Study of Undetected Error Probability of IEEE 802.3 CRC-32 code for MTTFPA analysis

Dunia Prieto
Rubén Pérez-Aranda
rubenpda@kdpof.com

IEEE 802.3bv Task Force - January 2015

Objectives

- We are interested to study the Undetected Error Probability (P_{ue}) of the 802.3 CRC used to compute the FCS field of the Ethernet frame
- We will show that the 802.3 CRC behaves pretty well as a proper CRC code, therefore, the P_{ue} is bounded by $P_{ue} \leq 2^{-32}$ for any input bit error probability $0 < p \leq 0.5$ and length of Ethernet frame ≥ 64 bytes
- This property of the 802.3 CRC code will be used for MTTFPA analysis of coded-modulations for GEPOF

CRCs - background

- Cyclic redundancy check (CRC) codes are shortened binary cyclic codes that are widely used for error detection on digital communication links and data storage

- In order to detect errors in an information block of k bits $i = [i_0, i_1, ..., i_{k-1}]$, a block $r = [r_0, r_1, ..., r_{m-1}]$ of m parity bits is added (the CRC field), yielding a codeword c = [i, r] consisting of n = k + m binary digits

- The block r of parity bits is computed from i, using a linear feedback shift register (LFSR) in such a way that $r(x) \equiv (x^m \cdot i(x)) \bmod g(x)$, where $i(x) = i_0 + i_1 x + ... + i_{k-1} x^{k-1}$ and $r(x) = r_0 + r_1 x + ... + r_{m-1} x^{m-1}$ are the information and parity bits, respectively, interpreted as polynomials, and where g(x) is the generator polynomial of the code implemented in the LFSR

- Error detection at the receiving end is made by computing the parity bits from the received information block, and comparing them with the received parity bits. An error is declared to have occurred if the received CRC and computed CRC values are not equal

Error detection properties of CRCs

- To measure the degree of goodness of an (n,k) CRC code C generated by g(x) we have to investigate about two properties:
  - **Minimum distance (d_{min}) of the code:** Minimum Hamming distance between all distinct pair of codewords $\rightarrow$ codewords differ in at least d_{min} positions
    - A code with minimum distance d_{min} can detect all error patterns of weight less than or equal to (d_{min}-1)
  - **Undetected error probability (P_{ue}):** Probability that an error occurs during transmission that cannot be detected by the decoder
    - An undetectable error pattern e can also be viewed as one transforming a given codeword c into a different codeword c' = c + e. This is only possible when the error pattern is a codeword by itself (because of the linearity of the code)
    - The undetected error probability is thus the probability that channel noise produces an error pattern equal to a nonzero codeword of the CRC code
    - For a binary symmetric channel (BSC) with bit error probability p, the probability of undetected errors for the code C is given by:

$$P_{ue}(C,p) = \sum_{j=d_{\min}}^{n} A_j p^j (1-p)^{n-j}, \text{ where } A_j \text{ is the number of codewords of weight } j$$

    - On a low-noise BSC, which tends to produce low-weight error patterns more frequently than error patterns with a large Hamming weight, it thus appears reasonable to use a CRC code that has a maximum minimum distance $\rightarrow$ d_{min} does dominate the undetected error probability on low-noise BSCs

Undetected error probability of CRCs (1/2)

- The most important expectation from a CRC code is a very low probability for undetected errors
  - P_{ue} is the popular appraisal parameter to decide whether CRCs are good or proper
- The probability for undetected errors depends on the generator polynomial g(x), the bit error probability p and the codeword length n
  - Choice of generator polynomial g(x) is a critical parameter for the performance of a CRC
- To compute the exact value of P_{ue} we need to know the weight distribution of the code. Unfortunately the determination of this distribution is a computationally hard problem and it is known only for a very small number of codes.
- If the errors on the channel occur randomly with p = 0.5, then P_{ue} is equal to $2^{-(n-k)} - 2^{-n} \sim 2^{-(n-k)}$
  - This stems from the fact that with p = 0.5, all 2^n received words are equally likely and out of them $2^k - 1$ will be accepted as valid codewords although they are different from the codeword transmitted

Undetected error probability of CRCs (2/2)

- In general, it is not necessary true that $P_{ue}(C,p) \le P_{ue}(C,0.5)$ for p<0.5
  - CRC codes do not necessarily obey the $2^{-(n-k)}$ bound
- A CRC code is said to be proper if P_{ue} is monotonically increasing in p for $0 \le p \le 0.5$

IEEE 802.3 CRC CODE (1/4)

- According to the IEEE Ethernet Standard 802.3, a 32-bit CRC is calculated and appended to an Ethernet frame prior to transmission
- The generator polynomial of these codes is

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

  which is a primitive polynomial of degree 32
- The code length n should be a multiple of 8 with $512 \le n \le 12144$ bits for the frame format of MAC (Media Access Control) sublayer of the data link layer for the Ethernet
- Fortunately, the error detecting capabilities of the CRC-32 IEEE 802.3 have been well studied in the literature: $P_{ue}(C, p < 0.5) \le 2^{-32}$ for $512 \le n \le 12144$

