

Error Masking in Compact Testing Based on the Hamming Code and its Modifications

Serge Demidenko

Singapore Polytechnic, 500 Dover Road, Singapore 0513, SINGAPORE

Alexander Ivanyukovich and Leonid Makhist

Institute of Engineering Cybernetics, Kuybisheva St. 34, Brest 224000, BELARUS

Vincenzo Piuri

Politecnico di Milano, Piazza Leonardo Da Vinci 32, Milano 20133, ITALY

Abstract

Probability that an invalid sequence at an output of a device under test is not detected (error masking) is the measure of the effectiveness of compact testing methods. This paper evaluates and analyses the probability distribution of error masking for compact testing by exploiting the characteristics both of the Hamming code (i.e., the signature analysis) and of some modified Hamming codes. To study the effectiveness of these methods, we derive also the analytical expressions for the number of code words of arbitrary weight. Finally, bounds for error masking probability are obtained.

1. Introduction

Validity, effectiveness and relevance of compact testing methods [1,2] consist of the capability of compressing the binary sequence generated at the output of the digital device under test. The probability P_H that an invalid sequence is not detected at the device output (error-masking) is a measure of validity of these methods. In the literature (e.g., see [3-5]), the comparative evaluation of compact testing approaches has been considered by taking into account both the properties of the device under test and the characteristics of the testing methods (namely, the probability distribution of undetecting an invalid sequence having arbitrary weight).

This paper analyses and evaluates the probability distribution of undetecting invalid sequences of arbitrary weight when the compact testing methods based on Hamming code and some of its modifications are used. We derive the formulae for a number of code words of given weight. From these results, we derive finally the bounds for the probability distribution.

2. Number of Code Words of Given Weight

In this paper, we consider the cyclic code C of length $n(C)=2^m-1$, whose characteristic polynomial $g(x)$ is a primitive polynomial of degree m over $GF(2)$. We analyse also the following modifications of this code:

- the expurgated code A of length $n(A)=2^m-1$, which is the code with the characteristic polynomial $(x+1)g(x)$
- the extended code E of length $n(E)=2^m$, that is created by adding the general even parity to the code C .

The code C has been proved [6] to be equivalent to the binary Hamming code of length 2^m-1 , where the number C_k of the code words having weight k is [7]:

$$C_k = 2^{-m} \left[\binom{2^m-1}{k} + (-1)^{\lfloor \frac{k}{2} \rfloor} \binom{2^{m-1}-1}{\lfloor \frac{k}{2} \rfloor} (2^m-1) \right]$$

where $m=1,2,3,\dots$; $k=0,1,2,\dots,2^m-1$; $\lfloor t \rfloor$ and $\lceil t \rceil$ are the floor and the ceiling functions, respectively (1).

We use this result to derive the formulae that give the numbers E_k and A_k of the code words, having weight k , for the extended Hamming code E and for the expurgated Hamming code A , respectively.

Theorem 1. In the extended Hamming code E of length 2^m , number E_k of code words having weight k ($k=0,1,2,\dots,2^m$) is given by:

$$E_k = 2^{-m} \left[\binom{k}{2^m} + (-1)^{\lfloor \frac{k}{2} \rfloor} \binom{\lfloor \frac{k}{2} \rfloor}{2^{m-1}} (2^m-1) \right], k \text{ is even,}$$

$$E_k = 0, \text{ if } k \text{ is odd} \quad (2)$$

Proof. The extended Hamming code is invariant in respect to the transient group of substitutions [8]. Therefore, by applying the Prange theorem [8], we can state that C_k and E_k are related to each other as follows

$$E_{2j} = \frac{C_{2j-1} 2^m}{2j}, \text{ where } j=1,2,3,\dots,2^{m-1}.$$

By using expression (1) and by properties of the binomial coefficients, we obtain:

$$E_{2j} = 2^{-m} \left[\binom{2^m - 1}{2j - 1} + (-1)^j \binom{2^{m-1} - 1}{j - 1} (2^m - 1) \right] \frac{2^m}{2j} \\ = 2^{-m} \left[\binom{2^m}{2j} + (-1)^j \left(\frac{2^{m-1}}{j} \right) (2^m - 1) \right]$$

This proves the case of even values of k . The case of odd values is obvious, since the code E does not contain odd-weight code words by its definition.

