Properties of Finite Response Input Sequences of Recursive Convolutional Codes

Didier Le Ruyet[1], Hong Sun[2], and Han Vu Thien[1]

[1] Conservatoire National des Arts et Métiers, Laboratoire Signaux et Systèmes,
75141 Paris Cedex 03, France,
leruyet@cnam.fr

[2] Huazhong University of Science and Technology, Departement of Electronic and
Information Engineering, 430074 Wuhan, China,
caes@blue.hust.edu.cn

Abstract. A recursive convolutional encoder can be regarded as an infinite impulse response system over the Galois Field of order 2. First, in this paper, we introduce finite response input sequences for recursive convolutional codes that give finite weight output sequences. In practice, we often need to describe the finite response sequence with a certain Hamming weight. Then, different properties of finite response input sequences are presented. It is shown that all finite response input sequences with a certain Hamming weight can be obtained in closed-form expressions from the so-called basic sequences. These basic sequences are presented for important recursive convolutional encoders and some possible applications are given .

1 Introduction

Recursive convolutional codes have seldom been employed in the past because their weight enumerating function is equivalent to that of the non recursive convolutional codes [1]. But they have been renewed since they have been used to construct serial and parallel concatenated convolutional codes (turbo codes) whose performances are near Shannon limit (see [2] and [3]).

The works of Battail *et al.* [4] have shown that recursive convolutional codes mimic random coding if the denominator polynomial is chosen as a primitive polynomial. In comparison with non recursive convolutional codes, the input sequences with finite weight are associated with output sequences with infinite weight, except for a fraction of finite weight input sequences which generate finite weight output sequences. These input sequences are called finite response input sequences (FRISs).

In [5], FRISs have been introduced ; the enumeration of FRISs for a Hamming weight w=2 is simple but however, no practical method to enumerate these sequences with a certain Hamming weight w greater than 2 has yet been given.

The goal of this paper is to study the properties of finite response input sequences with weight w and to show how these sequences can be enumerated from one or more basic FRISs.

In the next section, we recall some classical definitions of convolutional codes. The third section we give different properties of FRIS and introduce basic FRIS. An exemple is given to show how these properties can be used to enumerate all the FRIS in closed form. Then, the basic FRISs are presented for some important recursive convolutional encoders. Finally, we will show how these properties can be used to find the Hamming weight of the output sequence of any FRIS and to build interleavers for turbo codes.

2 Review of Basics

In order to keep the following expositions self-contained, we shall introduce recursive convolutional codes and some definitions to be used later in this section.

A rate $1/r$ recursive convolutional encoder maps the input sequence of information bits

$$u_0, u_1, u_2, \ldots$$

into the output sequence of r-dimensional code blocks

$$\mathbf{y}_0, \mathbf{y}_1, \mathbf{y}_2, \ldots$$

with

$$\mathbf{y}_n = (y_{1n}, y_{2n}, ..., y_{rn}) \ .$$

The encoder also goes through the internal state sequence

$$\mathbf{s}_0, \mathbf{s}_1, \mathbf{s}_2, ...,$$

where each encoder state $\mathbf{s}_n$ at time n is a M-tuple :

$$\mathbf{s}_n = [s_{1n}, s_{2n}, ...s_{Mn}] \ .$$

M is the number of delay cells of the encoder and s_{in} is the state at time n of the i-th delay cell.

The structure of a recursive systematic convolutional encoder of rate 1/2 is shown in Fig.1.

