Quasigroups and Related Systems **31** (2023), 207 – 220

https://doi.org/10.56415/qrs.v31.16

Quasigroups generated by shift registers and Feistel networks

Sucheta Chakrabarti, Alexei V. Galatenko, Valentin A. Nosov, Anton E. Pankratiev and Sharwan K. Tiwari

Abstract. Formula-based specification of large quasigroups with the use of complete mappings over Abelian groups is investigated. Complete mappings specified by generalized feedback registers and generalized Feistel networks are considered. In both cases criteria for the mapping completeness are established. A procedure for uniform sampling of quasigroups induced by complete mappings under study is suggested. The classes of quasigroups generated by generalized feedback shift registers or generalized Feistel networks and by the permutation construction applied to proper families of functions are shown to be disjoint.

1. Introduction

Finite quasigroups are a promising platform for the implementation of various cryptographic primitives [9, 18]. In particular, quasigroup-based algorithms regularly take part in NIST contest, e.g., hash functions NaSHA [10] and EDON-R$'$ [8] participated in SHA-3 contest, and GAGE and InGAGE suite [7] was a candidate for Lightweight Cryptography Standard.

Of special interest is the apparatus of binary networks proposed by Cherednik [2, 3]. The networks are parameterized by either a quasigroup operation or a left (or right) quasigroup operation. It turned out to be possible to construct networks such that the transform implemented for any sufficiently large domain size is transitive or even multiply transitive.

NaSHA hash function uses quasigroups of the order 2^{64}; tabular specification of such a large quasigroup is impossible due to memory limitations. A possible way around is to switch to some sort of a formula-based specification. The solution used in NaSHA is based on a recursive application

2010 Mathematics Subject Classification: 20N05, 05B15

Keywords: quasigroup, orthomorphism, feedback shift register, Feistel network

of extended Feistel networks introduced by Markovski and Mileva in [11]. The idea behind extended Feistel networks is the connection between complete mappings of Abelian groups and quasigroups noticed by Sade [17]: if σ is a complete mapping of an Abelian group $G = (Q, +)$, i.e., both $\sigma(x)$ and $\sigma(x) - x$ are bijective, then $(Q, \sigma(x - y) + y)$ is a quasigroup. Later Markovski and Mileva proposed other generalizations of Feistel networks and established sufficient conditions for completeness of the corresponding mappings [12, 13].

In our paper we consider generalized feedback shift registers (GFSR) over Abelian groups, a model that, on the one hand, is a straightforward extension of classic feedback registers, and, on the other hand, covers the major part of generalizations proposed by Markovski and Mileva. We prove a completeness criterion for the mapping specified by generalized feedback shift registers and use this criterion to obtain the cardinality of the set of quasigroups generated by GFSRs. We also describe a procedure for uniform sampling of quasigroups generated by GFSRs. If a quasigroup is used as a key of a cryptographic transform, then the cardinality of the set generated determines the strength against brute force attacks; a set of a high cardinality can also be viewed as an approximation of Cherednik's model. Random objects often possess a number of beneficial properties (in particular, random quasigroups are polynomially complete, i.e. simple and non-affine [1], and even not isotopic to quasigroups that are polynomially incomplete [5]), so selection of a quasigroup at random may be a good idea. Properties of "random" quasigroups generated by generalized feedback registers are the subject of future research.

The generalized Feistel network is another generalization of extended Feistel networks from [11]. In this case, we increase the number of non-linear feedback loops. Similarly to the case of GFSR, we establish a completeness criterion, evaluate the cardinality of the set of quasigroups generated and provide a procedure for uniform sampling.

Proper families of functions over Abelian groups and permutation construction applied to proper families over Abelian groups are another way to specify big families of large quasigroups in a memory-efficient way [14, 15]. Interestingly, this method is "orthogonal" to generalized feedback shift registers and generalized Feistel networks in a sense that the classes of quasigroups generated by generalized feedback shift registers or generalized Feistel networks and by the permutation construction applied to proper families of functions turn out to be disjoint.

The rest of the paper is organized as follows. Section 2 contains basic definitions. Section 3 is devoted to generalized feedback registers. Section 4 covers generalized Feiltel networks. Section 5 is the conclusion.

2. Main definitions

A *finite quasigroup* is a pair (Q, f), where Q is a finite set and f is a binary operation on Q invertible in each variable, i.e. for any $a, b \in Q$ the equations $f(x, a) = b$ and $f(a, y) = b$ are uniquely solvable. All objects considered in our paper are finite, so for the sake of brevity the word "finite" will be omitted.

Obviously (Q, f) is a quasigroup if and only if the Cayley table of f is a *Latin square*, i.e., the elements comprising any row or column are distinct.

