Quasigroups and Related Systems **32** (2024), 207 – 223

https://doi.org/10.56415/qrs.v32.16

Polynomial completeness and completeness of finite n-quasigroups

Svetlana S. Chaplygina and Alexy V. Galatenko

Abstract. Finite quasigroups and n-quasigroups are currently extensively utilized to implement various cryptographic functions. Cryptographic requirements lead to constraints imposed on quasigroups and n-quasigroups. In particular, V. A. Artamonov proposed using polynomially complete quasigroups. Polynomial completeness can be decided with the help of a criterion of J. Hagemann and C. Herrmann: a quasigroup is polynomially complete if and only if it is simple and non-affine. In our paper we generalize this result to the case of n-quasigroups and give a proof based on I. G. Rosenberg's description of maximal classes in k-valued logics. We also obtain a completeness criterion and show that completeness is a cryptographically reasonable requirement.

1. Introduction

Finite quasigroups are currently extensively used to implement various cryptographic functions. C. Shannon proved that the quasigroup-based tabular substitution cipher has the property of perfect secrecy, i.e., is theoretically unbreakable [24]. Quasigroup-based ciphers and hash functions regularly take part in NIST contests (e.g., hash functions NaSHA [22] and EDON-R′ [16] participated in SHA-3 contest, and hash function GAGE and authenticated encryption InGAGE [15] participated in Lightweight Cryptography contest). A wide spectrum of quasigroup-based cryptographic functions can be found in surveys [17, 25].

There is also an emerging interest in cryptographic applications of quasigroup analogues of greater arity. In particular, there is a number of research papers on ciphers based on 3-quasigroups (see, e.g., [5, 9, 26]).

2010 Mathematics Subject Classification: 20N05, 20N15

Keywords: quasigroup, n-quasigroup, k-valued logics, polynomial completeness, maximal class, completeness, affinity, simplicity.

There exist various constraints imposed on quasigroups in order to enhance cryptographic strength. V. A. Artamonov, S. Chakrabarti, S. Gangopadhyay and S. K. Pal in [1] proposed using polynomially complete quasigroups, i.e., quasigroups such that the quasigroup operation and all constants generate all operations via superposition. Polynomially complete quasigroups are beneficial in cryptographic applications due to the fact that deciding solvability of equations over polynomially complete algebras is NP-complete [19]. Later V. A. Artamonov, S. Chakrabarti, Sh. K. Tiwari and V. T. Markov additionally demanded the absence of proper subquasigroups [3]. D. Gligoroski, S. Markovski and L. Kocarev proposed using shapeless quasigroups, i.e., quasigroups that are non-idempotent, non-commutative, non-associative, do not have left or right unit, do not contain proper subquasigroups, and do not admit certain identities [14]. One more interesting (however not strictly defined) requirement is being non-fractal [8].

It is known that a quasigroup is polynomially complete if and only if it is simple and non-affine [18]. We investigate polynomial completeness from another perspective. We obtain a similar result for the case of n-quasigroups in terms of maximal classes of k-valued logics. We also consider a stronger property of completeness of n-quasigroups (an n-quasigroup is said to be complete if its operation generates all possible operations via superposition) and obtain a completeness criteria in terms of k-valued logics and from algebraic perspective. It turns out that completeness incorporates additional cryptographically beneficial properties in comparison with polynomial completeness.

The rest of the paper is organized as follows. In Section 2 we introduce basic concepts and provide required definitions. Section 3 is devoted to the investigation of the relationship between maximal classes of k-valued logics and n-quasigroup operations. In Section 4 we formulate the main lemmas obtained as corollaries of results from Section 3. Section 5 is a conclusion.

2. Basic concepts and definitions

First give a number of definitions related to n-quasigroups.

