Acta Societatis Mathematicae Latviensis
Abstracts of the 5^{th} Latvian Mathematical Conference, April 6–7, 2004, Daugavpils, Latvia

INVARIANCE OF INFINITE WORDS

JĀNIS BULS

University of Latvia
Raiņa bulvāris 19, LV-1586, Rīga, Latvia
E-mail: buls@fmf.lu.lv

The invention and financial exploitation of enciphering and deciphering machines is a lucrative branch of cryptography. Until the 19th century they there mechanical; from the beginning of the 20th century automation made its appearance, around the middle of the century came electronics and more recently microelectronic miniaturization. Today's microcomputers — roughly the size, weight, and price of a pocket calculator — have a performance as good as the best enciphering machines from the Second Word War. That restores the earlier significance of good methods, which had been greatly reduced by the presence of 'giant' computers in cryptanalysis centres [1].

A *cryptosystem* [3] is a five–tuple $\langle \mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D} \rangle$, where the following conditions are satisfied:
(i) $\mathcal{P}$ 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;
(ii) for each $K \in \mathcal{K}$, there is an encryption 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; besides, it may be considered as a special kind of a Mealy machine [4]. We investigate the lattice of machine invariant classes [2]. The design of stream ciphers motives the following constructions. 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, non"-empty 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. *An (indexed) infinite word x* on the alphabet A is any total map $x : \mathbb{N} \to A$. We shall set for any $i \geq 0$, $x_i = x(i)$ and write $x[n, n+k] = x_n x_{n+1} \ldots x_{n+k}$. The set of all the infinite words over A is denoted by A^ω. Let $(q_0, x, y) \in Q \times A^\omega \times B^\omega$. We write $y = q * x$ if $\forall n\ y[0,n] = q * x[0,n]$ and say an initial machine V *transforms* x to y.

Let $\mathfrak{A} = \{a_0, a_1, \ldots, a_n, \ldots\}$ be any fixed countable alphabet and consider the set $Fin(\mathfrak{A})$ of all non-empty finite subsets of $\mathfrak{A}$. Let $\mathfrak{M} = \{\langle Q, A, B, q_0, \circ, * \rangle \mid Q \in Fin(\mathfrak{Q}) \wedge A, B \in Fin(\mathfrak{A})\}$, where $\mathfrak{Q} = \{q_1, q_2, \ldots, q_n, \ldots\}$ is any fixed countable set. We say the word $x \in A_1^\omega$ is *apt* for $\langle Q, A, B, q_0, \circ, * \rangle$ if $A_1 \subseteq A$. A set $\emptyset \neq \mathfrak{K} \subseteq \mathfrak{F} = \{x \in A^\omega \mid A \in \mathfrak{A}\}$ is called *machine invariant* if every initial machine $V \in \mathfrak{M}$ all apt words of $\mathfrak{K}$ transforms to words of $\mathfrak{K}$.

Let $\mathfrak{L}$ be the set 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 smallest element in this lattice is the set of all ultimately periodic words.

REFERENCES

[1] Friedrich L. Bauer. *Decrypted secrets. Methods and maxims of cryptology.* Springer–Verlag, Berlin, 2000.

[2] J. Buls. Machine invariant classes. 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), 2003, 207–211.

[3] Douglas R. Stinson. *Cryptography. Theory and Practice.* CRC Press, 1995.

[4] В. М. Фомичев. *Дискретная математика и криптология.* Диалог-МИФИ, Москва, 2003.