Прилози, Одд. мат. тех. науки, МАНУ, **XXVII–XXVIII**, 1–2 (2006–2007), стр. 41–53
Contributions, Sec. Math. Tech. Sci., MANU, **XXVII–XXVIII**, 1–2 (2006–2007), pp. 41–53
ISSN 0351-3246
UDC: 512.54

QUASIGROUP STRING PROCESSING: PART 4

Smile Markovski and Verica Bakeva

A b s t r a c t: Given a finite alphabet A and a quasigroup operation $*$ on the set A, in earlier paper of ours we have defined the quasigroup transformation $E : A^+ \to A^+$, where A^+ is the set of all finite strings with letters from A. Here we present several generalizations of the transformation E and we consider the conditions under which the transformed strings have uniform distributions of n-tuples of letters of A. The obtained results can be applied in cryptography, coding theory, defining and improving pseudo random generators, and so on.

Key words: quasigroup, quasigroup string processing, uniform distribution

AMS Mathematics Subject Classification (2000): 20N05, 60E05

1. PRELIMINARIES

The quasigroup string transformations E and D, and their properties, were considered in several papers ([3], [4], [5], [6], [7]). Here we give generalizations of the transformation E and we investigate conditions under which the string obtained by such generalized transformations have uniform distributions of n-tuples of letters. The needed definitions used in this paper can be found in the above-cited papers and in [1], [2]. Here we give some of them for matter of completeness.

A quasigroup $(Q, *)$ is a groupoid (i.e. algebra with one binary operation $*$ on the set Q) satisfying the law:

$$(\forall u, v \in Q)(\exists! x, y \in Q) \ \ (x * u = v \ \& \ u * y = v) \tag{1}$$

In fact, (1) says that a groupoid $(Q, *)$ is a quasigroup if and only if the equations $x * u = v$ and $u * y = v$ have unique solutions x and y for each given $u, v \in Q$. It is usual the solutions x and y to be denoted by $x = v/u$ and $y = u \setminus v$. In such a way two new operations $/$ (a right division) and $\setminus$ (a left division) are defined on the set Q, and then also $(Q, /)$ and $(Q, \setminus)$ are quasigroups.

We define a quasigroup string transformation E as follows.

Let $A = \{1, \ldots, s\}$ be an alphabet ($s \geq 2$) and denote by $A^+ = \{x_1 \ldots x_k |\ \ x_i \in A,\ k \geq 1\}$ the set of all finite strings over A. Note that $A^+ = \bigcup (A^k |\ k \geq 1)$, where $A^k = \{x_1 \ldots x_k |\ x_i \in A\}$. Let $*$ be a quasigroup operation on the set A and take a fixed element $l \in A$, called a leader. Define a transformation $E = E_{l,*} : A^+ \to A^+$ as follows.

$$E(x_1 \ldots x_k) = y_1 \ldots y_k \Longleftrightarrow \left\{ \begin{array}{rcll} y_1 & = & l * x_1, & \\ y_{i+1} & = & y_i * x_{i+1}, & i = 1, \ldots, k-1, \end{array} \right. \tag{2}$$

where $x_i, y_i \in A$. We say that the string $x_1 \ldots x_k$ is an input message, while $y_1 \ldots y_k$ is the output message of E.

Using the transformation E, in Section 2 we prove that an input message with uniformly distributed n-tuples of letters is transformed to output message with uniformly distributed $n + 1$-tuples of letters. So, starting with an input message where the distribution of the letters is uniform, after one application of an E-transformation an output message with uniformly distributed pairs of letters will be obtained. Applying again an E-transformation on the output, the new output will have uniformly distributed triplets of letters. That way, after n applications of the E-transformation, we can obtain a message with uniformly distributed $n+1$-tuples of letters. By using Markov chains it was shown in the paper [4] that, after applying an E-transformation on arbitrary input message, an output message with uniformly distributed letters is obtained.

Generalizations of the transformation E are given in Section 3. It is shown that for the generalized transformations the following holds: if an input message has uniformly distributed n-tuples of letters, then the output message has uniformly distributed $n+d$-tuples of letters for $1 \leq d \leq n$. We made several experiments that support our results, and they are presented in Section 4. Possible applications of our results are discussed in Section 5.