Definition 2.1. Let $n \in \mathbb{N}, n \geqslant 2$. A *finite n-quasigroup* (Q, f) is defined as a set $Q = \{q_1, \ldots, q_k\}$ endowed with an n-ary operation $f\colon Q^n \to Q$

ssuch that for any i, $1 \leqslant i \leqslant n$, and any $a_1, \ldots, a_n, b \in Q$ the equation

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

is uniquely solvable.

Denote the set $\{0, \ldots, k-1\}$ by E_k. Without loss of generality one can assume that $Q = E_k$. Thus n-quasigroup operations can be considered as functions of k-valued logics. The case $k = 2$ is trivial, since for any n there are exactly two n-quasigroups of the order 2, so we assume that $k \geqslant 3$.

Hereinafter for the sake of brevity finite n-quasigroups will be referred to simply as quasigroups.

Definition 2.2. A *proper subquasigroup* (Q', f') of a quasigroup (Q, f) is defined as a set Q' with operation f', where Q' is a proper subset of Q closed with respect to the quasigroup operation f, and the operation f' is the restriction of f to Q'.

Definition 2.3. Two quasigroups (Q, f_1) and (Q, f_2) are *isotopic* if there exist permutations $\alpha, \alpha_1, \ldots, \alpha_n$ of the set Q such that

$$f_1(x_1, \ldots, x_n) \equiv \alpha^{-1}\left(f_2(\alpha_1(x_1), \ldots, \alpha_n(x_n))\right).$$

In this case the tuple $(\alpha, \alpha_1, \ldots, \alpha_n)$ is referred to as isotopy. If all permutations are equal, then isotopy is an isomorphism. On the other hand, if $f_1 = f_2$, then isotopy is called autotopy, and isomorphism is called automorphism.

Definition 2.4. A quasigroup is called *affine* if there exists an Abelian group $(Q, +)$, automorphisms $\alpha_1, \ldots, \alpha_n$ of this group and a constant $c \in Q$ such that the following identity holds:

$$f(x_1, \ldots, x_n) \equiv \alpha_1(x_1) + \ldots + \alpha_n(x_n) + c.$$

Definition 2.5. A quasigroup is called *simple* if it admits only trivial congruences.

Now let us introduce notation and definitions related to k-valued logics. Denote the set of all k-valued functions in m variables by P_k^m. Accordingly, P_k denotes the set of k-valued functions of any arity.

Definition 2.6. The *closure* $[A]$ of a set of functions $A \subseteq P_k$ is the set of all functions from P_k that can be obtained from functions of the set A using superposition operations, i.e. permutation of variables, identification of variables, adding or removing dummy (inessential) variables and substitution of a variable of a function with a function.

Detailed discussion of superposition and closure in k-valued logics can be found, e.g., in the monograph [21].

Definition 2.7. A set $A \subseteq P_k$ satisfying $[A] = A$ is said to be *closed*.

Definition 2.8. A quasigroup (Q, f) is is *polynomially complete* if $\left[\{f\} \cup P_k^0\right] = P_k$, where P_k^0 is the set of all constants.

Definition 2.9. A quasigroup (Q, f) is *complete* if $[\{f\}] = P_k$.

Completeness of an arbitrary set $A \subseteq P_k$ is defined in a similar way.

One of the ways to study completeness was given in the work of I. Rosenberg [23]. The method is based on determining the maximal classes of functions.

Definition 2.10. A set $A \subsetneq P_k$ is called a *maximal class* if $[A] \neq P_k$ and for any $f \in P_k \setminus A$ it holds that $[A \cup \{f\}] = P_k$.

In other words, a maximal class is an incomplete set of functions such that adding an arbitrary function not belonging to this set makes the set complete. It can be easily noticed that any maximal class is closed. Moreover, in k-valued logics the number of maximal classes is finite, and a system is complete if and only if it is not contained in any maximal class (see, e.g., [21, Part II, Theorem 11.1.1, Theorem 1.5.3.1]). I. Rosenberg in [23] gave a description of all maximal classes in P_k. Below we recall this description in accordance with the monograph [21] by D. Lau. In the current section we give necessary definitions, in the following section we list the classes and investigate the relationship between quasigroups and these classes.

