Discussiones Mathematicae
General Algebra and Applications 27 (2007) 109–121

THE COMPLETELY DISTRIBUTIVE LATTICE OF MACHINE INVARIANT SETS OF INFINITE WORDS

Aleksandrs Belovs and Jānis Buls

Department of Mathematics, University of Latvia
Raiņa bulvāris 19, Rīga, LV–1586 Latvia
e-mail: stiboh@inbox.lv
e-mail: buls@fmf.lu.lv

Abstract

We investigate the lattice of machine invariant classes. This is an infinite completely distributive lattice but it is not a Boolean lattice. The length and width of it is $\mathfrak{c}$. We show the subword complexity and the growth function create machine invariant classes.

Keywords: Mealy machine, machine invariant class, completely distributive lattice, length, width.

2000 Mathematics Subject Classification: 06D10, 68Q15, 68Q45, 68Q70, 68R15.

1. Motivation

In different areas of mathematics, people consider a lot of hierarchies which are typically used to classify some objects according to their complexity. Here we formulate and discuss some hierarchies of machine invariant classes.

We are inspired by Yablonski's result [10].

Theorem 1. *Every initial Mealy machine transforms an ultimately periodic word to an ultimately periodic word.*

A *cryptosystem* [9] is a five–tuple $\langle \mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D} \rangle$, where the following conditions are satisfied:

- $\mathcal{P}$ is a finite set of possible plaintexts,

- $\mathcal{C}$ is a finite set of possible ciphertexts,

- $\mathcal{K}$, the keyspace, is a finite set of possible keys;
- for each $K \in \mathcal{K}$, there is an encription rule $e_K \in \mathcal{E}$ and
- a corresponding decryption rule $d_K \in \mathcal{D}$;
- each $e_K : \mathcal{P} \to \mathcal{C}$ and $d_K : \mathcal{C} \to \mathcal{P}$ are functions such that $\forall x \in \mathcal{P}\ d_K(e_K(x)) = x$.

This leads to the concept of a ciphering machine [13]. A tuple $\langle X, S, Y, K, z, f, g, h \rangle$ is called a *ciphering machine* if:

- X is a finite alphabet of possible plaintexts,
- S is a finite set of states of the ciphering machine,
- Y is a finite alphabet of possible ciphertexts,
- K is a finite set of possible keys;
- $z : K \to S$, $f : S \times K \times X \to K$, $g : S \times K \times X \to S$, $h : S \times K \times X \to Y$ are functions.

Observe, it may be considered as a special kind of a Mealy machine [13]. Thus the Mealy machine appears in cryptography. This model, namely, Mealy machine, is being investigated intensively since the nineteen fifties (cf. [3, 6, 8, 11, 12]).

We shall describe one secret-key cryptosystem (Figure 1).

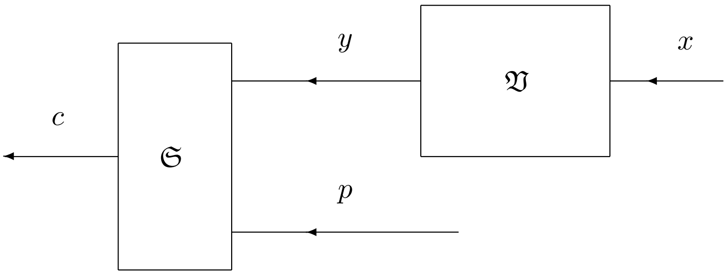

Figure 1.

Let $\mathfrak{S}$, $\mathfrak{V}$ be devices represent respectively the bitwise addition (modulo two) and a Mealy machine $V = \langle Q, A, \{0,1\}, \circ, *\rangle$. All users have identical devices.

The plaintext and cryptotext spaces are both equal to $\{0,1\}^*$. First the users choose a key, consisting of $x \in A^\omega$. Every session of communication begins with the choice of a session key, namely, sender chooses $n \in \mathbb{N}$, $q \in Q$ and then sends those securely to receiver. Now sender computes $y = q * x[n, n+l]$, where $l+1$ is the length of plaintext p. The encryption works in a bit-by-bit fashion, that is, $c_i = p_i + y_i (\mathrm{mod} 2)$.

