ is the input carries vector and $\mathbf{Y}_i$ is the output carries vector. Thus

$$\mathbf{X}_i=\mathbf{x}(i);\ \ \mathbf{y}_i=\mathbf{y}(i);\ \ \ \mathbf{Y}_i=\mathbf{Y}(i)$$

The cells are in cascade in such a way that the output carries from the (i-1)th cell constitute the input carries to the ith cell. The input signals are applied simultaneously to all cells and the outputs appear simultaneously, except for the delay introduced by the cells, depending on the number of gates each signal must pass through. Because of its modularity, an iterative circuit is suitable for easy integration.
The synthesis procedure of an iterative combinational circuit is the same as that of a synchronous sequential circuit [7].

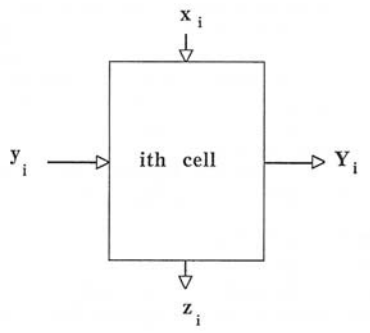

Fig.2 The generic cell composing an iterative circuit

In order to transform the sequential cyclic code encoder and decoder into combinational circuits it is necessary to define their state transition property. For the previous sequential circuits it assume the following expression:

$$Y_k=g_k(x \oplus y_{r-1}) \oplus y_{k-1} \qquad k=0,..., r-1$$

where $\oplus$ represents the mod-2 sum or the EXOR boolean function.
In the corresponding iterative cells encoder, n iterative cells are needed, into which the n message bits are fed. The number of input and output carries is r. The output carries from the nth cell are the check digits to be added as the final bits of the code word.
The parallel decoder needs for [2(n+r)-l] iterative cells. In fact, the whole code word is fed into (n+r) iterative cells, identical to those of the encoder. Moreover, as the syndrome is shifted (n+r-1) times into the shift register, n+r-1 cells are necessary in the iterative solution to perform the correction.
The output carries vector, $Y_{(n+r+i-1)}$ (for i= 1, .. , n+r), representing the parallel syndrome, allows the error in the ith position to be corrected.

4. Synthesis of the Hamming circuits

In order to evaluate the speed-up of the iterative cells circuits as to the sequential structures, the encoder and decoder for the systematic Hamming (15,11) code have been designed.
Every code word consists of 11 message bits and 4 parity check digits obtained adopting the following generator polynomial:

$$g(D) = D^4+ D + 1$$

From the previous formula derives that every cell has to implement the following logical functions:

$$Y_0 = y_4 \oplus x_i$$
$$Y_1 = y_0 \oplus Y_0$$
$$Y_2 = y_1$$
$$Y_3 = y_2$$

In fig.3 the logical structure of the designed cell is indicated.
The parallel encoder is composed of 11 identical cells; the output carries of the last cell represent the check bits to add to the message word.
To perform the error detection 15 cells are necessary while to correct the single error other 14 cells have to be designed. Therefore, the Hamming decoder is composed of 15 cells having the structure indicated in fig.3 and 14 other cells whose logical architecture is shown in fig.4.

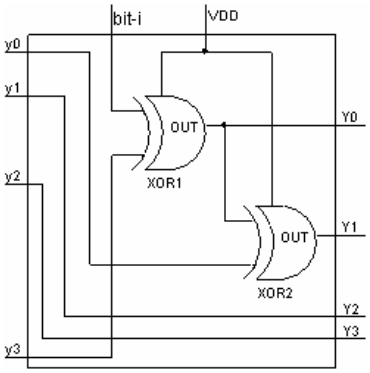

Fig.3 The logical architecture of the Hamming (15,11) encoder cell

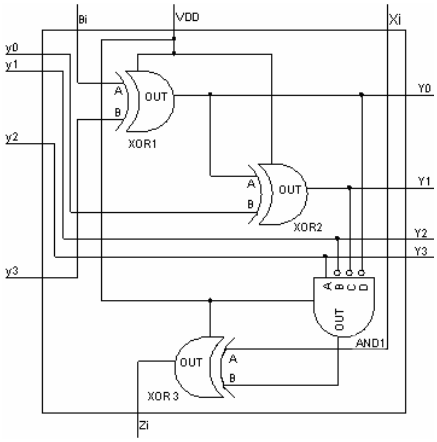

Fig.4 The logical architecture of the correcting section cell

This last cells are characterized by a logical zero input value which corresponds to the shift of the generated syndrome inside the sequential circuit (fig.5).