Definition 2.11. An *h-ary relation* ρ on E_k is a subset of the Cartesian product $E_k \times \ldots \times E_k = E_k^h, h \in \mathbb{N}$.

The elements $(a_1, a_2, \ldots, a_h) \in \rho$ can be considered as column vectors:

$$\begin{pmatrix} a_1 \\ a_2 \\ \ldots \\ a_h \end{pmatrix} = (a_1, \ldots, a_h)^T \in \rho$$

The set of all h-ary relations on E_k is denoted by R_k^h.

It is convenient to talk about maximal classes using relations and functions that preserve relations.

Definition 2.12. A function $f \in P_k^m$ *preserves* an h-ary relation $\rho \in R_k^h$ if

$$f\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ a_{21} & a_{22} & \dots & a_{2m} \\ \dots & \dots & \dots & \dots \\ a_{h1} & a_{h2} & \dots & a_{hm} \end{pmatrix} \stackrel{\text{def}}{=} \begin{pmatrix} f(a_{11}, a_{12}, \dots, a_{1m}) \\ f(a_{21}, a_{22}, \dots, a_{2m}) \\ \dots \\ f(a_{h1}, a_{h2}, \dots, a_{hm}) \end{pmatrix} \in \rho$$

for all

$$\begin{pmatrix} a_{11} \\ a_{21} \\ \dots \\ a_{h1} \end{pmatrix}, \begin{pmatrix} a_{12} \\ a_{22} \\ \dots \\ a_{h2} \end{pmatrix}, \dots, \begin{pmatrix} a_{1m} \\ a_{2m} \\ \dots \\ a_{hm} \end{pmatrix} \in \rho$$

In other words, we select m arbitrary column vectors from the relation ρ, write them in a matrix, apply the function f to each row of this matrix and obtain a column vector that also belongs to ρ. The set of all functions preserving ρ is denoted by $\mathrm{Pol}(\rho)$. It is known (see, e.g., [21, Part II, Theorem 2.6.2]) that $\mathrm{Pol}(\rho)$ is a closed class.

In Rosenberg's paper [23] it was shown that all maximal classes in P_k can be described using several classes of relations:

$$\{\mathrm{Pol}(\rho) \mid \rho \in \mathfrak{U}_k \cup \mathfrak{M}_k \cup \mathfrak{S}_k \cup \mathfrak{L}_k \cup \mathfrak{C}_k \cup \mathfrak{B}_k\}.$$

In other words, each maximal class is the class of functions that preserve a relation belonging to one of six finite families. Description of these classes of relations is presented in the subsequent section.

3. Maximal classes and quasigroups

In this section we give an overview of maximal classes in k-valued logics and investigate the relationship between these classes and quasigroups.

3.1. Classes of monotone functions

Informally maximal classes specified by relations from $\mathfrak{M}_k$ are comprised of functions preserving a partial order on E_k with a greatest and a least element. A more formal definition is presented below.

Definition 3.1. A binary relation ρ is called *monotone* (written as $\rho \in \mathfrak{M}_k$) if it reflexive, antisymmetric, transitive and $\exists o_\rho, e_\rho \colon \{(o_\rho, x)^T, (x, e_\rho)^T \mid x \in E_k\} \subseteq \rho$.

In other words, a monotone relation defines a partial order admitting the least and the greatest element on E_k. We say that a tuple $\bar{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_m)$ is greater or equal to a tuple $\bar{\beta} = (\beta_1, \beta_2, \ldots, \beta_m)$ if $(\alpha_i, \beta_i) \in \rho$ (i.e., $\alpha_i \geqslant \beta_i$) for $i = 1, \ldots, m$. By definition a function preserves a monotone relation if for any tuples $\bar{\alpha}, \bar{\beta}$, $\bar{\alpha} \geqslant \bar{\beta}$, it holds that $f(\bar{\alpha}) \geqslant f(\bar{\beta})$.