When this is done, the security of the scheme of course depends in a crucial way on the quality of the $x \in A^\omega$ and the machine V. It is worth to mention at this stage of investigation this scheme serves only as extra (but important) motivation for represented report, that is, why we examine infinite words with Mealy machines.

On the other hand if we restrict ourselves with finite words then we can state only: for every pair of words $u, v \in A^n$ there exists Mealy machine that transforms u to v. So we have not obtained the new interesting partition of A^*.

2. Preliminaries

In this section we present most of the notations and terminology used in this paper. Our terminology is more or less standard (cf. [7]) so that a specialist reader may wish to consult this section only if need arise.

Let A be a finite non-empty set and A^* the free monoid generated by A. The set A is also called an *alphabet*, its elements *letters* and those of A^* *finite words*. The identity element of A^* is called an *empty word* and denoted by λ. We set $A^+ = A^* \backslash \{\lambda\}$.

A word $w \in A^+$ can be written uniquely as a sequence of letters as $w = w_1 w_2 \ldots w_l$, with $w_i \in A$, $1 \leq i \leq l$, $l > 0$. The integer l is called the *length* of w and denoted $|w|$. The length of λ is 0. We set $w^0 = \lambda \wedge \forall i \; w^{i+1} = w^i w$.

A word $w' \in A^*$ is called a *factor* (or *subword*) of $w \in A^*$ if there exist $u, v \in A^*$ such that $w = uw'v$. A word u (respectively v) is called a *prefix* (respectively a *suffix*) of w. A pair (u, v) is called an *occurrence* of w' in w. A factor w' is called *proper* if $w \neq w'$. We denote respectively by $\mathrm{F}(w)$, $\mathrm{Pref}(w)$ and $\mathrm{Suff}(w)$ the sets of w factors, prefixes and suffixes.

An (indexed) infinite word x on the alphabet A is any total map $x : \mathbb{N} \to A$. We set for any $i \geq 0$, $x_i = x(i)$ and write

$$x = (x_i) = x_0 x_1 \dots x_n \dots$$

The set of all the infinite words over A is denoted by A^ω.

A word $w' \in A^*$ is a *factor* of $x \in A^\omega$ if there exist $u \in A^*$, $y \in A^\omega$ such that $x = uw'y$. A word u (respectively y) is called a *prefix* (respectively a *suffix*) of x. We denote respectively by $\mathrm{F}(x)$, $\mathrm{Pref}(x)$ and $\mathrm{Suff}(x)$ the sets of x factors, prefixes and suffixes. For any $0 \leq m \leq n$, $x[m,n]$ denotes a factor $x_m x_{m+1} \dots x_n$. An indexed word $x[m,n]$ is called an *occurrence* of w' in x if $w' = x[m,n]$. The suffix $x_n x_{n+1} \dots x_{n+i} \dots$ is denoted by $x[n,\infty]$.

If $v \in A^+$ we denote by v^ω an infinite word

$$v^\omega = vv \dots v \dots$$

This word v^ω is called a *periodic word.* The *concatenation* of $u = u_1 u_2 \dots u_k \in A^*$ and $x \in A^\omega$ is the infinite word

$$ux = u_1 u_2 \dots u_k x_0 x_1 \dots x_n \dots$$

A word x is called *ultimately periodic* if there exist words $u \in A^*$, $v \in A^+$ such that $x = uv^\omega$. In this case, $|u|$ and $|v|$ are called, respectively, an *anti-period* and a *period.*

A 3–sorted algebra $V = \langle Q, A, B, q_0, \circ, * \rangle$ is called *an initial Mealy machine* if Q, A, B are finite, nonempty sets, $q_0 \in Q$; $\circ : Q \times A \to Q$ is a total function and $* : Q \times A \to B$ is a total surjective function. The mappings $\circ$ and $*$ may be extended to $Q \times A^*$ by defining

$$q \circ \lambda = q, \qquad q \circ (ua) = (q \circ u) \circ a$$

$$q * \lambda = \lambda, \qquad q * (ua) = (q * u)((q \circ u) * a)\,,$$

for all $q \in Q$, $(u,a) \in A^* \times A$. Henceforth, we shall omit parentheses if there is no danger of confusion. So, for example, we will write $q \circ u * a$ instead of $(q \circ u) * a$.

