Fault Latencies of Concurrent Checking FSMs

Roman Goot
Academic Technological Institute
Golomb, 52, Holon, Israel
goot@hait.ac.il

Ilya Levin
Tel Aviv University
Ramat-Aviv 69978, Israel
ilia1@post.tau.ac.il

Sergei Ostanin
Tel Aviv University
Ramat-Aviv 69978, Israel
sostanin@post.tau.ac.il

Abstract

In this paper we introduce concepts of a potential fault latency and a real fault latency for Finite State Machines (FSMs). The potential latency defines a minimal value of the possible latency for an FSM, while the real latency relates to the certain implementation of the FSM. A method for investigation of latencies for on-line checking FSMs is described. This technique is based on selection of trajectories of the Markov chain, which describes behavior of the fault free FSM as well as the faulty FSM. We also estimate the lowest bound for an average latency. This estimation may be useful at an initial stage of the design when information concerning requirements to the FSM and conditions of its functioning is limited.

1. Introduction

A control part of digital systems is usually the most critical part from testability point of view. Irregularity and complexity of the control structure on the one hand, and its central role in functioning of the whole digital system to be controlled on the other hand, causes problems of both synthesis of self-checking controllers, and analysis of their efficiency. In this paper, we deal with the problem of analysis of the efficiency; namely, we focus on investigation of characteristics of latency for Finite State Machine (FSM) based controllers being checked on-line.

In paper [Shedletsky 76] a method for computation of testing sequence length required to detect faults of an off-line tested sequential circuits is proposed. The method consists of constructing a specific Markov process with (R + 1) states, where R is the number of states of the FSM. An additional (R + 1)-th state is an absorbing state, and the matrix of transient probabilities of the process is constructed in such a way, that the process moves to the additional state if a fault is manifested under the testing sequence.

Actually, the method described in [Shedletsky 76] can be adapted to the on-line testing. We propose a new method, which seems to be advantageous from the point of computational complexity. The obtained results allow fully considering the latency as a random value.

Since the method still requires accurate calculations and significant information about the FSM and conditions of its functioning, we propose especially at the initial state of the design, to estimate only the average latency using the limited preliminary information about structure of the FSM. Based on this, we will estimate the lower of the average latency, using only the number of states of FSM and the maximal length of a product term.

This paper is organized as follows. Section 2 describes the basic definitions and assumptions. The latency distribution functions for faults in the FSM and in the checker are shown in section 3. Section 4 considers the upper bound of the average fault latency. Experimental results are presented in section 5. The paper concludes with section 6.

2. Definitions and Assumptions

Let us describe a finite state machine (FSM) according to the Mealy model.

Let **Q**, **I**, **O** - the sets of state, input and output vectors accordingly. N_Q, N_I and N_O - numbers of elements in these sets.

Let q_1 be the initial state.

δ - the next state function: $\delta : \mathbf{Q} \times \mathbf{I} \rightarrow \mathbf{Q}$,

λ - the output function: $\lambda : \mathbf{Q} \times \mathbf{I} \rightarrow \mathbf{O}$.

We will use the following notations:

$X = \{x_1, ..., x_{N_x}\}$ are input variables of the FSM;

$Y = \{y_1, ..., y_{N_y}\}$ are state variables;

$Z = \{z_1, ..., z_{N_z}\}$ are output variables.

In our method, a somewhat different and refined definition of FSM will be useful. Namely, we say that an FSM with random primary inputs is the following entity:

Proceedings of the Euromicro Symposium on Digital System Design (DSD'02)
0-7695-1790-0/02 $17.00 © 2002 IEEE

$S = <\mathbf{Q}, \{\mathbf{I}, \Omega, p\}, \mathbf{O}, \delta, \lambda>$ where $\{\mathbf{I}, \Omega, p\}$ is an ordinary probability space with the set of elementary events $\mathbf{I}$ and σ-algebra Ω with the probability measure p [Feller 71]. We thus postulate a probabilistic model of random action on the FSM. The probabilistic behavior of an FSM can be analyzed by regarding its transition structure as a Markov chain [Kemeny 67]; in fact, it is sufficient to attach to the outgoing edges of each state a label, which represents the probability for the FSM to make that particular transition to obtain a finite state model that matches the definition of discrete-parameter Markov chain.

