ISSN 0146-4116, Automatic Control and Computer Sciences, 2015, Vol. 49, No. 6, pp. 395–403. © Allerton Press, Inc., 2015.
Original Russian Text © V.N. Yarmolik, I. Mrozek, S.V. Yarmolik, 2015, published in Avtomatika i Vychislitel'naya Tekhnika, 2015, No. 6, pp. 101–113.

Controlled Method of Random Test Synthesis

V. N. Yarmolik[a], I. Mrozek[b], and S. V. Yarmolik[a]

[a] *Belarusian State University of Informatics and Radioelectronics, ul. P. Brovki 6, Minsk, 220013 Belarus*
[b] *Bialystok Technical University, ul. Wiejska 45 A, Bialystok, Poland*
e-mail: yarmolik10ru@yahoo.com

Received May 18, 2015

Abstract—In this paper, controlled random tests have been analyzed, and the main criteria used for their synthesis, such as the Hamming distance and the Euclidean distance, have been presented. A method for synthesizing multiple controlled random tests based on the use of the initial random test and addition operation has been proposed. The resulting multiple tests can be interpreted as a single controlled random test. The complexity of its construction is significantly lower than the complexity of the construction of classical random tests. An algorithm for the synthesis of such tests is considered. Examples of tests and estimates of their effectiveness have been presented.

Keywords: controlled random tests, multiple tests, Hamming distance, Euclidean distance

DOI: 10.3103/S0146411615060115

1. INTRODUCTION

Currently, the complexity of modern computer systems and networks, such as embedded systems, systems-on-a-chip, and nets-on-a-chip is steadily increasing [1, 2]. Accordingly, the relevance of testing these systems in order to detect errors in their software and faults in the hardware increases [3, 4]. The variety of software errors or hardware faults of modern computing systems and networks determines the use of generic methodologies for testing them [5]. These methodologies primarily include modern modifications of random testing [6–12]. Existing varieties of random tests are combined under the principle of controlled random testing [5]. These tests are constructed based on the calculation of certain characteristics for the controlled selection of another random test set [5].

The use of controlled random tests is characterized by greater efficiency compared with other types of tests that has been confirmed in practice many times [5–12]. It should be noted that the need to sort potential candidates for test sets and calculate the numerical characteristics for them significantly increases the complexity of constructing controlled random tests [5–7, 9, 12].

The purpose of this paper is to develop a method for constructing multiple controlled tests [13] based on the initial controlled random test of a lesser length constructed by known methodologies [5–7, 9, 12]. The initial test is used to construct subsequent tests of multiple controlled random tests in the form of simple modifications that do not require further analysis or computational costs. The resulting multiple controlled random tests can be interpreted as a single random test or used for periodic testing in applications with time-limited test procedures.

2. ANALYSIS OF CONTROLLED RANDOM TESTS

All existing methods for constructing controlled random tests are based on the following assertion [5, 7–10]. Each subsequent test set of the controlled random tests should be constructed such that it is as different (distant) from all previously generated test sets as possible. In this case, the hypothesis is accepted that for the two test sets with minimal difference the number of additional faults (errors) detected by the second set is minimal and, conversely, for maximally different test sets the second one has the maximal detection capacity [5, 7–10]. In this case, the efficiency of the second set is estimated by the number of detected faults (errors) that are not detected by the first test set.

For methods of controlled random testing used to test digital devices and software with m inputs and the space of input patterns consisting of 2^m binary sets (vectors), the following definitions are correct [5, 7, 8, 14].

Definition 1. The test (T) is a set of $2 \le q \le 2^m$ test sets

$$\{T_0, T_1, T_2, \ldots, T_{q-1}\}, \text{ where } T_i = t_{i,m-1}t_{i,m-2}\ldots t_{i,2}t_{i,1}t_{i,0}, \quad t_{i,l} \in \{0, 1\},$$

and m is the size of the test set in bits.

Definition 2. The controlled random test $CRT = \{T_0, T_1, T_2, \ldots, T_{q-1}\}$ is the test T that consists of randomly generated test sets T_i, $i \in \{0, 1, 2, \ldots, q-1\}$ such that T_i meets a certain criterion or criteria derived from previous test sets $T_0, T_1, T_2, \ldots, T_{i-1}$.

The Hamming distance $HD(T_i, T_j)$ and the Euclidean distance $ED(T_i, T_j)$ are often used as the difference criteria of the test set $T_i = t_{i,m-1}t_{i,m-2}\ldots t_{i,2}t_{i,1}t_{i,0}$, where $t_{i,l} \in \{0, 1\}$; $i \in \{0, 1, 2, \ldots, q-1\}$, from the previous sets $T_0, T_1, T_2, \ldots, T_{i-1}$ [5, 7–10]. These characteristics are defined for binary test sets T_i and T_j consisting of m bits, for which the Hamming distance $HD(T_i, T_j)$ is calculated as the weight $w(T_i \oplus T_j)$ of the vector $T_i \oplus T_j$, and $ED(T_i, T_j) = \sqrt{HD(T_i, T_j)}$. Obviously, $minHD(T_i, T_j) = 0$ and $minED(T_i, T_j) = 0$ are obtained for $T_i = T_j$, and $maxHD(T_i, T_j) = m$ and $maxED(T_i, T_j) = \sqrt{m}$ at $T_j = \overline{T_i}$.