Let $(Q, +)$ be a finite Abelian group, σ be a bijective mapping (i.e., a permutation) on Q. The mapping σ is *complete* with respect to the group $(Q, +)$ if the mapping σ' specified by the rule $\sigma'(x) = \sigma(x) - x$ is also bijective. In this case the mapping σ' is called the *ortomorphism* associated with σ.

Complete mappings can be used to specify quasigroups. Namely, in [17] it is shown that if σ is complete with respect to an Abelian group $(Q, +)$ and

$$f(x, y) = \sigma(x - y) + y, \tag{1}$$

then (Q, f) is a quasigroup. It can be easily shown that the assertion also holds for

$$f(x, y) = \sigma(x + y) - y. \tag{2}$$

Indeed, the equation

$$f(a, y) = \sigma(a + y) - y = b$$

has a unique solution $y = (\sigma')^{-1}(b - a) - a$, and the equation

$$f(x, a) = \sigma(x + a) - a = b$$

has a unique solution $x = \sigma^{-1}(b + a) - a$. If $(Q, +)$ is an elementary Abelian 2-group (i.e., isomorphic to $\mathbb{Z}_2^m$ for some $m \in \mathbb{N}$), then $\sigma(x - y) + y = \sigma(x + y) - y = \sigma(x + y) + y$.

Assume that $|Q| = k^n$ for some $k, n \in \mathbb{N}$, $k \geqslant 2$. Then the elements $q_0, q_1, \ldots, q_{k^n-1}$ of Q can be naturally represented by n-tuples corresponding to the k-ary notation of the element indices. For example, q_0 is represented by the n-tuple $(0, \ldots 0)$ and q_{k^n-1} is represented by the n-tuple

$(k-1,\dots,k-1)$. Denote the set $\{0,1,\dots,k-1\}$ by E_k. Denote the set of all t-ary functions on E_k by P_k^t. Without loss of generality one can assume that $Q = E_k^n$ and write the equality $z = f(x,y)$ in the form

$$\begin{aligned} &z_1 = f_1(x_1,\dots,x_n,y_1,\dots,y_n)\\ &z_2 = f_2(x_1,\dots,x_n,y_1,\dots,y_n)\\ &\vdots\\ &z_n = f_n(x_1,\dots,x_n,y_1,\dots,y_n), \end{aligned} \tag{3}$$

where $f_i \in P_k^{2n}$. The relations (3) are referred to as a multivariate representation of the operation f.

Assume that $k \in \mathbb{N}$, $k \geqslant 2$, $G = (E_k,+)$ is an Abelian group, 0 is the neutral element of G, $n \in \mathbb{N}$, $n \geqslant 2$, $\mathcal{G} = G^n$. We will use the same notation for operations on G and $\mathcal{G}$; the domain of the operation will be clear from the context.

A multivariate mapping $\sigma = (f_1(x_1,\dots,x_n),\dots,f_n(x_1,\dots,x_n))\colon E_k^n \to E_k^n$ specified by the relations

$$\begin{aligned} &f_1 = x_2\\ &f_2 = x_3\\ &\vdots\\ &f_{n-1} = x_n\\ &f_n = x_1 + g(x_2,\dots,x_n), \end{aligned} \tag{4}$$

where g is some function from E_k^{n-1} to E_k, is referred to as a *feedback shift register*. Obviously the mapping σ is a permutation on E_k^n. In Section 3 we will establish a criterion for $\sigma(x)$ being a complete mapping.

A *Feistel network* is defined for the case $n = 2$ by the multivariate mapping $(f_1 = x_2, f_2 = x_1 + g(x_2))$, where g is a mapping on E_k. On the one hand, it is a special case of a feedback shift register; on the other hand, it is well known that a Feistel network is a complete mapping if and only if g is a bijection.

In [11, 12, 13] the authors analyzed a number of generalizations of Feistel networks. A Parametrized Feistel Network (PFN) is defined for $n = 2$ and is specified by the relations $f_1 = x_2 + c_1$, $f_2 = x_1 + c_2 + g(x_2)$, where $g \in P_k^1$, $c_1, c_2 \in E_k$. If g is a bijection, then the mapping specified by PFN is complete [12, Theorem 3.3]. Other generalizations are defined for arbitrary n. A type-1 Parameterized Extended Feistel Network (PEFN) is specified by the relations $f_1 = x_2 + g(x_1) + c_1$, $f_2 = x_3 + c_2$, $f_3 = x_4 + c_3$,

