Signature functional control of digital automatic device register operations

Tupkalo Vitalii 1, Cherepkov Serhii 2

1 Kyiv University of Intellectual Property and Law, Ukraine
2 SE «Kyivoblstandartmetrology», Ukraine
E-mail: tvn.prof@gmail.com

Abstract

The development of digital operating automatic devices models of the systems with the property of high functional controllability of hardware and software tools for the performance of computational functions (operations) on a real scale becomes a priority task in the context of ensuring high efficiency and reliability of monitoring the functioning of digital metrological telemetric measurement and control systems of critical infrastructure problem growing relevance. In the article, based on a critical analysis of known methods for digital systems functional control, a method of ensuring the operational controllability of digital automatic devices is proposed based on the concept implementation of predicting (forecasting) control signatures of tuples and their state. Relevant concepts are introduced, and a structural-functional model of functional control for digital automatic device with «hard» logic based on the method of signature prediction is proposed. In the context of the practical implementation of the proposed method of predicting signatures on each operating cycle of the digital automatic device, a system of control signature equations formulas (signature functional control rules) is given for the basic types of digital automatic device register operations with «hard» logic. This makes it possible to implement a new functional control principle (signature functional control by the method of signature prediction) of digital automatic devices by introducing a unified hardware redundancy (synthesized hardware node of a signature functional control) from functionally complete elementary combinational structures from a finite set (standard set). In this regard, the relevance of functional control by the method of predicting signatures for generators of pseudorandom sequences of the maximum length in the digital automatic device of cryptographic encryption by jamming measurement information during its transmission in telecommunication channels of management systems of critical infrastructure objects in the conditions of possible cyberattacks is reasonably grounded. The scientific novelty of the obtained theoretical results is the authors' proof of the need to develop further the methodology of functional control of a general-purpose digital automatic device and, in particular, of telemetric measurement and control systems of critical infrastructure based on the use of the author's mathematical apparatus of synthesis «signature Boolean-polynomial algebra».

Keywords: applied theory of digital automatic devices, functional signature control of digital automatic devices and systems, models and methods of control of digital systems, functional controllability of digital systems, operational control of computational operations, synthesis algebra of digital automatic devices.

1. Introduction

Today, one of the factors restraining the development of effective methods of functional (real-time) control (FC) of digital automatic devices (DAD) with «hard» logic of metrological telemetric measurement and control systems of critical infrastructure is the further aim to select and mathematically justify the FC model by introducing hardware redundancy (multiple duplication (redundancy) of DAD [1]) and information (code) redundancy [2]. In addition, there is a problem of ensuring the security of such machines against unauthorized access in the context of ensuring the efficiency and reliability of their real-time control. A
significant drawback of the method of introducing information (code) redundancy for each binary code is the dependence of the control code on the frequency of error occurrence (the degree of information distortion). Therefore, it is considered that the most common method of control based on the introduction of information redundancy in relation to various typical devices of computing equipment and digital control machines is control by the parity-oddity method of the binary number code (adding only one control digit to the significant digits of the number codes), which does not ensure multiple errors detection [3].

2. Main part

Latest sources and publications research. In the context of the defined problem of ensuring effective FC of multipurpose digital systems, a number of works are known [4-11] which consider the issue of choosing hardware control models by introducing hardware redundancy. As a rule, each author (authors) formulates his FC research task in relation to a specific type and purpose of a digital device. At the same time, it is not taken into account that these devices, according to their functional purpose, may be in an inseparable system connection of digital systems hardware and software of the corresponding intended purpose. From the above, it can be concluded that the need to develop a general methodological approach to the implementation of the FC of digital automatic devices with both “hard” and programmable logic, which would be based on the concept of an inseparable combination of digital systems hardware and software, is necessary. It can be argued that this approach is due to the fact that the systemology of modern digital systems for various purposes is based on a finite set of all known arithmetic and logical operations. In this regard, work [12] proposed a universal model of the infix notation of basic arithmetic and logical operations in relation to the implementation of their FC based on the above-mentioned methodological approach concept.

Unsolved part of the general problem. The unified methodological (system engineering) base for all arithmetic operations in digital systems is primary addition operations and register shift [13]. At the same time, it should be noted that the DAD shift register operations reduce the speed of performing arithmetic and logical operations. Therefore, in the context of this methodological approach to FC implementation, it is necessary to develop models and methods of synthesizing hardware redundancy to control multiple types of DAD registry operations.

