UDC 519.7 DOI 10.17223/20710410/50/4

PROBLEMS IN THEORY OF CRYPTANALYTICAL INVERTIBILITY OF FINITE AUTOMATA

G. P. Agibalov

National Research Tomsk State University, Tomsk, Russia

E-mail: agibalov@mail.tsu.ru

The paper continues an investigation of the cryptanalytical invertibility concept of finite automata with a finite delay introduced by the author in his previous papers where he also gave a constructive set theory test for an automaton A to be cryptanalytically invertible, that is, to have a recovering function f which allows to calculate a prefix of a length m in an input sequence of the automaton A by using its output sequence of a length $m+\tau$ and some additional information about A known to cryptanalysts, defining a type of its invertibility and of its recovering functon. Here, we expound a test for that of another kind, namely some logical necessary and sufficient conditions for an automaton A to have or not a recovering function f of a certain type. Results related to specific types of automata invertibility (invertibility tests, inversion algorithms, synthesis of inverse automata and others) are subjects of further researching and publications.

Keywords: *finite automata, information-lossless automata, automata invertibility, recovering function, cryptanalytical invertibility, cryptanalytical invertibility conditions.*

1. Introduction

The finite automata invertibility with a finite delay is studied from a cryptanalyst's point of view, namely in dependence on a priori information accessible to an inversion algorithm. In cryptanalysis of symmetric finite automata ciphers by attack with known ciphertext, the case, when there is a need for solution to an automaton inversion problem by a partially informed cryptanalyst, is very typical. The cryptanalysts can or can not know some information about the transfer or output functions of the automaton, about its initial, intermediate or final state, a part of input word, playing a service role, its length or the place in the input sequence and others. The variety of information, which can be known to a cryptanalyst, provides many different types of the automaton invertibility and many different classes of invertible automata. In this paper, it is assumed that the transfer and output functions of the automaton under consideration are known completely or up to accuracy of their classes and the cryptanalysis problem is to recover the prefix of input word.

The automaton cryptanalytic invertibility with a finite delay plays a very important role in the analysis and synthesis of finite automata cryptographic systems. In this paper it is studied with a delay denoted by an integer τ. From the cryptanalyst's point of view, this notion means the theoretical possibility for recovering, under some conditions, any prefix α of a length m in an unknown input sequence $\alpha\delta$ of an automaton from its output sequence γ of the length $m+\tau$ and perhaps an additional information such as parameters τ and m, initial, intermediate or final states of the automaton or the suffix δ of the length τ in the input sequence. The conditions imposed on the recovering algorithm require for prefix α to

be arbitrary and may require for the initial state q and suffix δ to be arbitrary or existent, that is, the variable α is always bound by the universal quantifier and each of variables q and δ may be bound by any of quantifiers — universal ($\forall$) or existential ($\exists$) one. The variety of information, which can be known to a cryptanalyst, provides many different types of the automaton invertibility and, respectively, many different classes of invertible automata.

Thus, in the paper, an invertibility with a finite delay τ of a finite automaton A is a property of this automaton that allows to precisely determine any input word α of a length m for the output word γ being the result of transforming by the automaton A at its initial state q the input word $\alpha\delta$ with the delay word δ of length τ and with the known m, τ, A, γ and a subset υ of the set, consisting of the delay word δ and initial, intermediate and final states $q, \psi(\alpha, q), \psi(\alpha\delta, q)$, to which A transits from q under acting of input words α and $\alpha\delta$ respectively and where q and δ may be arbitrary or some elements in their sets. According to this, the automaton A is called invertible with a delay τ if there exists a function $f(\gamma, \upsilon)$ and a triplet of quantifiers $\kappa \in \{K_1x_1K_2x_2K_3x_3 : K_ix_i \in \{\forall q, \exists q, \forall\alpha, \forall\delta, \exists\delta\}, i \neq j \Rightarrow$ $\Rightarrow x_i \neq x_j\}$ such that $\kappa(f(\gamma, \upsilon) = \alpha)$; in this case f is called a recovering function, κ — an invertibility type, υ — an invertibility order of the automaton A and $\exists f\kappa(f(\gamma, \upsilon) = \alpha)$ — an invertibility condition for the automaton A. The most known invertibility conditions for finite automata described earlier as strong and weak by scientists D. A. Huffman, A. Gill, Sh. Even, A. A. Kurmit, Z. D. Dai, D. F. Ye, K. Y. Lam, R. Tao from [1 – 8] are $(\forall q\forall\alpha\forall\delta, \varnothing)$ and $(\forall q\forall\alpha\forall\delta, \{q\})$ respectively.

There are many scientific problems which are related to the cryptanalytical notion of the automaton invertibility with finite delay and are thoroughly enumerated in the previous author's paper [9]. Some of them were particularly solved in [10]. Here we study the decision problem of finding out whether a given automaton is invertible of a given type with a given delay.

The main result of this study is presented by the logical expressions from quantifier logic that are constructively describe necessary and sufficient conditions for an automaton A to have a recovery function f of a certain type and, consequently, to be invertible with a finite delay and of a given type.

Further, in sections 3 and 4, as a short review, we tell some own results related to automaton and function cryptanalytical invertibility conditions.

2. Finite automata and normal logical formulas

A finite automaton is described as $A = (X, Q, Y, \psi, \varphi)$, where X, Q and Y are its input alphabet, state set and output alphabet respectively, ψ and φ — its transfer and output functions, $\psi : X \times Q \to Q$ and $\varphi : X \times Q \to Y$. The last ones being defined for pairs $xq \in X \times Q$, are extended to pairs $\alpha q \in X^* \times Q$ by induction on the length $|\alpha|$ of the word $\alpha \in X^*$, namely the functions $\psi : X^* \times Q \to Q$ and $\bar{\varphi} : X^* \times Q \to Y^*$ are defined as $\psi(\Lambda, q) = q$, $\psi(\alpha\beta, q) = \psi(\beta, \psi(\alpha, q))$, $\bar{\varphi}(\Lambda, q) = \Lambda$, $\bar{\varphi}(x, q) = \varphi(x, q)$ and $\bar{\varphi}(\alpha\beta, q) = \bar{\varphi}(\alpha, q)\bar{\varphi}(\beta, \psi(\alpha, q))$. Here the symbol Λ denotes the empty word in any alphabet. Thus, $\psi(\alpha, q)$ is a state, into which the automaton A comes from a state q under acting input word α, and $\bar{\varphi}(\alpha, q)$ is an output word which the automaton produces this time.

Everywhere further τ is a non-negative integer called a delay and it is supposed that in logical formulas $a \in X$, $b \in X$, $\alpha \in X^*$, $\beta \in X^*$, $\delta \in X^\tau$, $\varepsilon \in X^\tau$, $q \in Q$, $s \in Q$.