A discrete-parameter Markov chain $\{X(t) \mid t \in T\}$ is a stochastic process such that the number of possible states is finite, and the parameter space T is discrete. The Markov property says that the random variable representing the future behavior of the system does not depend on states reached in the past but only on the present state.

In this paper we consider homogeneous Markov chain. In this case, the Markov chain has stationary transition probabilities and it is defined by a transition probability matrix (p_{ms}), where p_{ms} is a probability of transition from the state m to the state s.

The fault model used in this paper is a general model of single stuck-at faults.

As commonly accepted [Lala 00], manifestation time of a fault is the time between the moment when the fault occurs, and the moment when the fault manifests itself. Unlike to the commonly used definition, we consider the manifestation to be any violation or distortion of the FSM correct operation, not obligatory followed by errors at the output. This suggestion enables distinguishing between *potential* and *real fault latencies* (Figure 1).

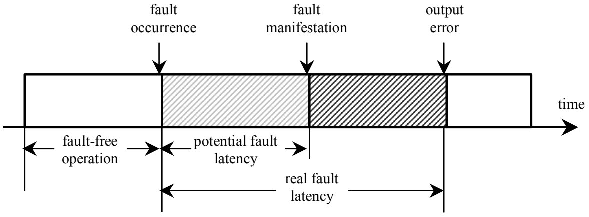

Figure 1. Fault latencies in a FSM

We say, that the manifestation time of a fault, taken in the above-mentioned sense, is *a potential fault latency.* A potential latency is a feature of the FSM as such, without any checker. The *real fault latency* is a feature of the FSM combined with a checker.

Note that one and the same checker may reach or not reach the potential fault latency. Moreover, the self-checking FSM (combined with a checker) may achieve a low latency (up to the potential) for one class of faults, and quite high latency for another class of faults. Below, we provide an example demonstrating the difference between the potential and the real fault latencies.

According to the definition of the *self-testing* feature, being the necessary requirement of the *totally self-checking* property (TSC), for each fault there is an input vector occurring during normal operation and producing a non-code output vector [Nicolaidis 98]. In light of that, manifestation of a fault does not necessary lead to the appearance of a non-code output vector. Consequently, the FSM does not possess TSC for such faults. At the same time, these faults could be detected by using a novel architecture of Algorithmic State Machine (ASM) based self-checking controllers [Levin 99].

In this paper, we assume that all faults are single, which means that the probability of occurring of the second fault during the latency of the first fault is negligibly small. We assume that the FSM has random inputs (is under random action); the latency of each fault is a random value that is characterized by its distribution function. Our purpose will be to determine the latency distribution function.

3. Latency distribution functions

The main idea of the proposed method is to divide of the whole set of possible trajectories of the random process describing behavior of the FSM, into two subsets. The first subset does not contain trajectories manifesting a particular fault. We will call it a non-manifesting subset of trajectories. The remaining (second) subset of trajectories includes the fault manifesting states. Then, the probability of the fault manifestation at the *t*-th step is equal to the probability that the process moves along the trajectories

Table 1. The transition table of the FSM

q_m	q_s	$X(q_m, q_s)$	$Z(q_m, q_s)$	h
q_1	q_2	x_1x_2	z_2, z_3	*1*
	q_4	$x_1\bar{x}_2x_3$	z_4	*2*
	q_1	$x_1\bar{x}_2\bar{x}_3$	–	*3*
	q_3	$\bar{x}_1$	z_2	*4*
q_2	q_4	*1*	z_1, z_4	*5*
q_3	q_1	x_4x_1	z_1, z_3	*6*
	q_4	$x_4\bar{x}_1$	z_1, z_4	*7*
	q_4	$\bar{x}_4$	z_1, z_4	*8*
q_4	q_5	x_2	z_5, z_6	*9*
	q_1	$\bar{x}_2$	–	*10*
q_5	q_1	*1*	z_1, z_3	*11*

from the first subset over *t*-1 steps and then, falls into the second subset at the *t*-th step. Consequently, the fault is detected exactly at the *t*-th step. The method is illustrated by an example of the FSM defined by the transition table (Table 1).

In Sections 3.1-3.3 we deal with the latency distribution functions for faults of input, output and state variables. By the fault of a variable we mean any stack-at fault of a literal of the transition table of the FSM. Section 3.4 describes construction of the latency distribution function for faults of the checker's.