The research goal is grounding and forming a proposition for the further direction of system engineering development of controllable DAD in relation to their types of register operations by unified structural FC redundancy based on the author’s «signature Boolean polygonic algebra» synthesis apparatus [12]. This makes it possible to implement a new FC principle of digital automatic device – signature functional control by predicting (forecasting) the control characteristics (signatures) of changes in the DAD state tuple at each operating cycle.

Task statement. The following two definitions are proposed according to the goal.

Definition 1. Functional controllability of DAD register operations is a property of DAD operational registers that characterizes their suitability for control of a certain type of operation performed by them on each operating cycle by predicting the register status code \( C_{i-1} \) number on each \((i-1)\)-th cycle of the control characteristic (signature) of the next register status code \( C_i \) number on the \(i\)-th operating cycle. That is, to allow the FC process to be displayed in time, as the relationship of preceding and following control characteristics on each pair of adjacent operating cycle. In the event of a discrepancy between the control (reference) code of the control characteristic (signature), which was formed on the \((i-1)\) cycle, with the code of the control characteristic (signature) of the shift result on the \(i\)-th operating cycle of the register, an error signal is generated.

Definition 2. A function for which the signature of each subsequent value of tuple \( C_i \) is uniquely determined by the previous \( C_{i-1} \) value of this tuple is called controllable by the signature prediction method.
In the context of the essence of Definitions 1 and 2, the structural FC model of DAD shift registers with «hard» logic based on the signature prediction method is presented in Fig. 1.

One of the ways to effectively solve the task of operational (functional) control of nodes with memory (registers) is the development of the idea of predicting control characteristics (signatures) on a more qualitative (from the point of view of control reliability) basis, in particular, on the basis of linear polynomial compression of binary number codes. In the case of using linear polynomial compression, the general reasoning for increasing the reliability of the operation control of arithmetic addition can be formulated as follows: if binary numbers $A$ and $B$ are matched with their control characteristics $R(A)$ and $R(B)$ of linear polynomial compression, then there is some control characteristic of the linear polynomial compression of the mutual correspondence of these numbers $R(A, B)$, in which the infix model of equality is valid:

$$R(A + B) = R(A) \ast R(B) \ast R(A, B), \quad (I)$$

where:

\* – the operation is performed by the corresponding DAD control device

Thus, according to (I), a necessary and sufficient condition for successful functional control is both the belonging of number codes to their classes of control characteristics and their belonging to a certain class of control characteristics of their mutual polynomial correspondence. In other words, equality (I) requires an additional (in contrast to the method of checking the parity or oddity of number codes) unambiguous division of the original sets of operands (additions)

\begin{figure}
\centering
\includegraphics[width=\textwidth]{fig1.png}
\caption{Structural-functional FC model of DAD shift registers with «hard» logic using the signature prediction method (author’s model):}
\end{figure}

\begin{itemize}
\item CD – control device;
\item GESRO – generator of expected signature of the register operation result;
\item GCR – generator of the control result;
\item SG – signature generator;
\item EC – equality comparator.
\end{itemize}
into allowed and forbidden subsets, which in principle makes it possible to increase the reliability of the control. The paper \cite{12} shows how equation (1) is transformed into an infix model of signature functional control:

\[ \text{sig}(A + B) = \text{sig}A \oplus \text{sig}B \oplus \text{sig}H(A + B), \quad (2) \]

where:

\( H(A + B) \) is the mutual polynomial characteristic of codes \( A \) and \( B \) when \( A \) and \( B \) involved in the arithmetic addition operation. The binary code \( H(A + B) \) is the code for the shift units transition that arises when adding the \( n \)-bit numbers \( A \) and \( B \).

**Definition 3** \cite{12}. The signature (\( \text{sig} \)) of the binary number \( A(x) \) is its convolution (linear transformation) \( \text{sig}A(x) = A(x) \mod P^m(x) \) by the modulus of an irreducible primitive polynomial \( P^m(x) \) of degree \( m \).

**Definition 4.** The signature FC formula in the form of a sum by the modulus two signatures is called a signature polynomial if at least one of the signatures is associated with a mutual polynomial characteristic.

