AN EFFICIENT TECHNIQUE FOR DETECTING CATASTROPHIC CONVOLUTIONAL CODES

Y.Z. Boutros, G.P. Fiani, E.S. Looka

Alexandria University, Alexandria, Egypt.

ABSTRACT

Catastrophic Convolutional Codes (CC) cause an infinite number of decoded data bit errors when decoding a finite number of code symbols. A CC displays a catastrophic error propagation if the generating polynomials have a common factor. An efficient algorithm for polynomial factorization in GF (2) is used for detecting catastrophic CC for any rate n/m and constraint length k. A general formula is derived to calculate the number of catastrophic codes in any (m,n,k) CC.

Keywords: Convolutional Code (CC), Catastrophic Code.

1.INTRODUCTION

In recent years, intensive research has been directed towards finding efficient and practical coding schemes for various types of noisy channels. Convolutional Codes (CC) are superior to block codes for the same implementation complexity of encoder-decoder [1]. However, there is a possibility of having a catastrophic CC [2]. Massey and Sain [3] have proved that the necessary and sufficient condition for a CC to display a catastrophic error propagation is that the generator polynomials of the code have a common factor.

In the present paper we use polynomial factorization in GF (2^m) as a tool to detect catastrophic CC. Tables of catastrophic codes are included. Computer results are in agreement with previous published results.

2.BASIC DEFINITIONS

2.1. Convolutional Codes

A convolutional code of rate R=n/m and constraint length k, denoted by (m,n,k), is defined as the output range of some n input, m output feed forward modular circuit over GF (2). K represents the number of n-tuple stages in the encoding shift register. For an information sequence of length nL, the corresponding output has a length of m(L+k), where the last mk outputs are generated by a string of nk zeros catenated to the input sequence to allow the encoder memory to clear. The output sequence is generated by convolving the input sequence with a fixed binary function. The encoder complexity is independent of the message and depends only on the code rate n/m and the shift register length k.

2.2. Connection representation

A CC encoder (m,n,k) can be represented by n shift register (s) of lengths ≤ k each and m modulo-2 adders (implemented by XOR gates) as shown in Figure (1).

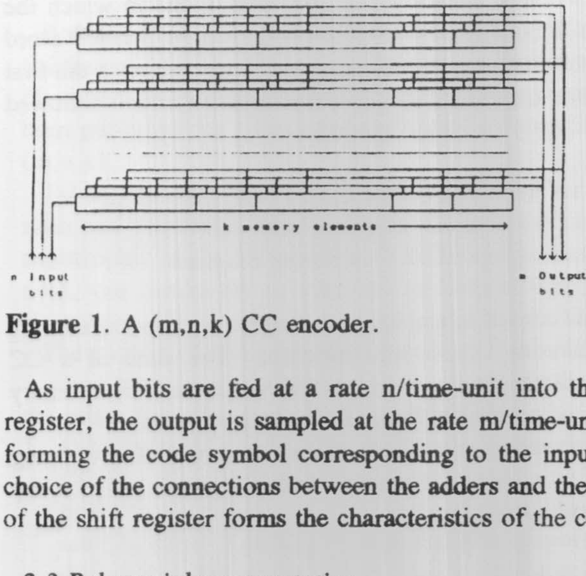


Figure 1. A (m,n,k) CC encoder.

As input bits are fed at a rate n/time-unit into the shift register, the output is sampled at the rate m/time-unit thus forming the code symbol corresponding to the input. The choice of the connections between the adders and the stages of the shift register forms the characteristics of the code.

2.3. Polynomial representation

The encoder connections are characterized by the generator polynomials

$$g_{ip}(k) = \sum_{J=0}^{k} = g_{ip,j} x^j \quad 1 \le i \le n,$$
$$1 \le p \le m,$$

where $g_{ip,j}$ is either 0 or 1 and it corresponds to whether the j^{th} stage of the i^{th} register is connected to the p^{th} output or not. If the input U is represented by a polynomial

$$U(x) = \sum_{i=1}^{n} U_i x^{i-1},$$

then the output sequences V are given by

$$V_p(x) = \sum_{i=1}^{n} U(x)\, g_{ip}(x). \quad 1 \leq p \leq m$$

The following is the polynomial representation of a typical (2,1,2)CC, where i is omitted for (n=1):

$$g_1(x) = 1 + x + x^2,$$

$$g_2(x) = 1 \quad + x^2,$$

The lowest-order term of the polynomial corresponds to the input stage of the register.