2. UNIFORMITY OBTAINED BY E-TRANSFORMATION

Let the alphabet A be as above. A randomly chosen element of the set A^k can be considered as a random vector $(X_1, X_2, \ldots, X_k)$, where A is the range of X_i, $i = 1, \ldots, k$. We consider these vectors as input messages. The transformation $E = E_{l,*} : A^+ \to A^+$ can be applied on random vectors as

$$E(X_1 \ldots X_k) = Y_1 \ldots Y_k \Longleftrightarrow \left\{ \begin{array}{rcl} Y_1 & = & l * X_1, \\ Y_{i+1} & = & Y_i * X_{i+1}, \quad (i = 1, \ldots, k-1) \end{array} \right. \tag{3}$$

Let $(X_1, X_2, \ldots, X_\alpha)$ be an input message such that, for any fixed $1 \leq n \leq \alpha$ and for each $0 \leq t \leq \alpha - n$, the vectors $(X_{t+1}, X_{t+2}, \ldots, X_{t+n})$ are uniformly distributed on the set $\{1, 2, \ldots, s\}^n$, i.e.

$$(X_{t+1}, X_{t+2}, \ldots, X_{t+n}) \sim U(\{1, 2, \ldots, s\}^n);$$

in other words, let the n-tuples in the input messages be uniformly distributed. As a consequence, note that k-tuples of the input messages will be also uniformly distributed for each $k \leq n$, i.e. $(X_{t+1}, X_{t+2}, \ldots$ $\ldots, X_{t+k}) \sim U(\{1, 2, \ldots, s\}^k)$, $t = 0, 1, \ldots$. Hence, for $k = 1$ we have that $X_{t+1} \sim U(\{1, 2, \ldots, s\})$, for each $t \geq 0$, i.e., the letters are uniformly distributed too.

Let $(Y_1, Y_2, \ldots, Y_\alpha)$ be a random vector obtained from the vector $(X_1, X_2, \ldots, X_\alpha)$ by an E-transformation of kind (3). According to the definition of (3), Y_t is independent of the random variables $X_{t+1}, X_{t+2}, \ldots$, for each $t \geq 1$.

Proposition 1 *$Y_t \sim U(\{1, 2, \ldots, s\})$ for each $t \geq 1$.*

Proof For $t = 1$, $X_1 \sim U(\{1, 2, \ldots, s\})$ implies

$$P\{Y_1 = i\} = P\{l * X_1 = i\} = P\{X_1 = l \setminus i\} = \frac{1}{s}, \qquad i = 1, 2, \ldots, s.$$

This means that $Y_1 \sim U(\{1, 2, \ldots, s\})$. We proceed by induction, and let suppose that $Y_r \sim U(\{1, 2, \ldots, s\})$. Using the equations (3), total probability theorem and the independence of Y_r and X_{r+1} we compute the distribution of Y_{r+1} as follows.

$$\begin{aligned} P\{Y_{r+1}=i\} &= P\{Y_r * X_{r+1}=i\} = \sum_{k=1}^{s} P\{Y_r * X_{r+1}=i, Y_r=k\} \\ &= \sum_{k=1}^{s} P\{k * X_{r+1}=i, Y_r=k\} = \sum_{k=1}^{s} P\{X_{r+1}=k \setminus i, Y_r=k\} \\ &= \sum_{k=1}^{s} P\{X_{r+1}=k \setminus i\} P\{Y_r=k\} = \sum_{k=1}^{s} \frac{1}{s}\cdot\frac{1}{s} = \frac{1}{s}, \end{aligned}$$

for $i=1,2,\ldots,s$. □

The Proposition 1 can be generalized as follows.

Theorem 1 *Let* $(X_1, X_2, \ldots, X_\alpha)$ *be a given random vector such that* $(X_{t+1}, X_{t+2}, \ldots, X_{t+n}) \sim U(\{1,2,\ldots,s\}^n)$ *for each* $t \geq 0$ *and for fixed* $n \geq 1$. *If* $(Y_1, Y_2, \ldots, Y_\alpha)$ *is a random vector obtained by E-transformation of the vector* $(X_1, X_2, \ldots, X_\alpha)$, *then* $(Y_{t+1}, Y_{t+2}, \ldots, Y_{t+m}) \sim U(\{1,2,\ldots,s\}^m)$ *for each* $m \leq n+1$ *and each* $t \geq 0$.