In the case of a binary \( n \)-bit totalizing counter, taking into account the fairness of the superposition of equality signatures (2), we have:

\[ A_{i-1} + \beta = A_{i-1} \oplus \beta \oplus H^1(A_{i-1} + \varphi), \quad (3) \]

where:

\( A_{i-1} \) — is the content of the \( n \)-bit counter on the \((i-1)\)-th cycle of the count;

\( \varphi = [0000...01]_n \) is the constant of the \( n \)-bit grid of the counter;

\( H^1(A + \varphi) \) is the value of \( n \) lower orders of the mutual polynomial characteristic \( H(A + \varphi) \).

Therefore, the absence of an overflow situation in the controlled summing counter is \( H^1(A + \varphi) = H(A + \varphi) \). Moving from the numbers of equality (3) to their signatures, we obtain the signature formula for predicting the control characteristics of the summative \( n \)-bit counter:

\[ \text{sig}C_i = \text{sig}C_{i-1} \oplus \text{sig}\varphi \oplus \text{sig}H^1(C_{i-1} + \varphi). \quad (4) \]

If a binary counter is used to form a consecutive series of numbers in which each previous number differs from the next by some constant amount \( Q \) in the context of «correct» operation (without an overflow situation within the \( n \)-bit grid of the counter), then the formula for predicting signatures by analogy to (3) and (4) will have the form:

\[ \text{sig}C_i = \text{sig}C_{i-1} \oplus \text{sig}Q \oplus \text{sig}H^1(C_{i-1} + Q). \quad (5) \]

It follows from (4) and (5) that the speed of predicting control signatures of the account result is determined by the execution time of the chain of operations:

- the operation of forming an \( n \)-bit mutual polynomial characteristic \( H^1(C_{i-1} + \varphi) \) or \( H^1(C_{i-1} + Q) \);
- the operation of forming \( m \)-bit signatures of \( n \)-bit \((m < n)\) parallel codes \( Q \) and \( H(...+\ldots) \);
- convolution operation by modulus two \( \oplus \) for three \( m \)-bit codes.

The technical implementation of the convolution operation by modulus two is known, and in this case, it is reduced to the construction of a pyramid-type convolution combination node with the number of steps equal to three. At the same time, the operation time is three times the delay of the two-input convolution element by modulus two. Unlike the convolution operation, the first two operations of the chain reflect the specificity of the proposed method of functional control by predicting the signatures of register operations.

The basis of the synthesis of the generator of the mutual polynomial characteristic of two numbers of the parallel combinational type is the following statement: if the polynomials of the operands (additions) \( C_{i-1} \) and \( Q \) have the form:
\[ C_{i-1}(x) = c_i x^n + c_{i-1} x^{n-1} + \ldots + c_1 x; \]
\[ Q(x) = q_n x^n + q_{n-1} x^{n-1} + \ldots + c_1 x, \quad (6) \]
then the polynomial of their mutual polynomial characteristic for an \( n \)-bit counter must be limited to degree \( n \) and have the form:
\[ H^1(x) = h_n x^n + h_{n-1} x^{n-1} + \ldots + h_2 x^2. \quad (7) \]

At the same time, the absence of the term of the first degree \( h_1x \) in \( H^1(x) \) is explained by the fact that when adding two numbers, there is no transfer to the least significant (first) digit \( h_1 \). In turn, the transition of the transfer unit from the \( i \)-th digit of the counter to the \( (i+1) \)-th digit is possible if the disjunction \( c_i \lor q_i = 1 \) and there is a transfer from the \( (i-1) \)-th digit or the conjunction \( c_i q_i = 1 \). For example, \( h_2 = 1 \) if the conjunction \( h_2 = c_3 q_1 = c_3 \); \( h_3 = 1 \), if \( c_2 q_2 = c_2 q_2 \lor c_3 = c_2 \lor c_1 = c_2 q_2 \lor c_3 q_3 \), \( h_4 = 1 \), if \( h_1 c_1 q_1 \lor c_2 q_3 \), and etc.

Thus, the task of forming the mutual polynomial characteristic of applications is reduced to the synthesis of a combinational device that implements Boolean functions on its outputs:
\[ h_i = 0; h_2 = c_3 q_i; h_{i+2} = h_{i+1} (c_{i+1} \lor q_{i-1}) \lor c_{i-1} q_{i-1}, \quad i = 3, \ldots, n+1. \quad (8) \]

An example of the implementation of the scheme for forming the mutual polynomial characteristic of the \( H^1(C_{i-1} + Q) \) parallel combinational type for \( n \)-bit terms is presented in Fig. 2.