3. Decision Problem for finite Automaton Cryptanalytical Invertibility

Consider a finite automaton $A = (X, Q, Y, \psi, \varphi)$. Let q, α, δ be variables with values in Q, X^*, X^τ, denoting respectively initial state, prefix and suffix of input word $\alpha\delta$ of the

automaton A, and $K = \{\forall q, \forall\alpha, \forall\delta, \exists q, \exists\delta\}$ be the set of universal and existential quantifiers bounding these variables. In reality, the quantifiers in K are $\forall q \in Q$, $\forall\alpha \in X^*$, $\forall\delta \in X^\tau$, $\exists q \in Q$, $\exists\delta \in X^\tau$. For brevity, we write them without ranges of its variables. Note, that K doesn't contain the quantifier $\exists\alpha$. Also, let V be the set of all subsets $\upsilon(q, \alpha, \delta)$ of the set $V_0 = \{q, \delta, \psi(\alpha, q), \psi(\alpha\delta, q)\}$ with the initial, intermediate, and final states $q, \psi(\alpha, q)$, and $\psi(\alpha\delta, q)$ respectively and a delay word δ.

We say, that the automaton A is *cryptanalytically invertible* (with a *delay* IDel $\tau = |\delta|$, of a *type* IT $= (K_1x_1, K_2x_2, K_3x_3)$ with $\{x_1, x_2, x_3\} = \{q, \alpha, \delta\}$, of a *degree* IDeg $= (K_1, K_2, K_3)$, $K_i \in \{\forall, \exists\}$, $K_ix_i \in K$, $i = 1, 2, 3$, and of *an order* IO $= \upsilon(q, \alpha, \delta) \in V$) if there exists an *inverse* (*recovering*) *function* IF $f : Y^* \times V \to X^*$ *with the invertibility property* expressed in the form

$$K_1x_1K_2x_2K_3x_3(f(\bar{\varphi}(\alpha\delta, q), \upsilon(q, \alpha, \delta)) = \alpha), \tag{1}$$

in this case the used delay IDel, type IT, degree IDeg, order IO and function IF we call the parameters of this invertibility.

In reality, 208 different kinds of cryptanalytical invertibility of finite automata are now defined. All of them are presented in the Table 1 [9].

Table 1

Formulas for cryptanalytical invertibility conditions of a finite automaton

No	Quantifier prefix	No	Underlying expression
		1	$f(\bar{\varphi}(\alpha\delta, q)) = \alpha$
		2	$f(\bar{\varphi}(\alpha\delta, q), q) = \alpha$
		3	$f(\bar{\varphi}(\alpha\delta, q), \psi(\alpha, q)) = \alpha$
1	$\exists f\,\forall q\,\forall\alpha\,\forall\delta$	4	$f(\bar{\varphi}(\alpha\delta, q), \psi(\alpha\delta, q)) = \alpha$
2	$\exists f\,\forall q\,\forall\alpha\,\exists\delta$	5	$f(\bar{\varphi}(\alpha\delta, q), \delta) = \alpha$
3	$\exists f\,\forall q\,\exists\delta\,\forall\alpha$	6	$f(\bar{\varphi}(\alpha\delta, q), q, \psi(\alpha, q)) = \alpha$
4	$\exists f\,\exists q\,\forall\alpha\,\forall\delta$	7	$f(\bar{\varphi}(\alpha\delta, q), q, \psi(\alpha\delta, q)) = \alpha$
5	$\exists f\,\exists q\,\forall\alpha\,\exists\delta$	8	$f(\bar{\varphi}(\alpha\delta, q), q, \delta) = \alpha$
6	$\exists f\,\exists q\,\exists\delta\,\forall\alpha$	9	$f(\bar{\varphi}(\alpha\delta, q), \psi(\alpha, q), \psi(\alpha\delta, q)) = \alpha$
7	$\exists f\,\forall\alpha\,\exists q\,\forall\delta$	10	$f(\bar{\varphi}(\alpha\delta, q), \psi(\alpha, q), \delta) = \alpha$
8	$\exists f\,\forall\alpha\,\exists q\,\exists\delta$	11	$f(\bar{\varphi}(\alpha\delta, q), \psi(\alpha\delta, q), \delta) = \alpha$
9	$\exists f\,\forall\alpha\,\forall\delta\,\exists q$	12	$f(\bar{\varphi}(\alpha\delta, q), q, \psi(\alpha, q), \psi(\alpha\delta, q)) = \alpha$
10	$\exists f\,\forall\alpha\,\exists\delta\,\forall q$	13	$f(\bar{\varphi}(\alpha\delta, q), q, \psi(\alpha, q), \delta) = \alpha$
11	$\exists f\,\forall\delta\,\exists q\,\forall\alpha$	14	$f(\bar{\varphi}(\alpha\delta, q), q, \psi(\alpha\delta, q), \delta) = \alpha$
12	$\exists f\,\exists\delta\,\forall q\,\forall\alpha$	15	$f(\bar{\varphi}(\alpha\delta, q), \psi(\alpha, q), \psi(\alpha\delta, q), \delta) = \alpha$
13	$\exists f\,\exists\delta\,\forall\alpha\,\exists q$	16	$f(\bar{\varphi}(\alpha\delta, q), q, \psi(\alpha, q), \psi(\alpha\delta, q), \delta) = \alpha$

The definition of the cryptanalytical invertibility of a finite automaton given above unfortunately is not constructive one. It doesn't contain any necessary and sufficient conditions for an automaton to be cryptanalytically invertible with the given parameters, but implies the existence of a recovering function, and should be provided with an algorithmic test in order to effectively find out whether there exist the function f such that the formula (1) is true and in case of a positive answer to produce an effective algorithm for constructing such a function, to become convinced in the automaton cryptanalytical invertibility with the nedeed properties and possibly with the existence of the inverse automaton and to design the last.

So, the following is the first Decision Problem which we need to put and try to solve for further developing the theory of Cryptanalytically Invertible finite automata — ACIDP: given a finite automaton A, the values of invertibility delay IDel τ, an invertibility type IT,

an invertibility degree IDeg and (or) an invertibility order IO for cryptanalytical invertibility of the automaton A, find out whether the automaton A is invertible of type IT with the delay τ and of order IO and if so, to construct a proper recovering function f satisfying the condition (1).

The important place in this row takes the problem of creation or generating invertible automata of all possible types. In various decisions of this problem different requirements to generated automata can be presented: with equal probability in given invertibility class, with bounded complexity, with the great or, otherwise, small delay of invertibility and so on. Its solution seems to be impossible without proper decision of the first problem.

Further, in this Section, we tell some results related to ACIDP, published in [9, 10] and given here in the form of Propositions.

