Check Sum Optimization for Transmission and Storage of Digital Information

N.G. Bardis[1,2], A. Drigas[1], A.P. Markovskyy[3], and I. Vrettaros[1]

[1] National Centre for Scientific Research "Demokritos", Institute of Informatics & Telecommunications - Net Media Lab, Terma Patriarchou Grigoriou & Neapoleos 27, Ag.Paraskevi - Athens, 15310, Greece
bardis@ieee.org,
dr@imm.demokritos.gr,
jvr@imm.demokritos.gr
[2] Hellenic Army Academy, Department of Mathematics and Engineering Science, Hellenic Army Academy, Vari, Greece
[3] National Technical University of Ukraine, Department of Computer Engineering, 37, Peremohy, pr. Kiev 252056, KPI 2003, Ukraine
markovskyy@mail.ru

Abstract. In this paper a new approach to increase the effectiveness of the errors detection using check sum during the data transmission based on the optimization of coding with special differential Boolean transformations is proposed. A method for obtaining such transformations are developed and examples of coding for check sum functions is given.

1 Introduction

The present level of computer networks and telecommunication systems development is inseparably connected with the problem information integrity, which includes: the ensuring of high reliability during information transmission and the information storage in memories. The dynamic expansion of using the communication channels which undergo potentially interferences and the complex methods of packing the transferred information are combined with the increase of appearing errors during the data transmission. A similar situation occurs also during the storage of data on magnetic means: a constant increase in the longitudinal and transverse density of information storage on such means is also combined with an increase of appearing errors [Klove 2007].

At the same time, the extensive usage of information technologies in all human activities, including in these IT's and the technogenic risks, requires the increasing in the reliability of all components of the computer systems, including the reliability during the transmission and the storage of information [Saxena et all, 1987]. A continuous increase in the speeds of data transmission in the telecommunications network systems dictates the stringent requirements for the effectiveness of the means of error

M.D. Lytras et al. (Eds.): WSKS 2010, Part I, CCIS 111, pp. 582–590, 2010.

control. This effectiveness must be commensurate with the channel characteristics as the bandwidth and the rate of transmitted data. This condition determines the needs for a radical increase of the error control reliability of the means of error control. These means should have an increased speed and allow the parallel processing in hardware implementation.

Thus, these characteristics specify the urgency and practical importance of the new development and the improvement of the known means for the increase of reliability during the data transmission and data storage in the computer systems and telecommunications networks.

2 Analysis of the Error Detection Problems during the Transmission and Storage of the Digital Information

The present level of computer networks and telecommunication systems development is inseparably connected with the problem information integrity, which includes: the ensuring of high reliability during information transmission and the information storage in memories. The dynamic expansion of using the communication channels which undergo potentially interferences and the complex methods of packing the transferred information are combined with the increase of appearing errors during the data transmission. A similar situation occurs also during the storage of data on magnetic means: a constant increase in the longitudinal and transverse density of information storage on such means is also combined with an increase of appearing errors [Klove 2007].

At the same time, the extensive usage of information technologies in all human activities, including in these IT's and the technogenic risks, requires the increasing in the reliability of all components of the computer systems, including the reliability during the transmission and the storage of information [Saxena et all, 1987]. A continuous increase in the speeds of data transmission in the telecommunications network systems dictates the stringent requirements for the effectiveness of the means of error control. This effectiveness must be commensurate with the channel characteristics as the bandwidth and the rate of transmitted data. This condition determines the needs for a radical increase of the error control reliability of the means of error control. These means should have an increased speed and allow the parallel processing in hardware implementation.

Thus, these characteristics specify the urgency and practical importance of the new development and the improvement of the known means for the increase of reliability during the data transmission and data storage in the computer systems and telecommunications networks.

For guaranteeing the reliable data transmission in communication channels of computer networks a large number of means is used, of which important place occupies the coding of the transmitted information. In the majority of systems the transmission and the storage of information are carried out by blocks and respectively the integrity data transmission or data storage of each block is controlled separately.

With the use of special coding it is possible to distinguish two approaches for the correction of the appearing errors:

- the error detection by special codes and their correction by retransmitting the block upon request during the error detection (ARQ-Automatic Repeat Request);

- the correction of the appearing errors due to applications of correcting codes without the repeated transmission (FEC-Forward Error Correction).

It is obvious that the first of the mentioned approaches is not applied for the error correction during data storage. The main advantage of ARQ besides the diagrams of the FEC lies in the fact that the error detection requires simpler decoding hardware and smaller redundancy than the error correction method. The implementation of error detection has substantial smaller computational complexity which makes it possible to calculate the error control functions considerably faster. Furthermore, the effectiveness of ARQ is less and depends on the multiplicity of the appearing errors [Shu Lin et all, 1983].

