Double Burst Error Detection Capability of Ethernet CRC

IEEE 802.3bj Task Force

July 16-19, 2012, San Diego, CA

Roy Cideciyan – IBM

Mark Gustlin – Xilinx

Introduction

- The random error detection capability of the Ethernet CRC [1], also known as CRC-32, has been studied for frame sizes up to (131072+32) bit = 131104 bit [2]-[3].
- Searches for generator polynomials of CRC codes that have better random error detection capability than CRC-32 have been made [3]-[5].
- The double burst error detection capability of CRC-32 has been determined for MAC frame sizes up to frame size of 13000 bit [2].
- Mark's comment #76 on 802.3bj draft standard D1.0 refers to MTTFPA concerns associated with 64b/66b coding in 100 Gb/s 20-lane PCS and bit-multiplexed PMA(20:4). The double burst error detection capability of CRC-32 for MAC frame sizes larger than the basic Ethernet frame size should be determined in order to compute the MTTFPA associated with jumbo frames.
- This paper calculates the double burst error detection capability of CRC-32 for MAC frame sizes larger than 13000 bit.

CRC-32 and Scrambling

- IEEE 802.3 CRC code [1] also referred to as CRC-32 is specified by the polynomial

$$x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^{8} + x^{7} + x^{5} + x^{4} + x^{2} + x + 1$$

- Interaction of scrambler and CRC-32 depends on the scrambler polynomial. IEEEE 802.3 scrambler polynomial is

$$1 + x^{39} + x^{58}$$

- Scrambler polynomial and CRC-32 polynomial do not have a common factor. This is a necessary but not a sufficient condition for not weakening CRC-32's error detection capability by the descrambler [6]. As the scrambler runs continuously on all payload bits (clause 49.2.6), the effects of error spilling should be considered in CRC-32 performance analysis. An exhaustive search for all error patterns with weight < 4 by explicitly checking all spill-in and spill-out errors showed that CRC-32's error detection capability is not weakened by 3x error multiplication in the descrambler [7].

- Error detection properties of CRC-32 in the presence of $1 + x^{43}$ scrambling was studied in [8].

Random Error Detection Capability of CRC-32

Table 1. Message lengths in bits (exclusive of CRC field) for which the specified HD is achieved. (Computed to data word length of 131072.)

HD	CRC-32 IEEE 802.3 0x82608EDB {32}	Castagnoli (iSCSI) 0x8F6E37A0 {1,31}	CRC-32K Koopman 0xBA0DC66B {1,3,28}	Castagnoli 0xFA567D89 {1,1,15,15}	Koopman 0x992C1A4C {1,1,30}	Koopman 0x90022004 {1,1,30}	Castagnoli 0xD419CC15 {32}	Koopman 0x80108400 {32}
15	8-10							
14	—	8						
13	—	—						
12	11-12	9-20	8-16	8-11	8-16		8-17	
11	13-21	—	—	—	—		18-21	
10	22-34	21-47	17-18	12-24	17-26		22-27	
9	35-57	—	—	—	—		—	
8	58-91	48-177	19-152	25-274	27-134		28-58	
7	92-171	—	—	—	—		59-81	
6	172-268	178-5243	**153-16360**	**275-32736**	**135-32737**	**8-32738**	82-1060	
5	269-2974	—	—	—	—	—	**1061-65505**	**8-65505**
4	**2975-91607**	**5244-131072...**	16361-114663	32737-65502	32738-65506	32739-65506	—	—
3	91608-131072...	...	—	—	—	—	—	—
2	...	...	114664+	65503+	65507+	65507+	65506+	65506+

Source:
P. Koopman, "32-bit cyclic redundancy codes for internet applications," *Int. Conf. Dependable Systems and Networks (DSN)*, July 2002.

- CRC-32 has Hamming distance HD=4 (or 5) ➔ CRC-32 can detect any HD-1=3 (or 4) erroneous bits per frame.
- CRC-32K has HD=6 for all 802.3 frame sizes and HD=4 for jumbo frames ➔ CRC-32K can detect any 5 erroneous bits in all 802.3 frames and 3 erroneous bits in jumbo frames

Random Error Detection Capability of CRC-32 (cont.)