Let $(x,y) \in A^\omega \times B^\omega$. We write $y = q_0 * x$ or $x \overset{V}{\rightarrow\!\!\!\!\neg} y$ if $\forall n \; y[0,n] = q_0 * x[0,n]$ and say machine V *transforms* x to y. We write $x \rightarrow\!\!\!\!\neg\, y$ if there exists such V that $x \overset{V}{\rightarrow\!\!\!\!\neg} y$; otherwise we write $x \not\rightarrow\!\!\!\!\neg\, y$.

3. The lattice of machine invariant sets

We say a word $x \in A_1^\omega$ is *apt* for $V = \langle Q, A, B, q_0, \circ, * \rangle$ if $A_1 \subseteq A$. Let $\mathfrak{K} \neq \emptyset$ be any class of infinite words. The class $\mathfrak{K}$ is called *machine invariant* if every initial machine transforms all apt words of $\mathfrak{K}$ to words of $\mathfrak{K}$.

Remark. If we like to operate with sets instead of classes then we may restrict ourselves with one fixed countable alphabet $\mathfrak{A}=\{a_0, a_1, \dots, a_n, \dots\}$ and consider the set $\mathrm{Fin}(\mathfrak{A})$ of all non-empty finite subsets of $\mathfrak{A}$. Now the set $\mathfrak{K}$ may be chosen as the subset of $\mathfrak{F} = \{\, x \in A^\omega \mid A \in \mathrm{Fin}(\mathfrak{A}) \,\}$. Similarly, we may restrict ourselves with one fixed countable set $\mathfrak{Q} = \{q_1, q_2, \dots, q_n, \dots\}$ and consider only machines from the set

$$\mathfrak{M} = \{\langle Q, A, B, q_0, \circ, * \rangle \mid Q \in \mathrm{Fin}(\mathfrak{Q}) \,\wedge\, A, B \in \mathrm{Fin}(\mathfrak{A})\}\,.$$

There by, the set $\emptyset \neq \mathfrak{K} \subseteq \mathfrak{F}$ is called *machine invariant* if every initial machine $V \in \mathfrak{M}$ transforms all apt words of $\mathfrak{K}$ to words of $\mathfrak{K}$.

We follow the well established approach (cf. [4]). For the reader's convenience, we briefly recall some basic definitions in the form appropriate for future use in the paper.

Let $\langle P; \leq \rangle$ be an ordered set.

Let $S = \{s_i \mid i \in \mathcal{I}\} \subseteq P$ and $S^u = \{y \mid \forall s \in S \ s \leq y\}$. An element $x \in P$ is called a *join* of S (we write $x = \cup S$ or $x = \cup_{i \in \mathcal{I}} s_i$) if $x \in S^u$ and $\forall s \in S^u \ x \leq s$. We write $x \cup y$ instead of $\{x\} \cup \{y\}$. Dually, let $S^l = \{y \mid \forall s \in S \ y \leq s\}$ then an element $x \in P$ is called a *meet* of S (we write $x = \cap S$ or $x = \cap_{i \in \mathcal{I}} s_i$) if $x \in S^l$ and $\forall s \in S^l \ s \leq x$. We write $x \cap y$ instead of $\{x\} \cap \{y\}$.

- An element $\perp \in P$ is called a *bottom*, if $\forall x \in P \ \perp \leq x$. Dually, $\top \in P$ is called a *top*, if $\forall x \in P \ x \leq \top$.
- If $x \cup y$ and $x \cap y$ exist for all $x, y \in P$ then P is called a *lattice.*
- If $\cup S$ and $\cap S$ exist for all $S \subseteq P$ then P is called a *complete lattice.*

A complete lattice L is said to be *completely distributive*, if for any doubly indexed subset $\{x_{ij} \mid i \in \mathcal{I}, j \in \mathcal{J}\}$ of L we have

$$\bigcap_{i\in\mathcal{I}}\left(\bigcup_{j\in\mathcal{J}} x_{ij}\right)=\bigcup_{\alpha\,:\,\mathcal{I}\to\mathcal{J}}\left(\bigcap_{i\in\mathcal{I}} x_{i\alpha(i)}\right).$$

Let L be a lattice with $\perp$ and $\top$. For $x\in L$ we say $y\in L$ is a *complement* of x if $x\cap y=\perp$ and $x\cup y=\top$. A lattice L is called a *Boolean* lattice if

- for all $x,y,z\in L$ we have $x\cap(y\cup z)=(x\cap y)\cup(x\cap z)$,
- L has $\perp$ and $\top$, and each $x\in L$ has a complement $x'\in L$.