$\ldots$, $f_{n-1} = x_n + c_{n-1}$, $f_n = x_1 + c_n$, where $g \in P_k^1$, $c_1, \ldots, c_n \in E_k$. A consistent renumbering of functions and variables makes these relations take the form $f_1 = x_2 + c_1$, $f_2 = x_3 + c_2$, $\ldots$, $f_{n-1} = x_n + c_{n-1}$, $f_n = x_1 + g(x_n) + c_n$. Similarly to the case of PFN, if g is a bijection, then the mapping is complete [12, Theorem 3.4]. A Parameterized Generalized Feistel Non Linear Feedback Shift Register (PGF-NLFSR) is specified by the relations $f_1 = x_2 + c_1$, $f_2 = x_3 + c_2$, $\ldots$, $f_{n-1} = x_n + c_{n-1}$, $f_n = x_2 + x_3 + \ldots + x_n + c_n + g(x_1)$ with $g \in P_k^1$ and $c_1, \ldots, c_n \in E_k$. If the group G is isomorphic to $\mathbb{Z}_2^m$ for some $m \in \mathbb{N}$, n is even and g is a bijection, then the mapping specified by PGF-NLFSR is complete [12, Theorem 3.5]. Finally, a type-4 Parameterized Extended Feistel Network (PEFN) is defined by the relations $f_1 = x_2 + c_1$, $f_2 = x_3 + c_2$, $\ldots$, $f_{n-1} = x_n + c_{n-1}$, $f_n = x_1 + c_n + g(x_2 + x_3 \ldots + x_n)$, where $c_1, \ldots, c_n$ are some constants from E_k, $g \in P_k^1$. Similarly to the case of PGF-NLFSR, if the group G is isomorphic to $\mathbb{Z}_2^m$ for some $m \in \mathbb{N}$, n is even and g is a bijection, then the mapping is complete [13, Theorem 5].

Similarly to the constructions from [11, 12, 13] we generalize the definition of a feedback shift register by adding linear summands to the relations (4). A multivariate mapping

$$\sigma = (f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n)) \colon E_k^n \to E_k^n$$

specified by the relations

$$\begin{aligned} &f_1 = x_2 + c_1 \\ &f_2 = x_3 + c_2 \\ &\vdots \\ &f_{n-1} = x_n + c_{n-1} \\ &f_n = x_1 + g(x_2, \ldots, x_n) + c_n, \end{aligned} \tag{5}$$

where g is some function from E_k^{n-1} to E_k, $c_1, \ldots, c_n \in E_k$, is referred to as a *generalized feedback shift register.* Identically to the case of "regular" feedback shift registers, the mapping σ is obviously a permutation on E_k^n. Note that PFN, type-1 PEFN (after renumbering) and type-4 PEFN are generalized feedback shift registers.

Consider another way of generalization of a Feistel network. A *generalized Feistel network* is defined for the case $n = 2$ by the relations

$$\begin{aligned} &f_1 = s(x_2) \\ &f_2 = x_1 + p(x_2), \end{aligned} \tag{6}$$

where s, p are some functions from E_k to E_k. In Section 4 we will establish a criterion of mapping completeness for the case of generalized Feistel networks.

Proper families of functions over Abelian groups is another way of a formula-based specification of large families of quasigroups. A family $(g_1, \ldots, g_n)$, $g_i \in P_k^n$, $i = 1, \ldots, n$, is *proper*, if for any $\alpha, \alpha' \in E_k^n$, $\alpha = (a_1, \ldots, a_n)$, $\alpha' = (a'_1, \ldots, a'_n)$, $\alpha \neq \alpha'$, there exists an index i, $1 \leqslant i \leqslant n$, such that $a_i \neq a'_i$ and $g_i(\alpha) = g_i(\alpha')$.

Suppose that $f \in P_k^n$ is some function, $1 \leqslant i \leqslant n$. The variable x_i is said to be *dummy* (or *inessential*) for the function f, if for any $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n \in E_k$ the function

$$f'(x) = f(a_1, \ldots, a_{i-1}, x, a_{i+1}, \ldots, a_n)$$

is a constant. In other words, the function f does not depend on the value of the ith variable. Obviously if a family $(g_1, \ldots, g_n)$ is proper, then for $i = 1, \ldots, n$ the variable x_i is dummy for g_i.