Proposition 1 [9]. The automaton A is cryptanalytically invertible with the delay $\tau = |\delta|$, of type $(\forall q, \forall\alpha, \forall\delta)$, and of an order $\upsilon(q, \alpha, \delta)$, that is, there exists a function $f : Y^* \times V \to X^*$ with the invertibility property

$$\forall q \forall\alpha \forall\delta (f(\bar{\varphi}(\alpha\delta, q), \upsilon(q, \alpha, \delta)) = \alpha),$$

if and only if

$$\forall q \forall\alpha \forall\delta \forall s \forall\beta \forall\varepsilon (\alpha \neq \beta \Rightarrow (\bar{\varphi}(\alpha\delta, q), \upsilon(q, \alpha, \delta)) \neq (\bar{\varphi}(\beta\varepsilon, s), \upsilon(s, \beta, \varepsilon)).$$

Proposition 2 [9]. If the automaton A is invertible of a delay $|\delta|$, of a type $K_1x_1K_2x_2K_3x_3$, and of an order $\upsilon(q, \alpha, \delta)$, that is, if there exists a function $f : Y^* \times V \to X^*$ with the invertibility property (1), then

$$K_1x_1K_2x_2K_3x_3K_1y_1K_2y_2K_3y_3\big(\alpha \neq \beta \Rightarrow (\bar{\varphi}(\alpha\delta, q), \upsilon(q, \alpha, \delta)) \neq (\bar{\varphi}(\beta\varepsilon, s), \upsilon(s, \beta, \varepsilon))\big),$$

where $\{x_1, x_2, x_3\} = \{q, \alpha, \delta\}, \{y_1, y_2, y_3\} = \{s, \beta, \varepsilon\}$.

Definition 1 [10]. Having a quantifier sequence $K_1x_1, \ldots, K_nx_n$ (a quantifier prefix of a predicate logical formula in a normal form), we believe $n = m + s$, $i_1 \leqslant \ldots \leqslant i_m$, $j_1 \leqslant \ldots \leqslant j_s$, $\{i_1, \ldots i_m, j_1, \ldots, j_s\} = \{1, \ldots, n\}$, $K_{i_1} = \ldots = K_{i_m} = \forall$, $K_{j_1} = \ldots = K_{j_s} = \exists$. Also, for $r \in \{j_1, \ldots, j_s\}$ let $\varepsilon_r : D_1 \times \ldots \times D_{r-1} \to D_r$ be a function (called existential) the value $\varepsilon_r(a_1, \ldots, a_{r-1})$ of which is computed by the quantifier K_rx_r with $K_r = \exists$ as a next value a_r of the variable x_r in dependence on the last values $a_1, \ldots, a_{r-1}$ of variables $x_1, \ldots, x_{r-1}$, predecessors to variable x_r. Finally, define the vector existential function $\varepsilon = \varepsilon_{j_1} \ldots \varepsilon_{j_s}$ and the set M_ε called the existential domain of the quantifier sequence $K_1x_1 \ldots K_nx_n$ corresponding to existential functions in ε. By the definition

$$a_1 \ldots a_n \in M_\varepsilon \Leftrightarrow (a_1 \ldots a_n \in D_1 \times \ldots \times D_n) \& (a_{j_1} \ldots a_{j_s} = \varepsilon_{j_1}(a_1 \ldots a_{j_1-1}) \ldots \varepsilon_{j_s}(a_1 \ldots a_{j_s-1}).$$

Proposition 3 [10]. The automaton A is cryptanalytically invertible of a delay $|\delta|$, of a type $K_1x_1K_2x_2K_3x_3$, where $\{x_1, x_2, x_3\} = \{q, \alpha, \delta\}$, and of an order $\upsilon(q, \alpha, \delta)$, that is, there exists a function $f : Y^* \times V \to X^*$ with the invertibility property, if and only if for $K_1x_1K_2x_2K_3x_3$ there is an existential vector function ε such that

$$\forall a_1a_2a_3 \in M_\varepsilon \forall b_1b_2b_3 \in M_\varepsilon (\alpha \neq \beta \Rightarrow ((\bar{\varphi}(\alpha\delta, q), \upsilon(q, \alpha, \delta)) \neq (\bar{\varphi}(\beta\varepsilon, s), \upsilon(s, \beta, \gamma)))),$$

where q and $s \in Q, \alpha$ and $\beta \in X^*, \delta$ and $\gamma \in X^\tau, a_1a_2a_3$ and $b_1b_2b_3 \in M_\varepsilon$, if $a_k = q, \alpha$ or δ, then $b_k = s, \beta$ or γ respectively, $k \in \{1, 2, 3\}$.

4. Decision Problem for Function Cryptanalytical Invertibility

This problem we use as an auxiliary one to the main problem — ACIDP.

Let $g(x_1, \ldots, x_n)$ be a function in variables $x_1, \ldots, x_n$ with a range D_g, $K_i x_i$ be a quantifier bounding the variable x_i, $i = 1, \ldots n$, $k_0 \in \{1, \ldots, n\}$, and $K_{k_0} = \forall$. Let $f : D_g \to D_{k_0}$ denote an arbitrary function with the domain D_g and the range D_{k_0} and, for definition correctness of f, let $|D_g| \geqslant |D_{k_0}|$. Moreover, always further we believe that each function under consideration has a domain with the number of elements not less than the number of elements in its range.

We say, that the function $g(x_1, x_2, \ldots, x_n)$ is *cryptanalytically invertible* (with respect to an invertibility variable IV $= x_{k_0}$ and of the type IT $= K_1 x_1 \ldots K_n x_n$) if there exists an *inverse* (*recovering*) *function* $f : D_g \to D_{k_0}$ with the *invertibility property* expressed in the form

$$K_1 x_1 \ldots K_n x_n (f(g(x_1, \ldots, x_n)) = x_{k_0}), \tag{2}$$

in this case the used number k_0, type IT, and the function f we call the parameters of this invertibility.

The following is the Decision Problem for Function Cryptanalytical Invertibility — FCIDP: given a function g, a variable x_{k_0} and invertibility type IT $= K_1 x_1 \ldots K_n x_n$ for cryptanalytical invertibility of the function g, find out whether the function g is invertible with respect to IV x_{k_0} and of type IT and if so, to construct a function f satisfying the condition (2).

We should see that our main problem ACIDP is obtained from the particular case of our auxiliary problem FCIDP by taking $n = 3$, $k_0 \in \{1, 2, 3\}$, $\{x_1, x_2, x_3\} = \{q, \alpha, \delta\}$, $x_{k_0} = \alpha$, $g(x_1, x_2, x_3) = (\bar{\varphi}(\alpha\delta, q), \upsilon(q, \alpha, \delta))$. Thus, a method deciding the auxiliary problem also decides the main one and so, our problem ACIDP reduces to our problem FCIDP.

Now we tell some theoretical results related to FCIDP published in [9, 10].