The choice between the two approaches for the elimination of the appearing errors depends on intensity and the nature of the appearing errors. The basic sources of errors in digital data channels are the inter bit interferences, the externally produced noise and the thermal noise of transmission means [Klove 2007].

The nature of the appearing errors depends not only on their source, but also on the type of transmission means and on modulation of signals method. Thus, in the ether communication channels the prevailing source of the transmitted errors is the externally produced noise and in this case the intensity of the appearing errors is sufficiently high so that the application of FEC technologies proves to be more preferable. In the wire systems of digital data transmission, in which the intensity of errors is several orders lower in comparison with the wireless channels, the use of ARQ is considered to be more effective [Fletcher, 1983].

In the cable channels with the sequential data transmission without modulation, the transmitted error has the same nature, and the channels themselves correspond to the binary symmetrical channel model. This model assumes the appearance of erroneous transmission of zero or one with equal probabilities, since the probability pj that j errors occur during the transmission of the n-bit code is determined for the binary symmetrical channel by the expression:

$$p_m = \binom{n}{j} \cdot p^j \cdot (1-p)^{n-j} \tag{1}$$

where p is the probability of the erroneous transmission of one bit.

For errors detection by the per block data transmission the CRC codes and the CS are used more often [Klove 2007]. The CS method in comparison with CRC is substantially simpler and ensures the maximum rate of the error control and it is an influential factor on a constant increase in the channel capacity of data transmission.

In contrast to CRC, the structure of the operations which are performed with the check sum calculation, it allows the parallel process which makes it possible to implement effectively this control by hardware, so that the time for the calculation of error control practically will not affect the performance of the data transmission.

Let us denote by $D_1,D_2,\ldots,D_k$ the k codes with n-bit size, which compose the transmission block, and by $D_1',D_2',\ldots,D_k'$ we denote the blocks on the receiver end. The CS's on the receiver and the sender are calculated with the same way: $S_S = D_1 \oplus D_2 \oplus \ldots \oplus D_k$ and $S_R = D_1' \oplus D_2' \oplus \ldots \oplus D_k'$.

The usual check sum assumes that the data transmission is carried out as a block and organized as k codes $D_1,D_2,\ldots,D_k$ with length n bits. In this case the length n of the code is determined by the architecture of the control organization and its value can coincide with the number of simultaneously transferred bits, and it can differ from it. At the end of the transmission of the data block, the transmitter sends to the receiver the check sum S_S, which is XORed with the check sum that is calculated on the receiver S_R and obtains the differential code $\Delta=S_S \oplus S_R$ of size n. If $\Delta=0$ then we consider that no errors have arisen. For the symmetrical binary channel and, taking into account that in practice the relation $k>> n$ holds, then we can consider that during the transmission of one code only one error can arise. The low reliability of the error detection of the even error multiplicity is the main disadvantage of the check sum. Actually, the most probable occurrence between them is the two-fold error (situation of appearance of single errors in two from k transmitted codes) and the code Δ can attain only n^2 different values of all the 2^n possible. It is means that for the studied model the usual check sum is ineffectively coding of two-fold error. Because of this the probability P_2 of the nondetection of the two-fold error is reasonable high and determined by formula:

$$P_2 = \frac{1}{n} \tag{2}$$

Thus, the reliability level of the error detection when using the check sum can increase due to the coding optimization, i.e., the calculation of check sums on the transmitter and the receiver in the form: $S_S=F(D_1)\oplus F(D_2)\oplus\ldots\oplus F(D_k)$ and $S_R=F(D_1')\oplus F(D_2')\oplus\ldots\oplus F(D_k')$, where F is the function of coding, defined by the system of Boolean functions.

In the paper [Bardis, 2004] an orthogonal system of Boolean functions that satisfy the SAC criterion is used as coding function. In this case, with the appearance of the two-fold error the code Δ has $n!/((n/2)!)^2$ different values and correspondingly the probability of the non detection of the two-fold error substantially decreases in comparison with the usual check sum. Usually these types of Boolean transformations are used in cryptographic algorithms and their design methods have been developed in [Klove 2007]. A Boolean function $f(x_1,\ldots,x_n)$ defined on a set Z of all possible 2^n n-tuples of n variables, satisfies the SAC, if a complement of a single incoming n-tuple data bit changes the output of the Boolean function with probability 50%:

$$\forall j\in\{1,\ldots,n\}:$$
$$\sum_{x_1,\ldots,x_n\in Z}(f(x_1,\ldots,x_j,\ldots,x_n)\oplus f(x_1,\ldots,\overline{x_j},\ldots,x_n))=2^{n-1} \tag{3}$$

If one of the n inputs of the avalanche transformation is changed then half of its outputs will be changed. This means, that there is an "avalanche amplifier" which by changing one of the n-tuple incoming data bit transforms half of the outputs. Because every function of this system satisfies the Avalanche Criterion, these transformations are called "avalanche".