Let

$$f_i(x_1, \ldots, x_n, y_1, \ldots, y_n) = x_i + y_i + g_i(p_1(x_1, y_1), \ldots, p_n(x_n, y_n)), \qquad (7)$$

where $p_1, \ldots, p_n$ are arbitrary functions from P_k^2. If the family $(g_1, \ldots, g_n)$ is proper, then $(f_1, \ldots, f_n)$ is a multivariate representation of a quasigroup operation [14, Theorem 1]. Thus a single proper family generates $\left(k^{k^2}\right)^n$ quasigroups, though some of these quasigroups may coincide. It is known [6, Theorem 8] that all quasigroups specified by proper families over Abelian groups contain a unique subquasigroup of the order 1 (i.e., a "fixed point" α such that $f(\alpha, \alpha) = \alpha$). A possible way to overcome this problem is to use the permutation construction proposed by Piven [15]. The construction consists in applying permutations $\beta, \gamma, \delta \in S_n$ to the indices of the variables x, y and functions in the representation (7), respectively, so that the relations (7) take the form

$$f_{\delta(i)} = x_{\beta(i)} + y_{\gamma(i)} + g_i(p_1(x_{\beta(1)}, y_{\gamma(1)}), \ldots, p_n(x_{\beta(n)}, y_{\gamma(n)})). \qquad (8)$$

If the family $(g_1, \ldots, g_n)$ is proper, then the relations (8) define a quasigroup operation for any choice of the internal functions $p_1, \ldots, p_n$ and permutations β, γ, δ [15, Theorem 2]. On the one hand, the permutations can be stored using $O(n \log_2 n)$ bytes which is negligible in comparison with the quasigroup order k^n. On the other hand, utilizing permutation construction allows one to increase the cardinality of the set of quasigroups generated and to improve some of important properties, e.g., to get rid of subquasigroups or affinity. Without loss of generality one can assume that δ is the identical permutation, since applying a non-trivial δ can be reduced to applying additional permutations β and γ and possibly changing the proper family [16, Theorem 1]. The assertions obtained by Piven are formally established for the case $k = 2$, $G = (E_2, \oplus)$, but the proofs do hold for the general case.

We will show that the set of quasigroups specified by permutation construction applied to proper families of functions does not intersect with the set of quasigroups specified by generalized feedback shift registers and generalized Feistel networks.

3. Quasigroups generated by feedback shift registers

Theorem 3.1. *A generalized feedback shift register is a complete mapping if and only if any non-trivial shift changes the value of the function g, i.e., for any tuple $(a_2, \ldots, a_n) \in E_k^{n-1}$ and any $a \in E_k$, $a \neq 0$, it holds that $g(a_2, \ldots, a_n) \neq g(a_2 + a, \ldots, a_n + a)$.*

Proof. Assume that a function g does not satisfy the hypothesis, i.e., there exist a tuple $(a_2, \ldots, a_n) \in E_k^{n-1}$ and a constant $a \neq 0$ such that $g(a_2, \ldots, a_n) = g(a_2 + a, \ldots, a_n + a)$. Show that in this case the mapping $\sigma(x) - x$ is not injective. Arbitrarily select the value of the variable x_1 and denote the selected value by a_1. Consider the tuples $\alpha = (a_1, \ldots, a_n)$ and $\alpha' = (a_1 + a, \ldots, a_n + a)$. If $1 \leqslant i \leqslant n - 1$, then the ith component of $\sigma(\alpha) - \alpha$ and $\sigma(\alpha') - \alpha'$ equals $a_{i+1} + c_i - a_i$. The nth component of $\sigma(\alpha) - \alpha$ equals $a_1 + g(a_2, \ldots, a_n) + c_n - a_n$. The nth component of $\sigma(\alpha') - \alpha'$ equals $a_1 + a + g(a_2 + a, \ldots, a_n + a) + c_n - a_n - a = a_1 + g(a_2, \ldots, a_n) + c_n - a_n + c_n$, thus injectivity is violated.

Conversely, assume that a function g satisfies the hypothesis. Assume that bijectivity of the mapping $\sigma(x) - x$ is violated. Since the set E_k^n is finite, it means that the mapping $\sigma(x) - x$ is not injective. Assume that $\alpha = (a_1, \ldots, a_n)$ and $\alpha' = (a'_1, \ldots, a'_n)$ are distinct tuples such that $\sigma(\alpha) - \alpha = \sigma(\alpha') - \alpha'$. Thus it holds that

$$\begin{aligned}
&a_2 + c_1 - a_1 = a'_2 + c_1 - a'_1 \\
&a_3 + c_2 - a_2 = a'_3 + c_2 - a'_2 \\
&\vdots \\
&a_n + c_{n-1} - a_{n-1} = a'_n + c_{n-1} - a'_{n-1} \\
&a_1 + g(a_2, \ldots, a_n) + c_n - a_n = a'_1 + g(a'_2, \ldots, a'_n) + c_n - a'_n.
\end{aligned} \tag{9}$$