Proof Let $m \leq n+1$ be a fixed positive integer. We will find the distribution of the vector $(Y_{t+1}, Y_{t+2}, \ldots, Y_{t+m})$ for arbitrary t.

$$\begin{aligned} &P\{Y_{t+1}=y_{t+1}, Y_{t+2}=y_{t+2}, \ldots, Y_{t+m}=y_{t+m}\} \\ &\quad = P\{Y_{t+1}=y_{t+1}, Y_{t+1} * X_{t+2}=y_{t+2}, \ldots, Y_{t+m-1} * X_{t+m}=y_{t+m}\} \\ &\quad = P\{Y_{t+1}=y_{t+1}, y_{t+1} * X_{t+2}=y_{t+2}, \ldots, y_{t+m-1} * X_{t+m}=y_{t+m}\} \\ &\quad = P\{Y_{t+1}=y_{t+1}, X_{t+2}=y_{t+1} \setminus y_{t+2}, \ldots, X_{t+m}=y_{t+m-1} \setminus y_{t+m}\} \\ &\quad = P\{Y_{t+1}=y_{t+1}\} P\{X_{t+2}=y_{t+1} \setminus y_{t+2}, \ldots, X_{t+m}=y_{t+m-1} \setminus y_{t+m}\}. \end{aligned}$$

The last equality is obtained by using that Y_{t+1} is independent of the vector $(X_{t+2}, \ldots, X_{t+m})$. Since $m \leq n+1$, the vector $(X_{t+2}, \ldots, X_{t+m})$ is uniformly distributed to the set $\{1,2,\ldots,s\}^{m-1}$. Applying this to the previous expression, we obtain that

$$P\{Y_{t+1}=y_{t+1}, Y_{t+2}=y_{t+2}, \ldots, Y_{t+m}=y_{t+m}\} = \frac{1}{s}\cdot\frac{1}{s^{m-1}} = \frac{1}{s^m}.$$

This means that for each $m \leq n+1$, the vectors $(Y_{t+1}, Y_{t+2}, \ldots, Y_{t+m})$ have uniform distribution on the set $\{1,2,\ldots,s\}^m$. □

Remark 1 Note that for $m > n+1$ the distribution of the vector $(X_{t+2}, \ldots, X_{t+m})$ is not known, so we cannot determine exactly the distribution of the random vector $(Y_{t+1}, Y_{t+2}, \ldots, Y_{t+m})$ (which generally is not uniform). We will discuss in Section 3 about the upper bounds of the distribution of the random vector $(Y_{t+1}, Y_{t+2}, \ldots, Y_{t+m})$.

Remark 2 Let consider the transformation $E_1 : A^+ \to A^+$ defined by

$$E_1(X_1 \dots X_k) = Y_1 \dots Y_k \Longleftrightarrow \left\{ \begin{array}{rcl} Y_1 & = & X_1 * l, \\ Y_{i+1} & = & X_{i+1} * Y_i, \quad (i = 1, \dots, k-1) \end{array} \right. \tag{4}$$

In the same way as Theorem 1 we can prove Theorem $1'$, where the transformation E is replaced by the transformation E_1.

3. GENERALIZED E-TRANSFORMATIONS

The transformation E defined in (3) is not the only one that can be used as quasigroup string transformation. Here we will consider some other kind of transformations that generalize the transformation E. We will show that they give uniform distribution of higher level than E. Namely, we define a transformation G_d with following property: after applying G_d on an input string with uniformly distributed n-tuples we obtain an output string with uniform distribution of $n + d$ -tuples, where $d \leq n$.