As a method of the parallel combinational type signatures generators (\( n \)-inputs, \( m \)-outputs, \( n > m \)) synthesis, it is proposed to use the author’s method \[ [12] \]. This method is based on the interpretation of the mechanism of linear convolution (transformation) of binary \( n \)-bit sequential codes of binary numbers by modulus the irreducible primitive polynomial \( P^m(x) \) of degree \( m \) into \( m \)-bit signature codes (the result of linear convolution) by analogy with the operation of a classical shift register with inverse links of the form \( P^m(x) \) \[ [14] \]. Fig. 3, as an example, schematically shows the process of forming a 3-bit signature of a 7-bit sequential code at \( P(x) = x^3 + x + 1 \).

It should be noted that a sign of the signature linearity formation (Fig. 3) is the equality of the next step content code of shift register with the sequential content code of the first (least significant) bit \( s_{i(r)} \) of the register for the number of cycles equal to the bit of the signature. Thus, these codes are equal to the cathetus of some imaginary triangle, the hypotenuse of which is a single or zero code of the same bit rate. Therefore, the connections of inputs \( x_r (r = 1, \ldots, n) \) and outputs \( s_{j[m]} (j = 1, \ldots, m) \) of the generator of
parallel type signatures are determined by the Boolean description of each of the \( m \) points of the cathetus of the last triangle according to the form of the polynomial \( P^m(x) \). Omitting elementary transformations, in the case of the generating polynomial of the \( m \)-th degree \( P^m(x) = \delta_n x^m + \delta_{m-1} x^{m-1} + \ldots + \delta_1 x + 1 \), the general formula for the connections of the outputs \( s_j[m] \) with the inputs \( x_r \) of the generators of signatures of the parallel combination type has the form:

\[
S_j[m] = x_{n-j-i} + \sum_{i, r \geq 1} \{ \delta_i x_{n-j-i} \oplus \delta_r x_{n-j-i} \}, \quad (9)
\]

where \( \Sigma \) is two by modulus.

**For example**, according to (9), for the polynomial \( P(x) = x^3 + x + 1 \), \( n = 7 \), \( m = 3 \), \( \delta_3 = \delta_1 = 1 \), the signature generator of the parallel combinational type must be synthesized according to the system of Boolean functions in Fig. 4.

From the above, it can be stated that the introduced author's interpretation of the concept of «signature» allows the task of ensuring the reliability of control (the ability to detect the fact of repeated distortions of digits in the binary code, which do not lead to a change in the parity or oddness of the code units) to be reduced to the task of choosing the form of the irreducible primitive polynomial \( P^m(x) \). At the same time, the number of stages of the signature formation node, and, therefore, the time of execution of the signature formation operation, depends on the ratio of the number of bits \( n \) of the controlled shift register and the bit rate \( m \) of the signature code (the degree of the selected polynomial \( P^m(x) \)).

**Statement 1.** The signature of a unit sequence \( L_{[n]} \) of length \( n = i(2^m - 1) \), where \( i = 1, 2, \ldots; m = \deg P(x) \), is equal to the zero sequence signature.

**Verification.** The unit sequence polynomial \( L_{[n]} \) of length \( n = 2^m - 1 \) is presented in the form:

\[
L_{[n]}(x) = x^{r-1} + x^{r-2} + \ldots + x^2 + x + 1, \quad r = 2^n - 1.
\]
Fig. 4. Combinational parallel type generator of signatures (author’s model [23])

Since the mutual polynomial characteristics between adjacent pairs of polynomials $x^k$, where $k = (1, \ldots, r)$ are equal to zero, then:

$$L_{[\phi]}(x) = \sum_{k=1}^{2^n-1} x^{k-1},$$  \quad \text{(10)}

where:

- $\Sigma$ is sum by modulus two.

Then:

$$\text{sig}_{[\phi]}(x) = \sum_{k=1}^{2^n-1} x^{k-1} \mod P(x).$$  \quad \text{(11)}

Since in equation (11), the sum by modulus two is the bitwise sum of all non-zero $m$-bit codes, it is zero, which indicates the validity of the statement when $i = 1$.