A recursive encoder can also be regarded as an infinite impulse response (IIR) system over the finite field GF(2) with input $u(D)$ and output $\mathbf{y}(D)$, where D is the unit-delay operator:

$$\mathbf{y}(D) = u(D)G(D) \tag{1}$$

with

$$G(D) = \left(\frac{P_1(D)}{Q(D)}, \frac{P_2(D)}{Q(D)}, ..., \frac{P_r(D)}{Q(D)}\right) \quad \text{and} \quad \mathbf{y}(D) = (y_1(D), y_2(D), ..., y_r(D)).$$

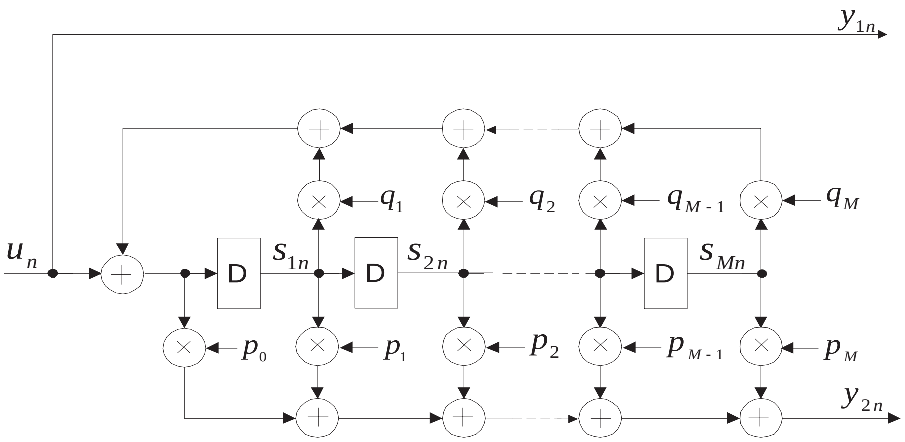

Fig. 1. The structure of a recursive systematic convolutional encoder of rate 1/2.

where $Q(D)$ is a primitive polynomial of degree M:

$$Q(D) = q_0 + q_1 D + ... + q_M D^M$$

and $P_i(D)$ is a polynomial of degree at most equal to M:

$$P_i(D) = p_{0i} + p_{1i} D + ... + p_{Mi} D^M \quad .$$

When the recursive convolutional encoder is systematic, we have $y_{1n} = u_n$ since $P_1(D) = Q(D)$.

Since $Q(D)$ is a primitive polynomial, the encoder generates a pseudo noise (PN) sequence or a maximum length sequence. The period of the PN sequence is $2^M - 1$. The weight of the output sequence for one period of the PN sequence is 2^{M-1} [6].

An example of state diagram is shown in Fig.2 for the primitive polynomial $Q(D) = 1 + D + D^3$. Each edge is labelled by $x^{w_I} y^{w_O}$ where w_I and w_O are respectively the weight of the corresponding input and output bit. As the edge drawn in dotted line corresponds to an input bit equal to 0, we can clearly observe the loop corresponding to the PN sequence of period 7 and that the output weight of the PN sequence is egal to 4.

We say that the encoder with $Q(D)$ is IIR, since the weight-one input sequence (impulse input) produces an infinite response, i.e. an infinite weight output sequence.

Definition 1. *A finite response input sequence (FRIS) is an input sequence whose first "1" causes the encoder state to leave the zero state $S_0 = [0, 0, ..., 0]$ at time n_0 and whose last "1" brings it back to S_0 at time $n_0 + L - 1$ $(L > 0)$.*

A FRIS will produce a finite weight output sequence. These FRISs are represented by $F(D)$.

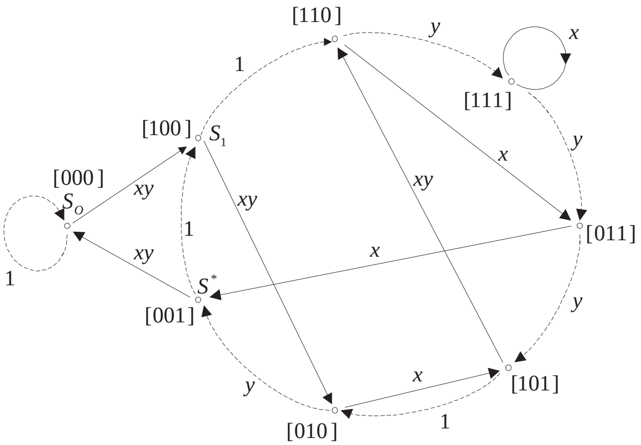

Fig. 2. The state diagram for a primitive polynomial $Q(D) = 1 + D + D^3$.

