Записки научных
семинаров ПОМИ
Том 402, 2012 г.

D. S. Ananichev, D. D. Dublennykh

LOWER BOUNDS FOR THE NUMBER OF KEYS IN ZAKREVSKIJ CIPHER

Abstract. We present a new lower bound for the number of pairwise non-equivalent invertible Mealy machines with strongly connected underlying digraphs.

§1. Used notations

A *cryptoautomaton* $C = \langle X, Q, Y, K, \psi, \varphi\rangle$ is defined by specifying a finite set Q of states, finite alphabets X and Y, finite set $K = Q \times K_0$ of keys, transition function $\psi{:}\, Q \times X \times K_0 \to Q$ and output function

$$\varphi{:}\, Q \times X \times K_0 \to Y.$$

If we fix a key $(q_0, k) \in Q \times K_0$ then we obtain the Mealy machine $C_{(q_0,k)} = \langle Q, X, Y, \psi_k, \varphi_k, q_0\rangle$, where the transition function $\psi_k : Q \times X \to Q$ defined as $\forall q \in Q, x \in X\ \psi_k(q, x) = \psi(q, x, k)$, the output function $\varphi_k : Q \times X \to Y$ defined as $\forall q \in Q, x \in X\ \varphi_k(q, x) = \varphi(q, x, k)$ and q_0 is the initial state. So, K_0 is some kind of a set of Mealy machines without defined initial state. For every $q \in Q$ the function $\varphi_{kq} : X \to Y$ is defined as $\forall x \in X\ \varphi_{kq}(x) = \varphi_k(q, x)$. We say that Mealy machine is *invertible* if all functions φ_{kq} are bijections.

A cryptoautomaton $C = \langle X, Q, Y, K, \psi, \varphi\rangle$ is called *Zakrevskij cipher* (see [2]) if the set $\Upsilon\{C_{(q_0,k)} | (q_0, k) \in Q \times K_0\}$ is the set of all invertible Mealy machines with strongly connected underlying digraphs. In particular, it means that $|X| = |Y|$.

Let $\mathscr{A} = \langle X, Q, Y, K, \psi, \varphi\rangle$ be a Mealy machine. The transition function ψ can be extended in a unique way to an action $Q \times X^* \to Q$. We still denote this extension by ψ. The output function φ also can be inductively extended to an action $Q \times X^* \to Y^*$ if for all $w \in X^*$, $a \in X$ and $q \in Q$ we set $\varphi(q, wa) = \varphi(q, w)\varphi(\psi(q, w), a)$. So every Mealy machine generates the word transformation function $\varphi_{q_0} : X^* \to Y^*$ $(\forall \omega \in X^*\ \varphi_{q_0}(\omega) = \varphi(q_0, \omega))$.

Key words and phrases: Mealy machine, Zakrevskij cipher, finite automata, cryptoautomata.

We say that two Mealy machines are *equivalent* if their word transformation functions coincide. If we take two equivalent Mealy machines from the set Υ we say that corresponding keys are equivalent.

It is the natural question: how many non-equivalent keys are there in Zakrevskij cipher with given number of states and given number of letters? Another formulation of this question is: how many non-equivalent invertible Mealy automata with strongly connected underlying digraphs are there?

As shown in [1] if $|Q| = n$ and $|X| = |Y| = m$ then the number of non-equivalent Zakrevskij cipher keys is at most $(mn)^{mn}/(n-1)!$ and at leas m^n. We present a new lower bound for this number.

§2. Lower bound

2.1. Notation and considerations. For a word $w \in \{a,b\}^*$, we denote by $|w|$ the length of w and by $w[i]$, where $1 \le i \le |w|$, the ith letter in w from the left. If $1 \le i \le j \le |w|$, we denote by $w[i,j]$ the word $w[i]\cdots w[j]$.

Throughout the paper we assume that the state set Q of automata under consideration is the set $\{0,1,2,\ldots,n-1\}$ of the first n nonnegative integers.

We denote by $a \bmod b$ such integer x that $0 \le x < b$, $b \mid (a-x)$.