Let A be as before and let define the transformation $G = G_d : A^+ \to A^+$ as follows. Take fixed leaders $l_1, l_2, \dots, l_d \in A$, where d is a positive integer. Then:

$$G(X_1 \dots X_k) = Y_1 \dots Y_k \Longleftrightarrow$$

$$\Longleftrightarrow \left\{ \begin{array}{rcl} Y_1 & = & l_1 * (l_2 * (\cdots * (l_{d-1} * (l_d * X_1)) \dots)) \\ Y_2 & = & l_2 * (l_3 * (\cdots * (l_d * (Y_1 * X_2)) \dots)) \\ \dots & & \\ Y_d & = & l_d * (Y_1 * (\cdots * (Y_{d-2} * (Y_{d-1} * X_d)) \dots)) \\ Y_{d+1} & = & Y_1 * (Y_2 * (\cdots * (Y_d * X_{d+1}) \dots)) \\ \dots & & \\ Y_k & = & Y_{k-d} * (Y_{k-d+1} * (\cdots * (Y_{k-1} * X_k) \dots)) \end{array} \right. \tag{5}$$

Proposition 2 *Let $d \leq n$ and $(X_{t+1}, X_{t+2}, \dots, X_{t+n}) \sim U(\{1, 2, \dots, s\}^n)$. Then $(Y_{t+1}, Y_{t+2}, \dots, Y_{t+d}) \sim U(\{1, 2, \dots, s\}^d)$, for arbitrary $t \geq 0$.*

Proof The distribution of the vector $(Y_{t+1}, Y_{t+2}, \ldots, Y_{t+d})$ for $t = 0$ is the following.

$$\begin{aligned}
&P\{Y_1 = y_1,\ \ldots,\ Y_d = y_d\}\\
&\quad = P\{l_1 * (\cdots * (l_d * X_1)\ldots) = y_1,\ \ldots,\ l_d * (Y_1 * (\cdots * (Y_{d-1} * X_d)\ldots)) = y_d\}\\
&\quad = P\{l_1 * (\cdots * (l_d * X_1)\ldots) = y_1,\ \ldots,\ l_d * (y_1 * (\cdots * (y_{d-1} * X_d)\ldots)) = y_d\}\\
&\quad = P\{X_1 = x_1,\ \ldots,\ X_d = x_d\}\\
&\quad = \frac{1}{s^d},
\end{aligned}$$

where x_1 is the solution of the quasigroup equation $l_1 * (\cdots * (l_{d-1} * (l_d * x)))) = y_1$, i.e. $x_1 = l_d \setminus (l_{d-1} \setminus (\cdots \setminus (l_1 \setminus y_1)))$, and so on, $x_d = y_{d-1} \setminus (y_{d-2} \setminus (\cdots \setminus (y_1 \setminus (l_d \setminus y_d))))$.

We proceed by induction. Suppose that

$$(Y_{t+1}, \ldots, Y_{t+d}) \sim U(\{1, 2, \ldots, s\}^d)$$

for each $t \leq r-1$. Now, the distribution of the vector $(Y_{r+1}, \ldots, \ldots, Y_{r+d})$ is the following.

$$\begin{aligned}
&P\{Y_{r+1} = y_{r+1}, \ldots, Y_{r+d} = y_{r+d}\}\\
&\quad = P\{Y_{r-d+1} * (\cdots * (Y_r * X_{r+1})\ldots) = y_{r+1}, \ldots\\
&\qquad\qquad \ldots, Y_r * (\cdots * (Y_{r+d-1} * X_{r+d})\ldots) = y_{r+d}\}\\
&\quad = \sum_{k_1,\ldots,k_d=1}^{s} P\{Y_{r-d+1} * (\cdots * (Y_r * X_{r+1})\ldots) = y_{r+1}, \ldots\\
&\qquad \ldots, Y_r * (\cdots * (Y_{r+d-1} * X_{r+d})\ldots) = y_{r+d}, Y_{r-d+1} = k_1, \ldots, Y_r = k_d\}\\
&\quad = \sum_{k_1,\ldots,k_d=1}^{s} P\{k_1 * (\cdots * (k_d * X_{r+1})\ldots) = y_{r+1}, \ldots\\
&\quad \ldots, k_d * (y_{r+1} * (\cdots * (y_{r+d-1} * X_{r+d})\ldots)) = y_{r+d}, Y_{r-d+1} = k_1, \ldots, Y_r = k_d\}\\
&\quad = \sum_{k_1,\ldots,k_d=1}^{s} P\{X_{r+1} = x_{r+1}, \ldots, X_{r+d} = x_{r+d}, Y_{r-d+1} = k_1, \ldots, Y_r = k_d\},
\end{aligned}$$

where x_j are the solutions of the corresponding quasigroup equations.