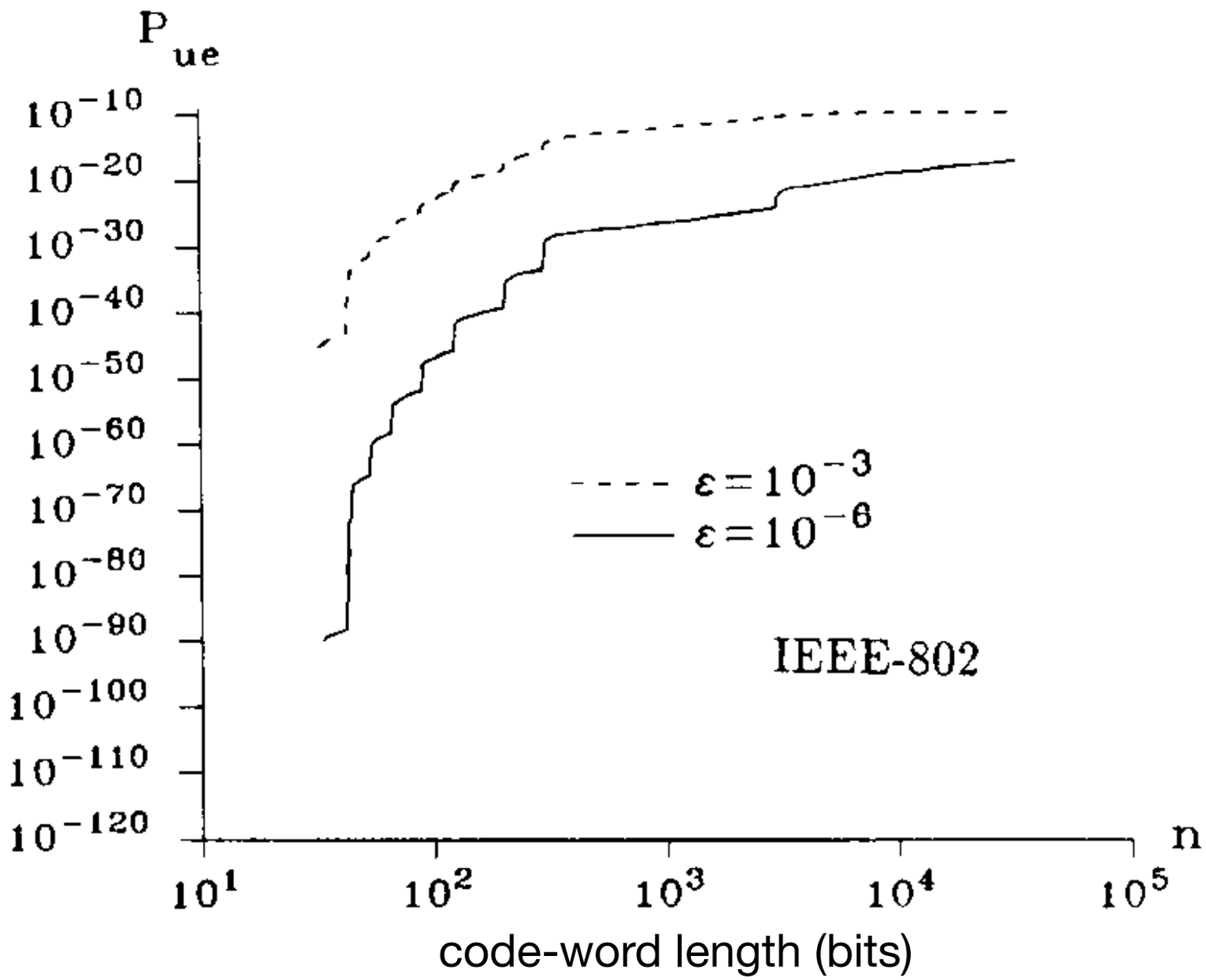
IEEE 802.3 CRC CODE (2/4)

- d_{min} profile for the standard 802.3 CRC-32 code [Fujiwara89] [Koopman02]

code length n	$d_{min}(n)$
3007,...,12144	4
301,...,3006	5
204,...,300	6
124,...,203	7
90,...,123	8
67,...,89	9
54,...,66	10
45,...,53	11
43,...,44	12
33,...,42	15