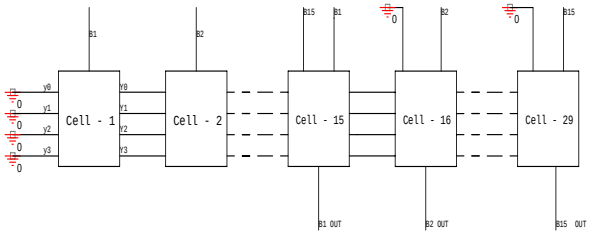

Fig.5 Schematic structure of the combinational decoder

The high degree of modularity of the previous circuits makes easy the layout process. Figgs.6 and 7 show the logical structure of the combinational decoder and the layout of the generic cell decoder realized adopting the CMOS AMS 0.35 technology. Moreover, the layout of the Hamming (15,11) decoder is indicated in fig.8.

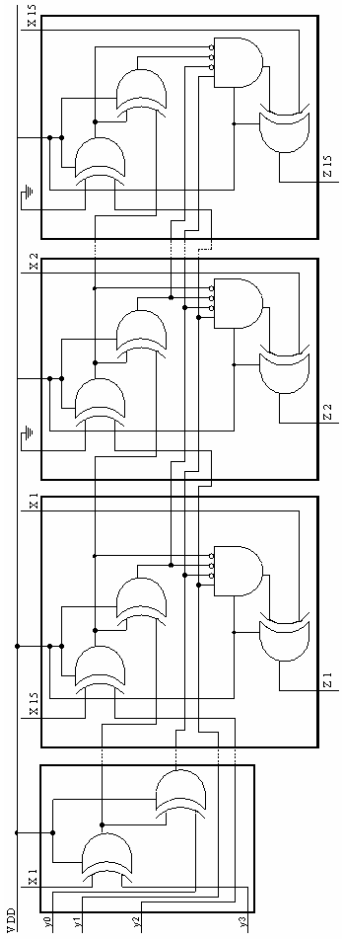

Fig.6 The parallel Hamming (15,11) decoder

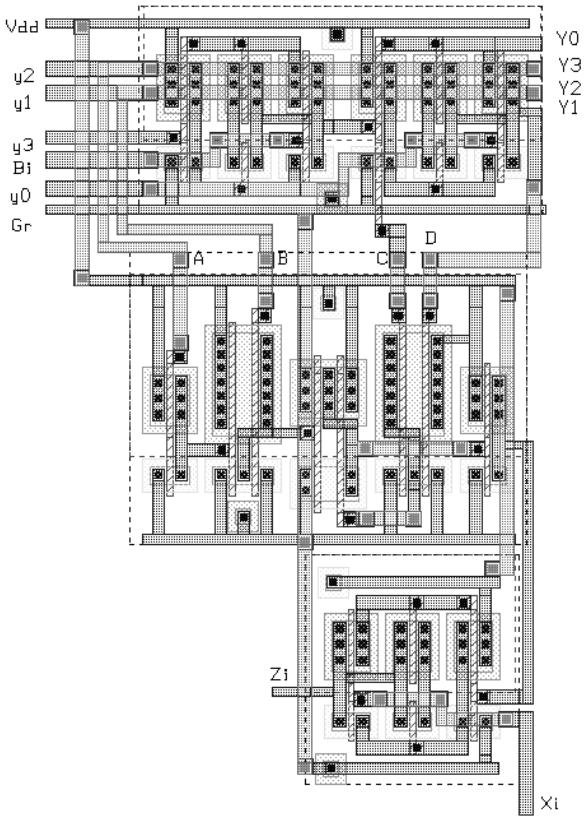

Fig.7 The layout of the single cell decoder

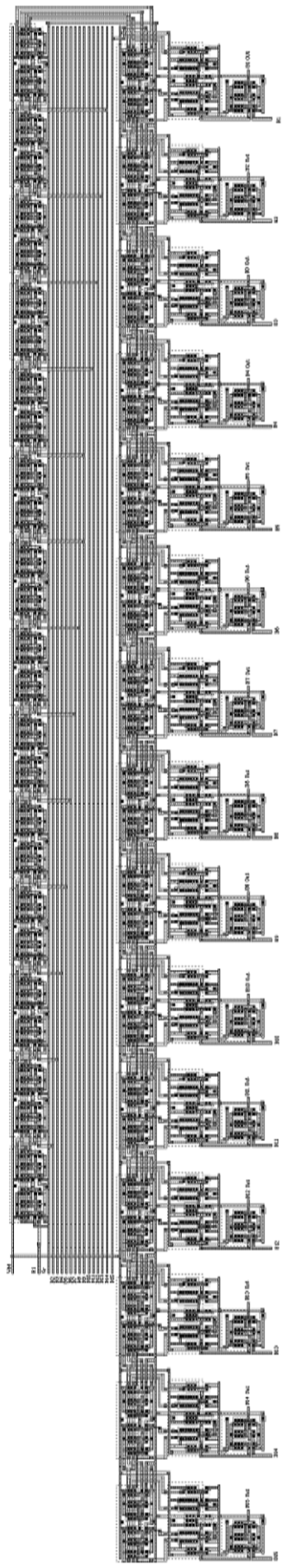

Fig.8 The layout of the Hamming decoder

5. Performance evaluation and comparative analysis

To evaluate the enhancement of the designed circuits many simulations with different message and code words have been performed adopting the ORCAD simulator. As the parameter to analyze has been the coding and decoding speed, the study in the time domain started after the last bit arrived. In this way the real delay introduced by the circuits has been considered.