Note that the vectors $(X_{r+1}, \ldots, X_{r+d})$ and $(Y_{r-d+1}, \ldots, Y_r)$ are independent; namely, by the definition (5) of the transformation G we have that the random variable Y_i depends only on the random variables $X_1, \ldots, X_i$. Therefore, we have

$$\begin{aligned} &P\{Y_{r+1} = y_{r+1}, \ldots, Y_{r+d} = y_{r+d}\} \\ &\quad = \sum_{k_1,\ldots,k_d=1}^{s} P\{X_{r+1} = x_{r+1}, \ldots, X_{r+d} = x_{r+d}\} P\{Y_{r-d+1} = k_1, \ldots, Y_r = k_d\} \\ &\quad = \sum_{k_1,\ldots,k_d=1}^{s} \frac{1}{s^d} \cdot \frac{1}{s^d} = \frac{1}{s^d} \end{aligned}$$

which means that $(Y_{t+1}, Y_{t+2}, \ldots, Y_{t+d}) \sim U(\{1, 2, \ldots, s\}^d)$. □

Theorem 2 *Let* $(X_1, X_2, \ldots, X_\alpha)$ *be a given random vector such that* $(X_{t+1}, X_{t+2}, \ldots, X_{t+n}) \sim U(\{1, 2, \ldots, s\}^n)$ *for each* $t \geq 0$ *and for fixed* $n \geq 1$. *If* $(Y_1, Y_2, \ldots, Y_\alpha)$ *is a random vector obtained by* G_d*-transformation of the vector* $(X_1, X_2, \ldots, X_\alpha)$, *then* $(Y_{t+1}, Y_{t+2}, \ldots, Y_{t+m}) \sim U(\{1, 2, \ldots, s\}^m)$ *for each* $m \leq n + d$ *and each* $t \geq 0$.

Proof The theorem is true for $m \leq d$ by Proposition 2. Let fix an integer m, $d < m \leq n + d$. We find the distribution of the vector $(Y_{t+1}, Y_{t+2}, \ldots, Y_{t+m})$, for arbitrary t, as follows.

$$\begin{aligned} &P\{Y_{t+1} = y_{t+1}, \ldots, Y_{t+d} = y_{t+d}, Y_{t+d+1} = y_{t+d+1}, \ldots, Y_{t+m} = y_{t+m}\} \\ &= P\{Y_{t+1} = y_{t+1}, \ldots, Y_{t+d} = y_{t+d}, Y_{t+1} * (\cdots * (Y_{t+d} * X_{t+d+1}) \ldots) = y_{t+d+1}, \ldots \\ &\qquad \ldots, Y_{t+m-d} * (\cdots * (Y_{t+m-1} * X_{t+m}) \ldots) = y_{t+m}\} \\ &= P\{Y_{t+1} = y_{t+1}, \ldots, Y_{t+d} = y_{t+d}, y_{t+1} * (\cdots * (y_{t+d} * X_{t+d+1}) \ldots) = y_{t+d+1}, \ldots \\ &\qquad \ldots, y_{t+m-d} * (\cdots * (y_{t+m-1} * X_{t+m}) \ldots) = y_{t+m}\} \\ &= P\{Y_{t+1} = y_{t+1}, \ldots, Y_{t+d} = y_{t+d}, X_{t+d+1} = x_{t+d+1}, \ldots, X_{t+m} = x_{t+m}\} \end{aligned}$$

where x_i are the solutions of the corresponding quasigroup equations (i.e. $x_{t+d+1} = y_{t+d} \setminus (y_{t+d-1} \setminus (\cdots \setminus (y_{t+1} \setminus y_{t+d+1}) \ldots))$, and so on.)