3 Properties of Finite Response Input Sequences (FRIS)

We have the following theorems about $F(D)$.

Theorem 1. *A FRIS of a recursive convolutional encoder satisfies the equation:*

$$F(D) \equiv 0 \qquad (\mathrm{mod}\ Q(D)) \quad (\mathrm{mod}\ 2)\ . \tag{2}$$

Proof. From (1), if and only if $Q(D)|u(D) \quad (\mathrm{mod}\ 2)$, i. e. $Q(D)$ is a factor of $u(D)$ over the finite field GF(2), then $y_i(D)$ becomes a finite order polynomial or a finite weight output sequence.

Since $Q(D)$ is a primitive polynomial, the encoder generates a maximum length sequence of period 2^{M-1}. We then have:

$$D^0 \equiv D^{2^M-1} \equiv 1 \qquad (\mathrm{mod}\ Q(D)) \quad (\mathrm{mod}\ 2)\ . \tag{3}$$

Then, (2) becomes:

$$F(D) \equiv 0 \qquad (\mathrm{mod}\ Q(D)) \quad (\mathrm{mod}\ D^{2^M-1} - 1) \quad (\mathrm{mod}\ 2)\ . \tag{4}$$

Theorem 2. *If we have a FRIS F(D) of weight w noted* $F^{(w)}(D)$*:*

$$F^{(w)}(D) = D^{n_1} + D^{n_2} + ... + D^{n_w} \tag{5}$$

where $n_1 = 0$ *and* $n_2, ..., n_w$ *are any positive integer, then there exists a family of weight w FRISs :*

$$F^{(w)}_{m_0 m_2 \dots m_w}(D) = D^{m_0}(D^{n_1+m_1(2^M-1)} + D^{n_2+m_2(2^M-1)} + ... + D^{n_w+m_w(2^M-1)}) \tag{6}$$

where $m_1 = 0$ *and* $m_0, m_2, ..., m_w$ *can be any integer, positive, negative, or zero.*

Proof. From (4),(5) and (6), we obtain:

$$F^{(w)}_{m_0 m_2 \ldots m_w}(D) \equiv D^{m_0} F^{(w)}(D) \equiv 0 \qquad (7)$$
$$(\mathrm{mod}\ Q(D)) \quad (\mathrm{mod}\ D^{2^M-1}-1) \quad (\mathrm{mod}\ 2)\ .$$

This theorem tells us that if we find any FRIS in a family, we can deduce all the FRISs of this family. We note that there are two different kinds of FRISs called simple and complex FRISs.

Definition 2. *A FRIS is simple if its last "1" solely brings back the encoder state to S_0. Otherwise, the FRIS is complex since the encoder state returns to S_0 more than once.*

We will now choose a unique representative for each family of simple FRISs, called basic FRIS.

Definition 3. $F_0^{(w)}(D)$ *is called a basic FRIS for weight w if and only if the following three conditions are satisfied:*

$$F_0^{(w)}(D) \textit{is a FRIS with the form (5)} \qquad (8)$$
$$0 < n_i - n_{i-1} < 2^M - 1 \quad (\forall i) \qquad (9)$$
$$n_w = min\ . \qquad (10)$$

Condition (8) means that the first "1" of a basic FRIS should occur at time 0; condition (9) means that after rearranging $n_1, n_2, ...n_w$ in ascendant form, the duration between two consecutive "1" should be less than 2^M-1; condition (10) means that we choose as the basic FRIS the sequence with the minimal length. The basic FRISs of a recursive convolutional encoder depend only on $Q(D)$.

We call $F^{(w)}(D)$ which satisfies conditions (8) and (9) a secondary basic FRIS $F_S^{(w)}(D)$.

The next theorem will show how to describe all the FRISs with weight w.

Theorem 3. *Supposing $w = \sum_i w_i (w_i > 1)$, all the FRISs can be obtained in the form (6) from $F_0^{(w)}(D)$ and from combinations of $F_0^{(w_i)}(D)$.*

In particular for w=2 and w=3, since we have no combination by $w = \sum_i w_i$ ($w_i > 1$), each FRIS is obtained from basic FRISs according to (6).