3.1 Latency distribution function for faults of input variables

Let probabilities of the random variables x_l: $\Pr(x_l = 1) = p_l, \Pr(x_l = 0) = \Pr(\overline{x}_l = 1) = q_l = 1 - p_l$, $l = \overline{1, N_x}$. Then, behavior of the fault free FSM is described by Markov chain with the following transition probabilities matrix:

$$(p_{ms}) = \begin{pmatrix} p_1q_2q_3 & p_1p_2 & q_1 & p_1q_2p_3 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ p_1p_4 & 0 & 0 & q_1p_4 + q_4 & 0 \\ q_2 & 0 & 0 & 0 & p_2 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}. \quad (1)$$

First, we consider the stuck-at-one fault of variable x_1, ($x_1/1$). Let denote by B the event, consisting in manifestation of the fault, and by $\overline{B}$ - the absence of the manifestation. Now we will construct two matrices, both for the case of $\overline{B}$. The first is for $x_1 = 1$ and the second – for $x_1 = 0$. Thus, fault $x_1/1$ coincides with $x_1 = 1$ and consequently it cannot be manifested for this case. The first matrix can be obtained from (1) by replacing p_1 with 1 and q_1 with 0:

$$\left(p_{ms}\middle|\overline{B}, x_1/1, x_1 = 1\right) = \begin{pmatrix} q_2q_3 & p_2 & 0 & q_2p_3 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ p_4 & 0 & 0 & q_4 & 0 \\ q_2 & 0 & 0 & 0 & p_2 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}. \quad (2)$$

The second matrix, corresponding to $x_1 = 0$, as it follows from Table 1, looks like:

$$\left(p_{ms}\middle|\overline{B}, x_1/1, x_1 = 0\right) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & q_4 & 0 \\ q_2 & 0 & 0 & 0 & p_2 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}. \quad (3)$$

Now the matrix of the transient probability for the cases $\overline{B}$ and $x_1/1$ will be:

$$\left(p_{ms}\middle|\overline{B}, x_1/1\right) =$$
$$= p_1\left(p_{ms}\overline{B}, x_1/1, x_1 = 1\right) + q_1\left(p_{ms}\middle|\overline{B}, x_1/1, x_1 = 0\right) =$$
$$= \begin{pmatrix} p_1q_2q_3 & p_1p_2 & 0 & p_1q_2p_3 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ p_1p_4 & 0 & 0 & q_4 & 0 \\ q_2 & 0 & 0 & 0 & p_2 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}. \quad (4)$$

Note that matrices (2) - (4) describe not all the possible transitions, but only the fault-free ones. Thus, the matrices are not stochastic, i.e. the sums of elements in some rows are not equal to one.

Let the following vector:

$$p\left(t-1, \overline{B}\middle|x_1/1\right) =$$
$$\left(p_1\left(t-1, \overline{B}\middle|x_1/1\right), \ldots, p_{N_Q}\left(t-1, \overline{B}\middle|x_1/1\right)\right) \quad (5)$$

is the vector state probabilities of the FSM at the (*t*-1)th step after the fault has occured but has been not yet manifested.

Let us introduce a vector-column**:**

$$p^T\left(B\middle|x_1/1\right) = (p_{ms})(1,0,0,1,0)^T \quad (6)$$

with ones placed at the positions of the fault. *T* is a symbol matrix transponing. This is vector state probability that the fault will be manifested during one step. The probability of manifestation of the fault $x_1/1$ at *t*-th step (that is the distribution function $P_f(t)$ of the latency) can be expressed as follows:

$$P_f(t) = p\left(t-1, \overline{B}\middle|x_1/1\right)\, p^T\left(B\middle|x_1/1\right) \quad (7)$$

where vector $p\left(t-1, \overline{B}\middle|x_1/1\right)$ is obtained by a recurrent manner:

$$p\left(t-1, \overline{B}\middle|x_1/1\right) = p\left(t-2, \overline{B}\middle|x_1/1\right)\left(p_{ms}\middle|\overline{B}, x_1/1\right) \quad (8)$$

and where vector $p\left(0,\overline{B}\middle|x_1/1\right)$ is the vector of the FSM state probabilities at the moment of the fault occurrence.

