Probability of Undetected Error with Redundant Data Transmission on a Binary Symmetric Channel without Memory

BÖRCSÖK J., HÖLZEL J., WACKER H. D.
Development
HIMA Paul Hildebrandt GmbH + Co KG
Albert-Bassermann-Strasse 28, D-68782 Bruehl
GERMANY
http://www.hima.com

Abstract: - This paper investigates redundant data transmission on binary symmetric channels without memory protected by a linear code and the probability of undetected error. A simple formula suitable for numerical calculations is proved, improving a commonly used formula. A second formula for data transmission without cross check is given. The formula is applied to some frequently used CRC-16 polynomials with well known minimum distance to calculate block lengths maximal in order to achieve a specific Safety Integrity Level (SIL).

Key-Words: - Linear Code, CRC, BSC, Probability Of Undetected Error, Bit Error Rate, Weight Distribution, Block length, Redundant Data Transmission, Cross Check, SIL

1 Introduction

Let there be given a binary symmetric channel without memory, a bit-error rate ε and a transmission procedure protected by a linear code C (i.e. a checksum procedure). Imagine for example a cyclic redundancy check CRC. Not the only one but a good measure for the performance of the code is the probability of undetected error (see [9]):

$$p_{ue}(\varepsilon, C) = \sum_{l=1}^{n} A_l \varepsilon^l (1-\varepsilon)^{n-l} \tag{1}$$

where

$A_l = \textit{weight distribution of } C$

$= \textit{number of code words of weight } l$

(weight of a code word = number of bits equal to 1)

$\varepsilon = \textit{bit error probability}$

$n = \textit{block length}$

In case of a poor (large) bit error probability a frequently used method to improve the performance of C is redundant (μ-fold) data transmission together with cross check in the receiving device.

2 Data Protection by the Use of Linear Codes and μ-fold Data Transmission

Each code word or block consists of a message to which a checksum is attached:

$$c = (m_1, \ldots, m_k, s_0, \ldots, s_{r-1})$$

Consider now a communication procedure transmitting each block twice and a linear code C performed separately on each of the two blocks. Further on, the receiving device is performing a cross check between both blocks (incl. both checksums). A block is accepted if only if there is no checksum fault and the two blocks inclusive checksum are identical.

Mathematically spoken this means that we defined a new Code $C^{(2)}$ consisting of the code words

$$\boldsymbol{c} = (m_1, \ldots, m_k, s_0, \ldots, s_{r-1}, m_1, \ldots, m_k, s_0, \ldots, s_{r-1}) .$$

More generally: A μ-fold transmission procedure together with μ-fold protection by a checksum is characterized by a code $C^{(\mu)}$ defined by its code words

$$\boldsymbol{c} = (\underbrace{m_1, \ldots, m_k, s_0, \ldots, s_{r-1}, \ldots, m_1, \ldots, m_k, s_0, \ldots, s_{r-1}}_{\mu}) ,$$

that is

$$C^{(\mu)} = \{(\underbrace{x, \ldots, x}_{\mu}) : x \in C\} . \tag{2}$$

$C^{(\mu)}$ has to be carefully distinguished from the Cartesian product

$$C^{\mu} = \{(x_1, \ldots, x_\mu) : x_1, \ldots, x_\mu \in C\} .$$

The elements of $C^{(\mu)}$ and C^{μ} are typed in bold letters.

The problem is now to find a relationship between

$$p_{ue}(\varepsilon, C) \;\; and \;\; p_{ue}(\varepsilon, C^{(\mu)}) .$$

A commonly used formula for the probability of undetected error with redundant transmission is given by (see [2]):

$$p_{ue}(\varepsilon, C^{(\mu)}) \le p_{ue}(\varepsilon, C)^{\mu} . \tag{3}$$

Normally deduced by heuristic arguments, equation (3) proves to be true. In section 3 we shall prove an exact formula for

$$p_{ue}(\varepsilon, C^{(\mu)})$$

improving and implicating (3). The new formula too will be suitable for numeric calculations.

3 The Probability of Undetected Error

3.1 The Main Result

At first let us state our main result: Theorem 1 will give a formula for $p_{ue}(\varepsilon, C^{(\mu)})$.