The next theorem will give us the total number of basic FRISs for each weight w.

Theorem 4. *For w=2, there exists only one basic FRIS:* $1 + D^{2^M-1}$
For w=3, there exists

$$\left\lceil \frac{2^M-2}{A_3^3} \right\rceil \qquad basic\,FRISs. \qquad (11)$$

For $4 \leq w < 2^M - 1$, *there exists*

$$\left\lceil \frac{(2^M-2)(2^M-3)^{w-3} - N_w}{A_w^w} \right\rceil \qquad \textit{basic FRISs.} \tag{12}$$

N_w is the number of $F^{(w)}(D)$ which are constructed from secondary basic FRISs $F_S^{(w_i)}(D)$; A_p^n is the number of ordered selections of p elements from a set of n elements, and $\lceil c \rceil$ means c rounded to the nearest integer towards plus infinity.

Proof. Since $Q(D)$ is a primitive polynomial of degree M, $(\mathbf{s}_1|\mathbf{s}_0 = S_0) = S_1$ when an input "1" occurs at time 0, where $S_1 = [1, 0, ...0]$; and then, in the absence of an input, $\mathbf{s}_n$ goes through all possible $2^M - 1$ nonzero encoder states and repeats with period $2^M - 1$; it returns to S_0 if and only if an input "1" occurs and the current state is $S^* = [0, ..., 0, 1]$. So, if we exclude the first "1" and the last "1" of this FRIS, the $w-2$ other "1"s can occur under any state $\mathbf{s}_{n_i}|\mathbf{s}_{n_i} \neq S_0, \mathbf{s}_{n_i} \neq S^*, \mathbf{s}_{n_i} \neq \mathbf{s}_{n_{i-1}}$. Note that, for the second "1" of the FRIS, $\mathbf{s}_{n_{i-1}} = \mathbf{s}_0$.

Therefore, there are $(2^M-2)(2^M-3)^{w-3}$ different secondary basic FRISs including those that are constructed from $F^{(w_i)}(D)$; on the other hand, from (6) each family includes A_w^w secondary basic FRISs if $n_i - n_{i-1} \neq n_j - n_{j-1} (i \neq j)$ and possibly less than A_w^w otherwise. As a result, we conclude that there exist $\lceil((2^M-2)(2^M-3)^{w-3} - N_w)/A_w^w\rceil$ basic FRISs.

For $w = 2$, there is only one basic FRIS which has the first "1" corresponding to the leaving of the zero state to S_1 and the other "1" for the return from $\mathbf{s}_{2^M-1} = S^*$ to the zero state S_0, that is, $F_0^{(2)}(D) = 1 + D^{2^M-1}$.

For $w = 3$, $N_3 = 0$, then there are $\lceil(2^M-2)/A_3^3\rceil$ basic FRISs.

Example 1. Supposing M=3 and $Q(D) = 1 + D + D^3$.

For w=2, since $2^M - 1 = 7$, $F_0^{(2)}(D) = 1 + D^7$.

All weight-2 FRISs can be written as follows according to (6) :

$F_{m_0m_2}^{(2)}(D) = D^{m_0}(1 + D^{7m_2})$,

For w=3, there exists $\lceil(2^M-2)/A_3^3\rceil = 1$ basic FRIS, $F_0^{(3)}(D) = 1 + D + D^3$.

All weight-3 FRISs can be written as follows according to (6) :

$F_{m_0m_2m_3}^{(3)}(D) = D^{m_0}(1 + D^{1+7m_2} + D^{3+7m_3})$,

for example,

$F_{6,-1,-1}^{(3)}(D) = 1 + D^2 + D^6$,

$F_{4,0,-1}^{(3)}(D) = 1 + D^4 + D^5$.