Corollary 2 [2] **.** *Let $\mathfrak{L}$ be the set that contains all machine invariant sets. Then $\langle\,\mathfrak{L},\cup,\cap\,\rangle$ is a completely distributive lattice, where $\cup$, $\cap$ are respectively the set union and intersection. The bottom $\perp$ is the set of all ultimately periodic words, the top $\top=\mathfrak{F}$.*

An infinite word $x\in A^\omega$ is called a *recurrent* word if any factor w of x has an infinite number of occurrences in x. Any word $x=uy$, where $u\in A^*$, $y\in A^\omega$ is called an *ultimately recurrent* word if y is a recurrent word.

Theorem 3 [2]**.** *Every initial Mealy machine transforms an ultimately recurrent word to an ultimately recurrent word.*

Example 4. Let $x=(x_i)=1010^210^31\dots0^n1\dots$ Then x is not an ultimately recurrent word. Assume $\{a,b\}\cap\{0,1\}=\emptyset$. Let $y\in\{a,b\}^\omega$ be any ultimately recurrent but not ultimately periodic word. Define z',z'' as follows:

$$z'_i=\begin{cases}1, & \text{if } x_i=1 \text{ and } y_i=a,\\ y_i, & \text{otherwise;}\end{cases}\qquad z''_i=\begin{cases}1, & \text{if } x_i=1 \text{ and } y_i=b,\\ y_i, & \text{otherwise.}\end{cases}$$

One of the words z', z'' neither is ultimately periodic nor ultimately recurrent. Consider the Mealy machines V_1 and V_2 shown in Figure 2.

Then $z' \xrightarrow{V_1} y$ and $z'' \xrightarrow{V_2} y$.

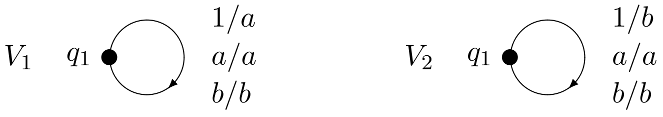

Figure 2.

So we have a method how to construct the infinite word that neither is ultimately periodic nor ultimately recurrent from an ultimately recurrent word if it is not ultimately periodic. We shall refer to this example in proof of such proposition.

Proposition 5. *$\mathfrak{L}$ is not a Boolean lattice.*

Proof. Let $\mathfrak{K} = \{x \in \mathfrak{F} \,|\, x \text{ is ultimately recurrent}\}$ then $\mathfrak{K} \in \mathfrak{L}$ by Theorem 3. Suppose $\mathfrak{K}' \in \mathfrak{L}$ is a complement of $\mathfrak{K}$ then $\mathfrak{K} \cap \mathfrak{K}' = \perp$ and $\mathfrak{K} \cup \mathfrak{K}' = \mathfrak{F}$ by Corollary 2. Let z be one of z', z'' of Example 4 such that $z \notin \mathfrak{K}$, and let y be as in Example 4. Since $\mathfrak{K}' \in \mathfrak{L}$ and $z \rightharpoondown y$ (see Example 4) then $y \in \mathfrak{K}'$. Hence, $y \in \mathfrak{K} \cap \mathfrak{K}' = \perp$. Contradiction.

4. The length

Let P be an ordered set. Then P is called a *chain* or *totally ordered set*, if for all $x, y \in P$, either $x \leq y$ or $y \leq x$ (that is, if any two elements of P are comparable). If $C = \{x_0, x_1, \ldots, x_n\}$ is a finite chain in P with $\mathrm{card}(C) = n+1$, then we say the *length* of C is n. If C is infinite chain in P, then we say the *length* of C is $\mathrm{card}(C)$. The size (cardinality) of the longest chain in P is called the *length* of P and is denoted by $\ell(P)$.