Proposition 4 [9]. For any function $g : D_1 \times \ldots \times D_n \to D_g$ a function $f : D_g \to D_{k_0}$ with the invertibility property

$$\forall x_1 \ldots \forall x_n (f(g(x_1, \ldots, x_n)) = x_{k_0})$$

exists if and only if

$$\forall x_1 \ldots \forall x_n \forall y_1 \ldots \forall y_n (x_{k_0} \neq y_{k_0} \Rightarrow g(x_1, \ldots, x_n) \neq g(y_1, \ldots, y_n)).$$

Proposition 5 [9]. For any function g, if there exists a function $f : D_g \to D_{k_0}$ with the invertibility property (2), then

$$K_1 x_1 \ldots K_n x_n K_1 y_1 \ldots K_n y_n (x_{k_0} \neq y_{k_0} \Rightarrow g(x_1, \ldots, x_n) \neq g(y_1, \ldots, y_n)).$$

Proposition 6 [10]. For any function $g(x_1, \ldots, x_n)$ there exists a function $f : D_g \to$ $\to D_{k_0}$ with the invertibility property (2), if and only if for each $k \in \{j_1, \ldots, j_s\}$ there exists an existential function $\varepsilon_k : D_1 \times \ldots \times D_{k-1} \to D_k$ such that the set M_ε corresponding to $\varepsilon = \varepsilon_{j_1} \ldots \varepsilon_{j_s}$ satisfies the following condition:

$$\forall a = a_1 \ldots a_n \in M_\varepsilon \forall b = b_1 \ldots b_n \in M_\varepsilon (a_{k_0} \neq b_{k_0} \Rightarrow g(a) \neq g(b)).$$

5. Formulas for cryptanalytical invertibility conditions for finite automata

The Table 1 from [9] is presented here for constructing invertibility condition of an automaton from its parts. The line number $i \in \{1, 2, \ldots, 13\}$ specifies the quantifier prefix $\exists f K_1 x_1 K_2 x_2 K_3 x_3$ and the line number $j \in \{1, 2, \ldots, 16\}$ describes the underlying expression $f(\bar{\varphi}(\alpha\delta, q), \upsilon(q, \alpha, \delta)) = \alpha$, where $\{x_1, x_2, x_3\} = \{q, \alpha, \delta\}$. These parts form the complete condition denoted $U_{i,j}$ or $U_{i,j}[\tau]$, if a reference to the invertibility delay is required. For instance, $U_{1,1}[\tau] = \exists f \forall q \forall \alpha \forall \delta (f(\bar{\varphi}(\alpha\delta, q)) = \alpha)$, $U_{1,2}[\tau] = \exists f \forall q \forall \alpha \forall \delta (f(\bar{\varphi}(\alpha\delta, q), q) = \alpha)$, $U_{5,10}[\tau] = \exists f \exists q \forall \alpha \exists \delta (f(\bar{\varphi}(\alpha\delta, q), \psi(\alpha, q), \delta) = \alpha)$.

Let $\kappa^{(i)}(q, \alpha, \delta)$ and $\upsilon_j(q, \alpha, \delta)$ be respectively $K_1 x_1 K_2 x_2 K_3 x_3$ where $\exists f K_1 x_1 K_2 x_2 K_3 x_3$ is the quantifier prefix from the line number i in the Table 1 and the invertibility order $\upsilon_j(q, \alpha, \delta)$ from the line number j in underlying expression $f(\bar{\varphi}(\alpha\delta, q), \upsilon_j(q, \alpha, \delta)) = \alpha$ in the Table 1. For example, $\kappa^{(5)}(q, \alpha, \delta) = \exists q \forall \alpha \exists \delta$ and $\upsilon_{13}(q, \alpha, \delta) = \{q, \psi(\alpha, q), \delta\}$.

So for any $i \in \{1, 2, \ldots, 13\}$ and $j \in \{1, 2, \ldots, 16\}$, $\kappa^{(i)}(q, \alpha, \delta)$ and $\upsilon_j(q, \alpha, \delta)$ present some cryptanalytical parameters of finite automata such as their invertibility type, degree, order and so on.

Let also $\kappa_i(q, \alpha, \delta, s, \beta, \varepsilon) = \kappa^{(i)}(q, \alpha, \delta)\kappa^{(i)}(s, \beta, \varepsilon)$, $\{x_1, x_2, x_3\} = \{q, \alpha, \delta\}$, $\{y_1, y_2, y_3\} = \{s, \beta, \varepsilon\}$, $x_{k_0} = \alpha$, $y_{k_0} = \beta$, $g(x_1, \ldots, x_n) = (\bar{\varphi}(\alpha\delta, q), \upsilon_j(q, \alpha, \delta))$,

$$K_1 x_1 K_2 x_2 K_3 x_3 K_1 y_1 K_2 y_2 K_3 y_3 = \kappa_i(q, \alpha, \delta, s, \beta, \varepsilon),$$

and we can write down the invertibility condition (1) in the following new form

$$U_{i,j} = \exists f \kappa^{(i)}(q, \alpha, \delta)[f(\bar{\varphi}(\alpha\delta, q), \upsilon_j(q, \alpha, \delta)) = \alpha],$$

its equivalent from Proposition 2 in the following new form

$$\kappa_i(q, \alpha, \delta, s, \beta, \varepsilon)[(\alpha \neq \beta \Rightarrow (\bar{\varphi}(\alpha\delta, q), \upsilon_j(q, \alpha, \delta)) \neq (\bar{\varphi}(\beta\varepsilon, s), \upsilon_j(s, \beta, \varepsilon)))].$$

where $\{x_1, x_2, x_3\} = \{q, \alpha, \delta\}, \{y_1, y_2, y_3\} = \{s, \beta, \varepsilon\}$.

Thus, the following assertion is proved.

Proposition 7. For all $i \in \{1, 2, \ldots, 13\}$ and $j \in \{1, 2, \ldots, 16\}$,

$$U_{i,j} = \kappa_i(q, \alpha, \delta, s, \beta, \varepsilon)[\alpha \neq \beta \ \& \ \upsilon_j(q, \alpha, \delta) = \upsilon_j(s, \beta, \varepsilon) \Rightarrow \bar{\varphi}(\alpha\delta, q) \neq \bar{\varphi}(\beta\varepsilon, s)]. \quad (3)$$

For example,

$$U_{2,7} = \forall q \forall \alpha \exists \delta \forall s \forall \beta \exists \varepsilon [\alpha \neq \beta \ \& \ q = s \ \& \ \psi(\alpha\delta, q) = \psi(\beta\varepsilon, s) \Rightarrow \bar{\varphi}(\alpha\delta, q) \neq \bar{\varphi}(\beta\varepsilon, s)].$$

For compact presentation of obtained so, including simplifications, logic formulas for all 208 invertibility conditions $U_{i,j}$ of automata A, below at first separately the notation in them is enumerated for all possible quantifier prefixes and underlying expressions, and then in the Table 2 the formulas themselfes in the form $\kappa\Gamma$, where κ and Γ — notation respectively of quantifier prefix and of underlying expression from the given list.

In some cases formula (3) for $U_{i,j}$ can be simplified, namely: if the condition $\upsilon_j(q, \alpha, \delta) = \upsilon_j(s, \beta, \varepsilon)$ includes the equalities $q = s$ and (or) $\delta = \varepsilon$, and the quantifier prefix $\kappa^{(i)}(q, \alpha, \delta)\kappa^{(i)}(s, \beta, \varepsilon)$ contains quantifiers $\forall q$, $\forall s$ and (or) $\forall\delta$, $\forall\varepsilon$, then it is possible to exclude simultaneously from this condition these equalities, to exclude from prefix quantifiers $\forall s$ and (or) $\forall\varepsilon$, and to put in conclusion $(\bar{\varphi}(\alpha\delta, q) \neq \bar{\varphi}(\beta\varepsilon, s))$ $s = q$ and (or) $\varepsilon = \delta$ respectively. This simplification is an equivalent transformation and doesn't change the truth value of the formula.