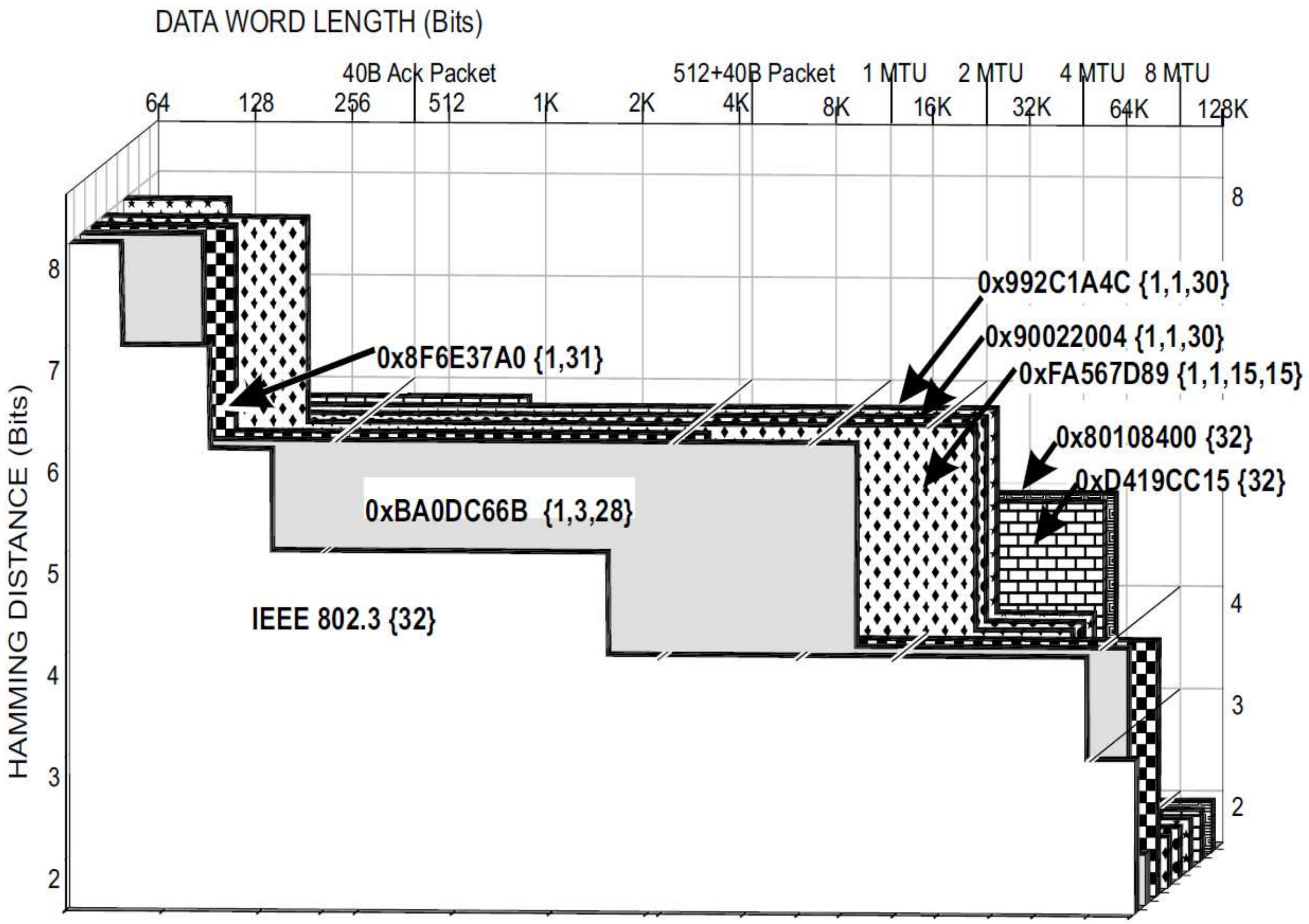

Figure 1. Error detection capabilities of selected 32-bit CRC polynomials.

Source: P. Koopman, “32-bit cyclic redundancy codes for internet applications,” *Int. Conf. Dependable Systems and Networks (DSN)*, July 2002.

Burst Error Detection Capability of CRC-32

- Because a CRC code is a linear code, each undetectable error pattern is a legal CRC codeword. IEEE 802.3 CRC code can detect any single burst error up to a length of 32 bits per frame [9].
- A linear code C can detect any double burst each of length up to b bits in a frame if and only if the code C has the capability of correcting any single burst error of length up to b bits [2].
- Kasami devised an algorithm to determine optimum shortened cyclic codes for burst-error correction [10].
- Using Kasami's algorithm [10] Fujiwara et al. computed the double burst error detection capability of CRC-32 for MAC frame sizes up to 13000 bit [2].
- MAC frame size includes 18 byte overhead consisting of destination address DA (6B), source address SA (6B), length/type field (2B) and frame check sequence FCS (4B). The MAC frame size does not include the preamble (7B) and start frame delimiter SFD (1B).