Figure 2 presents results of computation of the probability that the latency is more then t, i.e.

$F(t) = \Pr(latency > t) = \sum_{\tau=t+1}^{\infty} P_f(\tau)$, with use of (7).

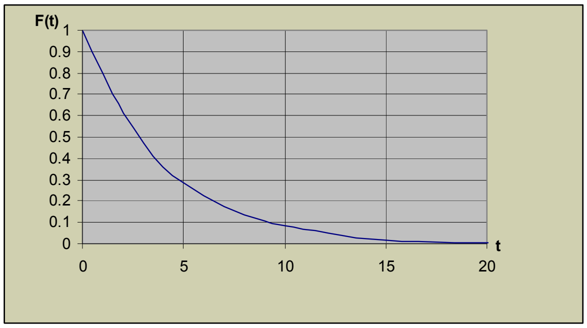

Figure 2. Cumulative curve for the fault $x_1/1$ latency.

To demonstrate the difference between the potential and the real latencies we will consider the fault $x_4/1$. Its character is seen in transitions 7 and 8 of Table 1. These transitions initiate one and the same microinstruction. For this fault, if input x_1 =0, and input x_4 =0, the both corresponding product terms will be equal to one. We consider this fact as a fault manifestation. Thus, though the fault is manifested, the manifestation at the output will be masked and consequently there will not be errors at the output of the FSM. An example of distribution functions of potential and real latencies, performed using the proposed method for fault $x_4/1$ is presented in Figure 3.

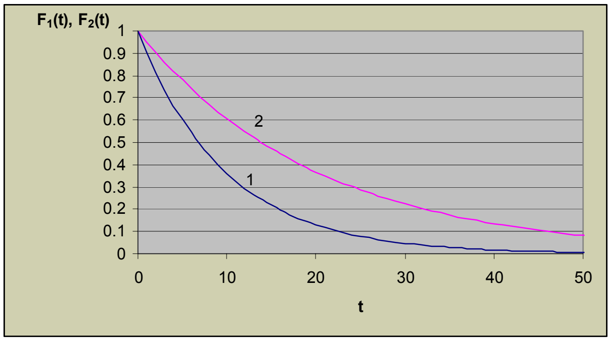

Figure 3. Cumulative curves for potential (1) and real (2) x_4/1 fault latencies.

The mentioned fault can be detected, for example, in the architecture from [Levin 99]. In this case, the real latency is actually equal to the potential latency (curve 1).

As it has been shown, manifestation of a fault may not lead to occurrence of errors at the output. Consequently, the FSM could not possess the TSC property for such faults. The self-checking architecture from [Levin99] enables detection of faults that may not lead to appearance of non-code outputs, although such faults can be detected

3.2. Fault latency distribution function for output variables

Let fault $z_1/1$ occurs. The fault will not be manifested if microinstructions containing variable z_1 are initiated (see states q_2, q_3 and q_5 of the exemplary FSM). Using the above described method, we separate such a subset from the whole set of the trajectories, which does not allow manifesting of the fault $z_1/1$. As it follows from Table 1, the matrix corresponding to the subset will be:

$$\left(p_{ms}\left(\overline{B}\right)\right)=\begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ p_1p_4 & 0 & 0 & q_1p_4+q_4 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}. \qquad (9)$$

The matrix, corresponding to the faulty states:

$$\left(p_{ms}(B)\right)=\begin{pmatrix} p_1q_2q_3 & p_1p_2 & q_1 & p_1q_2p_3 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ q_2 & 0 & 0 & 0 & p_2 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} (10)$$

is such that $\left(p_{ms}\left(\overline{B}\right)\right)+\left(p_{ms}(B)\right)=\left(p_{ms}\right)$.

The distribution function of the latency, that is the probability of the fault manifestation at the t-th step, is

$$P_f(t)=\ p\left(0,\overline{B}\middle|y_1/1\right)\left(p_{ms}\left(\overline{B}\right)\right)^{t-1}\left(p_{ms}(B)\right)(1,1,1,1,1)^T \ (11)$$

where $p\left(0,\overline{B}\middle|y_1/1\right)$ is the vector of the FSMs states at the moment of the fault rise.

3.3. Latency distribution function of the FSM memory

If states of the memory are coded by a non-redundant code, faults are not detectable, but if any redundant code is used, the memory latency depends on specific characteristics of the code. As an example, we will examine the "one-hot" code.