When constructing the set T_i, when $i > 2$, total values of distances for T_i with respect to previous sets $T_0, T_1, T_2, \ldots, T_{i-1}$ are used [5, 7–10, 12, 14]. Then, for the next set T_i the total Hamming distance ($THD(T_i)$) and the total Euclidean distance ($TED(T_i)$) with respect to $T_0, T_1, T_2, \ldots, T_{i-1}$ are calculated as

$$THD(T_i) = \sum_{j=0}^{i-1} HD(T_i, T_j); \quad TED(T_i) = \sum_{j=0}^{i-1} ED(T_i, T_j). \tag{1}$$

According to the methods of constructing controlled random tests discussed above, the new test set T_i is selected so that difference metrics (1) take the maximum value [5, 7–10, 12, 14]. Note that difference metrics (1) are characterized by a significant computational complexity, which increases with the growth of the index i of the test set T_i. The computational complexity increases significantly because of the reduction of the number of potential candidates for tests with the increasing value of i [8, 15]. This is mainly caused by the decrease in the search space for the new test set T_i, which is reduced because of the previous procedures used to obtain test sets $T_0, T_1, T_2, \ldots, T_{i-1}$, and, to a large extent, it depends on the threshold values of characteristics of (1).

As shown in [8, 13], the minimum Hamming distance $minHD(T_i, T_j)$ or the Euclidean distance $minED(T_i, T_j)$ is a more efficient metrics for the generation of a controlled random test. According to the method of synthesis of tests discussed in [8], the subsequent test set T_i is selected from possible candidates for the tests by the criterion of the maximum value

$$\min_{j \in \{0,1,\ldots,i-1\}} HD(T_i, T_j) \text{ or } \min_{j \in \{0,1,\ldots,i-1\}} ED(T_i, T_j), \tag{2}$$

which provides the maximum distance (difference) of the test set T_i from all previously generated sets T_0, $T_1, T_2, \ldots, T_{i-1}$. If the maximum value of (2) is achieved, it also maximizes values $THD(T_i)$ and $TED(T_i)$ according to (1) [13].

Let us define a multiple controlled test based on the methodology of single-step controlled random tests.

Definition 3. The multiple controlled random test $MCRT_r$ consists of r single-step controlled random tests $CRT(0), CRT(1), CRT(2), \ldots, CRT(r-1)$, each of which includes q test sets. In addition, the test $CRT(0)$ satisfies Definition 2 and subsequent tests $CRT(i)$, $i \in \{1, 2, 3, \ldots, r-1\}$ are constructed according to certain algorithms such that each subsequent test $CRT(i)$ meets a certain criterion or criteria derived from previous tests $CRT(0), CRT(1), CRT(2), \ldots, CRT(i-1)$.

Let us consider the Hamming distance and the Euclidean distance for two tests $CRT(k)$ and $CRT(l)$. Initially, we note that the Hamming distance $HD(CRT(k), CRT(l))$, which is the same as the number of distinct components $T_{k,i}$ and $T_{l,i}$ of the initial test $CRT(k)$ and the constructed one $CRT(l)$, can be considered as a prerequisite which the test $CRT(l)$ should meet. It is clear that a necessary requirement in terms of the maximum difference with which $CRT(k)$ and $CRT(l)$ should comply is the lack of matching sets $T_{k,i}$ and $T_{l,i}$ in them, which is equivalent to the inequality $T_{l,i} \ne T_{k,i}$, $i \in \{0, 1, 2, \ldots, q-1\}$.

The Euclidean distance for $CRT(k)$ and $CRT(l)$ is defined as $ED(CRT(k), CRT(l)) = \sqrt{\sum_{i=0}^{q-1} (T_{i,k} - T_{i,l})^2}$.

As for the total values of distances $THD(T_i)$ and $TED(T_i)$ according to (1) for the test set T_i, let us introduce similar distance measures for the controlled random test $CRT(i)$ as follows:

$$THD(CRT(i)) = \sum_{j=0}^{i-1} HD(CRT(i), CRT(j)); \quad TED(CRT(i)) = \sum_{j=0}^{i-1} ED(CRT(i), CRT(j)). \tag{3}$$

In order to use more effective criteria for estimating the quality of the controlled random test in the construction of the test $CRT(i)$, let us determine the maximum value of the Hamming distance $MHD(CRT(i))$ and the maximum value of the Euclidean distance $MED(CRT(i))$ as follows:

$$\begin{aligned} MHD(CRT(i)) &= \max_{CRT_v(i),\, v\in\{0,1,\ldots w\}} \left\{ \min_{j\in\{0,1,\ldots,i-1\}} HD(CRT_1(i), CRT(j)), \ldots, \min_{j\in\{0,1,\ldots,i-1\}} HD(CRT_w(i), CRT(j)) \right\}; \\ MED(CRT(i)) &= \max_{CRT_v(i),\, v\in\{0,1,\ldots w\}} \left\{ \min_{j\in\{0,1,\ldots,i-1\}} ED(CRT_1(i), CRT(j)), \ldots, \min_{j\in\{0,1,\ldots,i-1\}} ED(CRT_w(i), CRT(j)) \right\}. \end{aligned} \tag{4}$$

According to given metrics (4), the subsequent controlled random test $CRT(i)$ is selected from the set $\{CRT_1(i), CRT_2(i), \ldots, CRT_w(i)\}$ of to test candidates based on the criterion of the maximum minimum Hamming and Euclidean distances with respect to previously generated controlled random tests $CRT(j) = \{CRT(0), CRT(1), \ldots, CRT(i-1)\}$.