Theorem 1: The probability of undetected error of $C^{(\mu)}$ is given by

(4) $$p_{ue}(\varepsilon, C^{(\mu)}) = \sum_{l=1}^{n} A_l \varepsilon^{\mu l} (1-\varepsilon)^{\mu(n-l)}$$

Proof: Let $x, y \in C$ be code words then, in the course of the proof, we shall use some notations:

$p(y|x) =$ *probability that y is received, provided x is sent*

$d(x,y) =$ *Hamming distance between x and y* $=$ *number of bits in which x and y differ*

Then, by the formula of the total probability, we get

$$\begin{aligned}
p_{ue}(\varepsilon, C^{(\mu)}) &= \sum_{\mathbf{x}\in C^{(\mu)}} \Big(\sum_{\mathbf{y}\in C^{(\mu)}\setminus\{\mathbf{x}\}} p(\mathbf{y}|\mathbf{x}) \Big) p(\mathbf{x}) \\
&= \sum_{x\in C} \Big(\sum_{y\in C\setminus\{x\}} p(y|x)^{\mu} \Big) p(x) \\
&= \sum_{x\in C} \Big(\sum_{y\in C\setminus\{x\}} (\varepsilon^{d(y,x)}(1-\varepsilon)^{n-d(y,x)})^{\mu} \Big) \frac{1}{|C|} \\
&= \sum_{x\in C} \Big(\sum_{y\in C\setminus\{x\}} \varepsilon^{\mu d(y,x)} (1-\varepsilon)^{\mu(n-d(y,x))} \Big) \frac{1}{|C|} \\
&= \sum_{x\in C} \Big(\sum_{l=1}^{n} \Big(\sum_{\substack{y\in C \\ d(y,x)=l}} \varepsilon^{\mu l} (1-\varepsilon)^{\mu(n-l)} \Big) \Big) \frac{1}{|C|} \\
&= \sum_{x\in C} \Big(\sum_{l=1}^{n} \Big(\sum_{\substack{y\in C \\ d(y,x)=l}} 1 \Big) \varepsilon^{\mu l} (1-\varepsilon)^{\mu(n-l)} \Big) \frac{1}{|C|} \\
&= \sum_{x\in C} \left(\sum_{l=1}^{n} A_l \varepsilon^{\mu l} (1-\varepsilon)^{\mu(n-l)} \right) \frac{1}{|C|} \\
&= \sum_{l=1}^{n} A_l \varepsilon^{\mu l} (1-\varepsilon)^{\mu(n-l)}
\end{aligned}$$

∎

Corollary 1 states that the performance of the code $C^{(\mu)}$ at a bit-error rate ε is at least as good as the performance of the code C at a bit-error rate of ε^{μ}.

Corollary 2: We have

(5) $$p_{ue}(\varepsilon, C^{(\mu)}) \le p_{ue}(\varepsilon^{\mu}, C).$$

Proof: By induction for μ = 1, 2, 3, ... we get

$$(1-\varepsilon)^{\mu} \le 1-\varepsilon^{\mu},$$

and therefore we have

$$\begin{aligned}
p_{ue}(\varepsilon, C^{(\mu)}) &= \sum_{l=1}^{n} A_l \varepsilon^{\mu l} (1-\varepsilon)^{\mu(n-l)} \\
&\le \sum_{l=1}^{n} A_l (\varepsilon^{\mu})^{l} (1-\varepsilon^{\mu})^{n-l} \\
&= p_{ue}(\varepsilon^{\mu}, C).
\end{aligned}$$

∎

Corollary 2 is the well known result mentioned in section 2:

Corollary 3: We have

(6) $$p_{ue}(\varepsilon, C^{(\mu)}) \le p_{ue}(\varepsilon, C)^{\mu}.$$

Proof: Elementary calculus. ∎

In the situation of Theorem 1 a code word $\boldsymbol{x} \in C^{(\mu)}$ is sent, and the checksum procedure together with the cross check guarantee that the received $\boldsymbol{y}$ again lies in $C^{(\mu)}$. What happens if we only check whether $\boldsymbol{y}$ lies in the Cartesian product C^{μ}? This means that only the checksums are verified and no cross check is done. One might expect, that (6) is true even without cross check. Unfortunately Theorem 4 states that this is not true.