Notations of quantifier prefixes κ in the formulas of automaton A invertibility conditions:

$$
\begin{array}{lll}
a = \forall q \forall \alpha \forall \delta \forall s \forall \beta \forall \varepsilon; & i = \forall \alpha \forall \delta \exists q \forall \beta \forall \varepsilon \exists s; & b_2 = \forall q \forall \alpha \exists \delta \forall \beta \exists \varepsilon; \\
b = \forall q \forall \alpha \exists \delta \forall s \forall \beta \exists \varepsilon; & j = \forall \alpha \exists \delta \forall q \forall \beta \exists \varepsilon \forall s; & c_2 = \forall q \exists \delta \forall \alpha \exists \varepsilon \forall \beta; \\
c = \forall q \exists \delta \forall \alpha \forall s \exists \varepsilon \forall \beta; & k = \forall \delta \exists q \forall \alpha \forall \varepsilon \exists s \forall \beta; & d_1 = \exists q \forall \alpha \forall \delta \exists s \forall \beta; \\
d = \exists q \forall \alpha \forall \delta \exists s \forall \beta \forall \varepsilon; & l = \exists \delta \forall q \forall \alpha \exists \varepsilon \forall s \forall \beta; & g_1 = \forall \alpha \exists q \forall \delta \forall \beta \exists s; \\
e = \exists q \forall \alpha \exists \delta \exists s \forall \beta \exists \varepsilon; & m = \exists \delta \forall \alpha \exists q \exists \varepsilon \forall \beta \exists s; & i_1 = \forall \alpha \forall \delta \exists q \forall \beta \exists s; \\
f = \exists q \exists \delta \forall \alpha \exists s \exists \varepsilon \forall \beta; & a_2 = \forall q \forall \alpha \forall \delta \forall \beta \forall \varepsilon; & j_2 = \forall \alpha \exists \delta \forall q \forall \beta \exists \varepsilon; \\
g = \forall \alpha \exists q \forall \delta \forall \beta \exists s \forall \varepsilon; & a_1 = \forall q \forall \alpha \forall \delta \forall s \forall \beta & k_1 = \forall \delta \exists q \forall \alpha \exists s \forall \beta; \\
h = \forall \alpha \exists q \exists \delta \forall \beta \exists s \exists \varepsilon; & a_0 = \forall q \forall \alpha \forall \delta \forall \beta; & l_2 = \exists \delta \forall q \forall \alpha \exists \varepsilon \forall \beta.
\end{array}
$$

Notation of underlying expressions Γ in formulas of automaton A invertibility conditions:

$$
\begin{aligned}
A &= [\alpha \neq \beta \Rightarrow \bar{\varphi}(\alpha\delta, q) \neq \bar{\varphi}(\beta\varepsilon, s)]; \\
B &= [\alpha \neq \beta \ \& \ q = s \Rightarrow \bar{\varphi}(\alpha\delta, q) \neq \bar{\varphi}(\beta\varepsilon, s)]; \\
B_2 &= [\alpha \neq \beta \Rightarrow \bar{\varphi}(\alpha\delta, q) \neq \bar{\varphi}(\beta\varepsilon, q)]; \\
C &= [\alpha \neq \beta \ \& \ \psi(\alpha, q) = \psi(\beta, s) \Rightarrow \bar{\varphi}(\alpha\delta, q) \neq \bar{\varphi}(\beta\varepsilon, s)]; \\
D &= [\alpha \neq \beta \ \& \ \psi(\alpha\delta, q) = \psi(\beta\varepsilon, s) \Rightarrow \bar{\varphi}(\alpha\delta, q) \neq \bar{\varphi}(\beta\varepsilon, s)]; \\
E &= [\alpha \neq \beta \ \& \ \delta = \varepsilon \Rightarrow \bar{\varphi}(\alpha\delta, q) \neq \bar{\varphi}(\beta\varepsilon, s)]; \\
E_1 &= [\alpha \neq \beta \Rightarrow \bar{\varphi}(\alpha\delta, q) \neq \bar{\varphi}(\beta\delta, s)]; \\
F &= [\alpha \neq \beta \ \& \ q = s \ \& \ \psi(\alpha, q) = \psi(\beta, s) \Rightarrow \bar{\varphi}(\alpha\delta, q) \neq \bar{\varphi}(\beta\varepsilon, s)]; \\
F_2 &= [\alpha \neq \beta \ \& \ \psi(\alpha, q) = \psi(\beta, q) \Rightarrow \bar{\varphi}(\alpha\delta, q) \neq \bar{\varphi}(\beta\varepsilon, q)]; \\
G &= [\alpha \neq \beta \ \& \ q = s \ \& \ \psi(\alpha\delta, q) = \psi(\beta\varepsilon, s) \Rightarrow \bar{\varphi}(\alpha\delta, q) \neq \bar{\varphi}(\beta\varepsilon, s)]; \\
G_2 &= [\alpha \neq \beta \ \& \ \psi(\alpha\delta, q) = \psi(\beta\varepsilon, q) \Rightarrow \bar{\varphi}(\alpha\delta, q) \neq \bar{\varphi}(\beta\varepsilon, q)]; \\
H &= [\alpha \neq \beta \ \& \ q = s \ \& \ \delta = \varepsilon \Rightarrow \bar{\varphi}(\alpha\delta, q) \neq \bar{\varphi}(\beta\varepsilon, s)]; \\
H_2 &= [\alpha \neq \beta \ \& \ \delta = \varepsilon \Rightarrow \bar{\varphi}(\alpha\delta, q) \neq \bar{\varphi}(\beta\varepsilon, q)]; \\
H_1 &= [\alpha \neq \beta \ \& \ q = s \Rightarrow \bar{\varphi}(\alpha\delta, q) \neq \bar{\varphi}(\beta\delta, s)]; \\
H_0 &= [\alpha \neq \beta \Rightarrow \bar{\varphi}(\alpha\delta, q) \neq \bar{\varphi}(\beta\delta, q)]; \\
I &= [\alpha \neq \beta \ \& \ \psi(\alpha, q) = \psi(\beta, s) \ \& \ \psi(\alpha\delta, q) = \psi(\beta\varepsilon, s) \Rightarrow \bar{\varphi}(\alpha\delta, q) \neq \bar{\varphi}(\beta\varepsilon, s)]; \\
J &= [\alpha \neq \beta \ \& \ \delta = \varepsilon \ \& \ \psi(\alpha, q) = \psi(\beta, s) \Rightarrow \bar{\varphi}(\alpha\delta, q) \neq \bar{\varphi}(\beta\varepsilon, s)]; \\
J_1 &= [\alpha \neq \beta \ \& \ \psi(\alpha, q) = \psi(\beta, s) \Rightarrow \bar{\varphi}(\alpha\delta, q) \neq \bar{\varphi}(\beta\delta, s)]; \\
K &= [\alpha \neq \beta \ \& \ \delta = \varepsilon \ \& \ \psi(\alpha\delta, q) = \psi(\beta\varepsilon, s) \Rightarrow \bar{\varphi}(\alpha\delta, q) \neq \bar{\varphi}(\beta\varepsilon, s)]; \\
K_1 &= [\alpha \neq \beta \ \& \ \psi(\alpha\delta, q) = \psi(\beta\delta, s) \Rightarrow \bar{\varphi}(\alpha\delta, q) \neq \bar{\varphi}(\beta\delta, s)]; \\
L &= [\alpha \neq \beta \ \& \ q = s \ \& \ \psi(\alpha, q) = \psi(\beta, s) \ \& \ \psi(\alpha\delta, q) = \psi(\beta\varepsilon, s) \Rightarrow \bar{\varphi}(\alpha\delta, q) \neq \bar{\varphi}(\beta\varepsilon, s)]; \\
L_2 &= [\alpha \neq \beta \ \& \ \psi(\alpha, q) = \psi(\beta, q) \ \& \ \psi(\alpha\delta, q) = \psi(\beta\varepsilon, q) \Rightarrow \bar{\varphi}(\alpha\delta, q) \neq \bar{\varphi}(\beta\varepsilon, q)]; \\
M &= [\alpha \neq \beta \ \& \ q = s \ \& \ \delta = \varepsilon \ \& \ \psi(\alpha, q) = \psi(\beta, s) \Rightarrow \bar{\varphi}(\alpha\delta, q) \neq \bar{\varphi}(\beta\varepsilon, s)]; \\
M_2 &= [\alpha \neq \beta \ \& \ \delta = \varepsilon \ \& \ \psi(\alpha, q) = \psi(\beta, q) \Rightarrow \bar{\varphi}(\alpha\delta, q) \neq \bar{\varphi}(\beta\varepsilon, q)]; \\
M_1 &= [\alpha \neq \beta \ \& \ q = s \ \& \ \psi(\alpha, q) = \psi(\beta, s) \Rightarrow \bar{\varphi}(\alpha\delta, q) \neq \bar{\varphi}(\beta\delta, s)]; \\
M_0 &= [\alpha \neq \beta \ \& \ \psi(\alpha, q) = \psi(\beta, q) \Rightarrow \bar{\varphi}(\alpha\delta, q) \neq \bar{\varphi}(\beta\delta, q)]; \\
N &= [\alpha \neq \beta \ \& \ q = s \ \& \ \delta = \varepsilon \ \& \ \psi(\alpha\delta, q) = \psi(\beta\varepsilon, s) \Rightarrow \bar{\varphi}(\alpha\delta, q) \neq \bar{\varphi}(\beta\varepsilon, s)]; \\
N_2 &= [\alpha \neq \beta \ \& \ \delta = \varepsilon \ \& \ \psi(\alpha\delta, q) = \psi(\beta\varepsilon, q) \Rightarrow \bar{\varphi}(\alpha\delta, q) \neq \bar{\varphi}(\beta\varepsilon, q)]; \\
N_1 &= [\alpha \neq \beta \ \& \ q = s \ \& \ \psi(\alpha\delta, q) = \psi(\beta\delta, s) \Rightarrow \bar{\varphi}(\alpha\delta, q) \neq \bar{\varphi}(\beta\delta, s)]; \\
N_0 &= [\alpha \neq \beta \ \& \ \psi(\alpha\delta, q) = \psi(\beta\delta, q) \Rightarrow \bar{\varphi}(\alpha\delta, q) \neq \bar{\varphi}(\beta\delta, q)];
\end{aligned}
$$