Note that if $a_1 = a'_1$, then the first equality of the system (9) implies that $a_2 = a'_2$, the second equality implies that $a_3 = a'_3$, and so on. Hence the tuples are equal, which contradicts the assumption. Thus, $a_1 = a'_1 + a$ for some $a \in E_k$, $a \neq 0$. The first $n-1$ equalities of the system (9) yield the equalities $a_i = a'_i + a$, $i = 2, \dots, n$. Substitute these relations into the nth equality of (9):

$$a_1 + g(a_2, \dots, a_n) + c_n - a_n = a'_1 + a + g(a'_2 + a, \dots, a'_n + a) + c_n - a'_n - a = \\ a'_1 + g(a'_2 + a, \dots, a'_n + a) + c_n - a'_n = a'_1 + g(a'_2, \dots, a'_n) + c_n - a'_n.$$

As a result, we obtain the equality $g(a'_2 + a, \dots, a'_n + a) = g(a'_2, \dots, a'_n)$ which contradicts the assumption. □

Corollary 3.2. *A feedback shift register is a complete mapping if and only if any non-trivial shift changes the value of the function g, i.e., for any tuple $(a_2, \dots, a_n) \in E_k^{n-1}$ and any $a \in E_k$, $a \neq 0$, it holds that $g(a_2, \dots, a_n) \neq g(a_2 + a, \dots, a_n + a)$.*

Theorem 3.1 can be directly applied to the cases of PFN, type-1 PEFN (after renumbering) and type-4 PEFN. In the first two cases the function g is unary, so the condition on g in Theorem 3.1 is equivalent to bijectivity.

Corollary 3.3. *A mapping specified by PFN or by type-1 PEFN after renumbering is complete if and only if the function g is a bijection.*

Corollary 3.3 shows that sufficient completeness conditions established in [12] are actually necessary and sufficient.

If type-4 PEFN is rewritten as a generalized feedback shift register, then the function g takes the form $h(x_2 + \ldots + x_n)$, where h is a unary function. If h is not a bijection, i.e., some value $b \in E_k$ does not belong to the image of h, by Dirichlet box principle for any $(n-1)$-tuple $(a_2, \dots, a_n)$ the set $\{h(a_2 + a + \ldots + a_n + a) \mid a \in E_k\}$ contains equal elements. Now assume that h is a bijection. Then the hypothesis of Theorem 3.1 holds if the equality $x_2 + x_3 + \ldots + x_n = (x_2 + a) + (x_3 + a) + \ldots + (x_n + a)$ is satisfied only for $a = 0$, or, equivalently, the equation

$$\underbrace{a + a + \ldots + a}_{n-1} = 0 \tag{10}$$

has a unique solution $a = 0$. By Lagrange's theorem there are no non-zero solutions if and only if $n-1$ and k are coprime. In paricular, if G

is isomorphic to $\mathbb{Z}_2^m$ for some $m \in \mathbb{N}$, then the equation (10) has a unique solution $a = 0$ if and only if $n-1$ is odd and thus n is even. Thus the following assertion holds.

Corollary 3.4. *A mapping specified by type-4 PEFN is complete if and only if the function g is a bijection and $(n-1)$ and k are coprime.*

Corollary 3.4 extends sufficient conditions obtained in [13] for the case of elementary Abelian 2-groups to necessary and sufficient conditions for arbitrary Abelian groups.

PGF-NLFSR can be considered in a similar way after another model generalization (i.e., replacing x_1 in the last line of (5) with $s(x_1)$, $s \in P_k^1$; if s is not a bijection, then, by the cardinality argument, σ is also non-bijective, otherwise Theorem 3.1 and Corollary 3.4 hold for the generalized construction).

Generalized feedback shift registers that satisfy the hypothesis of Theorem 3.1 specify quasigroup operations of the form

$$\begin{aligned}
&z_1 = x_2 \pm y_2 + c_1 \mp y_1\\
&z_2 = x_3 \pm y_3 + c_2 \mp y_2\\
&\vdots\\
&z_{n-1} = x_n \pm y_n + c_{n-1} \mp y_{n-1}\\
&z_n = x_1 \pm y_1 + g(x_2 \pm y_2, \dots, x_n \pm y_n) + c_n \mp y_n.
\end{aligned} \tag{11}$$

It can be easily seen that changing the value of c_n can be compensated by shifting the value of the function g, thus without loss of generality one can assume that $c_n = 0$.

Remark 3.5. If $k = 2$, then the requirement imposed by Theorem 3.1 is equivalent to self-duality of the function g. Thus the construction (11) generates $2^{n-1} \cdot 2^{2^{n-2}}$ distinct quasigroup operations of the order 2^n.