□

Theorem 2. In the expurgated Hamming code A of length $2^m - 1$, the number A_k of code words having weight k ($k=0, 1, 2, \dots, 2^m - 2$) is given by:

$$A_k = 2^{-m} \left[\binom{2^m - 2}{k} + (-1)^{\frac{k}{2}} \binom{\frac{2^m - 1}{2} - 1}{\frac{k}{2}} (2^m - 2) \right],$$

if k is even, and

$A_k = 0$, if k is odd

(3)

Proof. According to the literature [8], the classical concept of the term "expurgation" implies that some code words' subset is removed from the source code to create the new (expurgated) code. In our case, the expurgation of the code C means deleting from this code a subset of code words having length n and odd weight. Therefore, in the case k is even, A_k and C_k are related to each other by $A_k = S_k$. By using expression (1), we derive easily the proof for even-weight code words. As for Theorem 1, the case of odd value of k is straightforward.

□

Example 1. Let $m_1=3$, $m_2=4$, $m_3=5$. The length of the codes being analysed will correspondingly be 7, 15 and 31 for the binary Hamming code (C) and expurgated code (A); and 8, 16 and 32 for the extended code (E). Table 1 shows the number of code words having weight k for the codes C , A , E .

3. The Probability of Undetecting Invalid Sequences Having Given Weight

The probability P_k of undetecting invalid sequence having weight k may be evaluated as ratio between the number S_k of invalid sequences having weight k that can not be detected by the given compact testing method and the total number of sequences of length n having the same weight

$$P_k = \frac{S_k}{\binom{n}{k}} \quad (4)$$

In this paper we analyse the compact testing methods C' , A' , and E' , with the characteristics of codes C , A , E . The hardware implementation of these compact testing methods is based on the use of shift registers with

feedback, namely:

- C' - on the basis of the characteristic polynomial $g(x)$ of degree m that is irreducible and primitive over field $GF(2)$; it is the traditional *signature analysis*;

- A' - on the basis of polynomial $(x+1)g(x)$;

- E' - on the basis of polynomial $g(x)$ with addition of general even parity.

As a consequence of these definitions, the signature length is m for C' , while it is $(m+1)$ for both A' and E' . The length of the sequence being analysed is the value of $n(A)$, $n(C)$ and $n(E)$ of corresponding codes.

Theorem 3. The probabilities $P_k(C)$, $P_k(A)$, $P_k(E)$ of undetecting invalid sequences having weight k by using compact testing methods C' , A' , E' are given by:

$$P_k(C) = 2^{-m} \left[1 + (-1)^{\left\lceil \frac{k}{2} \right\rceil} \frac{\binom{2^{m-1}-1}{\left\lfloor \frac{k}{2} \right\rfloor}}{\binom{2^m-1}{k}} (2^m - 1) \right];$$

$$P_k(A) = 2^{-m} \left[1 + (-1)^{\frac{k}{2}} \frac{\binom{2^{m-1}-1}{\frac{k}{2}}}{\binom{2^m-1}{k}} (2^m - 1) \right],$$

if k is even number, and

$P_k(A) = 0$, if k is odd.

$$P_k(E) = 2^{-m} \left[1 + (-1)^{\frac{k}{2}} \frac{\binom{2^{m-1}}{\frac{k}{2}}}{\binom{2^m}{k}} (2^m - 1) \right],$$

if k is even number, and

$P_k(E) = 0$, if k is odd

(5)

Proof. The number of invalid sequences having weight k that are not detected by the methods here considered is the number of code words having such a weight in the corresponding codes. By applying the formulae (1), (2) and (3) to the expression (4) and by simple algebraic manipulations, we easily derive the expressions (5).