$$O = [\alpha \neq \beta \ \& \ \delta = \varepsilon \ \& \ \psi(\alpha, q) = \psi(\beta, s) \ \& \ \psi(\alpha\delta, q) = \psi(\beta\varepsilon, s) \Rightarrow \bar{\varphi}(\alpha\delta, q) \neq \bar{\varphi}(\beta\varepsilon, s)];$$
$$O_1 = [\alpha \neq \beta \ \& \ \psi(\alpha, q) = \psi(\beta, s) \ \& \ \psi(\alpha\delta, q) = \psi(\beta\delta, s) \Rightarrow \bar{\varphi}(\alpha\delta, q) \neq \bar{\varphi}(\beta\delta, s)];$$
$$P = [\alpha \neq \beta \ \& \ q = s \ \& \ \delta = \varepsilon \ \& \ \psi(\alpha, q) = \psi(\beta, s) \ \& \ \psi(\alpha\delta, q) = \psi(\beta\varepsilon, s) \Rightarrow$$
$$\Rightarrow \bar{\varphi}(\alpha\delta, q) \neq \bar{\varphi}(\beta\varepsilon, s)];$$
$$P_2 = [\alpha \neq \beta \ \& \ \delta = \varepsilon \ \& \ \psi(\alpha, q) = \psi(\beta, q) \ \& \ \psi(\alpha\delta, q) = \psi(\beta\varepsilon, q) \Rightarrow \bar{\varphi}(\alpha\delta, q) \neq \bar{\varphi}(\beta\varepsilon, q)];$$
$$P_1 = [\alpha \neq \beta \ \& \ q = s \ \& \ \psi(\alpha, q) = \psi(\beta, s) \ \& \ \psi(\alpha\delta, q) = \psi(\beta\delta, s) \Rightarrow \bar{\varphi}(\alpha\delta, q) \neq \bar{\varphi}(\beta\delta, s)];$$
$$P_0 = [\alpha \neq \beta \ \& \ \psi(\alpha, q) = \psi(\beta, q) \ \& \ \psi(\alpha\delta, q) = \psi(\beta\delta, q) \Rightarrow \bar{\varphi}(\alpha\delta, q) \neq \bar{\varphi}(\beta\delta, q)].$$

Formulas $\kappa\Gamma$ for conditions of the automaton A invertibility of all possible types are presented in the Table 2. For any words ξ, ζ in X^* and states q, s in Q inequality $\bar{\varphi}(\xi, q) \neq \neq \bar{\varphi}(\zeta, s)$ is always provided when $|\xi| \neq |\zeta|$, therefore in any of these formulas it is possible to count $|\alpha| = |\beta|$. Further we use this possibility without additional reservations.