3. METHOD FOR GENERATING MULTIPLE CONTROLLED RANDOM TESTS

Let us use addition as the main operation in the construction of multiple random tests. It will make it possible to provide the minimal computational complexity in the construction of multiple random tests $MCRT_r$. Indeed, all subsequent tests $CRT(1), CRT(2), \ldots, CRT(r-1)$ can be easily constructed based on $CRT(0)$ by a single application of addition for each test set.

According to Definition 2, the controlled random test CRT consists of q test sets T_i, $i \in \{0, 1, 2, \ldots, q-1\}$, each of which represents a m-bit binary vector $T_i = t_{i,m-1}t_{i,m-2} \ldots t_{i,2}t_{i,1}t_{i,0}$, where $t_{i,l} \in \{0, 1\}$. Thus, test sets T_i of the controlled random test CRT can be interpreted as $g = 2^m$-ary data $T_i \in \{0, 1, 2, \ldots, 2^m - 1\}$. Then, for example, the test $CRT = \{0011, 0110, 1100, 0101, 1000\}$ can be represented as a set of 16-ary data $CRT = \{3, 6, 12, 5, 8\}$ shown in the decimal system. If the initial test is $CRT(k) = \{T_0(k), T_1(k), T_2(k), \ldots, T_{q-1}(k)\}$, the ratio that is used to obtain a new test $CRT(l) = \{T_0(l), T_1(l), T_2(l), \ldots, T_{q-1}(l)\}$ takes the following form:

$$T_i(l) = T_i(k) + d \bmod 2^m; \quad i = \overline{0, q-1}. \tag{5}$$

In the given ratio, the parameter $d \in \{1, 2, 3, \ldots, 2^m - 1\}$ is used to achieve the difference between test sets and, accordingly, between tests $CRT(l)$ and $CRT(k)$. This parameter is crucial for achieving the maximum difference of the test $CRT(l)$ from the test $CRT(k)$ in terms of the previously defined metrics. For relation (5) the following proposition is true.

Proposition 1. If the test $CRT(l)$ is derived from the initial test $CRT(k)$ based on relation (5) for the parameter $d \in \{1, 2, 3, \ldots, 2^m - 1\}$, then using the value $2^m - d$ as the parameter for the test $CRT(l)$ and using the same relation (5) we obtain the initial test $CRT(k)$. This proposition follows from the equality $d + 2^m - d \bmod 2^m = 0$.

Example 1. When $m = 4$ for the initial test $CRT(k) = \{3, 6, 12, 5, 8\}$ and the parameter $d = 8$, according to (5), we obtain $CRT(l) = \{11, 14, 4, 13, 0\}$. Using $CRT(l) = \{11, 14, 4, 13, 0\}$ as the initial test and the same value $d = 8$, we obtain the test $CRT(k) = \{3, 6, 12, 5, 8\}$, which corresponds to the Proposition 1. For the same initial test $CRT(k) = \{3, 6, 12, 5, 8\}$ and the other parameter $d = 5$, we will have a different result, namely, $CRT(l) = \{8, 11, 1, 10, 13\}$.

Example 2. For the test $CRT(k) = \{3, 7, 0, 6, 2, 5, 1, 4\}$ constructed for $m = 3$ and parameter $d = 4$, according to (5), we find that $CRT(l) = \{7, 3, 4, 2, 6, 1, 5, 0\}$. For the same initial test and parameter $d = 5$, we will have a different result, i.e., $CRT(l) = \{0, 4, 5, 3, 7, 2, 6, 1\}$. Note that, in the given example, tests include various octal data values.

In the analysis of the above examples, in each of which two new tests obtained according to (5) are represented, the question arises as to which of these two tests is more effective for multiple testing. Thus, the problem arises of determining the optimal parameter d when using the Euclidean distance as a quality metric for multiple tests. Let us prove the theory, first, for $ED(CRT(k)$ and $CRT(l))$, where the test $CRT(l)$ is obtained according to (5).

Table 1. Values of the Euclidean distance for $m = 3$

d	1	2	3	4	5	6	7
$ED(CRT(k), CRT(l))$	$\sqrt{56}$	$\sqrt{96}$	$\sqrt{120}$	$\sqrt{128}$	$\sqrt{120}$	$\sqrt{96}$	$\sqrt{56}$

THEOREM 1. The Euclidean distance $ED(CRT(k),CRT(l))$ for tests $CRT(k)$ and $CRT(l)$, where $CRT(k) = \{T_0(k), T_1(k), T_2(k), ..., T_{q-1}(k)\}$ consists of $q = 2^m$ m-bit nonrecurring randomly generated test sets $T_i(k) \in \{0, 1, 2, ..., 2^m - 1\}$, and where test sets $T_i(l)$ are obtained according to the expression $T_i(l) = T_i(k) + d \bmod 2^m$, $i = \overline{0, q-1}$, is calculated as

$$ED(CRT(k),CRT(l)) = \sqrt{2^m d(2^m - d)}. \tag{6}$$

Proof. The expression for the Euclidean distance $ED(CRT(k),CRT(l))$ becomes

$$ED(CRT(k),CRT(l)) = \sqrt{\sum_{i=0}^{2^m-1}[T_i(k) - T_i(l)]^2} = \sqrt{\sum_{i=0}^{2^m-1}\left[T_i(k) - (T_i(k) + d \bmod 2^m)\right]^2}.$$