2.4. Systematic codes

A systematic convolutional [6] code is one in which the input n-tuple appears as part of the output branch word m-tuple associated with that n-tuple. In each branch the first n symbols are exact replicas to the input n symbols followed by m-n parity or coded symbols.

$$V^{(i)} = U^{(i)} \quad i=1,2,3,\ldots\ldots,n; \quad n \leq m$$

2.5. State representation and state diagram

A fixed convolutional encoder may be regarded as a linear time invariant finite state machine. The state of a CC encoder is the contents of its shift registers. For a binary encoder of constraint length k there are 2^k states.

The encoder state is Markov, i.e., the probability of being in state x_{i+1} given all previous states depends only on the most recent state

$$p(x_{i+1} \backslash x_i, x_{i-1}, x_{i-2}, \ldots) = p(x_{i+1} \backslash x_i).$$

The state diagram representation of a (2,1,2) CC encoder is shown in Figure (2). The number of links emanating from each node is equal to the input alphabet (two in case of binary). Dotted lines designate a '1' input while continuous lines designate a '0'. The 'D' labels on the branches denote the Hamming distance between the output of the branch transition and the all-zeros path.

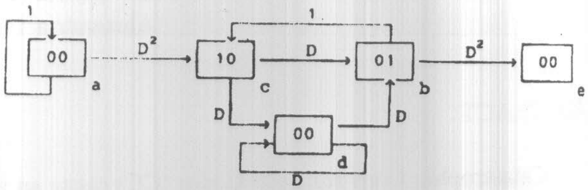


Figure 2. The state diagram representation of a (2,1,2) CC.

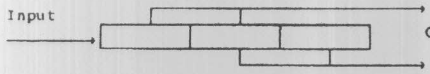
3. CATASTROPHIC ERRORS

A catastrophic error [7] is defined as an event whereby a finite number of code symbol errors cause an infinite number of decoded data bit errors. Massey & Sain [3] have derived a necessary and sufficient condition for the convolutional codes to display catastrophic error propagation, namely that the generators have a common polynomial factor. A simple example of a (2,1,2) catastrophic CC is

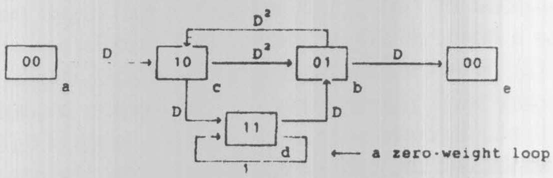
$$g_1(x) = 1 + x\,,$$

$$g_2(x) = x + x^2 = (x)(1+x).$$

The condition of a common factor occurs if any closed-loop path in the diagram has a zero-weight (zero distance from the all-zeros path). Thus for the CC of Figure (3), and assuming the correct path to be the all-zeros path a-a-a-........-a-a-a, the incorrect path a-b-d-.......-d-c-a has exactly 6 ones, no matter how many times we go around the self loop node at d. Thus three channel errors may force us to choose this incorrect path. The total number of errors is equal to (2 + the number of times the loop d is traversed).



The connection representation of a (2,1,2) catastrophic CC.



The state diagram representation of a (2,1,2) catastrophic CC.

Figure 3. A catastrophic (2,1,2) CC.

In the case of systematic codes, data symbols appear directly on each branch in the state diagram. Thus it is impossible to have a self-loop in which a distance to the all-zeros path does not increase and therefore these codes are

NON CATASTROPHIC

In the special case (m,1,k), if each adder in the encoder has an even number of connections, the self-loop corresponding to all ones data state will have a zero weight, and consequently the code will be catastrophic [8].

The problem is to find a simple and fast method for detecting catastrophic CC in the general case (m,n,k). In section 5 we present an efficient technique for catastrophic CC detection based on polynomial factorization described in section 4.