A machine $V = \langle Q_1 \times Q_2, A_1, B_2, (q_1, q_2), \circ, * \rangle$ is called a *composition* of $V_1 = \langle Q_1, A_1, B_1, q_1, \overset{\prime}{\circ}, \overset{\prime}{*} \rangle$ with $V_2 = \langle Q_2, B_1, B_2, q_2, \overset{\prime\prime}{\circ}, \overset{\prime\prime}{*} \rangle$ if

$$\begin{aligned} (q', q'') \circ a &= (q' \overset{\prime}{\circ} a, q'' \overset{\prime\prime}{\circ} q' \overset{\prime}{*} a), \\ (q', q'') * a &= q'' \overset{\prime\prime}{*} q' \overset{\prime}{*} a \end{aligned}$$

for all $(q', q'', a) \in Q_1 \times Q_2 \times A_1$.

Lemma 6. *If $x \rightharpoondown y$ and $y \rightharpoondown z$ then $x \rightharpoondown z$.*

Proof. Let $x \overset{V_1}{\rightharpoondown} y$ and $y \overset{V_2}{\rightharpoondown} z$. We can choose machines $V_1 = \langle Q_1, A_1, B_1, q_1, \overset{\prime}{\circ}, \overset{\prime}{*}\rangle$ and $V_2 = \langle Q_2, A_2, B_2, q_2, \overset{\prime\prime}{\circ}, \overset{\prime\prime}{*}\rangle$ so that $B_1 = A_2$. Then V the composition of V_1 with V_2 transforms x to z.

Corollary 7. *A set $\mathcal{V}(x) = \{y \mid \exists V \in \mathfrak{M}\ x \overset{V}{\rightharpoondown} y\}$, where $x \in A^\omega$ and $A \in \mathrm{Fin}(\mathfrak{A})$, is machine invariant.*

Proof. Let $y \in \mathcal{V}(x)$ and $y \rightharpoondown z$ then $x \rightharpoondown z$ by Lemma 6. Therefore $z \in \mathcal{V}(x)$.

Corollary 8. $\mathrm{card}(\mathcal{V}(x)) = \aleph_0$*, where $\aleph_0$ is the first infinite cardinality.*

Proof. Since $\mathrm{card}(\mathfrak{M}) = \aleph_0$ then $\mathrm{card}(\mathcal{V}(x)) \le \aleph_0$. Note $\perp \subseteq \mathcal{V}(x)$ by Corollary 2. Hence $\aleph_0 = \mathrm{card}(\perp) \le \mathrm{card}(\mathcal{V}(x))$. Therefore $\mathrm{card}(\mathcal{V}(x)) = \aleph_0$.

An order on C is called a *well-ordering* on C if C is a chain and every subset $S \subseteq C$ has a *minimal element*, that is, $\exists \cap S \in S$.

Theorem 9 (Zermelo). *For every non-empty set C there exists a well-ordering on C.*

Proposition 10. *There is a chain $\mathfrak{C}$ in $\mathfrak{L}$ such that* $\mathrm{card}(\mathfrak{C}) = \mathfrak{c}$*, where* $\mathfrak{c} = \mathrm{card}(\mathbb{R})$*, $\mathbb{R}$ denotes the set of real numbers.*

Proof. The proof is an application of Zermelo's theorem.

Let $A \in \mathrm{Fin}(\mathfrak{A})$ such that $\mathrm{card}(A) > 1$ and $\preceq$ be any well-ordering on A^ω, while $x \prec y$ means $x \preceq y$ and $x \ne y$. Then define $\mathfrak{K}(y) = \bigcup_{x \preceq y} \mathcal{V}(x)$ and a chain $\mathcal{I} = \{y \mid \forall x \prec y\ \mathfrak{K}(x) \ne \mathfrak{K}(y)\}$ in A^ω. Since A^ω is well-ordered there is the minimal element $x^{(1)}$ in $\mathcal{I}$.