Given the fact that test sets $T_i(k)$ consist of $q = 2^m$ m-bit nonrecurring data $\{0, 1, 2,..., 2^m - 1\}$, it is possible to draw the following conclusions. Values $T_i(l)$ according to (5) in $2^m - d$ cases will take the form of $T_i(l) = T_i(k) + d$. As can be seen from Example 2, for $d = 5$ in $2^m - d = 2^3 - 5 = 3$ cases $T_i(l) = T_i(k) + 5$, namely for $T_i(k) = \{0, 1, 2\}$. In addition, values $T_i(l)$ according to (5) in d cases take the form $T_i(l) = T_i(k) + 2^m - d$. Taking into account the given relations the expression for the Euclidean distance will take the form:

$$ED(CRT(k),CRT(l)) = \sqrt{\sum_{i=0}^{2^m-d-1} d^2 + \sum_{i=0}^{d-1}(2^m - d)^2} = \sqrt{(2^m - d)d^2 + d(2^m - d)^2} = \sqrt{2^m d(2^m - d)}.$$

Which is what we set out to prove.

Example 3. The Euclidean distance for tests $CRT(k) = \{3, 7, 0, 6, 2, 5, 1, 4\}$ and $CRT(l) = \{7, 3, 4, 2, 6, 1, 5, 0\}$ from Example 2 is defined as $ED(CRT(k), CRT(l)) = [(3 - 7)^2 + (7 - 3)^2 + (0 - 4)^2 + (6 - 2)^2 + (2 - 6)^2 + (5 - 1)^2 + (1 - 5)^2 + (4 - 0)^2]^{1/2} = \sqrt{128}$. The same value can be obtained based on Theorem $\sqrt{2^3 \times 4 \times (2^3 - 4)} = \sqrt{128}$.

Values of Euclidean distances for the case $m = 3$ and possible values of d are given in Table 1.

For the above Theorem 1 we have the following corollary.

Corollary 1. The Euclidean distance value $ED(CRT(k), CRT(l))$ will take the maximum value when $d = 2^{m-1}$, which corresponds to the solution of the equation

$$\frac{\partial\sqrt{2^m d(2^m - d)}}{\partial d} = 0.$$

The validity of this corollary is confirmed by the results shown in Table 1, where for $d = 2^{m-1} = 2^{3-1} = 4$ the Euclidean distance takes the maximum value of $\sqrt{128}$.

Corollary 2. The Euclidean distance $ED(CRT(k), CRT(l))$ obtained for the parameter d is equal to the Euclidean distance of the parameter $2^m - d$, which follows from the equality

$$\sqrt{2^m d(2^m - d)} = \sqrt{2^m(2^m - d)(2^m - (2^m - d))}.$$

This property is illustrated by numerical values of the Euclidean distance shown in Table 1.

Corollary 3. The value of the Euclidean distance $ED(CRT(k), CRT(l)) = \sqrt{2^m d(2^m - d)}$ obtained according to (6) for tests $CRT(k)$ and $CRT(l)$ consisting of $q = 2^m$ m-bit data $\{0, 1, 2, ..., 2^m - 1\}$ can be used as the mean Euclidean distance $AED(CRT(k), CRT(l))$ equal to $\sqrt{qd(2^m - d)}$, between tests $CRT(k)$ and $CRT(l)$ that include $q < 2^m$ test sets.

For Example 1 and test $CRT(l) = \{11, 14, 4, 13, 0\}$ obtained based on the initial test $CRT(k) = \{3, 6, 12, 5, 8\}$ at $d = 8$, according to (5), we find that

$$AED(CRT(k), CRT(l)) = \sqrt{5 \times 8 \times (2^3 - 8)} = \sqrt{320}.$$

Note that, for these tests, the Euclidean distance is strictly equal to its average value. Indeed, $ED(CRT(k), CRT(l)) = [(3 - 11)^2 + (6 - 14)^2 + (12 - 4)^2 + (5 - 13)^2 + (8 - 0)^2]^{1/2} = \sqrt{320}$.

Corollary 4. If the Euclidean distance $ED(CRT(k), CRT(l))$ between controlled random tests $CRT(k)$ and $CRT(l)$ according to Theorem 1 is equal to $\sqrt{2^m d_l(2^m - d_l)}$ and, for tests $CRT(k)$ and $CRT(n)$, $ED(CRT(k), CRT(n)) = \sqrt{2^m d_n(2^m - d_n)}$, then $ED(CRT(l), CRT(n)) = \sqrt{2^m d_c(2^m - d_c)}$, where $d_c = d_l - d_n \bmod 2^m$.

In accordance with Example 2 $CRT(l) = \{0, 4, 5, 3, 7, 2, 6, 1\}$ and $CRT(n) = \{7, 3, 4, 2, 6, 1, 5, 0\}$, from the Corollary 4, we obtain that $d_c = d_l - d_n \bmod 2^m = 5 - 4 \bmod 2^3 = 1$ and

$$ED(CRT(l), CRT(n)) = \sqrt{2^m d_c(2^m - d_c)} = \sqrt{2^3 \times 1 \times (2^3 - 1)} = \sqrt{56}.$$

Using the classic definition of the Euclidean distance, we will obtain $ED(CRT(l), CRT(n)) = [(0 - 7)^2 + (4 - 3)^2 + (5 - 4)^2 + (3 - 2)^2 + (7 - 6)^2 + (2 - 1)^2 + (6 - 5)^2 + (1 - 0)^2]^{1/2} = \sqrt{56}$.