The time necessary to code an information depends on the particular message word; in particular for the worst case the speed-up of the combinational encoder as regards the sequential solution is about 4. In fig.9 the simulation results for the message word [101000000000] are shown and the performance have been compared with the sequential solution (fig.10). In this situation the speed-up is about 8, in fact about 16ns are necessary to code the message word adopting the shift register solution while only 2ns are request in the iterative cell architecture.

For what the decoding circuit concerns, the analysis has been performed with an operating frequency of 1GHz. In this condition a speed-up of about 7 has been reached in the worst situation.

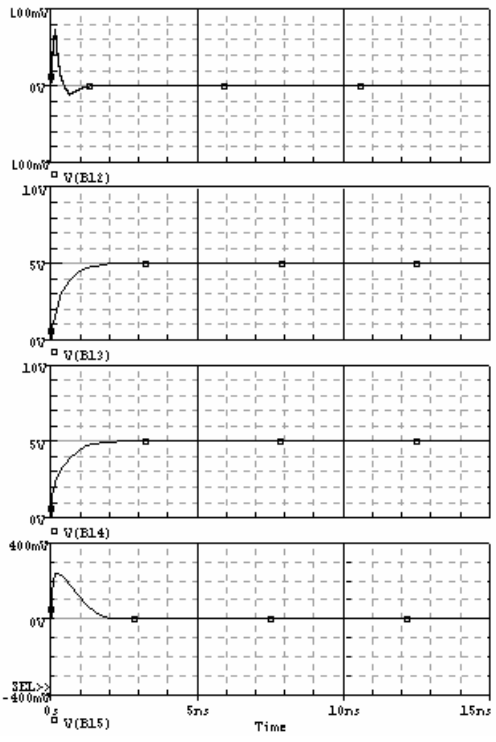

Fig.9 Time domain performance of the parallel encoder

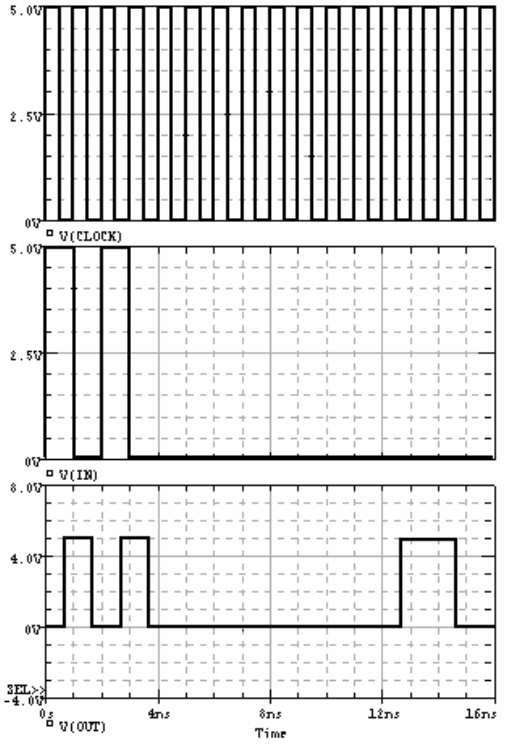

Fig.10 Time domain performance of the serial encoder

6. Conclusions

In this paper the designs of pure combinational Hamming code encoder and decoder have been indicated. The adopted procedure has a general validity in fact it can be used for every systematic cyclic code.

The high performance of the realized solutions and the limited number of logical gates composing the structures make the circuits easy to be implemented in photonic environment, too.

In particular having parallel data available, the designed encoder has a speed-up of about 4 as to the corresponding sequential solution while the performance of the decoder increases of about 7 with respect the serial structure.

References

[1] S. Benedetto, E. Biglieri, V: Castellani,: "Digital Transmission Theory", Prentice-Hall, Inc., 1988

[2] B. Sklar: "Digital Communications-Fundamentals and Applications", Prentice Hall International Editions, 1988

[3] O. Khalifa, M. D. Rafiqul Islam, S. Khan, "Cyclic redundancy encoder for error detection in communication channels", RF and Microwave Conference, 5-6 Oct. 2004 pag. 224 - 226

[4] S. J. Piestrak, A. Dandache, F. Monteiro, "Designing fault-secure parallel encoders for systematic linear error correcting codes", IEEE Transactions on Reliability, vol.52, n.4, Dec. 2003, pag. 492 - 500

[5] F. Monteiro, A. Dadanche, B. Lepley, "Fast Configurable Polynomial Division for Error Control Coding Applications", 7th IEEE Int. Online Testing Workshop, 2001

[6] B. Castagnolo, M. Rizzi "High-speed error correction circuit based on iterative cells", Int. J. Electronics, , Vol. 14, N°. 4, 1993, pag. 529-540

[7] Z. Kohavi: "Switching and Finite Automata Theory", McGraw-Hill Press, 1970