Let's denote with $F(D)$, the Boolean orthogonal avalanche transformation on the n-bits code D. So transformation $F(D)$ consist of orthogonal Boolean functions

$f_1(D),f_2(D),\ldots,f_n(D)$, every of which satisfies the Avalanche Criterion. The length of the transformed code $R=F(D)$ is n bits long, as well. The orthogonality of the $F(D)$ transformation indicates the one-to-one correspondence of codes D and R. The avalanche properties of the $F(D)$ transformation indicate that if one bit of the input code D is changed then, on average, $n/2$ bits of the output code $R=F(D)$ will be changed also.

Example of the Boolean orthogonal avalanche transformation $F(D)$ on the 8-bits code D (n=8) is given from [Bardis N.G, Markovskyy, 2004].

Thus, if a single error appears, then $n/2$ bits of the modified checksum will change. If a second error appears then another $n/2$ bits of the modified checksum will change. It is clear that the probability of the masking interaction of $n/2$ erroneous bit pairs is less than the probability of the masking interaction of a single bit pair.

It has been shown that the probability P_{2f} that the dual bit erors will not be detected in case orthogonal avalanche transformation $F(D)$ using is determined as follows:

$$P_{2f} = \frac{1}{\binom{n}{n/2}} = \frac{((n/2)!)^2}{n!} = \prod_{j=0}^{n/2-1} \frac{j+1}{(n-j)} \tag{4}$$

Thus, the probability of detecting dual errors during block transmission using the checksum control shceme orthogonal avalanche transformation $F(D)$, increases by t_2 times in comparion to the ordinary checksum scheme. The numerical value of the t_2 increase is determined by the formula:

$$t_2 = \prod_{j=1}^{n/2-1} \frac{n-j}{j+1} \tag{5}$$

For example, for n=8, the probability that the dual errors will not be detected is decreased by 8.7 times in comparison to the traditional checksum.

In case orthogonal avalanche transformation $F(D)$ using, with the appearance of the two-fold error the code Δ has $n!/((n/2)!)^2$ different values and correspondingly the probability of the non detection of the two-fold error substantially decreases in comparison with the usual check sum.

However in this case the $n!/((n/2)!)^2$ coding variants of the two-fold error are substantially less than the total number of all possible codes $\Delta - 2^n$ and therefore in this case the optimization of coding is not achieved. Consequently, an increase in the reliability of detection of prevailing type errors by check sum can be achieved due to further optimization of its coding via the selection of corresponding functional transformation.

The purpose of this approach is to increase the reliability of error control by using check sum due to development of the functional transformations which optimize its coding for the prevailing forms of errors in the binary symmetrical channel.

3 Optimization of the Check Sum Coding

For the practical implementation of error detection based on coding check sum optimization for detecting the appearing errors a calculation method of the modified

check sum is proposed, similarly as in work [Bardis and Markovskyy, 2004]. In this proposed method as terms are used codes which are obtained from Boolean transformations over the controlled codes. These Boolean transformations consist of a system of m Boolean functions with n variables:

$$F(D) = \{f_1(D), f_2(D), ..., f_m(D)\} \tag{6}$$

where D is an n-bit code: D={d1,d2,…,dn}, ∀j∈{1,…,n}: dj∈{0,1}.

With the appearance of a single error in the jth bit of the code Di it is transformed into Di′={d1,…,dj⊕1,…,dn} and the differential Δ of the check sum can be represented in the form of the differentials values of the functions f1,f2,…,fm with the variable dj on the binary tuples {d1,d2,…,dj-1,dj+1,…,dn}:

$$\begin{aligned} &\Delta = F(D_i) \oplus F(D_i^{'}) = \\ &\{f_1(D_i) \oplus f_1(D_i'), ..., f_m(D_i) \oplus f_m(D_i')\} = \\ &= \{\frac{\partial f_1}{\partial d_j}, \frac{\partial f_2}{\partial d_j}, ..., \frac{\partial f_m}{\partial d_j}\} \end{aligned} \tag{7}$$