In the context of this statement relative to the signature formula (4) for predicting the control characteristics of the summative $n$-digit counter, it can be stated that this formula is quite correct. For example, when the state of a seven-digit counter changes from $C_i = 1111111$ to the state $C_j = 0000000$ with a cycle of every seven counts.

By analogy with the previous one, let us check the correctness of the signature formula (5) regarding the situation of a possible transition between the numbers of an adjacent pair of numbers tuples of the summing $n$-bit counter: an $n$-bit number of the sum $(C_{i-1} + Q)$ to $(n+1) - \text{an odd number} C_i$. That is, situations of overflow of the bit grid of the $n$-bit counter.

**Example 1.** Counter digit $n = 7$, $Q = 0000111$, the initial state of the counter $C_i = 0000000$, $P^3(x) = x^3 + x + 1$. With these input data, a fragment of numbers tuple of the summing 7-bit counter looks like this:

$$\ldots < C_{19}[1110111] < C_{20}[1111110] < C_{21}[0000101] < C_{22}[0001100] < \ldots$$
It can be seen from this fragment that the overflow of the bit grid of the counter occurred on the 21st operating cycle.

**Statement 2.** The surjective reflection of the set of $2^n$ binary numbers $A(x)$ into the set of $2^m$ binary numbers $\text{sig}A(x)$ by modulus an irreducible primitive polynomial $p^n(x)$ of degree $m(n > m)$ is a complete finite field $\text{GSF}(n, m)$ under the condition $n = i(2^m - 1)$, where $i = 1, 2, \ldots$, and can be considered an extension (Galois Signature Field) of the known Galois field $GF(2^n)$.

**Verification.** The first part of the statement «is a complete finite field» is the essence of the proof of Statement 1. The second part of the statement «can be considered as an extension (Galois Signature Field) of the known Galois field $GF(2^n)$» is based on the fact that the Galois field $GF(2^n)$, like field $\text{GSF}(n, m)$ is a finite set consisting of $2^n$ $n$-bit binary numbers, in which the rules for performing operations on numbers are defined. Performing these operations for the field $GF(2^n)$, and for the field $\text{GSF}(n, m)$ has limitations: in a finite field, all operations are performed on a finite number of elements of this field, and the results of operations (numbers) must belong to this field. For example, if two numbers $1101 + 1000$ are added in the field $GF(2^4)$, then the number $F_{[5]} = 10101$ cannot be obtained, since this number no longer belongs to the Galois field $GF(2^4)$.

In turn, in the $\text{GSF}(n, m)$ field, when performing operations in the context of the infix model of signature functional control (2), all components of the signature polynomials must be in the same bit grid. Based on this, the extension of the field $\text{GSF}(n, m)$ relative to the field $GF(2^n)$ is confirmed by the difference between the elements of the sets of algebras of these fields:

- Boolean algebra: $A_{\text{GF}} = \{0, 1\}$, $\land, \lor, \lnot$;
- Boolean-polynomial algebra by Vitalii Tupkalo $^{12}$;

$$A_{\text{GSF}} = (R; \ominus, H, H^1, \text{sig}, \alpha, \beta, \varphi),$$

where:
- $R$ — arithmetic and logical functions of binary numbers;
- two binary logical operations: addition by modulus two $\ominus$ and logical operation $H$ forming the mutual polynomial characteristic of two numbers that enter into the operation of arithmetic addition;
- two unary operations: operation of single-digit truncation of mutual polynomial characteristic $H^1$, operation of formation of $\text{sig}$ signature of binary number;
- constants: $\varphi$ — a binary number with a unit only in the lower digit, $\alpha$ — a number with units in all digits (inversion constant), $\beta$ — a number with a unit only in the upper digit.