Now suppose that $x^{(1)} \prec x^{(2)} \prec \ldots \prec x^{(k)}$ are the first k elements of the chain $\mathcal{I}$. Since $\forall i\ \mathrm{card}(\mathcal{V}(x^{(i)})) = \aleph_0$ and $\mathfrak{K}(x^{(k)}) = \bigcup_{i=1}^{k} \mathcal{V}(x^{(i)})$ then $\mathrm{card}(\mathfrak{K}(x^{(k)})) = \aleph_0$. Since $\mathrm{card}(A^\omega) > \aleph_0$ then $\exists x \in A^\omega\ x \notin \mathfrak{K}(x^{(k)})$. Hence, the chain $\mathcal{I}$ has at least the $k+1$-st element $x^{(k+1)}$. Therefore, we can say proceeded by induction that $\mathrm{card}(\mathcal{I}) \ge \aleph_0$.

$\bigcup_{x \in \mathcal{I}} \mathcal{V}(x) \supseteq A^\omega$ it must follow that $\mathfrak{c} = \mathrm{card}(A^\omega) \le \mathrm{card}(\bigcup_{x \in \mathcal{I}} \mathcal{V}(x))$ $= \mathrm{card}(\mathcal{I}) \le \mathfrak{c}$. Let $\mathfrak{C} = \{\mathfrak{K}(x) \mid x \in \mathcal{I}\}$ then $\mathfrak{C}$ is a chain in $\mathfrak{L}$ and $\mathrm{card}(\mathfrak{C}) = \mathrm{card}(\mathcal{I}) = \mathfrak{c}$.

Corollary 11. $\ell(\mathfrak{L}) = \mathfrak{c}$.

Corollary 12. $\operatorname{card}(\mathfrak{L}) \geq \mathfrak{c}$.

5. THE WIDTH

The ordered set $\bar{P}$ is called an *antichain* if $x \leq y$ in $\bar{P}$ only if $x = y$. Let P be an ordered set. The *width* of P is defined to be the size (cardinality) of the largest antichain in P and is denoted by $w(P)$.

Lemma 13. *Let $V = \langle Q, A, B, \circ, * \rangle$ be any Mealy machine and $q_0 \in Q$. If exists $s \geq \operatorname{card}(Q)$ such that $q_0 * 0^s = 0^s$ then*

$$\forall n \in \mathbb{N} \;\; q_0 * 0^{s+n} = 0^{s+n}.$$

Proof. Let $q_k = q_0 \circ 0^k$ and $Q_s = \{q_0, q_1, q_2, \ldots, q_{s-1}\}$. Then $\forall q' \in Q_s \; q' * 0 = 0$ and $Q_s \subseteq Q$. Hence, by pigeon-hole principle, there exist $0 \leq i < j \leq s - 1$ such that $q_i = q_j$; otherwise $Q_s = Q$.

(i) If $Q_s = Q$ then $\forall q' \; (q' \in Q \Rightarrow q' \in Q_s)$. Hence $\forall q' \in Q \;\; q' * 0 = 0$. Therefore $\forall n \in \mathbb{N} \;\; q * 0^{s+n} = 0^{s+n}$.

(ii) If $Q_s \neq Q$ then $q_i = q_j$. Hence $q_{j+1} = q_0 \circ 0^{j+1} = q_j \circ 0 = q_i \circ 0 = q_{i+1} \in Q_s$. Now by induction we have $\forall k \; q_k \in Q_s$. Therefore $\forall n \in \mathbb{N} \;\; q * 0^{s+n} = 0^{s+n}$.

Proposition 14. *There is an antichain $\bar{\mathfrak{C}}$ in $\mathfrak{L}$ such that* $\operatorname{card}(\bar{\mathfrak{C}}) = \mathfrak{c}$.

Proof. Let $c : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ be any bijection, for example,

$$c_{ij} = \frac{1}{2}\Big((i + j)^2 + 3i + j\Big).$$

Now define a map

$$T : \{0,1\}^\omega \to \{0,1\}^\omega : x \mapsto y = y_0 y_1 \ldots y_n \ldots$$

as follows

$$y_n = \begin{cases} 1, & \text{if } \exists k \in \mathbb{N} \; \big(n = k^2 \wedge c_{ij} = k \wedge x_i \equiv j (\operatorname{mod} 2)\big); \\ 0, & \text{otherwise.} \end{cases}$$

We claim: if $u \neq x$ then $T(u) \not\rightharpoondown T(x)$ and $T(x) \not\rightharpoondown T(u)$.