Since the vectors $(X_{t+d+1}, \ldots, X_{t+m})$ and $(Y_{t+1}, \ldots, Y_{t+d})$ are independent, we have

$$\begin{aligned} &P\{Y_{t+1} = y_{t+1}, \ldots, Y_{t+m} = y_{t+m}\} \\ &\quad = P\{Y_{t+1} = y_{t+1}, \ldots, Y_{t+d} = y_{t+d}\} P\{X_{t+d+1} = x_{t+d+1}, \ldots, X_{t+m} = x_{t+m}\}. \end{aligned}$$

Now, since $m - d \leq n$, the vector $(X_{t+d+1}, \ldots, X_{t+m})$ is uniformly distributed on the set $\{1, 2, \ldots, s\}^{m-d}$. Then, by Proposition 2, we have

$$P\{Y_{t+1} = y_{t+1}, \ldots, Y_{t+m} = y_{t+m}\} = \frac{1}{s^d} \cdot \frac{1}{s^{m-d}} = \frac{1}{s^m}.$$

□

The distributions of the vectors $(Y_{t+1}, \ldots, Y_{t+m})$ must not be uniform in the case $m > n + d$. By the next theorem, it can be seen that the distribution of the m-tuples is becoming closer to the uniform distribution with increasing of d ($d < m - n$).

Theorem 3 *Let* $(X_1, X_2, \ldots, X_\alpha)$ *be a given random vector such that* $(X_{t+1}, X_{t+2}, \ldots, X_{t+n}) \sim U(\{1, 2, \ldots, s\}^n)$ *for each* $t \geq 0$ *and for fixed* $n \geq 1$. *If* $(Y_1, Y_2, \ldots, Y_\alpha)$ *is a random vector obtained by* G_d*-transformation of the vector* $(X_1, X_2, \ldots, X_\alpha)$, *then all probabilities in the distribution of the vectors* $(Y_{t+1}, Y_{t+2}, \ldots \ \ldots, Y_{t+m})$ *are upper bounded by* $\frac{1}{s^{n+d}}$ *for each* $m > n + d$ *and each* $t \geq 0$.

Proof We have

$$\begin{aligned} &P\{Y_{t+1} = y_{t+1}, \ldots, Y_{n+d} = y_{n+d}, Y_{n+d+1} = y_{n+d+1}, \ldots, Y_{t+m} = y_{t+m}\} \\ &= P\{Y_{t+1} = y_{t+1}, \ldots, Y_{n+d} = y_{n+d}\} \times \\ &\quad \times P\{Y_{n+d+1} = y_{n+d+1}, \ldots, Y_{t+m} = y_{t+m} |\ Y_{t+1} = y_{t+1}, \ldots, Y_{n+d} = y_{n+d}\} \end{aligned}$$

By Theorem 2, for $m = n + d$, we have $P\{Y_{t+1} = y_{t+1}, \ldots, Y_{n+d} = y_{n+d}\} = 1/s^{n+d}$. On the other hand, $P\{Y_{n+d+1} = y_{n+d+1}, \ldots, Y_{t+m} = y_{t+m} |\ Y_{t+1} = y_{t+1}, \ldots, Y_{n+d} = y_{n+d}\} \leq 1$. □

The transformation G_d is not the unique possible generalization of the E-transformation. We can change the way of application of the quasigroup operation $*$ and we can obtain several other kind of transformations. As an example, for $d = 3$ we can use the following applications of the operation $*$ (altogether, there are 120 different forms):

$Y_4 = Y_1 * (Y_2 * (Y_3 * X_4))$ - this was used for definition of G_3 as in (5);
$Y_4 = Y_1 * (Y_3 * (Y_2 * X_4))$; $\quad Y_4 = Y_2 * (Y_1 * (Y_3 * X_4))$;
$Y_4 = Y_2 * (Y_3 * (Y_1 * X_4))$; $\quad Y_4 = Y_3 * (Y_1 * (Y_2 * X_4))$;
$Y_4 = Y_1 * (Y_2 * (X_4 * Y_3))$; $\quad Y_4 = Y_1 * (Y_3 * (X_4 * Y_2))$; $\quad$ and so on.

For arbitrary d, we can choose any bracketing and we can place the variables $Y_1, \ldots, Y_d$ and X_{d+1} in arbitrary order. By using the obtained form we can define a transformation $T : A^+ \to A^+$ in the same way as (5). Then we can state and proof theorems like Theorem 2 and Theorem 3; namely, as one can notice, the proof of Theorem 2 depends strongly on the possibilities a quasigroup equation with one unknown to be solved.