MAC Frame Type	MAC Frame Size
Smallest 802.3 frame	64B
Basic 802.3 frame	1518B
Largest 802.3 frame	2000B
Jumbo frame	9018B

Kasami's Algorithm (1963)

A shortened cyclic binary code is completely determined by its generating polynomial over $GF(2)$,[6] $g(x)$, and its code length n.[7] The degree of this polynomial is equal to the number of check digits r. Let us write as

$$g(x) = g_0 + g_1 x + \cdots\cdots + g_r x^r, \tag{3}$$

where

$$g_0 = g_r = 1.$$

Let $d(f)$ denote the degree of a polynomial $f(x)$, and let $E_{g,b}$ denote the set of all polynomials $f(x)$ which are divisible by $g(x)$ and can be written in the form:

$$f(x) = e_1(x) + x^l e_2(x) \not\equiv 0, \tag{4}$$

where $d(e_1) \leq b - 1$, $d(e_2) \leq b - 1$ and $l \geq b$. Let $N(g, b)$ be defined by

$$N(g, b) = \min_{f \in E_{g,b}} d(f). \tag{5}$$

Then, the following lemma is known.[8]

Lemma 1: A shortened cyclic code generated by $g(x)$ can simultaneously correct every burst-error of length b or less, if and only if

$$n \leq N(g, b). \tag{6}$$

Now, consider a matrix $M = (m_{ij})$ over $GF(2)$. Let $M^{(l)}$ be the matrix obtained as the intersection of the first l rows and the first $l + \sigma$ columns of M, and let $L(M)$ be the largest of all the integers L such that for any l less than $L + 1$,

$$\text{rank of } \quad M^{(l)} = l. \tag{7}$$

Associated with generator $g(x)$, an infinite matrix will be defined as

$$M_g = \begin{bmatrix} g_b & g_{b+1} & \cdots & g_r & 0 & 0 & \cdots \\ g_{b-1} & g_b & \cdots & g_{r-1} & g_r & 0 & \cdots \\ \vdots & & \ddots & & & & \\ g_0 & g_1 & & & & & \\ 0 & g_0 & & & & & \\ 0 & 0 & & & & & \\ \vdots & \vdots & & & & & \end{bmatrix}. \tag{9}$$

Now, we have Theorem 1.

Theorem 1: The following equation holds.

$$N(g, b) = L(M_g) + r. \tag{10}$$

Theorem 2: $L(M_g)$ can be found through the following sequential procedures:

1) Set

$$\bar{M}_0 = \underbrace{\begin{bmatrix} g_b & g_{b+1} & \cdots & g_i & \cdots & g_r \\ g_{b-1} & g_b & & & \ddots & \vdots \\ \vdots & & \ddots & & & \vdots \\ g_0 & & & \ddots & & g_i \\ 0 & \ddots & & & \ddots & \vdots \\ \vdots & & \ddots & & & \vdots \\ 0 & 0 & g_0 & & \cdots & g_b \end{bmatrix}}_{b+\sigma+1} \Big\} b + \sigma + 1$$

2) Suppose that

$$\bar{m}_{iJ}^{(\nu)} = 1, \qquad 1 \leq J \leq 1 + \sigma,$$

$$\bar{m}_{ij}^{(\nu)} = 0, \qquad 1 \leq j < J,$$

i=1

where $\bar{m}_{ij}^{(\nu)}$ denotes the entry in the ith row and jth column of $\bar{M}_\nu$. Then,

3) Add the first row to every ith row such that

$$\bar{m}_{iJ}^{(\nu)} = 1, \qquad i \geq 2,$$

then

4) Delete the first row and the Jth column, and

5) Set

$$\bar{M}_{\nu+1} = \begin{bmatrix} & & \bar{M}_\nu' & & & g_r \\ & & & & & g_{r-1} \\ & & & & & \vdots \\ 0 & \cdots & 0 & g_0 & g_1 & \cdots & g_b \end{bmatrix},$$

where $\bar{M}_\nu'$ denotes the matrix obtained from $\bar{M}_\nu$ by 3) and 4).