An example of the $\text{GSF}(n, m)$ field at $n = 7$, $P(x) = x^3 + x + 1$ in tabular form is shown in Table 1. Returning to the signature polynomial (5), based on Statement 2 for example $1$ $\ldots < C_{20}[1111110] < C_{21}[10000101] < C_{22}[0001100] < \ldots$, we have the following tuple of control actions and results (signatures):

$$\ldots < \text{sig}C_{20} = \text{sig}C_{19} \oplus \text{sig}Q \oplus \text{sig}H^1(C_{19} + Q)$$

$$001 = 110 \oplus 101 \oplus 010 = 001;$$

$$\text{sig}C_{21[7]} = \text{sig}C_{20[7]} \oplus \text{sig}Q_{[7]} \oplus \text{sig}H^1_{[7]}(C_{20} + Q)$$

$$110 = 001 \oplus 101 \oplus 010 = 110;$$

$$\text{sig}C_{22} = \text{sig}C_{21[7]} \oplus \text{sig}Q \oplus \text{sig}H^1(C_{21[7]} + Q) < \ldots$$

$$001 = 110 \oplus 101 \oplus 010 = 001.$$

From this example, it can be concluded that in the case of the bit grid overflow of the register generator of the DAD management code tuple with «hard» logic, the continuous formation of its other management tuple code (numbers) begins. This change in the tuple of codes (numbers) depends on the choice of the $Q$ number when programming the DAD. At the same time, the correctness of the signature FC according to the signature polynomial (5) is not violated.
Example 2. The authors used the input data of Example 1, but when generating the code of the number $C_{21}$, a triple error occurred (register failure). That is, the code $C_{21}[10000101]$ was formed as $C_{E21}11000101$. At the same time, the parity of the code was not violated, and therefore, in the case of the organization of functional control of the DAD on the parity of the code of numbers, the error cannot be detected. The situation will be different if functional control is carried out according to the proposed signature prediction method, namely:

$$\text{Table 1. Field GSF}(7,3),\, P(x) = x^3 + x + 1.$$
1. Register subtraction operation, when each previous number differs from the next one by some constant value $Q$.

As a result of performing primitive-recursive operations of subtraction taking into account superposition (3) at each cycle of execution, we have:

$$C_i = C_{i-1} \oplus (-Q) \oplus H^1[C_{i-1} + (-Q)]$$  (12)

and then the task of control by the method of predicting the control signatures of the subtracting $n$-bit DAD counter is reduced to the task of controlling the summing counter with the difference that the second term $(-Q)$ according to the author’s Boolean-polynomial algebra must be represented in the form of an additional code [12]:

$$(-Q)_{add} = \text{const} = D = (Q \oplus \alpha) \oplus \varphi \oplus H^1[(Q \oplus \alpha) + \varphi]$$  (13)

and then:

$$C_i = C_{i-1} \oplus Q \oplus \alpha \oplus \varphi \oplus H^1[(Q \oplus \alpha) + \varphi] \oplus \varphi \oplus H^1[C_{i-1} + (Q \oplus \alpha \oplus \varphi \oplus H^1[(Q \oplus \alpha) + \varphi])]$$.  (14)

When passing from (13) to the signature prediction formula according to (11), we have the following signature control rule:

$$\text{sig}C_i = \text{sig} C_{i-1} \oplus \text{sig} D \oplus \text{sig} H^1(C_{i-1} + D)$.  (15)

**Example 3.** The counter digit is $n = 7$, $Q = 0001111 = 7_{10}$, the initial state of the counter is $C_i = 1111111 = 127_{10}$, $P^3(x) = x^3 + x + 1$,

with

$$(-Q)_{add} = D = 0000111 \oplus 1111111 \oplus 0000001 \oplus 0000000 = 1111001.$$

With these input data, a fragment of the tuple of numbers of the subtracting 7-bit DAD counter looks like this:

$$C_2 = C_1 \oplus D \oplus H^1(C_1 + D) = 1111111 \oplus 1111001 \oplus 1111110 = 1111000 = 120_{10};$$

$$C_3 = C_2 \oplus D \oplus H^1(C_2 + D) = 1111000 \oplus 1111001 \oplus 1110000 \oplus 1110001 \oplus 113_{10};$$

$$C_i[1111111] < C_2 [1111000] < C_3 [1110001] < \ldots$$

127 120 113

For this fragment, we have the following tuple of control actions and results (signatures):

$$\text{sig}C_2 = \text{sig} C_1 \oplus \text{sig} D \oplus \text{sig} H^1(C_1 + D);$$

$$101 = 000 \oplus 100 \oplus 001 = 101;$$

$$\text{sig}C_3 = \text{sig} C_2 \oplus \text{sig} D \oplus \text{sig} H^1(C_2 + D);$$

$$010 = 101 \oplus 100 \oplus 011 = 010.$$

2. Recurrent register polynomial operations of DAD generation of binary pseudorandom sequences of maximum length (PSML).

The relevance of FC PSML generators based on the method of signature prediction is due, for example, to their use in DAD of cryptographic encryption by jamming [15] of measurement information during its transmission in telecommunication channels of management systems of critical infrastructure objects in conditions of possible cyberattacks.