For w=4, since 4 = 2+2, and $F_0^{(2)}(D) = 1 + D^7$, we have $F^{(4)}(D)$ which are combinations of secondary basic FRISs $F_S^{(2)}(D)$ written by $F_*^{(4)}(D)$:

$F_*^{(4)}(D) = F_0^{(2)}(D) + D^{l_i}F_0^{(2)}(D), \qquad l_i = 1, 2, ..., 6.$

Clearly, here $N_4 = 6$, $\lceil((2^M-2)(2^M-3)^{4-3} - N_4)/A_4^4\rceil = 1$ and we have one $F_0^{(4)}(D)$ that is, $F_0^{(4)}(D) = 1 + D^2 + D^3 + D^4$. Therefore, the following two equations describe all simple weight-4 FRISs :

$F^{(4)}(D) = D^{m_0}(1 + D^{2+7m_2} + D^{3+7m_3} + D^{4+7m_4})$,

$F_*^{(4)}(D) = D^{m_0}[(1 + D^{7m_1}) + D^{l_i}(1 + D^{7m_2})]$,
where m_0, m_i can be any integer and $l_i = 1, 2, ..., 6$.
And the following equation describe all complex weight-4 FRISs:
$F_{com}^{(4)}(D) = D^{m_0}(1 + D^{7m_1} + D^{7m_2} + D^{7m_3})$
where m_0, m_i can be any integer and $m_i \neq m_j (i \neq j)$.

4 Tables

In this section, we will give a list of basic FRISs for recursive convolutional encoders with M=2, 3, 4 and 5. The following basic FRISs have been obtained from an exhaustive search since there is no known method to find them.

Table 1. Basic FRISs for $M = 2$ $Q(D) = 1 + D + D^2$.

w	$F_0^{(w)}$
2	$1 + D^3$
3	$1 + D + D^2$
4	$1 + D + D^3 + D^4$

Table 2. Basic FRISs for $M = 3$ $Q(D) = 1 + D + D^3$.

w	$F_0^{(w)}$
2	$1 + D^7$
3	$1 + D + D^3$
4	$1 + D^2 + D^3 + D^4$

Table 3. Basic FRISs for $M = 4$ $Q(D) = 1 + D + D^4$.

w	$F_0^{(w)}$	w	$F_0^{(w)}$	w	$F_0^{(w)}$
2	$1 + D^{15}$	4	$1 + D^2 + D^4 + D^5$	4	$1 + D^3 + D^6 + D^8$
3	$1 + D + D^4$	4	$1 + D^5 + D^6 + D^7$	4	$1 + D^3 + D^4 + D^9$
3	$1 + D^2 + D^8$	4	$1 + D + D^3 + D^7$	4	$1 + D^4 + D^8 + D^{10}$
3	$1 + D^5 + D^{10}$	4	$1 + D + D^5 + D^8$		

Table 4. Basic FRISs for $M = 5$ $Q(D) = 1 + D + D^2 + D^3 + D^5$.