2.2. Lower bound.

Theorem 2.1. *Let $n, m \geqslant 2$, $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, where p_i are pairwise different primes, $\alpha_i \ge 1$. Then there are at least*

$$n^{n\cdot(m-1)} \cdot (m!^{p_1-1} - 1) \ldots (m!^{p_k-1} - 1) \cdot m!^{n-p_1-p_2-\ldots-p_k+k}$$

pairwise non-equivalent keys in Zakrevskij cipher over automata with n states and alphabet with m letters.

Proof. Consider the set Υ_1 of all Mealy machines with n states, input alphabet X and output alphabet Y of following structure:
$q_0 = 0$;
$\forall i < n-1 \;\; \psi(i,a) = i+1$; $\psi(n-1,a) = 0$;
$\forall i \in \{1,2,\ldots,k\} \;\; \exists j \in \{1,\ldots,p_i-1\}$, $c \in X$: $\varphi(\frac{j\cdot n}{p_i}, c) \ne \varphi(0,c)$;
$\forall i \in Q \;\; \forall c,d \in X \;\; c \ne d \Rightarrow \varphi(i,c) \ne \varphi(i,d)$.

That is letter a from input alphabet X is special and always transfers the automaton into next state in linear order. For all other transitions restrictions are weaker and we only require that if we choose any prime

divisor p of n and consider states 0, $\frac{n}{p}$, $\frac{2\cdot n}{p}$, $\ldots$, $\frac{(p-1)\cdot n}{p}$, then not all of them have the same output function.

Notice that the transfers by letter a makes underlying graphs of all these automata strongly connected and restrictions on output function φ provide that every automaton from Υ_1 is invertible, that is $\Upsilon_1 \subset \Upsilon$.

Choose arbitrary $\mathscr{A}_1 \neq \mathscr{A}_2 \in \Upsilon_1$. Prove that they are non-equivalent.

Let $\mathscr{A}_1 = \langle X, Q, Y, \psi_1, \varphi_1\rangle$, $\mathscr{A}_2 = \langle X, Q, Y, \psi_2, \varphi_2\rangle$.

There are two possible cases:

Case 1. $\exists i \in Q, c \in X$: $\varphi_1(i,c) \neq \varphi_2(i,c)$, that is output functions differ in some state i. Consider words $\omega_1 d_1 = \varphi_1(0, a^i c)$ and $\omega_2 d_2 = \varphi_2(0, a^i c)$. Notice that they differ in last letter because $d_1 = \varphi_1(i,c) \neq \varphi_2(i,c) = d_2$.

Case 2. $\forall q \in Q, b \in X$ $\varphi_1(q,b) = \varphi_2(q,b) = \varphi(q,b)$. Then it must be $\psi_1 \neq \psi_2$, that is there are such state $e \in Q$ and letter $c \in X$ that $\psi_1(e,c) \neq \psi_2(e,c)$. Let $\psi_1(e,c) = q_1$, $\psi_2(e,c) = q_2$.

Denote $d(p_1,p_2) = \min\{i \mid \psi_1(p_1, a^i) = p_2\}$. Note that this denotement is correct for any $p_1, p_2 \in Q$ because transitions by letter a produce a cycle over all states of automaton. Later on we will call this function distance between pair of states. It is easy to see that in our notations $d(p_1,p_2) = (p_2 - p_1) \bmod n$ and $d(\psi_1(p_1,a), \psi_2(p_2,a)) = d(p_1,p_2)$, that is transitions by letter a do not change distance between states.

Let $d(q_1,q_2) = t$. If we consider

$$(\psi_1(q_1,a^0), \psi_2(q_2,a^0)),$$
$$(\psi_1(q_1,a^1), \psi_2(q_2,a^1)), \ldots, (\psi_1(q_1,a^{n-1}), \psi_2(q_2,a^{n-1})),$$

then we get all pairs of states with distance t between them. If we recall that $q_1 = \psi_1(0, a^e c)$, $q_2 = \psi_2(0, a^e c)$, it means that for any pair of states p_1, p_2 if $d(p_1,p_2) = t$ then there is such a word $\omega_1 = a^e c a^s$ that $\psi_1(0,\omega_1) = p_1$, $\psi_2(0,\omega_1) = p_2$.