4. POLYNOMIAL FACTORIZATION IN GF (2^m)

Given the polynomial f(x) of order n

$$f(x) = \sum_{i=0}^{m} a_i x^i ; a_i \epsilon GF(2)$$

The prime factor polynomials of f(x) in GF (2^m) are determined from look-up tables, if available, or generated by special techniques [9]. In the following, some interesting properties of prime polynomials, which will be used subsequently, are given.

1. Up to a given order n, there exist 2^{n+1} -1 polynomials, of which, exactly 2^{n+1-d} -1 polynomials have a common factor of order (d).
2. Up to a given order n, there exist exactly (n/d) polynomials having identical common factors of order (d).
3. The number of polynomials divisible by the product of two or more prime polynomials follows the same rule mentioned in 1.

Table I lists the number of prime polynomial factors taken n at a time and the corresponding order of their product. We denote this table by T and an entry in the j^{th} row and i^{th} column by T_{ji}.

5. PROPOSED METHOD FOR CATASTROPHIC CC DETECTION

Extensive computer search is required to find a good code. For an (m,n,k) CC there are $2^{(n+k)m}$ different connections (or codes). The present method detects which of these are catastrophic. In a previous paper [9] we have presented an efficient and easy to use algorithm for polynomial factorization. Using this polynomial factorization technique, a simple method is proposed for catastrophic CC detection. The procedure is as follows:

1) Given an (m,n,k) CC with prespecified n connection vectors, we determine the generator polynomials.
2) Determine all prime polynomial factors for each generator polynomial.
3) The polynomial factors are compared. If there exists at least one common polynomial factor for all generator polynomials, the code is CATASTROPHIC.

Table I. The member of prime polynomial factors taken n at a time and the corresponding order of their product.

Polynomial Order \ Number of factors (n)	1	2	3	4
1	2	-	-	-
2	1	1	-	-
3	2	2	-	-
4	3	4	1	-
5	6	8	2	-
6	9	16	7	-
7	18	30	14	2
8	31	60	34	4

6. ESTIMATION OF THE NUMBER OF CATASTROPHIC CC

Rosenberg [8] has shown that for (m,1,k) CC, only a fraction of 1/(2^m-1) of nonsystematic codes are catastrophic. However, to our knowledge, no corresponding results have been published for other values of n or for the general case (m,n,k).

Table II gives a list of all catastrophic codes for selected rates and constraint lengths. Table III lists the number of catastrophic codes for selected CC. For the particular case n=1, our results are in complete agreement with those of Rosenberg. [8]

The results of the computer search in Table III can be verified by a computational manner using the properties of the prime factor polynomials [9] as follows:

1. Calculation of the number of catastrophic codes for the CC (2,1,2): The Max polynomial order (k+n) is 3. The prime factor polynomials and their combination products are (2), (3), (7) and(2)(3). The Number of polynomials divisible by the prime factors and/or their combinations are: 3, 3, 1 and 1 respectively.

Since only two outputs are required, the corresponding number of codes for each category is as follows:

\# of codes with a common factor (2) are ${}^3C_2 = 3$.
\# of codes with a common factor (3) are ${}^3C_2 = 3$.
\# of codes with a common factor (7) are ${}^1C_2 = 0$.
\# of codes with a common factor (2)(3) are ${}^1C_2 = 0$.
\# of codes with similar connections (excluding systematic codes) 2^{k+n}-2 = 6.

Therefore the number of catastrophic codes in (2,1,2) are 3+3+6=12.

2. Calculation of the number of catastrophic codes for the CC (3,1,4): The max order (k+n) is 5. The number of prime factors of orders 1, 2, 3 and 4 are 2, 1, 2, and 3 respectively and the number of bi-prime factors of order 2,3 and 4 are 1,2 and 4 respectively and there is only one tri-prime factor of order 4. Since 3 outputs are required, the corresponding number of codes in each category is:

Table II. Catastrophic CC codes.
(The generator polynomials are expressed in their decimal equivalents.