4. EXPERIMENTAL RESULTS

We made many experiments in order to check our theoretical results. Here we give an example. We have randomly chosen a string with 1,000,000 letters of the alphabet $A = \{1, 2, 3, 4\}$ with only letters uniformly distributed. A G_d transformation was defined by using the quasigroup (6).

$*$	1	2	3	4
1	2	1	3	4
2	3	4	2	1
3	1	3	4	2
4	4	2	1	3

(6)

We took leaders $l_0 = 1$, $l_1 = 1, \ldots, l_d = 1$.

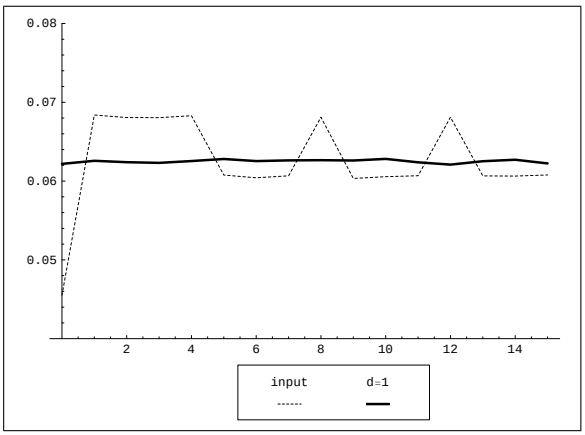

Figure 1. The distribution of the pairs in the input message and the output message for $d = 1$

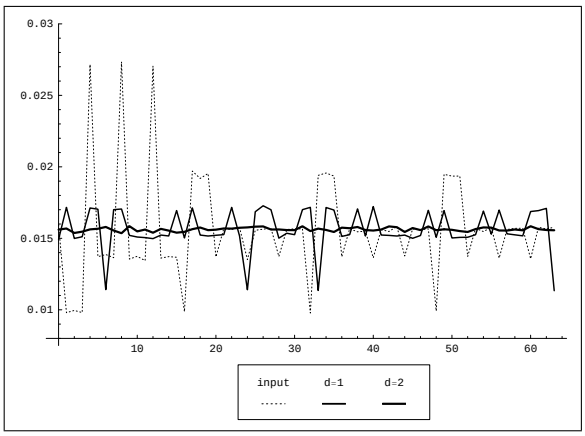

Figure 2. The distribution of the triplets in input message and output messages for $d = 1$ and $d = 2$

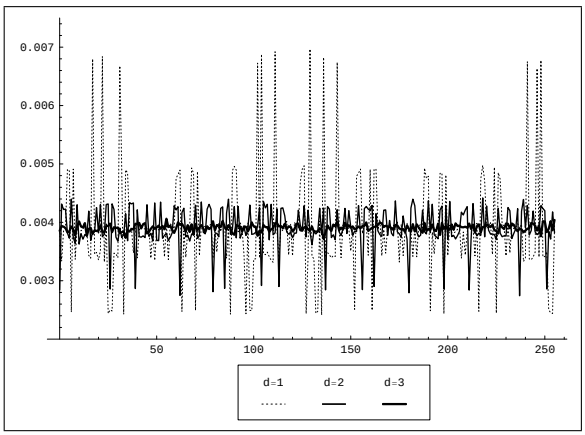

Figure 3. The distribution of the 4-tuples in output messages strings for $d = 1$, $d = 2$ and $d = 3$

The distributions of pairs in the input message and output message for $d = 1$ are presented on the Figure 1. The distributions of triplets in input message and output messages for $d = 1, 2$ are presented on the Figure 2 and the distributions of 4-tuples for $d = 1, 2, 3$ are presented on the Figure 3.

We can see on Figure 1 that, for $d = 1$, the pairs are uniformly distributed. Also, we can see on Figure 2 that the distribution of the triplets for $d = 1$ is closer to the uniform distribution than the distribution of triplets in the input message (which is in correlation with Theorem 3). The same is true for the 4-tuples (Figure 3).