4. THE CONSTRUCTION OF MULTIPLE CONTROLLED RANDOM TESTS

As a basis for constructing multiple controlled random tests

$$MCRT_r = \{CRT(0), CRT(1), CRT(2), ..., CRT(r - 1)\}, \quad (7)$$

we use relation (5), which is characterized by the minimal computational complexity in obtaining subsequent tests $CRT(1)$, $CRT(2)$, ..., $CRT(r - 1)$ based on the initial one $CRT(0)$.

Then, the maximum minimum Hamming distance $MHD(CRT(k), CRT(l))$ and the maximum minimum Euclidean distance $MED(CRT(k), CRT(l))$, $k \neq l \in \{0, 1, 2, ..., r - 1\}$, according to (5), will be used in the construction of multiple random tests (7) as measures of efficiency.

Firstly, let us note that the maximum of $MHD(CRT(k), CRT(l))$ is achieved through the fulfillment of the following condition: $d_1 \neq d_2 \neq d_3 \neq ... \neq d_{r-1}$. Indeed, as previously noted, a prerequisite in terms of the maximum Hamming distance $MHD(CRT(k), CRT(l))$, with which the tests $CRT(k)$ and $CRT(l)$, $k \neq l \in \{0, 1, 2, ..., r - 1\}$, should comply, is the lack of matching test sets $T_i(k)$ and $T_i(l)$, $i \in \{0, 1, 2 , ..., q - 1\}$, in them, which is equivalent to fulfilling the condition $T_i(k) \neq T_i(l)$. Since the test sets $T_i(k)$ and $T_i(l)$ are interconnected by relation (5), the condition $T_i(k) \neq T_i(l)$ is fulfilled by using a nonzero value of the parameter $d \neq 0$ in order to obtain test sets $T_i(l)$ of the test $CRT(l)$ based on test sets $T_i(k)$ of the initial test $CRT(k)$.

Let us successively consider multiple controlled random tests $MCRT_r$ of various multiplicity ranging from double tests $MCRT_2$ that consist of $CRT(0)$ and $CRT(1)$, where the second test $CRT(1)$ is generated based on the initial test $CRT(0)$ according to (5). According to Corollary 1, the optimum value of the parameter d in order to obtain $CRT(1)$ is 2^{m-1}. In this case, the Euclidean distance between the tests $CRT(0)$ and $CRT(1)$ takes the maximum value that maximizes the difference between these tests and the maximum effectiveness of their joint application.

Let us prove the following theorem for tests $MCRT_r$ with the multiplicity $r > 2$.

THEOREM 2. The maximum value $MHD(CRT(k),CRT(l))$ with which the tests $CRT(k)$ and $CRT(l)$ ($k \neq l \in \{0, 1, 2, ..., r - 1\}$) of the multiple controlled random test $MCRT_r$ that consists of $r > 2$ random tests $\{CRT(0), CRT(1), CRT(2),...,CRT(r-1)\}$, each of which contains $q \leq 2^m$ m-bit test sets, should comply is achieved in the case of the maximum minimum value $d_k - d_l$ ($k \neq l \in \{0, 1, 2, ..., r - 1\}$), and $d_k \neq d_l \in \{1, 2, ..., 2^m - 1\}$.

Proof. When constructing the multiple controlled random test

$$MCRT_r = \{CRT(0), CRT(1), CRT(2), ..., CRT(r - 1)\},$$

further tests $CRT(1)$, $CRT(2)$, ..., $CRT(r - 1)$ are constructed based on $CRT(0)$ using relation (5) and a set of parameters $d \in \{d_1, d_2, d_3, ..., d_{r-1}\}$. When $r > 2$, values of the parameter d are selected so as to maximize the Hamming distance, namely, to satisfy the inequality $d_1 \neq d_2 \neq d_3 \neq ... \neq d_{r-1}$.

Table 2. Values of the Euclidean distance for $m = 4$

d	1	2	3	4	5	6	7	8
$ED(CRT(k), CRT(l))$	15.5	21.2	24.9	27.7	29.7	30.9	31.7	32.0
d	9	10	11	12	13	14	15	16
$ED(CRT(k), CRT(l))$	31.7	30.9	29.7	27.7	24.9	21.2	15.5	0

Table 3. Values of the Euclidean distance for the test $MCRT_4$

	$CRT(0)$	$CRT(1)$	$CRT(2)$	$CRT(3)$
$CRT(0)$	–	27.7	32.0	27.7
$CRT(1)$	27.7	–	27.7	32.0
$CRT(2)$	32.0	27.7	–	27.7
$CRT(3)$	27.7	32.0	27.7	–

Assuming that $q = 2^m$, it can be concluded that according to property 4 for two arbitrary tests $CRT(k)$ and $CRT(l)$ ($k \neq l \in \{0, 1, 2, ..., r-1\}$) the Euclidean distance is equal to the expression $\sqrt{2^m d(2^m - d)}$ for the parameter d equal to $d_l - d_k \bmod 2^m$. When $r > 2$ for arbitrary pairs of parameters d_l and d_k ($k \neq l \in \{0, 1, 2, ..., r-1\}$), minimum difference $d_l - d_k \bmod 2^m$ between them is always greater than zero and less than 2^{m-1}. Note that the function of the Euclidean distance $\sqrt{2^m d(2^m - d)}$ is an increasing function for $d = \overline{0, 2^{m-1}}$. Then, we can conclude that the larger the minimum difference $d_l - d_k \bmod 2^m$, the greater the value $MED(CRT(k), CRT(l))$, $k \neq l \in \{0, 1, 2, ..., r-1\}$ according to (5). Which is what we set out to prove.