When describing the RG shift register (Fig. 5) with inverse internal connections according to the chosen degree $m$ the primitive irreducible polynomial generation $P(x) = b_0 x^m + b_{m-1} x^{m-1} + \ldots + b_1 x + 1$ linear recurrent equation looks like:

$$a_{r(i)} = \sum_{r=0}^{m} b_r a_{r(i)},$$  (16)

where:

$a_{r(i)}$ is the value of the bit at the input of the lower bit of the RG after the $i$-th shift cycle;

$a_{r(i)}$ is the value of the $r$-th digit of the RG after the $i$-th shift cycle.

The execution of this operation is carried out without loss of information, and therefore, the state of RG after the $(i + 1)$-th cycle of generation has the following description:
Fig 5. Model of the recurrent register polynomial operation DAD (author’s model)

\[
A_{i+1}^{RG} = (A_i^{RG} + \varphi_{[m]} \sum_{r=1}^{m} b_r a_{r(i)}) \tag{17}
\]

where:

\[
A_i^{RG} = H^1 \left[ \left( A_i^{RG} \oplus a_{m(i)} b_{[m]} \right) + \left( A_i^{RG} \oplus a_{m(i)} b_{[m]} \right) \right] = H^1 (A_i^{RG} + A_i^{RG}). \tag{18}
\]

When passing from (16) to the formula for predicting the signatures of each RG state, we have the following rule for signature control of PSML generation:

\[
sig A_{i+1}^{RG} = sig H^1 (A_i^{RG} + A_i^{RG}) \oplus (\varphi_{[m]} \sum_{r=1}^{m} b_r a_{r(i)}). \tag{19}
\]

It should be noted that the output PSML can be taken from any state of the register (except for the zero combination). Moreover, PSML symbols can be read from any register output. In this case, time-shifted sequences are obtained.

Example 4. Let us check the correctness of rule (18). Let us choose the PSML generation polynomial of the form \( P(x) = x^3 + x + 1 \). The process of generation of the PSML according to the model of Fig. 5 is presented in Fig. 6.

For this example, we have the following tuple of control actions and results according to rule (18):

\[
sig A_0 = sig H^1 (A_0 + A_0) \oplus [001] \land [1 \oplus 1]
\]

\[
\begin{align*}
100 &= 100 = 110 \\
110 &= 111 \oplus 001 = 110 \\
011 &= 011 = 110 \\
111 &= 111 = 111 \\
001 &= 000 \oplus 001 = 001
\end{align*}
\]

By analogy with Example 2, it can be asserted that the FC of PSML generators by the method of predicting control signatures has no fundamental restrictions regarding the type of the chosen irreducible primitive polynomial of generation.

3. Conclusions

The scientific novelty of the obtained theoretical results is the proof by the article authors of the need to develop further the methodology of functional control of general-purpose digital automatic devices and, in particular, of telemetric measurement and control systems of critical infrastructure based on the use of the author’s mathematical apparatus of synthesis «signature Boolean-polynomial algebra». In this regard, a method of ensuring the operational controllability of the DAD is proposed based on the implementation of the concept of prediction (forecasting) of the control signatures of tuples of their state.
text of the practical implementation of the proposed method of predicting signatures on each operating cycle of the DAD, a system of formulas of control signature equations (rules of signature functional control) is given for the basic types of register operations of the DAD with «hard» logic. This makes it possible to implement a new principle of FC (signature FC) of digital automatic device by introducing unified hardware redundancy from functionally complete elementary structures from a finite set (standard set). The further development of the article's topic is the development of the method of signature functional control based on the method of prediction of signatures for DAD with flexible (programmed) logic.

Fig. 6. PSML generation process (author’s model)
References


7. Fedukhin A., Cespedes Garcia P. 2018 To the question of the structures of fault-tolerant computers of the firm stratus computer inc [К вопросу о структурах отказоустойчивых компьютеров фирмы stratus computer inc]. Mathematical machines and systems. № 4, pp. 87-100. [In Russian]