□

Remark. It can be easily seen that the probabilities of undetecting invalid sequences having even weight k ($k=0, 1, 2, \dots, 2^{m-1}-2$) are similar in all the codes we are analysing. Besides, the relation

$$P_{2j}(C) = P_{2j-1}(C),$$

where $j=0, 1, 2, \dots, 2^{m-1}-1$, is satisfied for the signature analysis (i.e., the method having the Hamming code characteristics).

Example 2. Let $m_1=3$, $m_2=4$, $m_3=5$. The length of the codes is the same as in the Example 1. Table 2 shows the probabilities $P_k(C)$, $P_k(A)$, $P_k(E)$ of undetecting invalid sequences having weight k .

4. Bounds for the Probability of Undetecting of Invalid Sequences

Let us consider the probability distribution P_{kn} of undetecting of an invalid sequences which contain errors of multiplicity k . It is given by the following relation:

$$P_{kn} = P_{kc} P_k,$$

where P_{kc} is the probability of occurrence of the error having multiplicity k ; P_k is the probability of undetecting the error of the such a multiplicity. The probability P_n of undetecting invalid sequences is therefore given by:

$$P_n = \sum_{k=1}^L P_{kn} = \sum_{k=1}^L P_{kc} P_k \quad (6)$$

This figure of merit can be used as a measure of the efficiency of the compact testing method (e.g., see [3]).

Since it is practically not feasible to obtain an accurate estimation of the probability distribution P_{kc} determined by the characteristic features of the circuit under test, by the wide spectrum of possible faults and induced errors, and by the test sequence, we derive a bound for the undetecting probability P_n for the compact testing methods with the characteristics of the codes C , A , E . For these codes, there are the weights for which the probability of undetecting error by using existing methods is equal to zero. For instance,

$$P_k(C) = 0, \text{ at } k=1, 2, 2^m-3, 2^m-2;$$

$$P_k(A) = 0, \text{ at } k=2, 2^m-2, \text{ and when } k \text{ is odd};$$

$$P_k(E) = 0, \text{ at } k=2, 2^m-2, \text{ and when } k \text{ is odd}.$$

Therefore, the minimum value of the probability P_k , which is determined in accordance with expression (5), is equal to zero for all methods being analysed.

Theorem 4. The maximum non-one value $\max P_k$ and the minimum non-zero value $\min P_k$ for the probability of undetecting invalid sequences having weight k , by applying the compact testing methods with the characteristics of the codes C , A , and E , are given by:

$$\max P_k = \frac{1}{2^{m-3}}, \text{ and}$$

$$\min P_k = \frac{2^{m-8}}{(2^{m-3})(2^{m-5})}.$$

Proof. We give the proof for the method E' ; the other cases can be easily proved in the same way. The relation $P_k = P_{n-k}$, where n is the code length, holds for all the three codes E , C and A . Therefore, we need to examine the sequences $\{P_{2i}\}$ only for $i=2, 3, 4, \dots, 2^{m-2}$. As $\frac{\binom{2^{m-1}}{i}}{\binom{2^m}{2i}} = \frac{\binom{2^{m-1}}{i-1}}{\binom{2^m}{2i-2}} \frac{2i-1}{2^{m-2i+1}}$, the function $\frac{\binom{2^{m-1}}{i}}{\binom{2^m}{2i}}$ rigorously diminishes as i grows from 2 to 2^{m-2} . Since it is

$$P_{2i} = \frac{1}{2^m} \left[1 + (-1)^i \frac{\binom{2^{m-1}}{i}}{\binom{2^m}{2i}} (2^m - 1) \right],$$

as a consequence, $P_{2i} > 1/2^m$ when i is even, while $P_{2i} < 1/2^m$ when i is odd.

The sequence $\{P_{2i}\}$ decreases monotonously and is bounded by $1/2^m$ for odd values of the index i . The maximum value $\max P_k$ and minimum value $\min P_k$ are therefore reached when i has the lowest even value (i.e., $i=2$) and the lowest odd value (i.e., $i=3$), respectively.