Fault $y_r/0$ for specific state q_r can be detected immediately at the moment of reaching the state q_r.

Let the transient probabilities matrix (p_{ms}) of the general form, is

$$(p_{ms}) = \begin{pmatrix} p_{1,1} & \ldots & p_{1,r-1} & p_{1,r} & p_{1,r+1} & \ldots & p_{1,N_Q} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \\ p_{r,1} & \ldots & p_{r,r-1} & p_{r,r} & p_{r,r+1} & \ldots & p_{1,N_Q} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ p_{N_Q,1} & \ldots & p_{N_Q,r-1} & p_{N_Q,r} & p_{N_Q,r+1} & \ldots & p_{1,N_Q} \end{pmatrix}. (12)$$

Then the matrix that allows separating the non-manifesting set of trajectories has zeros in r-th row and r-th column:

$$\left(p_{ms}^{(f)}\right) = \begin{pmatrix} p_{1,1} & \ldots & p_{1,r-1} & 0 & p_{1,r+1} & \ldots & p_{1,N_Q} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \\ 0 & \ldots & 0 & 0 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ p_{N_Q,1} & \ldots & p_{N_Q,r-1} & 0 & p_{N_Q,r+1} & \ldots & p_{1,N_Q} \end{pmatrix}. (13)$$

In our example matrix (12) takes form (1). If $p(0) = (p_1(0),..., p_{N_Q}(0))$ is the vector of initial states probabilities (at the moment of the fault rise), the latency distribution function, being the probability that by k-th step the fault will not be manifested, is:

$$\Pr(\ t>k\ ) = p(0)\ \left(p_{ms}^{(f)}\right)^k (1,\ldots,0,\ldots,1)^T \qquad (14)$$

with zero at the r-th position.

Fault $st/1$ of state q_r is manifested at the first step of entering into a state, which is not q_r. Consequently,

$$\Pr\ (t{=}1){=}p(0)\left(p_{ms}^{(f)}\right)(1,\ldots,0,\ldots,1)^T,$$
$$\Pr(\ t>k\ ) =\ p_r(0)p_{r,r}^k \qquad (15)$$

where $p_r(0)$ is r-th element of vector $p(0)$, and $p_{r,r}$ is the element of matrix (12).

3.4. Latency distribution function of the checker

For obtaining the distribution function of the checker we use the above-described method of constructing two matrixes $\left(p_{ms}(\overline{B})\right)$ and $\left(p_{ms}(B)\right)$. According to Table 1, these matrices acquire the following form:

$$\left(p_{ms}\left(\overline{B}\middle|R_1/1\right)\right) = \begin{pmatrix} 0 & 0 & q_1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ p_1p_4 & 0 & q_4 & 0 & 0 \\ p_2 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix} \qquad (16)$$

$$\left(p_{ms}\left(B\middle|R_1/1\right)\right) = \begin{pmatrix} p_1q_2q_3 & p_1p_2 & q_1 & p_1q_2p_3 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & q_1p_4 & 0 & 0 \\ 0 & 0 & 0 & 0 & q_2 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}. (17)$$

Now, to obtain the distribution function we apply formula (11) with $p\left(0, \overline{B}\middle|R_1/1\right)$.

3.5. Latency of a group of faults and average latency

Let now $\{f_u\}_{u=1}^U$ is a group of faults with probabilities of rise $\Pr(f_u) = s_u$. Then the latency distribution function of the group as a whole is $\overline{P}_f(t) = \sum_{u=1}^{U} s_u P_{f_u}(t)$, and for the average duration of the group we obtain $\overline{t} = \sum_{u=1}^{U} s_u \overline{t_u}$ with $\overline{t_u}$ being an average latency of u-th fault.

4. Upper bound of the average fault latency

The described above method of latencies computation allows for completely describing the latency as a random value. These methods require considerable calculations and significant preliminary information about the structure and parameters of the FSM. However, especially at the initial stage of design, it is possible to estimate only the average latency on the basis of quite limited information about the FSM.

We will estimate the average fault latencies of FSM by constructing the "worst" case of the FSM. We also assume that: $\Pr(x_l{=}1) = p_l = 0.5$, $l = \overline{1, N_x}$. It allows obtaining an unimprovable upper bound, for the structure of the FSM as defined.