The optimization of single error coding in the modified *m* bits check sum can be achieved, if the number of possible values of the code of Δ equals 2^m. Since the number of versions of the single error localization in the code *D* is equal to *n*, so that the single error could be one way coded by check sum it is enough that $m = \lceil \log_2 n \rceil$ holds. In this case the binary code formed by a change in the functions with the appearance of error in the jth bit of the code *D*, i.e., with a change in the variable d_j, is equal to j-1:

$$\forall j \in \{1,...,n\}: \sum_{t=0}^{\lceil \log_2 n \rceil - 1} \frac{\partial f_t}{\partial d_j} \cdot 2^t = j - 1 \tag{8}$$

It is obvious that the condition (8) is satisfied if each of the functions $f_1,f_2,…,f_m$ is linear, and the *q* function f_q includes the variable d_j (i.e., the value of the q bit of the binary number j-1 is equal to one). For example, if *n=8*, then *m=3* and the system of functions which satisfy (8) can be as follows:

$$\begin{aligned} f_1 &= d_2 \oplus d_4 \oplus d_6 \oplus d_8 \\ f_2 &= d_3 \oplus d_4 \oplus d_7 \oplus d_8 \\ f_3 &= d_5 \oplus d_6 \oplus d_7 \oplus d_8 \end{aligned} \tag{9}$$

In this case, the length size of check sum of its coding is substantially lower than the code length size of Δ: *m<n*, however, the probability that the error of any multiplicity larger than one (single errors they are detected always) corresponds to expression (2). For example, the two-fold error is not detected only when both errors occurred in one and the same bit.

In order to decrease the probability of not detecting the multiplicity errors, it is necessary in addition of the Boolean system (8) which forms the set Ξ_1, to use a system of u functions which compose the set Ξ_2 so that $F=\{\Xi_1, \Xi_2\}$.

In order to detect the two-fold error with high reliability it is necessary that a number of conditions are fulfilled. Since two errors, localized in different bits of the transferred codes are always detected using the functions of the set Ξ_1, and so for detecting the errors which appear in the same bit on different codes of block it is necessary that the probability of the values agreeing of the differentials functions of the set Ξ_2 with the change of one variable, should be as small as possible or near to zero. Therefore the functions differentials of this set must not be constant, i.e., the functions must be nonlinear, moreover the functions differentials $f_{m+1}, f_{m+2}, \ldots, f_{m+u}$, on any of the variables must constitute an orthogonal system of functions.

For the realization of this condition two methods for the functions synthesis of the set of Ξ_2 are proposed. According to the first method the functions of $f_{m+1}, f_{m+2}, \ldots, f_{m+u}$ are defined on a set with n variables, which coincide with the values of the bits of the transferred codes and the set of their possible values forms the set Z. In this case the number of functions of the set Ξ_2 is equal to $n-1$, i.e., $u=n-1$, and the functions $f_{m+1}, f_{m+2}, \ldots, f_{m+u}$ must satisfy the condition:

$$\forall j \in \{1,\ldots, n\}, a_t \in \{0,1\}: \quad \sum_{D \in Z} \bigoplus_{t=1}^{u} a_t \cdot \frac{\partial f_{m+t}}{\partial d_j} = 2^{u-1} \tag{10}$$

Below is given an example of a system of 7 Boolean functions with eight variables (n=8), which compose the set Ξ_2 and satisfy the condition (10):

$$\begin{aligned}
f_4 &= d_1 \cdot d_2 \oplus d_3 \cdot d_4 \oplus d_5 \cdot d_7 \oplus d_6 \cdot d_8 \\
f_5 &= d_1 \cdot d_3 \oplus d_2 \cdot d_4 \oplus d_5 \cdot d_8 \oplus d_6 \cdot d_7 \\
f_6 &= d_1 \cdot d_4 \oplus d_2 \cdot d_5 \oplus d_3 \cdot d_6 \oplus d_7 \cdot d_8 \\
f_7 &= d_1 \cdot d_5 \oplus d_2 \cdot d_6 \oplus d_3 \cdot d_7 \oplus d_4 \cdot d_8 \\
f_8 &= d_1 \cdot d_6 \oplus d_2 \cdot d_7 \oplus d_3 \cdot d_8 \oplus d_4 \cdot d_5 \\
f_9 &= d_1 \cdot d_7 \oplus d_2 \cdot d_8 \oplus d_3 \cdot d_5 \oplus d_4 \cdot d_6 \\
f_{10} &= d_1 \cdot d_8 \oplus d_2 \cdot d_3 \oplus d_4 \cdot d_7 \oplus d_5 \cdot d_6
\end{aligned} \tag{11}$$