Consider set $Q_1 = \{0, t \bmod n, 2\cdot t \bmod n, \ldots, n\cdot t \bmod n = 0\}$.

Proposition 2.2. $\exists p_1, p_2 \in Q_1, b \in X$: $\varphi(p_1,b) \neq \varphi(p_2,b)$.

Proof. Let $\gcd(n,t) = d$. According to Bezout's identity,

$$\exists x, y \in \mathbb{Z}\colon 0 \leq x < n,\ t\cdot x + n\cdot y = d.$$

Choose any prime p such that $p \mid \frac{n}{d}$. Then $d \mid \frac{n}{p}$, therefore

$$\exists x_1, y_1 \in \mathbb{Z}\colon 0 \leq x_1 < n,\ t\cdot x_1 + n y_1 = \frac{n}{p};$$

hence, $x_1 \cdot t \bmod n = \frac{n}{p}$, thus $\frac{n}{p} \in Q_1$. Analogically, $\forall i \in \{0,1,\ldots,p-1\}$ $\frac{ni}{p} \in Q_1$. According to definition of φ,

$$\exists j \in \{1,\ldots,p-1\},\ b \in X : \varphi\Big(\frac{nj}{p}, b\Big) \neq \varphi(0,b). \qquad \square$$

Consider $p_1, p_2 \in Q_1$ from Proposition 2.2. Let

$$p_1 = i \cdot t \bmod n, \quad p_2 = j \cdot t \bmod n.$$

Without loss of generality $i < j$. Since

$$\varphi(i \cdot t \bmod n, b) \neq \varphi(j \cdot t \bmod n), b),$$

there is such $l \in \mathbb{Z}$ that $i \leq l < j$, $\varphi(l \cdot t \bmod n, b) \neq \varphi((l+1) \cdot t \bmod n), b)$.

We have $d(l \cdot t \bmod n, (l+1) \cdot t \bmod n) = t$, therefore

$$\exists s \in \{0,1,\ldots,n-1\} : \psi_1(0, a^e c a^s) = l \cdot t \bmod n,$$
$$\psi_2(0, a^e c a^s) = (l+1) \cdot t \bmod n,$$

thus $\varphi_1(0, a^e c a^s b) \neq \varphi_2(0, a^e c a^s b)$.

So, any two automata from set Υ_1 are non-equivalent, therefore total amount of non-equivalent keys of Zakrevskij cipher is at least $|\Upsilon_1|$.

The cardinality of Υ_1 is the number of admissible pairs of transition function and output function.

The number of admissible transition functions is equal to $n^{n(m-1)}$, because for any state $q \in Q$ and for any letter $b \in X$ except a we can choose arbitrary $p \in Q$ as result of $\psi(q,b)$.

In any state $q \in Q$ we can choose as output function in this state any of $m!$ bijections $X \to Y$. But we have restriction that for any set $\{\frac{n}{p_i}, \frac{2n}{p_i}, \ldots, \frac{(p_i-1)n}{p_i}\}$ at least in one of elements of such set output function differs from output function in first state. So, there are

$$(m!^{p_1-1} - 1) \cdot (m!^{p_2-1} - 1) \ldots (m!^{p_k-1} - 1) m!^{n-p_1-p_2-\ldots-p_k+k}$$

admissible output functions.

So,

$$|\Upsilon_1| = n^{n(m-1)} (m!^{p_1-1} - 1) \cdot (m!^{p_2-1} - 1) \ldots (m!^{p_k-1} - 1) \cdot m!^{n-p_1-p_2-\ldots-p_k+k}.$$

$\square$

References

1. Г. П. Агибалов, *Конечные автоматы в криптографии.* — Прикладная дискретная математика **2** (2009), 43–73.
2. А. Д. Закревский, *етод автоматической шифрации сообщений.* — Прикладная дискретная математика **2** (2009), 127–137.

Department of Mathematics and Mechanics
Ural State University
620083 Ekaterinburg, Russia
E-mail: Dmitry.Ananichev@usu.ru,
stigius@gmail.com

Поступило 2 июля 2012 г.