(2,1,2) : 2,2 2,4 2,6 3,3 3,5 3,6 4,4 4,6 5,5 5,6 6,6 7,7
(3,1,2) : 2,2,2 2,2,4 2,2,6 2,4,4 2,4,6 2,6,6 3,3,3 3,3,5 3,3,6
3,5,5 3,5,6 3,6,6 4,4,4 4,4,6 4,6,6 5,5,5 5,5,6 5,6,6
6,6,6 7,7,7
(2,1,3) : 2,2 2,4 2,6 2,8 2,10 2,12 2,14 3,3 3,5 3,6 3,9 3,10
3,12 3,15 4,4 4,6 4,8 4,10 4,12 4,14 5,5 5,6 5,9 5,10
5,12 5,15 6,6 6,8 6,9 6,10 6,12 6,14 6,15 7,7 7,9
7,14 8,8 8,10 8,12 8,14 9,9 9,10 9,12 9,14 9,15 10,10
10,12 10,14 10,15 11,11 12,12 12,14 12,15 13,13 14,14
15,15
(3,1,3) : 2,2,2 2,2,4 2,2,6 2,2,8 2,2,10 2,2,12 2,2,14 2,4,4 2,4,6
2,4,8 2,4,10 2,4,12 2,4,14 2,6,6 2,6,8 2,6,10 2,6,12
2,6,14 2,8,8 2,8,10 2,8,12 2,8,14 2,10,10 2,10,12 2,10,14
2,12,12 2,12,14 2,14,14 3,3,3 3,3,5 3,3,6 3,3,9 3,3,10
3,3,12 3,3,15 3,5,5 3,5,6 3,5,9 3,5,10 3,5,12 3,5,15
3,6,6 3,6,9 3,6,10 3,6,12 3,6,15 3,9,9 3,9,10 3,9,12
3,9,15 3,10,10 3,10,12 3,10,15 3,12,12 3,12,15 3,15,15
4,4,4 4,4,6 4,4,8 4,4,10 4,4,12 4,4,14 4,6,6 4,6,8 4,6,10
4,6,12 4,6,14 4,8,8 4,8,10 4,8,12 4,8,14 4,10,10 4,10,12
4,10,14 4,12,12 4,12,14 4,14,14 5,5,5 5,5,6 5,5,9 5,5,10
5,5,12 5,5,15 5,6,6 5,6,9 5,6,10 5,6,12 5,6,15 5,9,9
5,9,10 5,9,12 5,9,15 5,10,10 5,10,12 5,10,15 5,12,12
5,12,15 5,15,15 6,6,6 6,6,8 6,6,9 6,6,10 6,6,12 6,6,14
6,6,15 6,8,8 6,8,10 6,8,12 6,8,14 6,9,9 6,9,10 6,9,12
6,9,15 6,10,10 6,10,12 6,10,14 6,10,15 6,12,12 6,12,14
6,12,15 6,14,14 6,15,15 7,7,7 7,7,9 7,7,14 7,9,9 7,9,14
7,14,14 8,8,8 8,8,10 8,8,12 8,8,14 8,10,10 8,10,12
8,10,14 8,12,12 8,12,14 8,14,14 9,9,9 9,9,10 9,9,12
9,9,14 9,9,15 9,10,10 9,10,12 9,10,15 9,12,12 9,12,15
9,14,14 9,15,15 10,10,10 10,10,12 10,10,14 10,10,15