The differentials on any of the 8 variables in the 7 functions, which compose the set Ξ_2, form the system of orthogonal Boolean functions. For example, the differentials of the 4th variable $d4$ form the system of linear functions, the orthogonality property of which is obvious:

$$\frac{\partial f_4}{\partial d_4} = d_3; \frac{\partial f_5}{\partial d_4} = d_2; \frac{\partial f_6}{\partial d_4} = d_1; \frac{\partial f_7}{\partial d_4} = d_8;$$
$$\frac{\partial f_8}{\partial d_4} = d_5; \frac{\partial f_9}{\partial d_4} = d_6; \frac{\partial f_{10}}{\partial d_4} = d_7$$

The differentials of functions f_1, f_2, f_3 in terms of the variable $d4$ are equal and they correspond to the number of the variable x_4: $j-1=011_2=3$.

The validity of the conditions (10) ensures the two errors detection, if they occur in the same bits of different codes. This means that the two-fold error will not be detected only when both errors will occur in one and the same bit j during the transmission of the two codes D_i and D_e, i.e., $i,e \in \{1,\ldots,k\}$, which either are equal or they are different only on the j^{th} bit. This probability is determined by the formula:

$$p_2 = \frac{1}{2^{n-1} \cdot n} \tag{12}$$

It is obvious that formula (12) determines the probability of the non detection not only of two-fold, but also of errors of any multiplicity larger than one. Comparison with the expression (2) shows that the reliability of the two-fold error detection is substantially increased in comparison with the usual check sum. Thus, the essence of the first of the proposed methods for the coding optimization of the check sum lies in the fact that the transformation function of the total components of the set Ξ_2 is selected in such a way that their differentials on any of the variables will depend on the code D. The two-fold error will not be detected only when both errors will occur in one and the same bit of the pair of the same codes, or the pair of the codes is different only in this bit.

If we consider that the appearance of each of the n-bit codes in the block is equally probable, then the probability of the two-fold error which satisfied these conditions is determined by the formula (12). However, in practice very frequent is the situation, when some codes in the block are repeated sufficiently frequently. This situation is characteristic for the text documents and for the images. Hence, in this case, the effectiveness of the proposed method of coding the components of check sum decreases. .

4 Conclusions

The proposed method is based on the coding optimization to increase the effectiveness of the error detection during data transmission and data storage using the check sums. This makes it possible to significantly decrease the probability of the mutual masking of even multiplicity errors both in comparison with the usual check sum and the use of SAC transformations for coding of its components.

A method for obtaining special differential Boolean functional transformations which optimize the check sum coding of the codes in block are developed. This method are developed from the point of view of the criterion of error detection which appears in the binary symmetrical channel. Example of the transformations which optimize coding check sum for both the proposed methods are given.

The estimations of the probability of error detecting of different multiplicity are theoretically substantiated. It is proven that during coding of the check sum components using functions which depend both on the transmitted codes and on the number of the code in the block, all errors of multiplicity less than 3 will be detected.

The analysis carried out showed that using the proposed method makes it possible to decrease in several orders the probability of the non detection of multiply errors in comparison with the known schemes of the check sum calculation.

The structure of the functional transformation is considerably simpler in comparison with the transformations of the CRC method and allows multilevel parallel process on hardware implementation which makes it possible to ensure the high performance of the error control without delays in the process of data transmission.

The developed method can be used for the effective errors control realization in the promising high-speed transmission channels of the digital information of computer networks.

References

Bardis, N.G., Markovskyy, A.P.: Utilization of of Avalanche Transformation for Increasing of Echoplex and Checksum Data Transmission Control Reliability. In: 2004 International Symposium on Information Theory and its Applications (ISITA 2004), Parma, Italy, Okt 10-13, pp. 656–660 (2004)

Torleiv, K.: Codes for Error Detection, Serial on Coding Theory and Cryptography, vol. 2, p. 201. World Scientific, Singapore (2007)

Saxena, N.R., McCluskey, E.J.: Extended precision checksums. In: Proc.17-th Intern. Symp. Fault-Tolerant Comput.: FCTS-17, Pittsburgrh, USA, pp. 142–147 (1987)

Fletcher, J.: An Arithmetic Checksum for Serial Transmissions. IEEE Transaction on Communication 30(1), 76–85 (1983)

Lin, S., Costello Jr., D.J.: Error Control Coding, p. 603. Prentice-Hall, Inc., Englewood Cliffs (1983) ISBN 0-13-283796-X