w	$F_0^{(w)}$	w	$F_0^{(w)}$	w	$F_0^{(w)}$
2	$1 + D^{31}$	4	$1 + D^2 + D^{12} + D^{13}$	4	$1 + D^3 + D^{15} + D^{17}$
3	$1 + D^3 + D^8$	4	$1 + D + D^5 + D^{14}$	4	$1 + D^5 + D^{16} + D^{17}$
3	$1 + D^7 + D^9$	4	$1 + D^6 + D^7 + D^{14}$	4	$1 + D^6 + D^9 + D^{18}$
3	$1 + D + D^{12}$	4	$1 + D^2 + D^8 + D^{14}$	4	$1 + D^5 + D^{12} + D^{18}$
3	$1 + D^6 + D^{16}$	4	$1 + D^{10} + D^{13} + D^{14}$	4	$1 + D^7 + D^{16} + D^{18}$
3	$1 + D^4 + D^{17}$	4	$1 + D^4 + D^8 + D^{15}$	4	$1 + D^3 + D^7 + D^{19}$
4	$1 + D^4 + D^5 + D^6$	4	$1 + D^9 + D^{10} + D^{15}$	4	$1 + D^8 + D^9 + D^{19}$
4	$1 + D + D^4 + D^7$	4	$1 + D^5 + D^{11} + D^{15}$	4	$1 + D^4 + D^{10} + D^{19}$
4	$1 + D + D^3 + D^{10}$	4	$1 + D^3 + D^{11} + D^{16}$	4	$1 + D^{11} + D^{18} + D^{19}$
4	$1 + D^2 + D^7 + D^{11}$	4	$1 + D^9 + D^{14} + D^{16}$	4	$1 + D^{10} + D^{17} + D^{20}$
4	$1 + D^6 + D^8 + D^{11}$	4	$1 + D^{13} + D^{15} + D^{16}$	4	$1 + D^3 + D^9 + D^{20}$
4	$1 + D^4 + D^9 + D^{12}$	4	$1 + D + D^9 + D^{17}$	4	$1 + D^6 + D^{13} + D^{21}$
4	$1 + D^8 + D^{10} + D^{12}$	4	$1 + D^7 + D^{12} + D^{17}$	4	$1 + D^8 + D^{17} + D^{21}$
4	$1 + D^3 + D^5 + D^{13}$	4	$1 + D^{11} + D^{13} + D^{17}$		

5 Exemples of Application

5.1 Hamming Weight of the Output Sequences of Finite Input Response Sequences

In this section, we will show how to use the properties introduced above to compute the Hamming weight of the output sequence of any FRIS.

Theorem 5. *Consider an arbitrary FRIS of weight w $F^{(w)}(D)$:*

$$F^{(w)}(D) = D^{m_0}(D^{n_1} + D^{n_2} + ... + D^{n_w}),$$

where $n_1 = 0$ and $n_i > n_{i-1}$, $(\forall i)$. $d[F^{(w)}(D)]$ denotes the Hamming weight of the output sequence. We have

$$d[F^{(w)}(D)] = d[F_S^{(w)}(D)] + d[PN] \sum_{i=2}^{w} b_i \tag{13}$$

where $F_S^{(w)}(D)$ is the secondary basic FRIS

$$F_S^{(w)}(D) = D^{l_1} + D^{l_1 + l_2} + ... + D^{\sum_i l_i}, \tag{14}$$

$$\begin{aligned} \textit{with} \quad & l_1 = 0 \\ & l_i \equiv n_i - n_{i-1} - 1 \pmod{2^M - 1} + 1 \\ & b_i = \left[\frac{(n_i - n_{i-1} - l_i)}{2^M - 1} \right]. \end{aligned}$$

$d[PN]$ is the weight of the output sequence for one period of the PN sequence. $d[PN] = 2^{M-1}$ since $Q(D)$ is a primitive polynomial.

This theorem tells us that we can calculate the Hamming weight of the output sequence of any FRIS from its associated secondary basic FRIS. We will now give a method to find the A_w^w secondary basic FRISs from the basic FRIS. Consider a basic FRIS $F_0^{(w)}(D)$

$$F_0^{(w)}(D) = D^{n_1} + D^{n_2} + ... + D^{n_w}, \tag{15}$$

where $n_1 = 0$, $n_i > n_{i-1}(\forall i)$. From this basic FRIS, we can deduce all the simple FRIS of the family

$$\begin{aligned} F^{(w)}(D) &= D^{m_0}(D^{n_1+m_1(2^M-1)} + D^{n_2+m_2(2^M-1)} + ... + D^{n_w+m_w(2^M-1)}) \\ &= D^{l_1} + D^{l_2} + ... + D^{l_w}, \end{aligned} \tag{16}$$

where $m_1 = 0$, $l_i = m_0 + n_i + m_i(2^M - 1)(\forall i)$.

All the secondary basic FRISs can be obtained from the basic FRIS by permutation of $n_1, n_2, ..., n_w$ and then searching $m_0, m_2, ..., m_w$ to satisfy the inequality $l_1 < l_2 < ... < l_w$ and $l_1 = 0$, $l_i - l_{i-1} < 2^M - 1$.