We say, that the set of product-terms is of the *triangular* form of the length K, ($K \leq N_x$), if

$$G_{K+1} = \prod_{l=1}^{K} x_l\ ;\ G_k = \prod_{l=1}^{k-1} x_l \overline{x}_k,\ \ k = 1,\ldots,K\ . \quad (18)$$

Then, the following two theorems we formulate without proofs.

Theorem 1. For FSM with the triangular set of product-terms of length K as transition functions and equiprobable single faults, the average probability of the fault manifestation (over the single faults of all variables) is minimal and equals to

$$\overline{p}_f = \frac{1}{K}\left(1 - \frac{1}{2^K}\right). \qquad (19)$$

Theorem 2: Among all FSMs with N_Q states and N_x input variables the automaton that is shown in Figure 4 has the maximal value of the average latency for single faults. This value is equal to:

$$\overline{T} = \frac{2N_Q}{N_x}\left(2^{N_x} - 1\right) - \left(\frac{N_Q}{2} + 1\right). \qquad (20)$$

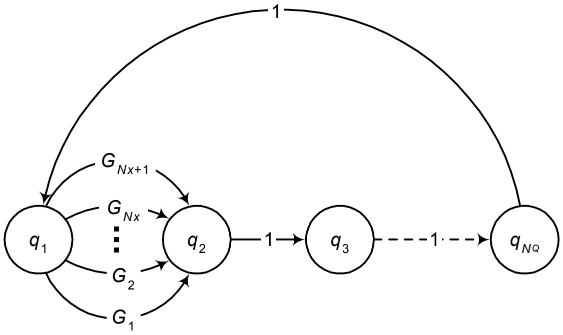

Figure 4. The graph of the FSM for the worst case of the average fault latency

5. Experimental results

Several FSM controllers were used as benchmarks in the research. Each FSM describes functioning of a special purpose microprocessor. Table 2 illustrates FSM benchmarks parameters and results of:

N_x - number of primary inputs;

N_y - number of primary outputs;

N_Q - number of states;

h – number of transitions;

$\overline{t}$ - exact values of the average potential fault latency calculated according to a method in section 3.5 of this paper; $\overline{T}$ - maximum values of the average potential fault latency calculated according to the formula (20).

Table 2. Latencies results for FSM benchmarks

Name	N_x	N_y	N_Q	h	$\overline{t}$	$\overline{T}$
big	18	28	17	185	747	2420
bs	19	13	17	185	247	903
acdl	16	27	22	214	456	1742
cow	49	24	24	261	366	1486
v1_6	14	18	17	169	237	608
v1_10	15	18	18	264	300	907
v11_20	14	29	18	367	360	1630

6. Conclusion

The paper introduces concepts of the potential and the real latencies and proposes a methodology of computation thereof for on-line checking FSMs. The concept of the potential latency allows to estimate a theoretical lower bound of the real latency for self-checking systems.

Exact expressions of statistical characteristics for the latencies are obtained. The upper bound of the average latency and the corresponding "worst" case FSM are presented. The proposed approach can be used at the initial stage of designing a self-checking FSM for estimating a possible latency of the FSM to be design.

References

[Feller 71] Feller, W., "An Introduction to Probability Theory and Its Applications", John Wiley & Sons Inc, N.Y., 1971.

[Kemeny 67] Kemeny, J., J. Snell, "Finite Markov Chains", D.Van Nostrand Comp., 1967.

[Lala 00] Lala, P., "Self-Checking and Fault Tolerant Digital Design", Morgan Kaufman Publishers, 2000.

[Levin 99] Levin, I., V. Sinelnikov, "Self-checking of FPGA based Control Units", Proceedings of 9th Great Lakes Symposium on VLSI, Ann Arbor, Michigan, 1999, IEEE press, pp. 292-295.

[Nicolaidis 98] Nicolaidis, M., Y. Zorian, "On-Line Testing for VLSI - A Compendium of Approaches", Journal of Electronic Testing: Theory and Applications, 1998, No12, pp.7-20.

[Shedletsky 76] Shedletsky, J., E. McCluskey, "The Error Latency 0f Fault in a Sequential Digital Circuit", IEEE Transaction on Computers, vol. 25, No 6, 1976, pp. 655-659.