If $u \neq x$ then there exists i such that $u_i \neq x_i$. Without restriction, we assume that $u_i = 0$ but $x_i = 1$. Then $T(u)(c_{ij}^2) = 0$ for every odd j and

$$T(u)\Big[\big(c_{ij} - 1\big)^2 + 1, c_{ij}^2\Big] = 0^{2c_{ij}-1}$$

but $T(x)(c_{ij}^2) = 1$ and

$$T(x)\Big[\big(c_{ij} - 1\big)^2 + 1, c_{ij}^2\Big] = 0^{2c_{ij}-2}1.$$

Let $V = \langle Q, \{0,1\}, \{0,1\}, q_0, \circ, *\rangle$ be any initial Mealy machine that transforms $T(u)$ to $T(x)$. We can choose odd j such that $2c_{ij} - 2 \geq \mathrm{card}(Q)$. Let $q = q_0 \circ T(u)[0, (c_{ij} - 1)^2]$ then

$$\begin{aligned} q * 0^{2c_{ij}-1} &= q * T(u)\Big[\big(c_{ij} - 1\big)^2 + 1, c_{ij}^2\Big] \\ &= T(x)\Big[\big(c_{ij} - 1\big)^2 + 1, c_{ij}^2\Big] = 0^{2c_{ij}-2}1. \end{aligned}$$

This is contradiction by Lemma 13.

Corollary 15. $w(\mathfrak{L}) = \mathfrak{c}$.

6. Subword complexity

Let A be an alphabet then for each $n \geq 0$ we denote by A^n the set of all words of length n. The function $f_x(n) = card(A^n \cap \mathrm{F}(x))$, where $x \in A^\omega$, is called the *subword complexity* of the word x (cf. [1]). The *growth* function of the word x is defined as $g_x(n) = \sum_{i=0}^{n} f_x(i)$.

Let f, g be total functions. We write $g = O(f)$, if there exists such $c > 0$ that $\forall n \in \mathbb{N}\ |g(n)| \leq c\,|f(n)|$. Let $\emptyset \neq \mathfrak{K} \subseteq \mathfrak{F}$. We say the *subword complexity* of the set $\mathfrak{K}$ is f if $\forall x \in \mathfrak{K}\ f_x = O(f)$. Similarly, we say the *growth* function of the set $\mathfrak{K}$ is f if $\forall x \in \mathfrak{K}\ g_x = O(f)$.

Lemma 16. *Let $V = \langle Q, A, B, q_0, \circ, *\rangle$ be any Mealy machine. If $x \overset{V}{\rightharpoondown} y$ then $\forall n\ f_y(n) \leq |Q|\, f_x(n)$.*

Proof. Let $x \overset{V}{\rightharpoondown} y$ and $u \in F(x)$ then there exist $q \in Q$ and $v \in F(y)$ such that $q * u = v$. Since $q \in Q$, it follows that machine V can transform the word u to $|Q|$ distinct words v at the very most.

Let $v \in F(y)$ and $|v| = n$ then there exist $u \in F(x)$ and $q \in Q$ such that $q * u = v$. Hence, u is transformed to v. Note $|u| = |v|$. Therefore, $f_y(n) \leq |Q|\, f_x(n)$.

Proposition 17. *Let $f : \mathbb{N} \to \mathbb{R}$ be any total function.*

(i) *The set $\mathfrak{K}_1 = \{x \in \mathfrak{F} \,|\, f_x = O(f)\}$ is machine invariant.*

(ii) *The set $\mathfrak{K}_2 = \{x \in \mathfrak{F} \,|\, g_x = O(f)\}$ is machine invariant.*

Proof.

(i) Let $x \in \mathfrak{K}_1$ then $\forall n \in \mathbb{N}\ f_x(n) \leq c\,|f(n)|$ for some $c > 0$. Let $x \overset{V}{\rightharpoondown} y$, where $V = \langle Q, A, B, q_0, \circ, * \rangle$, then by Lemma 16 $f_y(n) \leq |Q|\, f_x(n) \leq c\,|Q|\,|f(n)|$. Hence $f_y = O(f)$, that is, $y \in \mathfrak{K}_1$.