Based on the proved theorem, we can conclude that for the general case of the multiple test $MCRT_r$ optimal values of parameters $d_1, d_2, ..., d_{r-1}$ are the values that divide the range of integers of $0 - 2^m$ into regular intervals and are calculated according to the following relation:

$$d_i = \left\lfloor \frac{i2^m}{r} + 0.5 \right\rfloor, \quad i \in \{1, 2, \ldots, r-1\}. \tag{8}$$

In the case of the triple random test $MCRT_3$, in order to obtain the second $CRT(1)$ and third $CRT(2)$ tests based on the initial test $CRT(0)$, it is necessary to use optimum combinations of parameters d_1 and d_2 according to (8) used to obtain tests $CRT(1)$ and $CRT(2)$ according to (5). Correspondingly, for triple random tests,

$$d_1 = \left\lfloor 1 \times 2^m/3 + 0.5 \right\rfloor, \text{ and } d_2 = \left\lfloor 2 \times 2^m/3 + 0.5 \right\rfloor.$$

For $m = 3$, we find that $d_1 = 3$ and $d_2 = 5$ and, for $m = 4$, $d_1 = 5$ and $d_2 = 11$.

Let us consider $MCRT_3 = \{CRT(0), CRT(1), CRT(2)\}$ when $m = 4$ using $d_1 = 5$ and $d_2 = 11$. The Euclidean distance between the tests $CRT(0)$ and $CRT(1)$ is calculated as follows $ED(CRT(0), CRT(1)) = \sqrt{16 \times 5 \times (16 - 5)} = \sqrt{880} = 29.7$. Other values of Euclidean distances for an arbitrary value d are shown in Table 2. According to this table, the value of the Euclidean distance is $ED(CRT(0), CRT(2)) = 29.7$. At the same time, in accordance with Corollary of 4, the distance between tests $CRT(1)$ and $CRT(2)$ is determined for d equal to $d_2 - d_1 = 11 - 5 = 6$ as $ED(CRT(1), CRT(2)) = 29.7$.

The analysis of given values of Euclidean distances for the considered $MCRT_3$ indicates that

$MED\,(CRT(k), CRT(l)) = 29.7$ for $k \neq l \in \{0, 1, 2\}$ according to (4) and

$TED\,(CRT(2)) = ED(CRT(2), CRT(0)) + ED(CRT(2), CRT(1)) = 29.7 + 29.7 = 59.4$ according to (3) take the maximum value.

For the quadruple test $MCRT_4 = \{CRT(0), CRT(1), CRT(2), CRT(3)\}$ using (8), e.g., for $m = 4$, we find that $d_1 = 4$, $d_2 = 8$ and $d_3 = 12$. The values of the distances between any two tests $MCRT_4$ are given in Table 3.

As can be seen from Table 3, the value $MED(CRT(k), CRT(l))$, $k \neq l \in \{0, 1, 2, 3\}$ for $MCRT_4$ takes the maximum possible value of 27.7.

Table 4. Estimation of the effectiveness of the double test for the storage device consisting of eight memory cells ($2m = 8$) for $k = 3, 4, 5, 6$

d	$E(k, 2^m)$ is the additional number of binary combinations on all possible k from 2^m bits			
	$E(3, 8)$	$E(4, 8)$	$E(5, 8)$	$E(6, 8)$
1	42	105	140	105
2	72	165	200	135
3	90	195	220	140
4	96	204	224	140
5	90	195	220	140
6	72	165	200	135
7	42	105	140	105

5. EXPERIMENTAL

As a measure of the effectiveness of multiple controlled random test $MCRT_r$ we used the metric $E(k, 2^m)$ introduced in [15] in order to construct subsequent test sets in the generation of the single-step controlled random test. In the case of multiple tests similar characteristic for the subsequent test $CRT(i)$ is formulated and can be determined as follows.

Definition 4. The additional number of binary combinations at all possible k from 2^m bits generated by test sets of the test $CRT(i)$ with respect to the plurality k from 2^m binary combinations generated by previous tests of the multiple test $CRT(0)$, $CRT(1)$, $CRT(2)$, ..., $CRT(i-1)$ is the measure of effectiveness $E(k, 2^m)$ for the subsequent controlled test $CRT(i)$.

Obviously, the larger the value of this metric, the more effective is the subsequent controlled test $CRT(i)$, which together with the previous tests makes it possible to achieve maximum efficiency. Note that in previous sections it was shown that in order to achieve the maximum efficiency of multiple controlled random tests $MCRT_r$ the Euclidean distance for the test $CRT(i)$ should be maximum in relation to previously generated tests $CRT(0)$, $CRT(1)$, $CRT(2)$, ..., $CRT(i-1)$.

The problem of testing storage devices was used for the comparative analysis of the effectiveness of multiple controlled random tests $MCRT_r$ [13, 18]. First, let us consider a storage device that consists of $2^3 = 8$ memory cells. In order to test it, we used the test $CRT(0)$, which includes all possible three-bit addresses generated according to the scheme of march tests [13, 18]. In the formation of the next address the initial zero state of the memory cell is changed to a one state. Thus, the initial zero state of all cells of the storage device is changed to the one state. Note that values $ED(CRT(0), CRT(1))$ for two tests $CRT(0)$, $CRT(1)$ and $m = 3$ are given in Table 1. The test obtained according to (5) for all possible values of the parameter d was used as the second controlled random test $CRT(1)$. The resulting values of the metric $E(k, 2^m)$ for the double test $MCRT_2$ that consists of tests $CRT(0)$ and $CRT(1)$ are shown in Table 4.