10,12,12 10,12,14 10,12,15 10,14,14 10,15,15 11,11,11
12,12,12 12,12,14 12,12,15 12,14,14 12,15,15 13,13,13
14,14,14 15,15,15
(2,1,4) : 2,2 2,4 2,6 2,8 2,10 2,12 2,14 2,16 2,18 2,20 2,22
2,24 2,26 2,28 2,30 3,3 3,5 3,6 3,9 3,10 3,12 3,15
3,17 3,18 3,20 3,23 3,24 3,27 3,29 3,30 4,4 4,6 4,8
4,10 4,12 4,14 4,16 4,18 4,20 4,22 4,24 4,26 4,28
4,30 5,5 5,6 5,9 5,10 5,12 5,15 5,17 5,18 5,20 5,23
5,24 5,27 5,29 5,30 6,6 6,8 6,9 6,10 6,12 6,14 6,15
6,16 6,17 6,18 6,20 6,22 6,23 6,24 6,26 6,27 6,28
6,29 6,30 7,7 7,9 7,14 7,18 7,21 7,27 7,28 8,8 8,10
8,12 8,14 8,16 8,18 8,20 8,22 8,24 8,26 8,28 8,30
9,9 9,10 9,12 9,14 9,15 9,17 9,18 9,20 9,21 9,23
9,24 9,27 9,28 9,29 9,30 10,10 10,12 10,14 10,15
10,16 10,17 10,18 10,20 10,22 10,23 10,24 10,26 10,27
10,28 10,29 10,30 11,11 11,22 11,29 12,12 12,14 12,15
12,16 12,17 12,18 12,20 12,22 12,23 12,24 12,26 12,27
12,28 12,29 12,30 13,13 13,23 13,26 14,14 14,16 14,18
14,20 14,21 14,22 14,24 14,26 14,27 14,28 14,30 15,15
15,17 15,18 15,20 15,23 15,24 15,27 15,29 15,30 16,16
16,18 16,20 16,22 16,24 16,26 16,28 16,30 17,17 17,18
17,20 17,23 17,24 17,27 17,29 17,30 18,18 18,20 18,21
18,22 18,23 18,24 18,26 18,27 18,28 18,29 18,30 19,19
20,20 20,22 20,23 20,24 20,26 20,27 20,28 20,29 20,30
21,21 21,27 21,28 22,22 22,24 22,26 22,28 22,29 22,30
23,23 23,24 23,26 23,27 23,29 23,30 24,24 24,26 24,27
24,28 24,29 24,30 25,25 26,26 26,28 26,30 27,27 27,28
27,29 27,30 28,28 28,30 29,29 29,30 30,30 31,31

Table III. The number of catastrophic codes for CC of different rates and constraint length.

Table III. The number of catastrophic codes for CC of different rates and constraint lengths.

Code	Catastrophic	NonCatast.	TotalNumber	Ratio
(2, 1, 2)	12	16	28	0.429
(2, 1, 3)	56	64	120	0.467
(2, 1, 4)	240	256	496	0.484
(2, 1, 5)	992	1024	2016	0.492
(2, 1, 6)	4032	4096	8128	0.496
(2, 1, 7)	16256	16384	32640	0.498
(2, 1, 8)	65281	65536	130817	0.499
(2, 1, 9)	261638	262144	523782	0.500
(2, 1, 10)	1047580	1048576	2096156	0.500
(2, 1, 11)	4192376	4194304	8386680	0.500
(2, 1, 12)	16773620	16777220	33550830	0.500
(2, 1, 13)	67102690	67108860	134211600	0.500
(2, 1, 14)	268427200	268435500	536862700	0.500
(3, 1, 2)	20	64	84	0.238
(3, 1, 3)	168	512	680	0.247
(3, 1, 4)	1360	4096	5456	0.249
(3, 1, 5)	10912	32768	43680	0.250
(3, 1, 6)	87360	262144	349504	0.250
(3, 1, 7)	699008	2097152	2796160	0.250
(3, 1, 8)	5592321	16777220	22369540	0.250
(3, 1, 9)	44739070	134217700	178956800	0.250
(3, 1, 10)	357913700	1073742000	1431655000	0.250
(3, 1, 11)	2863310000	8589934000	11453250000	0.250
(3, 1, 12)	22906490000	68719480000	91625970000	0.250
(3, 1, 13)	183251900000	549755800000	733007700000	0.250
(3, 1, 14)	1466016000000	4398047000000	5864062000000	0.250
(4, 1, 2)	30	256	286	0.105
(4, 1, 3)	420	4096	4516	0.093
(4, 1, 4)	6120	65536	71656	0.085
(4, 1, 5)	92752	1048576	1141328	0.081
(4, 1, 6)	1441440	16777220	18218660	0.079
(4, 1, 7)	22717760	268435500	291153200	0.078
(4, 1, 8)	360704700	4294968000	4655672000	0.077
(4, 1, 9)	5748970000	68719480000	74468450000	0.077
(4, 1, 10)	91804820000	1099512000000	1191316000000	0.077
(4, 1, 11)	1467446000000	17592190000000	19059630000000	0.077
(4, 1, 12)	23467690000000	281475000000000	304942700000000	0.077
(4, 1, 13)	375391600000000	4503600000000000	4878991000000000	0.077
(5, 1, 2)	42	1024	1066	0.039
(5, 1, 3)	924	32768	33692	0.027
(5, 1, 4)	23256	1048576	1071832	0.022
(5, 1, 5)	649264	33554430	34203700	0.019
(5, 1, 6)	19315300	1073742000	1093057000	0.018
(5, 1, 7)	595205500	34359740000	34954950000	0.017
(5, 1, 8)	18684490000	1099512000000	1118196000000	0.017
(5, 1, 9)	592143700000	35184370000000	35776520000000	0.017
(5, 1, 10)	18856710000000	1125900000000000	1144757000000000	0.016