If $k > 2$, then the requirement imposed on the function g can be written out in the following form. The set of input tuples is split into the union of equivalence classes with respect to shifts ($(a_2, \dots, a_n) \sim (a'_2, \dots, a'_n)$ if there exists a constant $a \in E_k$ such that $a_i = a'_i + a$, $i = 2, \dots, n$). Obviously the cardinality of any class equals k, so the number of classes is the number of $(n-1)$-tuples divided by k, i.e., k^{n-2}. Different inputs from the same class give different outputs, so inside a class the function g is a permutation. For any class one can select the permutation arbitrarily ($k!$ options), thus the number of distinct quasigroups generated is $k^{n-1} \cdot (k!)^{k^{n-2}}$.

The considerations presented above lead to the following procedure that allows uniform sampling of quasigroups generated by generalized feedback shift registers. In the Boolean case ($k = 2$) one just has to perform uniform independent selection of the values of the function g on all tuples with $x_2 = 0$ and to extend the function by self-duality. If $k \geqslant 3$, then it is sufficient to select independent uniformly distributed permutations (e.g., with the help of well-known Fisher–Yates shuffle, see [4, p. 26–27]) for all equivalence classes. Constants $c_1, \ldots, c_{n-1}$ are selected independently and uniformly from the set E_k. Obviously, in both cases all results are equiprobable.

Now show that quasigroups specified by the relations (11) can not be generated by proper families over the group G or by permutation construction applied to proper families over the group G. The first assertion follows from the fact that the first variable is dummy for the first function of a proper family, thus the identity

$$x_2 \pm y_2 + c_1 \mp y_1 = x_1 + y_1 + g_1(p_1(x_1, y_1), \ldots, p_n(x_n, y_n))$$

can not be satisfied for any proper family, since the left-hand side does not contain x_1, but the right-hand side does.

Prove the following assertion required to consider the case of permutation construction.

Lemma 3.6. *Let $(g_1, \ldots, g_n)$ be a proper family, $p_1, \ldots, p_n \in P_k^2$ be arbitrary functions and*

$$h_i(x_1, \ldots, x_n, y_1, \ldots, y_n) = g_i(p_1(x_1, y_1), \ldots, p_n(x_n, y_n)),\ i = 1, \ldots, n.$$

Then for any distinct $2n$-tuples $\alpha = (a_1, \ldots, a_n, b_1, \ldots, b_n)$ and $\alpha' = (a'_1, \ldots, a'_n, b'_1, \ldots, b'_n)$ from E_k^{2n} there exists an index j, $1 \leqslant j \leqslant n$, such that $(a_j, b_j) \neq (a'_j, b'_j)$, but $h_j(\alpha) = h_j(\alpha')$.

Proof. There are two possible cases. If $p_1(a_1, b_1) = p_1(a'_1, b'_1), \ldots, p_n(a_n, b_n) = p_n(a'_n, b'_n)$, then the assertion is trivial, since for any j such that $(a_j, b_j) \neq (a'_j, b'_j)$ it obviously holds that $h_j(\alpha) = h_j(\alpha')$.

Now, if $(p_1(a_1, b_1), \ldots, p_n(a_n, b_n))$ and $(p_1(a'_1, b'_1), \ldots, p_n(a'_n, b'_n))$ are distinct, then by definition of properness there exists an index j such that $p_j(a_j, b_j) \neq p_j(a'_j, b'_j)$ (and thus $(a_j, b_j) \neq (a'_j, b'_j)$) and $g_j(p_1(a_1, b_1), \ldots, p_n(a_n, b_n)) = g_j(p_1(a'_1, b'_1), \ldots, p_n(a'_n, b'_n))$. □

Theorem 3.7. *The classes of quasigroups generated by generalized feedback shift registers using relation* (1) *or* (2) *and by permutation construction applied to proper families over the group G are disjoint.*

Proof. We will conduct the proof for the case of the relation (1). The case of the relation (2) can be considered in a similar way. Assume that there exists a generalized feedback shift register that satisfies the hypothesis of Theorem 3.1, a proper family $(g_1, \ldots, g_n)$, functions $p_1, \ldots, p_n \in P_k^2$ and permutations β and γ (as it was noticed, without loss of generality one may assume that the permutation δ is identical) such that the corresponding quasigroup operations coincide, i.e. it holds that

$$x_{i+1} - y_{i+1} + c_i + y_i = x_{\beta(i)} + y_{\gamma(i)} + g_i(p_1(x_{\beta(1)}, y_{\gamma(1)}), \ldots, p_n(x_{\beta(n)}, y_{\gamma(n)})) \tag{12}$$

for $i = 1, \ldots, n-1$ and

$$\begin{aligned} x_1 - y_1 + g(x_2 - y_2, \ldots, x_n - y_n) + y_n &= \\ = x_{\beta(n)} + y_{\gamma(n)} + g_n(p_1(x_{\beta(1)}, y_{\gamma(1)}), &\ldots, p_n(x_{\beta(n)}, y_{\gamma(n)})). \end{aligned} \tag{13}$$