As can be seen from given numerical values, the effectiveness of the double test is in strict accordance with the values $ED(CRT(0), CRT(1))$ listed in Table 1. Indeed, for $d = 1$ and $d = 7$ the Euclidean distance between $CRT(0)$ and $CRT(1)$ equals the minimum value $\sqrt{56}$ (Table 1), respectively, and the number of additional binary combinations is minimum for all the values k. At the same time, for $d = 4$ and, consequently, for the maximum value $ED(CRT(0), CRT(1)) = \sqrt{128}$, the number of additional combinations is maximum (Table 4).

Similar results for a storage device that consists of 128 cells and $k = 3$ that confirm the efficiency of the Euclidean distance as a measure of the effectiveness of the multiple test by the example of the double test $MCRT_2$ are shown in Fig. 1.

The results in Table 4 and Fig. 1 confirm the validity of theoretical provisions and, above all, the validity of Theorem 1.

When using controlled random tests, in most cases, the number q of test sets is less than the total number of 2^m m-bit input patterns [5, 7–10]. Accordingly, the validity of the results of Theorem 1 for the case $q < 2^m$ and, above all, for Corollary 3 is significant for the proposed method of constructing controlled random tests. According to this corollary, the Euclidean distance $ED(CRT(k), CRT(l)) = \sqrt{2^m d(2^m - d)}$

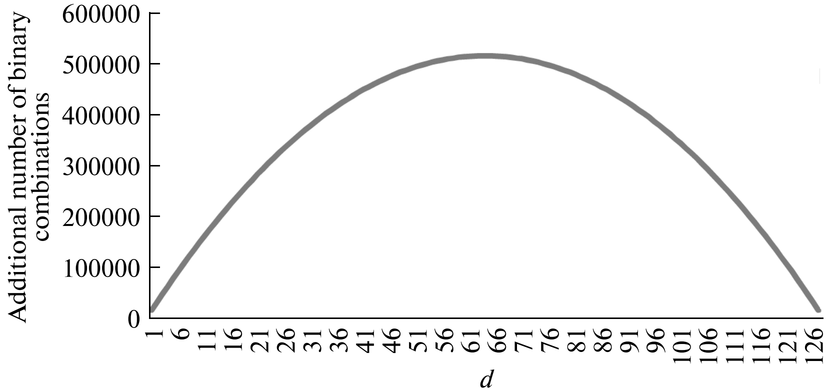

Fig. 1. $E(3, 2^7)$ is the additional number of binary combinations for all possible $k = 3$ from $2^m = 128$ bits.

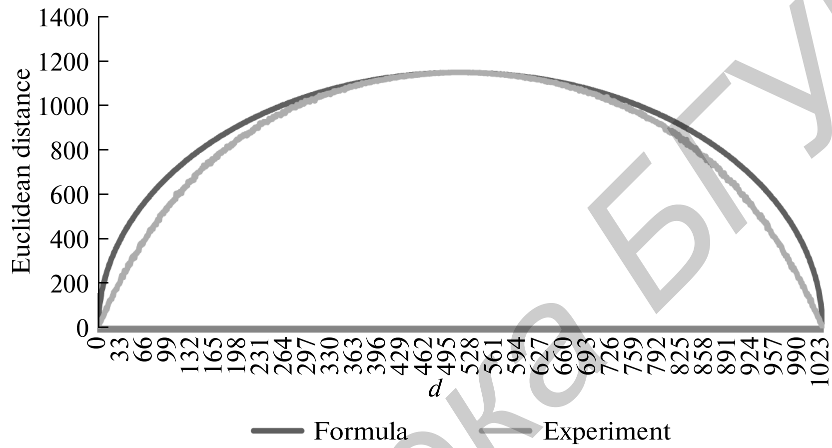

Fig. 2. Average value of the Euclidean distance $AED(CRT(k), CRT(l))$ (*experiment*) for $m = 10$ and $q = 5$ and calculated in accordance with Corollary 3 (*formula*).

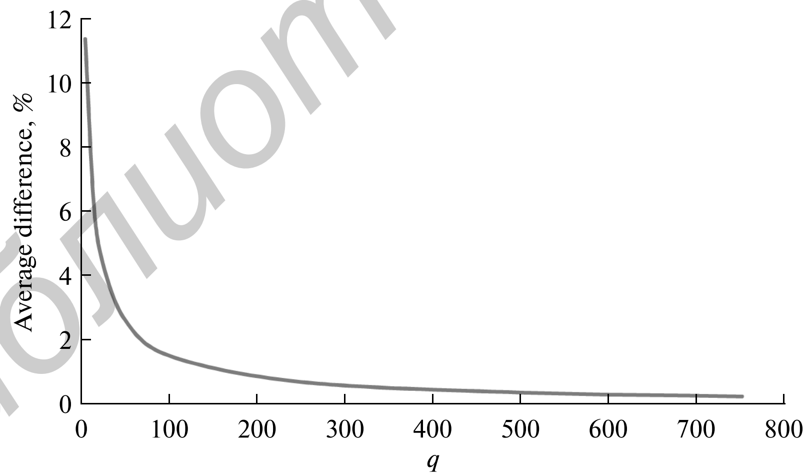

Fig. 3. Average difference value (%) of the experimental value $AED(CRT(k), CRT(l))$ from the theoretical value obtained by the formula for $m = 10$.

obtained for $q = 2^m$ can be used as a mean value for $q < 2^m$ and can be determined by the relation $AED(CRT(k), CRT(l)) = \sqrt{qd(2^m - d)}$.