Number of codes in case all outputs are different is where 1 $^1C_3$ is equal to zero.

Number of codes in case exactly two outputs are similar [2 (number of catastrophic codes in (2,1,4) - 30)] = 2(210) = 420

Number of codes in case all outputs are similar (excluding all systematic codes) is $2^{k+n}-2=2^{4+2}-2=30$.

Therefore the total number of catastrophic codes for (3,1,4) is 910 + 420 + 30 = 1360.

3. The total number of possible (m,n,k) CC is

$$\sum_{p=o}^{m-1} m-1\, C_p^{(2^{n+k}-1)} C_{m-p}$$

where the summation counts the number of similar outputs.

4. The total number of non-catastrophic codes is 2^{mk}.

5. An expression to calculate the total number of catastrophic codes for a general (m,n,k) CC is

$$\sum_{p=o}^{m-1} m-1\, C_p \sum_{j=1}^{k+n-1} (-1)^{j+1} \sum_{i=1}^{k+n-1} T_{ij}(2^{k+n-1}-1) C_{m-p}$$

where T_{ij} is an entry in Table II. The first summation counts the number of similar outputs, the second counts the number of prime factors in a polynomial and the last one counts the prime factor orders.

7. CONCLUSION

We have presented a method for detecting a catastrophic CC. We have also estimated the number of catastrophic codes. The present method provides an efficient tool for recognizing catastrophic CC for any values of (m,n,k) which may be helpful in the design of good convolutional codes.

REFERENCES

[1] G.C.Clark and J.B.Cain, *Error-Correction Coding for Digital communications*, Plenum Press, New York, 1981.

[2] P.J.Lee, "Further Results on Rate 1/N Convolutional Code, Construction With Minimum Required SNR Criterion", *IEEE Trans. Comm.*, Vol. COM34, No. 4, pp.396-399, April 1986.

[3] J.L.Massey and M.K.Sain, "Inverses Of Linear Sequential Circuits", *IEEE Trans. Comput.*, Vol. C17, pp. 330-337, April 1968.

[4] A.M.Michelson and A.H.Levesque, *Error-Control Techniques For Digital Communication*, John Wiley & Sons, New York, 1985.

[5] S.Lin and D.J.Costello, *Error Control Coding*, Prentice Hall, New Jersey, 1983.

[6] A.J.Viterbi and J.K.Omura, *Principles of Digital Communication and Coding*, Mc-Graw Hill, 1979.

[7] B.Sklar, *Digital Communications Fundamentals and Applications* Prentice Hall, Englewood Cliffs, New Jersey, 1988.

[8] W.J.Rosenberg, "Structural Properties of Convolutional Codes", *Ph.D. Dissertation*, Univ. of California, Los Angeles, 1971.

[9] Y.Z.Boutros, G.P.Fiani and E.S.Looka, "Polynomial Factorization, 1in GF (2^m)", Submitted to *Alexandria Engineering Journal*, Faculty of Engineering, Alexandria University.