Theorem 4: The probability of undetected error of C^{μ} is given by

(7) $$p_{ue}(\varepsilon, C^{\mu}) = ((1-\varepsilon)^n + p_{ue}(\varepsilon, C))^{\mu} - (1-\varepsilon)^{\mu\cdot n}.$$

Proof: Similar to the proof of Theorem 1 by means of the multinomial theorem we get:

$$\begin{aligned}
p_{ue}(\varepsilon, C^{\mu}) &= \sum_{\boldsymbol{x}\in C^{(\mu)}} \Big(\sum_{\boldsymbol{y}\in C^{\mu}\setminus\{\boldsymbol{x}\}} p(\boldsymbol{y}|\boldsymbol{x}) \Big) p(\boldsymbol{x}) \\
&= \sum_{x\in C} \Big(\sum_{(y_1,\ldots,y_\mu)\in C^{\mu}\setminus\{(x,\ldots,x)\}} \prod_{k=1}^{\mu} p(y_k|x) \Big) p(x) \\
&= \sum_{x\in C} \Big(\sum_{y_1,\ldots,y_\mu\in C} \prod_{k=1}^{\mu} p(y_k|x) - p(x|x)^{\mu} \Big) p(x) \\
&= \sum_{x\in C} \Big(\Big(\sum_{y\in C} p(y|x) \Big)^{\mu} - p(x|x)^{\mu} \Big) p(x) \\
&= \sum_{x\in C} \Big(\Big(\sum_{l=0}^{n} A_l \varepsilon^{l} (1-\varepsilon)^{n-l} \Big)^{\mu} - (1-\varepsilon)^{\mu\cdot n} \Big) p(x) \\
&= ((1-\varepsilon)^n + p_{ue}(\varepsilon, C))^{\mu} - (1-\varepsilon)^{\mu\cdot n}
\end{aligned}$$

∎

In fact, (6) is not true for redundant transmission without cross check:

$$p_{ue}(\varepsilon, C^{\mu}) = ((1-\varepsilon)^n + p_{ue}(\varepsilon, C))^{\mu} - (1-\varepsilon)^{\mu \cdot n}$$
$$= p_{ue}(\varepsilon, C)^{\mu} + \sum_{k=1}^{\mu} \binom{n}{k} (1-\varepsilon)^{nk} p_{ue}(\varepsilon, C)^{\mu-k}$$
$$> p_{ue}(\varepsilon, C)^{\mu} \quad for\ \varepsilon < 1$$

Theorem 4 is only of theoretical interest, because redundant transmission without cross check normally makes no sense.

3.2 Safety Integrity Levels

Let us now have a closer look at data integrity according to IEC 68508 and analyze the effect of redundant transmission on maximal block lengths feasible for a specific Safety Integrity Level (SIL). Our calculations are based on the results about three CRC-16 C_1, C_3 and C_5 generated by polynomials g_1, g_3 and g_5 analyzed in [4].

$$C_1 : g_1 = x^{16} + x^{13} + x^{12} + x^{11} + x^{10} + x^8 + x^6 + x^5 + x^2 + 1,$$

$$C_3 : g_3 = x^{16} + x^{14} + x^{12} + x^{11} + x^8 + x^5 + x^3 + x + 1$$

and

$$C_5 : g_5 = x^{16} + x^{15} + x^{13} + x^9 + x^7 + x^6 + x^5 + x^3 + x + 1$$

C_1 is optimal for a minimum distance (Hamming distance) of $d = 6$, C_3 is optimal for $d = 5$ and C_5 is suitable for long block lengths. They are exemplary for a lot of other CRCs for which similar results are known. We did not check the rest of the CRC-16 treated in [4], because they are not proper for all block lengths, which means that $p_{ue}(\varepsilon, C)$ is not an increasing function of $\varepsilon \in [0,1/2]$. This means that a specific SIL being achieved for one ε could be violated for another smaller one, and more detailed inspections would be necessary.

According to IEC 68508 the quantity Λ of undetected errors per hour is given by

$$\Lambda = 3600 \cdot p_{ue}(\varepsilon, C) \cdot \upsilon \cdot (m-1) \cdot 100$$

where

$\nu = number\ of\ safety\ related\ messages\ per\ second$

$m = number\ of\ communicating\ devices$

$100 = 1\%\text{-}rule$

For an example we decided to choose a relatively small ν because for bigger ν not all of the higher Safety Integrity Levels would be feasible. So for $\nu = 1$ and $m = 1$, we get

(8) $$\Lambda = 3{,}6 \cdot 10^5 \cdot p_{ue}(\varepsilon, C)$$

If no details are known about the quality of the transmission especially about the electromagnetic compatibility (EMC) and nothing can be said about the bit error rate ε, the German TÜV requires to do all calculations concerning Λ with $\varepsilon = 10^{-2}$. Therefore for our analysis we took account of this bad value of the bit error rate. With the help of (8) and Theorem 1 the content of tables 1, 2 and 3 can be derived from the results in [4]. For our calculations we used the so called worst case formula

$$p_{ue}(\varepsilon, C) = \sum_{l=d}^{n} \binom{n}{l} \varepsilon^l (1-\varepsilon)^{n-l},$$

where d is the minimum distance of the CRC, and the results on d published in [4].