(ii) Let $x \in \mathfrak{K}_2$ then $\forall n \in \mathbb{N}\ g_x(n) \leq c\,|f(n)|$ for some $c > 0$. Let $x \overset{V}{\rightharpoondown} y$, where $V = \langle Q, A, B, q_0, \circ, * \rangle$, then $g_y(n) = \sum_{i=0}^{n} f_y(i) \leq \sum_{i=0}^{n} |Q|\, f_x(i) = |Q| \sum_{i=0}^{n} f_x(i) = |Q|\, g_x(n) \leq c\,|Q|\,|f(n)|$. Hence $g_y = O(f)$, that is, $y \in \mathfrak{K}_2$.

7. Problem

What is the structure of lattice $\mathfrak{L}$? At this moment we have recognized a few features of $\mathfrak{L}$.

8. Conclusion

We say a word $x \in \mathfrak{F}$ is *more complicated as* $y \in \mathfrak{F}$ if

$$\forall \mathfrak{K} \in \mathfrak{L}\, (x \in \mathfrak{K} \Rightarrow y \in \mathfrak{K}) \;\&\; \exists \mathfrak{K} \in \mathfrak{L}\, (x \notin \mathfrak{K} \,\&\, y \in \mathfrak{K})\,.$$

So the lattice $\mathfrak{L}$ gives classification of infinite words that covers some aspects of complexity. It seems natural if we choose more complicate words as ciphers. Proposition 17 comes up to our expectations that the lattice $\mathfrak{L}$ would serve as a measure of words cryptographic quality.

It is worth to mention the idea that a lattice would serve as a measure of quality comes from fuzzy mathematics [5].

References

[1] J. Berstel and J. Karhumäki, *Combinatorics on Words – A Tutorial*, Bulletin of the European Association for Theoretical Computer Science **79** (2003), 178–228.

[2] J. Buls, *Machine Invariant Classes*, p. 207–211 in: "*Proceedings of WORDS'03, 4th International Conference on Combinatorics on Words", September 10–13, 2003, Turku, Finland,* Tero Harju and Juhani Karhumäki (Eds.), TUCS General Publication (No 27, August).

[3] J. Dassow, *Completeness Problems in the Structural Theory of Automata*, Mathematical Research (Band 7), Akademie–Verlag, Berlin 1981.

[4] B.A. Davey and H.A. Priestley, *Introduction to Lattices and Order*, Cambridge University Press, 2002.

[5] J.A. Goguen, *L-fuzzy sets*, J. Math. Anal. Appl. **8** (1967), 145–174.

[6] J. Hartmanis and R.E. Stearns, *Algebraic Structure Theory of Sequential Machines*, Prentice–Hall, Inc., Englewood Cliffs, New Jersey 1966.

[7] A. de Luca and S. Varricchio, *Finiteness and Regularity in Semigroups and Formal Languages*, Springer–Verlag, Berlin, Heidelberg 1999.

[8] B.I. Plotkin, I.Ja. Greenglaz and A.A. Gvaramija, *Algebraic Structures in Automata and Databases Theory*, World Scientific, Singapore, New Jersey, London, Hong Kong 1992.

[9] D.R. Stinson, *Cryptography*, Theory and Practice, CRC Press 1995.

[10] V.B. Kudryavcev, S.V. Aleshin and A.S. Podkolzin, *Vvedenie v teoriyu avtomatov*, An Introduction to the Theory of Automata, Moskva, Nauka (Russian) 1985.

[11] A.A. Kurmit, *Posledovatel′naya dekompoziciya konechnyh avtomatov*, Sequential Decomposition of Finite Automata, Riga, Zinatne (Russian) 1982.

[12] B.A. Trahtenbrot and Ya.M. Barzdin, *Konechnye avtomaty povedenie i sintez*, Finite Automata (Behaviour and Synthesis) Moskva, Nauka (Russian) 1970.

[13] V.M. Fomichev, *Diskretnaya matematika i kriptologiya*, (Discrete Mathematics and Cryptology), Moskva, DIALOG–MIFI (Russian) 2003.

Received 25 April 2006
Revised 6 July 2006