Applications of Quasigroup String Transformations - Results of 20 Years of Investigation of Macedonian Researchers

SMILE MARKOVSKI
Faculty of Computer Science and Engineering &
Institute of Informatics of Faculty of Natural Sciences and Mathematics
Ss. Cyril and Methodius University, Skopje, Republic of Macedonia
smile.markovski@gmail.com

Many applications of mathematics use transformations of strings of symbols. Given a nonempty finite set $A = \{a_1, a_2, \ldots, a_n\}$ of symbols (or letters) a_i, denote by $A^n = \{(a_1, a_2, \ldots, a_n) | \ a_i \in A, i = 1, 2, \ldots, n\}$ the n-th power set of A. We usually identify the n-tuple $(a_1, a_2, \ldots, a_n)$ with the string $a_1 a_2 \ldots a_n$ and we denote by $A^+ = \cup_{n>0} A^n$ the set of all nonempty strings over the set A. Any mapping $f : B \to A^+$, where $B \subseteq A^+$, is said to be a transformation of strings of symbols of A.

We mention here two important fields where applications of transformations of strings of symbols are essential. One is the cryptography and the other is the coding theory.

There are several cryptographic products or crypto-primitives based on such transformations. As simple examples, let mention that a cipher is a mapping $f : A^+ \to A^+$ such that the original message $a_1 a_2 \ldots a_n$ cannot be effectively recovered by knowing only the cipher-text $f(a_1 a_2 \ldots a_n)$, and a hash function $f : A^+ \to A^k$ has, among others, the property to be effectively impossible to find two messages $m_1,\ m_2 \in A^+$ such that $h(m_1) = h(m_2)$, i.e., with same message digest.

In coding theory one has to recover the message m sent through an insecure channel from the message m' obtained at the end of the channel after transmission. Here, at first the original message $m = m_1 m_2 \ldots m_k,\ m_i \in A$, is expanded to a codeword $c(m) = c_1 c_2 \ldots c_n,\ c_i \in A$, where $k < n$. Then the codeword is sent through an insecure channel and a message $m' = d_1 d_2 \ldots d_n$ is obtained, usually different than $c(m)$, since the channel produces errors ($d_i \neq c_i$ for some indexes i). Now, the coding $c : A^+ \to A^+$ has to be defined in such a way the probability of recovering the original message m from the obtained m' to be as high as possible.

Twenty years ago a group of mathematicians from the Institute of informatics of the Faculty of Sciences at University in Skopje started to investigate transformations of strings by using quasigroups. Given a quasigroup $(Q, *)$, several quasigroup string transformations $f : Q^+ \to Q^+$ can be defined, and it happened the so called e-transformations and d-transformations to be most useful. For example, an e-transformation is defined by $e(a_1 a_2 \ldots a_n) = b_1 b_2 \ldots b_n,\ a_i, b_i \in Q$, if and only if $b_j = b_{j-1} * a_j,\ j = 1, 2, \ldots, n$ and b_0 is some fixed element of Q. Then $e : Q^+ \to Q^+$ is a permutation of Q^+ that has several useful properties, suitable for applications in cryptography and coding theory. Based on quasigroup string transformations there were designed many different types of crypto-primitives and new error detecting and error correcting codes.

By working on the applications of quasigroup string transformations, many open problems in quasigroup theory were opened too, like classification of the sets of quasigroups of given order, effective constructions of quasigroups of huge

orders (like those of order 2^{512}), representation of quasigroups by Boolean functions or by matrices, and so on. Many of these problems were successively solved as well.