Then it is:

$$\max P_k = \frac{1}{2^m} \left[1 + (2^m - 1) \frac{\binom{2^{m-1}}{2}}{\binom{2^m}{4}} \right] = \frac{1}{2^{m-3}},$$

$$\min P_k = \frac{1}{2^m} \left[1 - (2^m - 1) \frac{\binom{2^{m-1}}{3}}{\binom{2^m}{6}} \right] = \frac{2^{m-8}}{(2^{m-3})(2^{m-5})}.$$

□

The theorem provides the bounding values of the probability of undetecting invalid sequences for the weights where the probability is different from 1 or 0. Moreover, it is not difficult to determine the weights at which these bounding values are reached (Table 3).

The maximum value $\max P_n$ of the probability P_n of undetecting invalid sequences by using a compact testing method is equal to the maximum value of the probability distribution P_k [3]. A similar statement holds for the minimum value $\min P_n$ of the non-zero probability P_n .

Finally:

$$\max P_n(C) = \max P_n(A) = \max P_n(E) = \frac{1}{2^{m-3}}$$

$$\min P_n(C) = \min P_n(A) = \min P_n(E) = \frac{2^{m-8}}{(2^{m-3})(2^{m-5})}.$$

5. Conclusions

The asymptotic bounds proposed in the literature for numbers of masked errors, and for the probabilities of undetecting errors having given weight do not allow to evaluate correctly methods of compact testing. By using the analytical expressions proposed in this paper, we have obtained the bounding values for the probability of undetecting invalid sequences by the method of compact testing having the characteristics of the Hamming code and its modifications.

References

1. K.P. Parker, "Compact testing: testing with compressed data", *Fault Tolerant Computer Symposium FTCS-6 Proceedings*, pp. 93-98, 1976.
2. S.K. Kazmina, "Compact testing", *Automation and Remote Control*, 43, pp. 412-424, 1982.
3. V.N. Yarmolik, *Fault diagnosis of digital circuits*, 1990.
4. E.P. Kalosha, E.I. Katsnelson, V.N. Yarmolik, "On validity of compact testing methods", *Automation and Remote Control*, No 9, pp. 160-166, 1989.
5. V. Yarmolik, S. Demidenko, *Generation and application of pseudorandom sequences for random testing*, 1989.
6. R. Lidl, H. Niederreiter, *Finite fields*, 1983.
7. S. Demidenko, A. Ivanyukovich, L. Makhist, V. Piuri, "On the binary sequences with indistinguishable signature for a given error multiplicity in electronic testing" *JES Journal*, No 1, 1995, p. 63-66.
8. E.R. Berlekamp, *Algebraic coding theory*, 1968.

Table1. Number of code words of weight k

$m=3$

k	C_k	A_k	E_k
0	1	1	1
1	0	0	0
2	0	0	0
3	7	0	0
4	7	7	14
5	0	0	0
6	0	0	0
7	1	0	0
8	-	-	1

$m=4$

k	C_k	A_k	E_k
0	1	1	1
1	0	0	0
2	0	0	0
3	35	0	0
4	105	105	140
5	168	0	0
6	280	280	448
7	435	0	0
8	435	435	870
9	280	0	0
10	168	168	448
11	105	0	0
12	35	35	140
13	0	0	0
14	0	0	0
15	1	0	0
16	-	-	1

$m=5$

k	C_k	A_k	E_k
0	1	1	1
1	0	0	0
2	0	0	0
3	155	0	0
4	1,085	1,085	1,240
5	5,208	0	0
6	22,568	22,568	27,776
7	82,615	0	0
8	247,845	247,845	330,460
9	628,680	0	0
10	1,383,096	1,383,096	2,011,776
11	2,648,919	0	0
12	4,414,865	4,414,865	7,063,784
13	6,440,560	0	0
14	8,280,720	8,280,720	14,721,280
15	9,398,115	0	0
16	9,398,115	9,398,115	18,796,230
17	8,280,720	0	0
18	6,440,560	6,440,560	14,721,280
19	4,414,865	0	0
20	2,648,919	2,648,919	7,063,784
21	1,383,096	0	0
22	628,680	628,680	2,911,776
23	247,845	0	0
24	82,615	82,615	330,460
25	22,568	0	0
26	5,208	5,208	27,776
27	1,085	0	0
28	155	155	1,240
29	0	0	0
30	0	0	0
31	1	0	0
32	-	-	1