5. CONCLUSION

We show in this paper that quasigroup transformations can be applied for improving the uniformly distributed strings, in the sense that from strings with uniformly distributed n-tuples it can be obtained strings with uniformly distributed $n + d$-tuples ($d \geq 1$). The results can be applied in cryptography and coding theory for:

- improving the existing and defining new kinds of pseudo random number (and sequence) generators [11];
- defining primitives for hash functions [8], [9];
- defining primitives for stream cipher [7];
- design of random codes [10];

and many others.

REFERENCES

[1] Belousov, V.D.: *Osnovi teorii kvazigrup i lup (The fundament of the theory of quasigroups and loops)*, (1967) "Nauka", Moskva.

[2] Denes, J., Keedwell, A.D.: Latin Squares and their Applications (1974) "The English Universities Press Ltd", Budapest.

[3] Markovski, S., Gligoroski, D., Andova, S.: *Using quasigroups for one-one secure encoding.*, Proc. VIII Conf. Logic and Computer Science "LIRA '97", Novi Sad, (1997) 157–162.

[4] Markovski,S., Gligoroski,D., Bakeva,V.: *Quasigrouop string processing: Part 1*, Contributions, Sec. Math. Tech. Sci., MANU, **XX 1-2** (1999) 13–28.

[5] Markovski, S., Kusakatov, V.: *Quasigroup String Processing: Part 2*, Contributions, Sec. Math. Tech.Sci., MANU, XXI, 1-2 (2000) 15–32.

[6] Markovski, S., Kusakatov, V.: *Quasigroup String Processing: Part 3*, Contributions, Sec. Math. Tech.Sci., MANU, XXIII-XXIV, 1-2 (2002-2003), 7–27.

[7] Markovski, S.: *Quasigroup string processing and applications in cryptography*, First Intern. Conf. Mathematics and Informatics for Industry, Thessaloniki, Greece (2003), 278–289.

[8] Gligoroski, D., Markovski, S. and Bakeva, V.: *On infinite class of strongly collision resistant hAsh functions 'Edon-F' with variable length of output*, First Intern. Conf. Mathematics and Informatics for Industry, Thessaloniki, Greece (2003), 302–308.

[9] Markovski, S., Gligoroski, D., and Bakeva, V.: *Quasigroup and Hash Functions*, Disc. Math. and Appl, Sl.Shtrakov and K. Denecke ed., Proceedings of the 6th ICDMA, Bansko (2001), 43-50.

[10] Gligoroski, D., Markovski, S., Kocarev, Lj.: *New Directions in Coding: From Statistical Physics to Quasigroup String Transformations*, 2004 Inter. Symp. on Nonlinear Theor. and its Applic (NOLTA2004), Fukuoka, Japan, Nov.29 - Dec. 3, 2004, 545–548.

[11] Markovski, S., Gligoroski, D., Kocarev, Lj.: *Unbiased Random Sequences from Quaisgroup String Transformations*, H. Gilbert and H. Handschuh (Eds.): FSE 2005, LNCS 3557 (2005), 163–180.

Р е з и м е

КВАЗИГРУПНИ ТРАНСФОРМАЦИИ НА НИЗИ: ДЕЛ 4

За дадена азбука A и квазигрупна трансформација $*$ на множеството A, во наш претходен труд, е дефинирана квазигрупна трансформација $E : A^+ \to A^+$, каде A^+ е множеството од сите непразни конечни низи над A. Во овој труд, се дадени неколку генерализации на E и се разгледуваат условите при кои трансформираните низи имаат рамномерна распределба на n-торки од букви од A. Добиените резултати може да се применат во криптографија, теорија на кодирање, дефинирање и подобрување на генератори на псевдо-случајни броеви итн.

Клучни зборови: квазигрупа, квазигрупна трансформација на низи, рамномерна распределба

Address:
Smile Markovski
Faculty of Natural Sciences and Mathematics, Institute of Informatics,
Ss Cyril and Methodius University, Skopje
P. O. Box 162, MK-1001 Skopje, Republic of Macedonia
smile@ii.edu.mk

Verica Bakeva
Faculty of Natural Sciences and Mathematics, Institute of Informatics,
Ss Cyril and Methodius University, Skopje
P. O. Box 162, MK-1001 Skopje, Republic of Macedonia
verica@ii.edu.mk

Прилози, Одд. мат. тех. науки, **XXVII–XXVIII**, 1–2 (2006–2007), стр. 41–53