Since the ith variable is dummy for g_i, the identities (12) yield the equalities $\beta(i) = i + 1$, $\gamma(i) = i$, $i = 1, \ldots, n-1$. Since β and γ are permutations, $\beta(n) = 1$, $\gamma(n) = n$. Cancel equal terms on the left-hand and on the right-hand side of the identities (12), (13) and impose inverse permutations on variable indices to obtain the relations

$$\begin{aligned}
&g_1(p_1(x_1, y_1), \ldots, p_n(x_n, y_n)) = -y_2 + c_1 \\
&g_2(p_1(x_1, y_1), \ldots, p_n(x_n, y_n)) = -y_3 + c_2 \\
&\vdots \\
&g_{n-1}(p_1(x_1, y_1), \ldots, p_n(x_n, y_n)) = -y_n + c_{n-1} \\
&g_n(p_1(x_1, y_1), \ldots, p_n(x_n, y_n)) = -y_1 + g(x_1 - y_2, \ldots, x_{n-1} - y_n).
\end{aligned}$$

Substitute the values $x_1 = \ldots = x_n = y_1 = \ldots = y_n = 0$ and $x_1 = \ldots = x_n = y_1 = \ldots = y_n = 1$ in these relations. Note that the inputs of the function g for these substitutions coincide, and the subtracted values y_i are different. Thus there is no index j such that the values of g_j coincide for the substitutions considered, which contradicts Lemma 3.6. Thus the family $(g_1, \ldots, g_n)$ is not proper. □

4. Quasigroups and generalized Feistel networks

Theorem 4.8. *A generalized Feistel network specifies a complete mapping if and only if the mappings $s(x)$ and $s(x) + p(x) + x$ are bijective.*

Proof. First note that the relations (6) specify a permutation on E_k^2 if and only if s is a bijection. Indeed, if s is not bijective, then the cardinality of the image of a generalized Feistel network is less than the cardinality of the preimage. Conversely, if s is a bijection, then obviously the inverse of the transform (6) is the mapping $\left(f_1 = x_2 - p\left(s^{-1}(x_1)\right), f_2 = s^{-1}(x_1)\right)$. Further in the course of the proof we assume that s is a bijection.

Assume that $s(x) + p(x) - x$ is a bijection. Suppose that there exist pairs (x_1, x_2) and (y_1, y_2) such that

$$\begin{array}{l} s(x_2) - x_1 = s(y_2) - y_1 \\ x_1 + p(x_2) - x_2 = y_1 + p(y_2) - y_2 \end{array} \tag{14}$$

Sum these equalities up to obtain the relation

$$s(x_2) + p(x_2) - x_2 = s(y_2) + p(y_2) - y_2,$$

thus by the assumption $x_2 = y_2$ and so $s(x_2) = s(y_2)$. The latter equality and the first equality of (14) directly imply the relation $x_1 = y_1$. Hence the mapping is complete.

Conversely, assume that there exist $x_2 \neq y_2$ such that $s(x_2) + p(x_2) - x_2 = s(y_2) + p(y_2) - y_2$. Let $x_1 = s(x_2)$, $y_1 = s(y_2)$ and note that the pairs (x_1, x_2) and (y_1, y_2) satisfy the relations (14). Thus, the mapping is not complete. □

By Theorem 4.8 the number of quasigroups specified by generalized Feistel networks via the relation (1) or (2) equals $(k!)^2$. Indeed, $s(x)$ and $s'(x) = s(x) + p(x) - x$ can be set equal to arbitrary permutations on E_k, and the function p can be easily recovered from s and s'. Uniform and independent selection of the permutations allows one to perform uniform sampling on the set of quasigroups generated.

Generalized Feistel networks specify quasigroup operations

$$\begin{array}{l} f_1 = s(x_2 \mp y_2) \pm y_1 \\ f_2 = x_1 \mp y_1 + p(x_2 \mp y_2) \pm y_2 \end{array}$$

It can be easily shown that these operations can not be generated by proper families over the group G or by permutation construction applied to proper families over G. Indeed, any transformation of the functions f_1, f_2 to the form $x_i + y_j + g(p(x_{i'}, y_{j'}))$ is such that the third summand is not constant. On the other hand, all proper families of the size 2 must contain a constant function [6, Assertion 1].

5. Conclusion

We considered complete mappings specified by generalized feedback registers and generalized Feistel networks. In both cases, criteria for the mapping completeness have been established. A procedure for uniform sampling of quasigroups induced by complete mappings under study has been suggested. The classes of quasigroups generated by generalized feedback shift registers or generalized Feistel networks and by the permutation construction applied to proper families over the group G are shown to be disjoint.