Table2. Probability of undetecting erroneous sequences having weight k

$m=3$

k	$P_k(C)$	$P_k(A)$	$P_k(E)$
0	1.00000000	1.00000000	1.00000000
1	0.00000000	0.00000000	0.00000000
2	0.00000000	0.00000000	0.00000000
3	0.20000000	0.00000000	0.00000000
4	0.20000000	0.20000000	0.20000000
5	0.00000000	0.00000000	0.00000000
6	0.00000000	0.00000000	0.00000000
7	1.00000000	0.00000000	0.00000000
8	-	-	1.00000000

$m=4$

k	$P_k(C)$	$P_k(A)$	$P_k(E)$
0	1.00000000	1.00000000	1.00000000
1	0.00000000	0.00000000	0.00000000
2	0.00000000	0.00000000	0.00000000
3	0.07692308	0.00000000	0.00000000
4	0.07692308	0.07692308	0.07692308
5	0.05594406	0.00000000	0.00000000
6	0.05594406	0.05594406	0.05594406
7	0.06759907	0.00000000	0.00000000
8	0.06759907	0.06759907	0.06759907
9	0.05594406	0.00000000	0.00000000
10	0.05594406	0.05594406	0.05594406
11	0.07692308	0.00000000	0.00000000
12	0.07692308	0.07692308	0.07692308
13	0.00000000	0.00000000	0.00000000
14	0.00000000	0.00000000	0.00000000
15	1.00000000	0.00000000	0.00000000
16	-	-	1.00000000

Table 3. Bounding values of the probability of undetecting invalid sequences of weight k

P_k		C	A	E
min	value	$\frac{2^{m-8}}{(2^m-3)(2^m-5)}$	$\frac{2^{m-8}}{(2^m-3)(2^m-5)}$	$\frac{2^{m-8}}{(2^m-3)(2^m-5)}$
P_k	weight	5; 6; 2^m-6 ; 2^m-5	6; 2^m-6	6; 2^m-6
max	value	$\frac{1}{2^{m-3}}$	$\frac{1}{2^{m-3}}$	$\frac{1}{2^{m-3}}$
P_k	weight	3; 4; 2^m-4 ; 2^m-5	4; 2^m-4	4; 2^m-4

$m=5$

k	$P_k(C)$	$P_k(A)$	$P_k(E)$
0	1.00000000	1.00000000	1.00000000
1	0.00000000	0.00000000	0.00000000
2	0.00000000	0.00000000	0.00000000
3	0.03448276	0.00000000	0.00000000
4	0.03448276	0.03448276	0.03448276
5	0.03065134	0.00000000	0.00000000
6	0.03065134	0.03065134	0.03065134
7	0.03141762	0.00000000	0.00000000
8	0.03141762	0.03141762	0.03141762
9	0.03118441	0.00000000	0.00000000
10	0.03118441	0.03118441	0.03118441
11	0.03128436	0.00000000	0.00000000
12	0.03128436	0.03128436	0.03128436
13	0.03122649	0.00000000	0.00000000
14	0.03122649	0.03122649	0.03122649
15	0.03127074	0.00000000	0.00000000
16	0.03127074	0.03127074	0.03127074
17	0.03122649	0.00000000	0.00000000
18	0.03122649	0.03122649	0.03122649
19	0.03128436	0.00000000	0.00000000
20	0.03128436	0.03128436	0.03128436
21	0.03118441	0.00000000	0.00000000
22	0.03118441	0.03118441	0.03118441
23	0.03141762	0.00000000	0.00000000
24	0.03141762	0.03141762	0.03141762
25	0.03065134	0.00000000	0.00000000
26	0.03065134	0.03065134	0.03065134
27	0.03448276	0.00000000	0.00000000
28	0.03448276	0.03448276	0.03448276
29	0.00000000	0.00000000	0.00000000
30	0.00000000	0.00000000	0.00000000
31	1.00000000	0.00000000	0.00000000
32	-	-	1.00000000