The tables below list the block lengths maximal in order to meet a specific Safety Integrity level (SIL) with C_1, C_3 and C_5. Column 2 is taken from [8]. It contains the bounds on Λ for a specific Safety Integrity Level (SIL). Columns 3 and 4 contain the bounds on n for the single transmission mode respectively the double transmission. If the weight distribution of a code is completely known, better values of maximal block lengths are to be expected. Since the authors of [4] did not publish the weight distributions of their CRCs, we had to restrict our calculations to only making use of the minimum distances at different block lengths published in [4]. But for a demonstration of the effect of redundancy this should be sufficient.

Table 1: Maximal block lengths for g_1

SIL	Λ high demand	n_{max} for single transmission	n_{max} for single transmission
4	10^{-8}	22	151
3	10^{-7}	22	151
2	10^{-6}	22	151
1	10^{-5}	23	151

Table 2: Maximal block lengths for g_3

SIL	Λ high demand	n_{max} single transm.	n_{max} double transm.
4	10^{-8}	23	247
3	10^{-7}	24	257
2	10^{-6}	26	257
1	10^{-5}	26	257

Table 3: Maximal block lengths for g_5

SIL	Λ high demand	n_{max} single transm.	n_{max} double transm.
4	10^{-8}	22	76
3	10^{-7}	27	126
2	10^{-6}	27	211
1	10^{-5}	27	353

More results with various CRCs about the size of the undetected error probability and their minimum distances as a function of the block length can be found

in [1], [3], [5], [6], [7],and [10]. With all these results, tables similar to those presented here, can be derived.

4 Conclusions

This paper contains two formulas for the probability of undetected error of redundant data transmission protected by a linear code on the binary symmetric channel without memory. A normally used formula is improved. Using results in [4], the effect of redundant transmission on maximal block lengths for achieving a specific Safety Integrity Level is investigated.
The results are suitable for numerical calculations. They can be applied to CRCs with known minimum distances at different block lengths.

References:

[1]Baicheva, T., Dodunekov, S., Kazakov, P., *Undetected error probability performance of cyclic redundancy-check codes of 16-bit redundancy,* IEE Proc.- Commun., Vol. 147, No. 5, October 2000.

[2]Berufsgenossenschaft der Elektrotechnik und Feinmechanik, Fachausschuss Elektrotechnik, *SCHLUSSENTWURF Vorschlag eines Grundsatzes für die Prüfung und Zertifizierung von „Bussystemen für die Übertragung sicherheitsrelevanter Nachrichten“, Köln 2001*

[3]Castagnoli, G., Braeuer, S. & Herrman, M., *Optimization of Cyclic Redundancy-Check Codes with 24 and 32 Parity Bits,* IEEE Trans. on Communications, Vol. 41, No. 6, June 1993.

[4]Castagnoli, G., Ganz, J. & Graber, P., *Optimum Cyclic Redundancy-Check Codes with 16-Bit Redundancy,* IEEE Trans. on Communications, Vol. 38, No. 1, 1990, pp. 111-114.

[5]Fujiwara, T., Kasami, T., Lin, S., *Error Detecting Capabilities of the Shortened Hamming Codes Adopted for Error Detection in IEEE Standard 802.3,* IEEE Trans. on Communications, Vol. 37, No. 9, Sept. 1989.

[6]Fujiwara, T., Kasami, T., Lin, S., *On the Undetected Error Probability for Shortened Hamming Codes,* IEEE Trans. on Communications, Vol. COM-33, No. 6, Sept. 1985.

[7]Funk, G., *Determination of Best Shortened Linear Codes,* IEEE Trans. on Communications, Vol. 4, No. 1, Jan. 1996.

[8]IEC 61508, *International Standard 61508: Functional safety of electrical/electronic/ Programmable electronic safety-related systems*, Geneva, International Electrotechnical Commission, 2000

[9]W. W. Peterson, E. J. Weldon, *Error Correcting Codes,* The MIT Press Cambridge, Massachusetts , and London, England, Second Edition 1972..

[10]Wolf, J.K., Blakeney, R.D., *An exact Evaluation of the Probability of Undetected Error for certain Shortened Binary CRC Codes,* Qual.Comm, Inc., San Diego, CA 92121. Proc. Milcom IEEE 1988.