6. Acknowledgments.

The research has been supported by the Interdisciplinary Scientific and Educational School of Moscow University "Brain, Cognitive Systems, Artificial Intelligence".

The authors thank the reviewer for correcting inaccuracies and useful remarks that contributed to the improvement of the presentation of the material.

The authors started this research in the framework of the Indo-Russian joint project "Quasigroup based cryptography: security, analysis and development of crypto-primitives and algorithms (QGSEC)" headed by V. A. Artamonov.

References

[1] **P.J. Cameron**, *Almost all quasigroups have rank* 2, Discrete Math. **106–107** (1992), 111 – 115.

[2] **I.V. Cherednik**, *Using binary operations to construct a transitive set of block transformations*, Discrete Math. Appl. **30** (2020), no. 6, 375 – 389.

[3] **I.V. Cherednik**, *On the use of binary operations for the construction of a multiply transitive class of block transformations*, Discrete Math. Appl. **31** (2021), no. 2, 91 – 111.

[4] **R.A. Fisher, F. Yates**, *Statistical tables for biological, agricultural and medical research*, London: Oliver & Boyd, 1948.

[5] **A.V. Galatenko, V.V. Galatenko, A.E. Pankratiev**, *Strong polynomial completeness of almost all quasigroups*, Math. Notes **111** (2022), no. 1, 7 – 12.

[6] **A.V. Galatenko, V.A. Nosov, A.E. Pankratiev**, *Latin squares over quasigroups*, Lobachevskii J. Math. **41** (2020), no. 2, 194 – 203.

[7] **D. Gligoroski, H. Mihajloska, D. Otte, M. El-Hadedy**, *GAGE and InGAGE*, `http://gageingage.org/upload/GAGEandInGAGEv1.03.pdf`

[8] **D. Gligoroski, R.S. Ødegărd, M. Mihova, S.J. Knapskog, A. Drapal, V. Klíma, J. Amundse, M. El-Hadedy**, *Cryptographic hash function EDON-R′*, Proceedings of the 1st International Workshop on Security and Communication Networks, IWSCN (2009), 1 – 9.

[9] **M. M. Glukhov**, *Some applications of quasigroups in cryptography*, Prikl. Diskr. Mat. (2008), no. 2(2), 28 – 32.

[10] **S. Markovski, A. Mileva**, *NaSHA — family of cryptographic hash functions*, The First SHA-3 Candidate Conference, Leuven, 2009.

[11] **S. Markovski, A. Mileva**, *Generating huge quasigroups from small non-linear bijections via extended Feistel function*, Quasigroups Related Systems **17** (2009), 91 – 106.

[12] **A. Mileva, S. Markovski**, *Shapeless quasigroups derived by Feistel orthomorphisms*, Glasnik Matematicki **47** (2012), no. 2, 333 – 349.

[13] **A. Mileva, S. Markovski**, *Quasigroup representation of some Feistel and Generalized Feistel ciphers*, Advances in Intelligent Systems and Computing — ICT Innovations 2012, **207**, Springer (2013), 161 – 171.

[14] **V.A. Nosov, A.E. Pankratiev**, *Latin squares over Abelian groups*, J. Math. Sci. **149** (2008), no. 3, 1230 – 1234.

[15] **N.A. Piven**, *Investigation of quasigroups generated by proper families of Boolean functions of order 2*, Intell. Syst. Theory Appl. **22** (2018), no. 1, 21 – 35.

[16] **N.A. Piven**, *Some properties of the permutation construction for parametric quasigroup specification*, Intell. Syst. Theory Appl. **23** (2019), no. 2, 71 – 78.

[17] **A. Sade**, *Quasigroups automorphes par le groupe cyclique*, Canadian J. Math. **9** (1957), 321 – 335.

[18] **V. A. Shcherbacov**, *Quasigroups in cryptology*, Comput. Sci. J. Mold. **17** (2009), no. 2(50), 193 – 228.

Received February 07, 2023

S. Chakrabarti*, S.K Tiwari
Scientific Analysis Group, DRDO, Delhi, India (* Former)
* Visiting Scientist (Honorary), Indian Statistical Institute, Kolkata, India
E-mail: suchetadrdo@hotmail.com, shrawant@gmail.com

A.V. Galatenko, V.A. Nosov, A.E. Pankratiev
Faculty of Mechanics and Mathematics, Lomonosov Moscow State University
Main Building, GSP-1, 1 Leninskiye Gory, Moscow, Russia
E-mail: agalat@msu.ru, vnosov40@mail.ru, apankrat@intsys.msu.ru