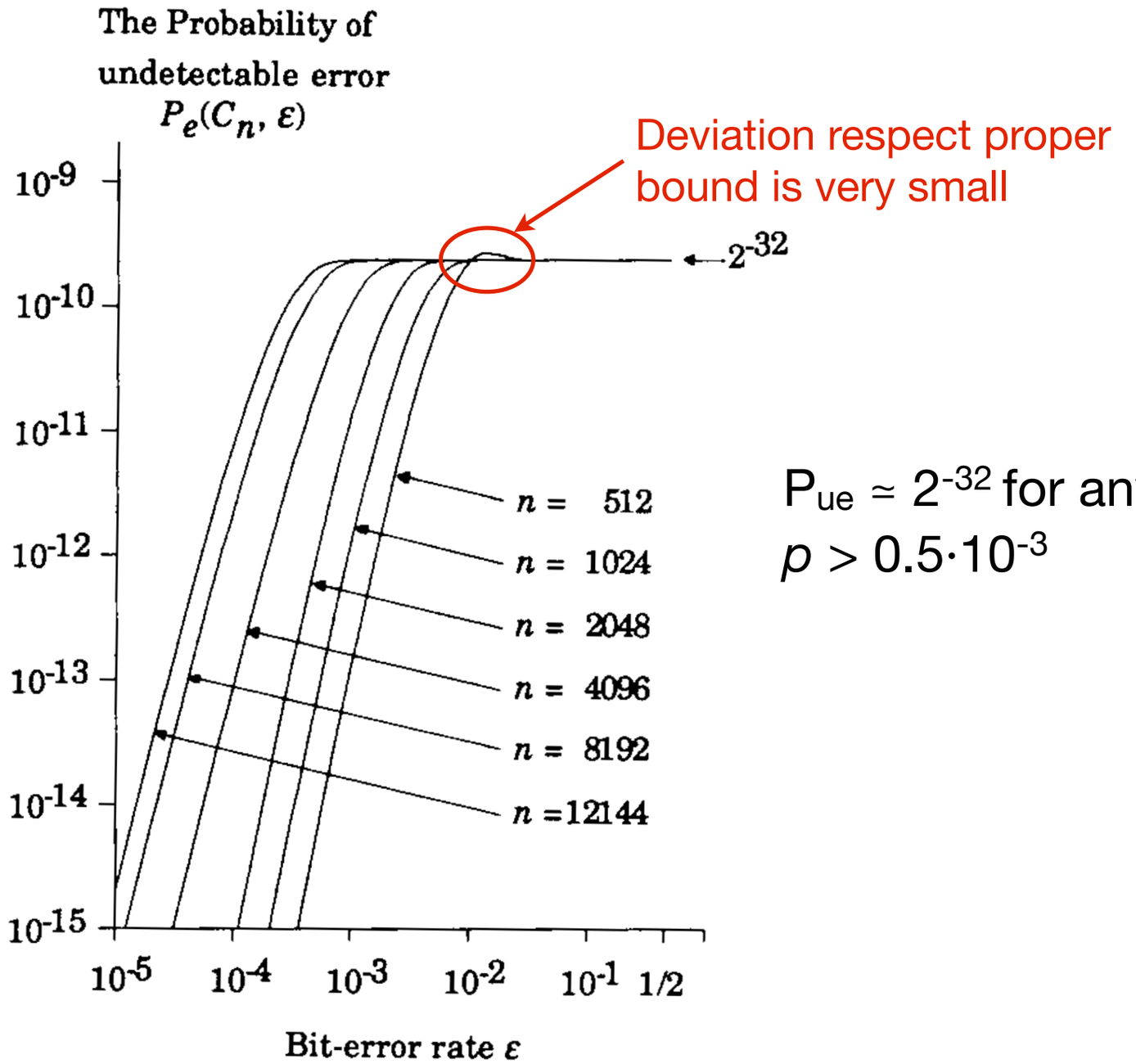
IEEE 802.3 CRC CODE (3/4)

- $P_{ue}(n)$ versus n for the IEEE-802 code on the BSC's with $p = 10^{-3}$ and $p = 10^{-6}$ [Castagnoli93]



IEEE 802.3 CRC CODE (4/4)

- $P_{ue}(p)$ versus p for the IEEE-802 code on the BSC's for $n = 2^i$ with $9 \le i \le 13$ and n = 12144 [Fujiwara89]



$P_{ue} \simeq 2^{-32}$ for any n and $p > 0.5 \cdot 10^{-3}$

Conclusion

- The 802.3 CRC approximates pretty well the performance of a proper CRC code, therefore, the undetected error probability (P_{ue}) is bounded by $P_{ue} \leq 2^{-32}$ for any input bit error probability $0 < p \leq 0.5$ and length of Ethernet frame ≥ 64 bytes

References

- [Castagnoli93] G. Castagnoli, S. Bräuer and M. Herrmann. “Optimization of Cyclic Redundancy-Check Codes with 24 and 32 Parity Bits”. *IEEE Transactions on Communication*s, vol. 41, no. 6, pp. 883-892, June 1993.

- [Fujiwara89] 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 Transactions on Communications*, vol. 37, no. 9, pp. 986-989, September 1989.

- [Koopman02] P. Koopman. “32-Bit Cyclic Redundancy Codes for Internet Applications”. *International Conference on Dependable Systems and Networks (DSN)*, pp. 459-468, July 2002.

Questions?