Table 2

Formulas $\kappa\Gamma$ for conditions of the automaton invertibility of all possible types

i	1	2	3	4	5	6	7	8	9	10	11	12	13
$U_{i,1}$	aA	bA	cA	dA	eA	fA	gA	hA	iA	jA	kA	lA	mA
$U_{i,2}$	a_2B_2	b_2B_2	c_2B_2	dB	eB	fB	gB	hB	iB	j_2B_2	kB	l_2B_2	mB
$U_{i,3}$	aC	bC	cC	dC	eC	fC	gC	hC	iC	jC	kC	lC	mC
$U_{i,4}$	aD	bD	cD	dD	eD	fD	gD	hD	iD	jD	kD	lD	mD
$U_{i,5}$	a_1E_1	bE	cE	d_1E_1	eE	fE	g_1E_1	hE	i_1E_1	jE	k_1E_1	lE	mE
$U_{i,6}$	a_2F_2	b_2F_2	c_2F_2	dF	eF	fF	gF	hF	iF	j_2F_2	kF	l_2F_2	mF
$U_{i,7}$	a_2G_2	b_2G_2	c_2G_2	dG	eG	fG	gG	hG	iG	j_2G_2	kG	l_2G_2	mG
$U_{i,8}$	a_0H_0	b_2H_2	c_2H_2	d_1H_1	eH	fH	g_1H_1	hH	i_1H_1	j_2H_2	k_1H_1	l_2H_2	mH
$U_{i,9}$	aI	bI	cI	dI	eI	fI	gI	hI	iI	jI	kI	lI	mI
$U_{i,10}$	a_1J_1	bJ	cJ	d_1J_1	eJ	fJ	g_1J_1	hJ	i_1J_1	jJ	k_1J_1	lJ	mJ
$U_{i,11}$	a_1K_1	bK	cK	d_1K_1	eK	fK	g_1K_1	hK	i_1K_1	jK	k_1K_1	lK	mK
$U_{i,12}$	a_2L_2	b_2L_2	c_2L_2	dL	eL	fL	gL	hL	iL	j_2L_2	kL	l_2L_2	mL
$U_{i,13}$	a_0M_0	b_2M_2	c_2M_2	d_1M_1	eM	fM	g_1M_1	hM	i_1M_1	j_2M_2	k_1M_1	l_2M_2	mM
$U_{i,14}$	a_0N_0	b_2N_2	c_2N_2	d_1N_1	eN	fN	g_1N_1	hN	i_1N_1	j_2N_2	k_1N_1	l_2N_2	mN
$U_{i,15}$	a_1O_1	bO	cO	d_1O_1	eO	fO	g_1O_1	hO	i_1O_1	jO	k_1O_1	lO	mO
$U_{i,16}$	a_0P_0	b_2P_2	c_2P_2	d_1P_1	eP	fP	g_1P_1	hP	i_1P_1	j_2P_2	k_1P_1	l_2P_2	mP

Let in the Table 2 for any $i = 1, 2, \ldots, 13$ and $j = 1, 2, \ldots, 16$ element on intersection of line with $U_{i,j}$ at the head and column with the number i is denoted T_{ij}. Then $U_{i,j} = T_{ij}$.

So, for instance, $U_{1,1} = aA = \forall q \forall \alpha \forall \delta \forall s \forall \beta \forall \varepsilon [\alpha \neq \beta \Rightarrow \bar{\varphi}(\alpha\delta, q) \neq \bar{\varphi}(\beta\varepsilon, s)]$; $U_{4,8} = d_1H_1 = \exists q \forall \alpha \forall \delta \exists s \forall \beta [\alpha \neq \beta \ \& \ q = s \Rightarrow \bar{\varphi}(\alpha\delta, q) \neq \bar{\varphi}(\beta\delta, s)]$; $U_{10,13} = j_2M_2 = = \forall \alpha \exists \delta \forall q \forall \beta \exists \varepsilon [\alpha \neq \beta \ \& \ \delta = \varepsilon \ \& \ \psi(\alpha, q) = \psi(\beta, q) \Rightarrow \bar{\varphi}(\alpha\delta, q) \neq \bar{\varphi}(\beta\varepsilon, q)]$, and so on.

If in expression for $U_{i,j}$ in (3) the condition $\upsilon_j(q, \alpha, \delta) = \upsilon_j(s, \beta, \varepsilon)$ includes into itself equalities $q = s$ and (or) $\delta = \varepsilon$, and quantifier prefix $\kappa^{(i)}(q, \alpha, \delta)\kappa^{(i)}(s, \beta, \varepsilon)$ contains quantifiers $\exists q, \exists s$ and (or) $\exists \delta, \exists \varepsilon$, then, putting down from it these equalities and quantifiers $\exists s$ and (or) $\exists \varepsilon$ and placing in its conclusion $\bar{\varphi}(\alpha\delta, q) \neq \bar{\varphi}(\beta\varepsilon, s)$ respectively $s = q$ and (or) $\varepsilon = \delta$, we obtain expression, denoted further $U'_{i,j}$, for which the implication $U'_{i,j} \Rightarrow U_{i,j}$ is true. This means that the condition $U'_{i,j}$ is sufficient, but not obligatory necessary for invertibility of type $\kappa^{(i)}$ and order υ_j for automaton A. All obtained so sufficient conditions of invertibility for automaton A are represented in Table 3. In it quantifier prefixes have the following notation:

$b_1 = \forall q \forall \alpha \exists \delta \forall s \forall \beta$; $e_1 = \exists q \forall \alpha \exists \delta \exists s \forall \beta$; $h_2 = \forall \alpha \exists q \exists \delta \forall \beta \exists \varepsilon$; $k_2 = \forall \delta \exists q \forall \alpha \forall \varepsilon \forall \beta$;
$b_0 = \forall q \forall \alpha \exists \delta \forall \beta$; $e_0 = \exists q \forall \alpha \exists \delta \forall \beta$; $h_1 = \forall \alpha \exists q \exists \delta \forall \beta \exists s$; $k_0 = \forall \delta \exists q \forall \alpha \forall \beta$;

$c_1 = \forall q \exists \delta \forall \alpha \forall s \forall \beta$; $f_2 = \exists q \exists \delta \forall \alpha \exists \varepsilon \forall \beta$; $h_0 = \forall \alpha \exists q \exists \delta \forall \beta$; $l_1 = \exists \delta \forall q \forall \alpha \forall s \forall \beta$;
$c_0 = \forall q \exists \delta \forall \alpha \forall \beta$; $f_1 = \exists q \exists \delta \forall \alpha \exists s \forall \beta$; $i_2 = \forall \alpha \forall \delta \exists q \forall \beta \forall \varepsilon$; $l_0 = \exists \delta \forall q \forall \alpha \forall \beta$;
$d_2 = \exists q \forall \alpha \forall \delta \forall \beta \forall \varepsilon$; $f_0 = \exists q \exists \delta \forall \alpha \forall \beta$; $i_0 = \forall \alpha \forall \delta \exists q \forall \beta$; $m_2 = \exists \delta \forall \alpha \exists q \exists \varepsilon \forall \beta$;
$d_0 = \exists q \forall \alpha \forall \delta \forall \beta$; $g_2 = \forall \alpha \exists q \forall \delta \forall \beta \forall \varepsilon$; $j_1 = \forall \alpha \exists \delta \forall q \forall \beta \forall s$; $m_1 = \exists \delta \forall \alpha \exists q \forall \beta \exists s$;
$e_2 = \exists q \forall \alpha \exists \delta \forall \beta \exists \varepsilon$; $g_0 = \forall \alpha \exists q \forall \delta \forall \beta$; $j_0 = \forall \alpha \exists \delta \forall q \forall \beta$; $m_0 = \exists \delta \forall \alpha \exists q \forall \beta$.