6) If $\bar{m}_{ij}^{(\nu)} = 0$ $(1 \leq j \leq 1 + \sigma)$, then

i=1

$$\nu = L(M_g).$$

ν+1

Source: T. Kasami, "Optimum shortened cyclic codes for burst-error correction," *IEEE Trans. Inform. Theory*, vol. 9, pp. 105-109, 1963.
Note: Typographical errors marked in red.

Double Burst Error Detection Results for CRC-32

TABLE III
DOUBLE-BURST ERROR DETECTING CAPABILITY OF C_n

code length n	burst error length b^*
$11994 \leq n \leq 13000$	9
$5681 \leq n \leq 11993$	10
$1730 \leq n \leq 5680$	11
$731 \leq n \leq 1729$	12
$39 \leq n \leq 730$	13
$33 \leq n \leq 38$	16

* C_n has the capability of detecting any double-burst error which consists of two single-burst errors of length b or less.

Source: T. Fujiwara, T. Kasami and S. Lin, "Error detecting capabilities of the shortened Hamming codes adopted for error detection in IEEE standard 802.3," *IEEE Trans. Commun*., vol. 37, pp. 986-989, Sep. 1989.

New Double Burst Error Detection Results for CRC-32

Code word length n [bit]	Burst error length b [bit]
11994 ≤ n ≤ 49614	9
49615 ≤ n ≤ 1077947	8
1077948 ≤ n ≤ 3932613	7
3932614 ≤ n ≤ 14373575	5 or 6
14373576 ≤ n ≤ 30435038	4
30435039 ≤ n ≤ 376820508	2 or 3

- 2000B (n=16000) Ethernet frames can detect two bursts of length up to 9 bits.
- 9018B jumbo frames (n=72144) can detect two bursts of length up to 8 bits.

Summary

- Presented random error detection properties of Ethernet CRC
- Computed the double burst error detection capability of CRC-32 for MAC frame sizes much larger than 13000 bit
- 2000B Ethernet frames can detect two bursts of length up to 9 bits
- 9018B jumbo frames can detect two bursts of length up to only 8 bits

References

[1] J. L. Hammond, J. E. Brown and S. S. Liu, “Development of a transmission error model and an error control model,” Tech. Rep., Rome Air Develop. Cen., RADC-TR-75-138, May 1975.

[2] T. Fujiwara, T. Kasami and S. Lin, “Error detecting capabilities of the shortened Hamming codes adopted for error detection in IEEE standard 802.3,” *IEEE Trans. Commun*., vol. 37, pp. 986-989, Sep. 1989.

[3] P. Koopman, “32-bit cyclic redundancy codes for internet applications,” *Int. Conf. Dependable Systems and Networks (DSN)*, Washington DC, pp. 459-468, July 2002.

[4] T. Fujiwara, T. Kasami, A. Kitai and S. Lin, “On the undetected error probability for shortened Hamming codes,” *IEEE Trans. Commun*., vol. 33, pp. 570-574, June 1985.

[5] G. Castagnoli, S. Bräuer and M. Herrmann, “Optimization of cyclic redundancy check codes with 24 and 32 parity bits,” *IEEE Trans. Commun*., vol. 41, pp. 883-892, June 1993.

References (cont.)

[6] P. E. Boudreau, W. C. Bergman and D. R. Irvin, "Performance of a cyclic redundancy check and its interaction with a data scrambler," IBM J. Res. Develop., vol. 38, pp. 651-658, Nov. 1994.

[7] R. Walker and R. Dugan, "64b/66b low-overhead coding proposal for serial links," IEEE 802.3 Higher Speed Study Group, Jan. 2000. http://grouper.ieee.org/groups/802/3/10G_study/public/jan00/walker_1_0100.pdf

[8] N. Figueira, "Impact of the $1 + x^{43}$ scrambler on the error detection capabilities of the ethernet CRC," IEEE 802.3 Higher Speed Study Group, July 1999. http://grouper.ieee.org/groups/802/3/10G_study/public/july99/figueira_1_0799.pdf

[9] W. W. Peterson and E. J. Weldon, Jr., *Error-Correcting Codes*, 2nd ed. Cambridge, MA: M.I.T. Press, 1972.

[10] T. Kasami, "Optimum shortened cyclic codes for burst-error correction," *IEEE Trans. Inform. Theory*, vol. 9, pp. 105-109, 1963.

Thank You