Statistical tests were conducted in order to confirm this corollary. In particular, 5000 initial controlled random tests were generated for $m = 10$ and various $q < 2^m$. Then, tests $CRT(k)$ were constructed using all possible values of $CRT(k)$. Next, the experimental value of $d \in \{0, 1, ..., 1023\}$ was determined as a result of averaging over 5000 pairs of tests *CRT*(*k*) and *CRT*(*l*) and, according to Corollary 3, by the formula $\sqrt{qd(2^m - d)}$. Figure 2 shows the results for the case of the small value $q = 5$ when the experimental error is maximum with respect to the analytical result.

It is obvious that, according to Corollary 3, the error between the experimental values *AED*(*CRT*(*k*), *CRT*(*l*)), and theoretical values should decrease with increasing value of q. When $q = 2^m$, experimental and theoretical values should be equal, which is confirmed by practical results given in Fig. 3. The figure shows averaged values of deviations of the experimental data from the theoretical results depending on q.

As can be seen from Fig. 3, even for $q > 100$, the experimental results hardly differ from the theoretical values, which confirms the validity of using the results of Theorem 1 to generate controlled random tests.

6. CONCLUSIONS

The concept of multiple controlled random tests has been considered. Existing solutions have been analyzed, and a formal method for generating multiple tests has been proposed. The efficiency of using the Euclidean distance to construct multiple tests has been confirmed based on the experimental results for the case of multiple tests of storage devices.

ACKNOWLEDGMENTS

This work was carried out as part of the international cooperation between universities, project no. S/WI/3/13.

REFERENCES

1. Rajsuman, R., *System-On-A-Chip: Design and Test,* London: Artech House Publishers, 2000.
2. Ivanyuk, A.A., Proektirovanie vstraivaemykh tsifrovykh ustroistv i sistem (Designing Embedded Digital Devices and Systems), Minsk: Best-print, 2012.
3. Appelo, D., et al., On the automation of the test flow of complex SoCs, *Proc. IEEE VLSI Test Symposium (VTS 2006),* Berkeley: USA, 2006.
4. Petersen, K., Oberg, J., and Magnhagen, B., Towards an almost C-testable NoC test strategy, *Proc. East-West Design and Test Symposium (EWDTS'07),* Kharkov: Ukraine, 2007, pp. 126–132.
5. Anand, S., et al., An orchestrated survey on automated software test case generation, *J. Syst. Software,* 2014, vol. 39, no. 4, pp. 582–586.
6. Malaiya, Y.K. and Yang, S., The coverage problem for random testing, *Proc. IEEE ITC,* Las Vegas, USA, 1984, pp. 237–242.
7. Chen, T.Y., Kuo, F.-C., Merkel, R.G., and Tse, T.H., Adaptive random testing: The ART of test case diversity, *J. Syst. Software,* 2010, vol. 83, no. 1, pp. 60–66.
8. Yarmolik, S.V. and Yarmolik, V.N., Synthesis of probability tests with a small number of sets, *Avtom. Vychisl. Tekh.,* 2011, no. 3, pp. 19–30.
9. Zhou, Z.Q., Using coverage information to guide test case selection in adaptive random testing, *Proc. 34th IEEE Comp. Soft. and Applications Conf.,* 2010, pp. 208–213.
10. Sahari, M.S., A'ain, A.K., and Grout, I.A., Scalable antirandom testing (SAT), *Int. J. Innov. Sci. Modern Eng.,* 2015, vol. 3, no. 4, pp. 33–35.
11. Mrozek, I. and Yarmolik, V.N., Iterative antirandom testing, *J. Electron. Test., Theory Appl.,* 2012, vol. 9, no. 3, pp. 251–266.
12. Mrozek, I. and Yarmolik, V.N., Antirandom test vectors for BIST in hardware/software systems, *Fundamenta Informaticae,* 2012, vol. 119, no. 2, pp. 1–23.
13. Yarmolik, C.V. and Yarmolik, V.N., Multiple nondestructive march tests with variable address sequences, *Avtom. Telemekh.,* 2007, no. 4, pp. 126–137.
14. Yarmolik, S.V. and Yarmolik, V.N., Controlled random testing, *Informatika,* 2011, no. 1, pp. 79–88.
15. Yarmolik, S.V. and Yarmolik, V.N., Controlled probabilistic tests, *Avtom. Telemekh.,* 2012, no. 10, pp. 142–155.
16. Huang, R., Chen, J., and Lu, Y., Adaptive random testing with combinatorial input domain, *Sci. World J.,* 2014, vol. 2014, pp. 1–16.
17. Chen, T.Y., Huang, D.H., and Zhou, Z.Q., On adaptive random testing through iterative partitioning, *J. Inf. Sci. Eng.,* 2011, vol. 27, pp. 1449–1472.
18. Yarmolik, S.V., Zankovich, A.P., and Ivanyuk, A.A., *Marshevye testy dlya samotestirovaniya OZU* (Marching Tests for RAM Self-Testing), Minsk: Izdatel'skii tsentr BGU, 2009.

Translated by O. Pismenov