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. IEEE 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].
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.

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].


- 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).

<table>
<thead>
<tr>
<th>MAC Frame Type</th>
<th>MAC Frame Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smallest 802.3 frame</td>
<td>64B</td>
</tr>
<tr>
<td>Basic 802.3 frame</td>
<td>1518B</td>
</tr>
<tr>
<td>Largest 802.3 frame</td>
<td>2000B</td>
</tr>
<tr>
<td>Jumbo frame</td>
<td>9018B</td>
</tr>
</tbody>
</table>
Kasami’s Algorithm (1963)

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

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

where

$$g_0 = g_r = 1.$$

Let $d(f)$ denote the degree of a polynomial $f(x)$, and let $E_{b+1}$ denote the set of all polynomials $f(x)$ which are divisible by $g(x)$ and can be written in the form:

$$f(x) = e_s(x) + x^e_0(x) \neq 0,$$ \quad (4)

where $d(e_s) \leq b - 1$, $d(e_0) \leq b - 1$ and $l \geq b$. Let $N(g, b)$ be defined by

$$N(g, b) = \min_{e_s, e_0} d(f).$$ \quad (5)

Then, the following lemma is known.

**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

$$n \leq N(g, b).$$ \quad (6)

Now, consider a matrix $M = (m_{ij})$ over $GF(2)$. Let $M^{(1)}$ 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 $L + 1$,

$$\text{rank of } M^{(1)} = l. \quad (7)$$

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

$$M_0 = \begin{bmatrix}
g_0 & g_{r+1} & \cdots & g_r & 0 & 0 & \cdots 
g_{r+1} & g_0 & \cdots & g_{r-1} & 0 & 0 & \cdots 
\vdots & \vdots & \ddots & \vdots & \ddots & \ddots & \ddots 
g_0 & g_1 & \cdots & g_{r-1} & 0 & 0 & \cdots 
0 & g_0 & \cdots & 0 & 0 & 0 & \cdots 
0 & 0 & \cdots & 0 & 0 & 0 & \cdots 
\vdots & \vdots & \ddots & \vdots & \ddots & \ddots & \ddots
\end{bmatrix}.$$ \quad (9)

Now, we have Theorem 1.

**Theorem 1:** The following equation holds.

$$N(g, b) = L(M_0) + r. \quad (10)$$

**Theorem 2:** $L(M_0)$ can be found through the following sequential procedures:

1) Set

$$M_0 = \begin{bmatrix}
g_0 & g_{r+1} & \cdots & g_r & 0 & 0 & \cdots 
g_{r+1} & g_0 & \cdots & g_{r-1} & 0 & 0 & \cdots 
\vdots & \vdots & \ddots & \vdots & \ddots & \ddots & \ddots 
g_0 & g_1 & \cdots & g_{r-1} & 0 & 0 & \cdots 
0 & g_0 & \cdots & 0 & 0 & 0 & \cdots 
0 & 0 & \cdots & 0 & 0 & 0 & \cdots 
\vdots & \vdots & \ddots & \vdots & \ddots & \ddots & \ddots
\end{bmatrix}.$$ \quad (11)

2) Suppose that

$$\overline{m_{i,j}} = 1, \quad 1 \leq J \leq 1 + \sigma, \quad i = 1$$

$$\overline{m_{i,j}} = 0, \quad 1 \leq j < J,$$

where $\overline{m_{i,j}}$ denotes the entry in the $i$th row and $j$th column of $M_0$. Then,

3) Add the first row to every $i$th row such that

$$\overline{m_{i,j}} = 1, \quad i \geq 2,$$

then

4) Delete the first row and the $J$th column, and

5) Set

$$\tilde{M}_{i+1} = \begin{bmatrix}
\tilde{M}_i & g_j \\
0 & g_0 & \cdots & g_r \cdot 0 & 0 & \cdots 
\vdots & \vdots & \ddots & \vdots & \ddots & \ddots & \ddots
\end{bmatrix},$$

where $\tilde{M}_i$ denotes the matrix obtained from $M_0$ by 3) and 4).

6) If $\overline{m_{i,j}} = 0 (1 \leq j \leq 1 + \sigma)$, then

$$r = L(M_0).$$


Note: Typographical errors marked in red.
Double Burst Error Detection Results for CRC-32

TABLE III
DOUBLE-BURST ERROR DETECTING CAPABILITY OF $C_n$

<table>
<thead>
<tr>
<th>code length $n$</th>
<th>burst error length $b^*$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$11994 \leq n \leq 13000$</td>
<td>9</td>
</tr>
<tr>
<td>$5681 \leq n \leq 11993$</td>
<td>10</td>
</tr>
<tr>
<td>$1730 \leq n \leq 5680$</td>
<td>11</td>
</tr>
<tr>
<td>$731 \leq n \leq 1729$</td>
<td>12</td>
</tr>
<tr>
<td>$39 \leq n \leq 730$</td>
<td>13</td>
</tr>
<tr>
<td>$33 \leq n \leq 38$</td>
<td>16</td>
</tr>
</tbody>
</table>

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

New Double Burst Error Detection Results for CRC-32

<table>
<thead>
<tr>
<th>Code word length n [bit]</th>
<th>Burst error length b [bit]</th>
</tr>
</thead>
<tbody>
<tr>
<td>$11994 \leq n \leq 49614$</td>
<td>9</td>
</tr>
<tr>
<td>$49615 \leq n \leq 1077947$</td>
<td>8</td>
</tr>
<tr>
<td>$1077948 \leq n \leq 3932613$</td>
<td>7</td>
</tr>
<tr>
<td>$3932614 \leq n \leq 14373575$</td>
<td>5 or 6</td>
</tr>
<tr>
<td>$14373576 \leq n \leq 30435038$</td>
<td>4</td>
</tr>
<tr>
<td>$30435039 \leq n \leq 376820508$</td>
<td>2 or 3</td>
</tr>
</tbody>
</table>

- 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 (cont.)


Thank You