Example 2. Supposing M=3, w=3 and $Q(D) = 1 + D + D^3$. There is only one basic FRIS :

$F_0^{(3)}(D) = D^0 + D + D^3 = 1 + D + D^3$.

We have

$F_{S1}^{(3)}(D) = D^0 + D^3 + D^{1+7} = 1 + D^3 + D^8$ with m_0=0,m_2=0, m_3=1 .

$F_{S2}^{(3)}(D) = D^{-1}(D^1 + D^3 + D^{0+7}) = 1 + D^2 + D^6$ with m_0=-1,m_2=0,m_3=1 .

...

5.2 Interleaver Construction for Turbo Codes

Turbo codes are a parallel concatenation of recursive systematic convolutional codes [2]. The turbo encoder consists of two recursive convolutional codes and an interleaver of size N. An exemple of a turbo encoder is shown in Fig.3.

The N bits information sequence $u(D)$ is encoded twice : firstly by $C1$ and secondly after interleaving by $C2$. A tail sequence composed of M bits is added after the information sequence in order to bring the internal state of the first encoder to the zero state. As a consequence only FRISs are allowed.

So we can use the properties of FRISs for the construction of the interleaver. The interleaver should improve the weight distribution and the free distance of turbo codes. An optimal interleaver should map the input sequences $u(D)$ which generate low weight output sequences $y_1(D)$ with sequences $v(D)$ which generate high weight output sequence $y_2(D)$ and vice versa.

For the construction of the interleaver, we can take into account only the input sequences $u(D)$ which generate low weight output sequences. These sequences can be enumerated using the properties of FRISs introduced above. The

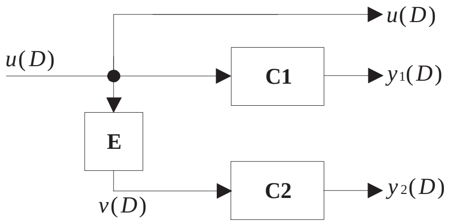

Fig. 3. The structure of a turbo encoder of rate 1/3.

weight of the associated output sequence $y_1(D)$ is calculated by using (13). The weight of the output sequence $y_2(D)$ can also be obtained using a generalisation of this principle.

In [7], we have shown that these properties combined with a tree research method for construction of the interleaver can produce very good interleavers.

6 Conclusion

The finite response input sequences (FRISs) for a recursive convolutional encoder with a primitive polynomial can be defined by (4). In this paper, new practical properties of FRISs with a certain Hamming weight w are presented. We have introduced the basic FRIS and shown that we could write all FRISs with weight w in closed-form expressions from these basic FRISs.

These properties can be employed in many applications, such as the computing of the weight enumerators of these codes and the construction of efficient interleavers for turbo codes.

References

1. Forney, G. D.: Convolutional codes I: Algebraic structure. IEEE Trans. Inform. Theory **IT16** (1970) 720–738
2. Berrou, C., Glavieux, A.,Thitimajshima, P.: Near Shannon limit error correcting coding and decoding : Turbo-codes. Proc. of Int. Conf. on Comm., Geneva, Switzeland (1993) 1064–1070
3. Benedetto, S., Divsalar, D., Montorsi, G., Pollara, F.: Serial concatenation of interleaved codes : performance analysis, design and iterative decoding. IEEE Trans. Inform. Theory **IT44** (1998) 909–926
4. Battail, C., Berrou, C.,Glavieux, A.: Pseudo-random recursive convolutional coding for near-capacity performance. Proc. of GLOBECOM'93, Houston, Texas, USA (1993) 23–27
5. Podemski, R.,Holubowicz, W.,Berrou, C.,Battail, G.: Hamming distance spectra of turbo-codes. Ann.Telecommun. **50** (1995) 790–797
6. Golomb, S. W.: Shift register sequences. revised version Aegean Park, Laguna Hills, CA (1982)
7. Le Ruyet, D., Sun, H., Vu Thien, H.: New method for the construction of interleavers. submit to Int. Symp. on Info. Theory, Sorrento, Italia (2000)