Table 3

Formulas for sufficient conditions of the automaton invertibility of some types

i	2	3	4	5	6	7	8	9	10	11	12	13
$U'_{i,2}$			d_2B_2	e_2B_2	f_2B_2	g_2B_2	h_2B_2	i_2B_2		k_2B_2		m_2B_2
$U'_{i,5}$	b_1E_1	c_1E_1		e_1E_1	f_1E_1		h_1E_1		j_1E_1		l_1E_1	m_1E_1
$U'_{i,6}$			d_2F_2	e_2F_2	f_2F_2	g_2F_2	h_2F_2	i_2F_2		k_2F_2		m_2F_2
$U'_{i,7}$			d_2G_2	e_2G_2	f_2G_2	g_2G_2	h_2G_2	i_2G_2		k_2G_2		m_2G_2
$U'_{i,8}$	b_0H_0	c_0H_0	d_0H_0	e_0H_0	f_0H_0	g_0H_0	h_0H_0	i_0H_0	j_0H_0	k_0H_0	l_0H_0	m_0H_0
$U'_{i,10}$	b_1J_1	c_1J_1		e_1J_1	f_1J_1		h_1J_1		j_1J_1		l_1J_1	m_1J_1
$U'_{i,11}$	b_1K_1	c_1K_1		e_1K_1	f_1K_1		h_1K_1		j_1K_1		l_1K_1	m_1K_1
$U'_{i,12}$			d_2L_2	e_2L_2	f_2L_2	g_2L_2	h_2L_2	i_2L_2		k_2L_2		m_2L_2
$U'_{i,13}$	b_0M_0	c_0M_0	d_0M_0	e_0M_0	f_0M_0	g_0M_0	h_0M_0	i_0M_0	j_0M_0	k_0M_0	l_0M_0	m_0M_0
$U'_{i,14}$	b_0N_0	c_0N_0	d_0N_0	e_0N_0	f_NH_0	g_0N_0	h_0N_0	i_0N_0	j_0N_0	k_0N_0	l_0N_0	m_0N_0
$U'_{i,15}$	b_1O_1	c_1O_1		e_1O_1	f_1O_1		h_1O_1		j_1O_1		l_1O_1	m_1O_1
$U'_{i,16}$	b_0P_0	c_0P_0	d_0P_0	e_0P_0	f_0P_0	g_0P_0	h_0P_0	i_0P_0	j_0P_0	k_0P_0	l_0P_0	m_0P_0

6. Problems in the theory of automata cryptanalytical invertibility

ACIDP. Given a cryptanalyical invertibility type (quantifier prefix $K_1x_1K_2x_3K_3x_3$, $\{x_1, x_2, x_3\} = \{q, \alpha, \delta\}$, and invertibility order $\upsilon(q, \alpha, \delta)$), as well as an invertibility delay τ, a number $k_0 \in \{1, 2, 3\}$ such that $K_{k_0} = \forall$, $x_{k_0} = \alpha$, a subject direct transformation $g(x_1, x_2, x_3) = (\bar{\varphi}(\alpha\delta, q), \upsilon(q, \alpha, \delta))$, and a subject inverse transformation $f(\bar{\varphi}(\alpha\delta, q), \upsilon(q, \alpha, \delta))$, find out whether f is a proper recovering function, that is, (1) is true, and hence the automaton under consideration is really invertible of the given type and with the given delay.

FIDP. Given a cryptanalytical invertibility type (quantifier prefix $K_1x_1 \dots K_nx_n$), a number $k_0 \in \{1, \dots, n\}$ such that $K_{k_0} = \forall$, and an abstract function $g(x_1, \dots, x_n)$, find out whether there exists a recovering function f such that $f(g(x_1, \dots, x_n)) = x_{k_0}$, and if it exists, then construct it.

For any specific j, classes $C_{i,j}(\tau)$ [9] with all possible i and τ and automata in them we call respectively classes of invertibility and invertible automata *of one propositionality* (j), or *one-propositional* (*of index* j). Due to the fact that, for any predicates $P(x)$ and $R(x, y)$, implications $\forall xP(x) \Rightarrow \exists xP(x)$, $\forall x \forall yR(x, y) \Rightarrow \exists x \forall yR(x, y)$ and $\exists x \forall yR(x, y) \Rightarrow$ $\Rightarrow \forall y \exists xR(x, y)$ are true, the inclusion relation is possible between some one-propositional classes of invertibility with equal delay [9].

The invertibility notion of finite automaton considered in this paper doesn't foresee for invertible automaton of obligatory existence of an inverse automaton. Moreover, it is admitted that the function of recovering input prefix for some types of automata invertibility can not be finite automaton. In this situation, naturally, the problem arises to find out for given invertible (of a certain) type automaton whether it has inverse automaton, and if it has, then to construct it. Decision of this problem, in turn, intends the introduction of the definition of an inverse automaton for an arbitrary automaton of every invertibility class.

The important place in this row takes the problem of creation invertible automata of all possible types. In various formulations of this problem different requirements to generated automata can be considered — with equal probability in given invertibility class, with bounded complexity, with a great or, otherwise, small delay of invertibility and so on. Its solution seems to be impossible without proper decision of the ACIDP.

REFERENCES

1. *Huffman D. A.* Canonical forms for information-lossles finite-state logical machines. IRE Trans. Circuit Theory, 1959, vol. 6, spec. suppl., pp. 41–59.
2. *Huffman D. A.* Notes on information-lossles finite-state automata. Nuovo Cimento, 1959, vol. 13, suppl. 2, pp. 397–405.
3. *Gill A.* Introduction to the Theory of Finite-State Machines. N.Y., McGraw-Hill Book Company, 1962. 300 p.
4. *Even Sh.* On information-lossles automata of finite order. IEEE Trans. Electron. Comput., 1965, vol. 14, no. 4, pp. 561–569.
5. *Kurmit A. A.* Information Lossless Automata of Finite Order. N.Y., John Wiley, 1974.
6. *Zakrevskiy A. D.* Metod avtomaticheskoy shifratsii soobshcheniy [The method for messages automatic encryption]. Prikladnaya Diskretnaya Matematika, 2009, no. 2(4), pp. 127–137. (in Russian)
7. *Dai Z. D., Ye D. F., and Lam K. Y.* Weak invertibility of finite automata and cryptanalysis on FAPKC. LNCS, 1998, vol. 1514, pp. 227–241.
8. *Tao R.* Finite Automata and Application to Cryptography. N.Y., Springer, 2009. 406 p.
9. *Agibalov G. P.* Cryptanalytic concept of finite automaton invertibility with finite delay. Prikladhaya Diskrethaya Matematika, 2019, no. 44, pp. 34–42.
10. *Agibalov G. P.* Cryptanalytical finite automaton invertibility with finite delay. Prikladnaya Diskretnaya Matematika, 2019, no. 46, pp. 27–37.