Lemma 3.2. *Suppose that (E_k, f) is a quasigroup. Then the function f preserves no monotone relation $\rho \in \mathfrak{M}_k$.*

Proof. Assume that there exists some $\rho \in \mathfrak{M}_k$ preserved by the quasigroup operation f. Denote the greatest element with respect to ρ by a_{max}.

Let $\alpha = (a_1, \ldots, a_n) \in E_k^n$ be a tuple such that at least one component is less than a_{max} and $f(a_1, \ldots, a_n) = a_{max}$. Such a tuple obviously exists by Definition 2.1. Replace the non-maximum component with a_{max} to obtain the tuple α'. By definition the value of the quasigroup operation on α' is distinct from $a_{max} = f(\alpha)$, thus it is less than a_{max} with respect to ρ, however α' is greater than α. The contradiction obtained completes the proof. □

3.2. Classes of autodual functions

Denote by $\mathfrak{S}_k$ the set of all relations ρ_s of the form

$$\rho_s = \{(x, s(x))^T \mid x \in E_k\},$$

where $s \in S_k$ is a permutation with k/p cycles of the same prime length p.

Definition 3.3. A function $f \in P_k^m$ is called *autodual* if it preserves at least one relation $\rho_s \in \mathfrak{S}_k$, i.e.,

$$f(s(x_1), s(x_2), \ldots, s(x_m)) = s(f(x_1, x_2, \ldots, x_m)).$$

Lemma 3.4. *For any non-trivial permutation s on E_k there exists a constant function that does not preserve ρ_s.*

Proof. Since the permutation s is non-trivial, there exists an element $c \in E_k$ that does not preserve its position. Thus the constant function $f(x) \equiv c$ does not preserve the relation s:

$$f\begin{pmatrix} c \\ s(c) \end{pmatrix} = \begin{pmatrix} c \\ c \end{pmatrix} \notin \rho_s. \qquad \square$$

Remark 3.5. A quasigroup operation can be autodual. Consider the quasigroup operation from P_3^2 defined by the equality

$$f(x,y) = 2x + 2y + 2 \pmod 3$$

and the permutation $s(x) = x + 1 (\mathrm{mod}\, 3)$. The inverse permutation is $x - 1 \pmod 3$. Since

$$s^{-1}(f(s(x), s(y))) = 2(x+1) + 2(y+1) + 2 - 1 \equiv 2x + 2y + 2 \pmod 3,$$

the function f preserves the relation ρ_s and thus is autodual.

Remark 3.6. Definition 3.3 directly implies the following fact. Consider a quasigroup (Q, f). The function f is autodual only if the quasigroup admits a non-trivial automorphism. Thus autoduality looks undesirable from cryptographic perspective, since in this case the quasigroup (Q, f) has some "internal structure", or, in terms of the paper [14], some "shape".

Remark 3.7. In the case of $n = 2$ almost all quasigroups have a trivial automorphism group (see, e.g., [7]). To the best of our knowledge the situation in the case $n \geqslant 3$ is still to be investigated.

3.3. Classes of functions which preserve central relations

Definition 3.8. A relation ρ of the arity h belongs to the class $\mathfrak{C}_k^h$ if:

1. ρ is *totally reflexive* and non-trivial, i.e., $\rho \neq E_k^h$ and

   $$(\exists i \neq j \quad a_i = a_j) \quad \Rightarrow \quad (a_1, \ldots, a_h)^T \in \rho$$

   (in other words, ρ is non-trivial, and if the elements of an h-tuple are not distinct, then this tuple belongs to ρ);

2. ρ is *totally symmetric*, i.e., for any permutation s of the set $\{1, \ldots, h\}$ it holds that

   $$(a_1, \ldots, a_h)^T \in \rho \quad \Rightarrow \quad (a_{s(1)}, \ldots, a_{s(h)})^T \in \rho;$$

3. there exists at least one central element $c \in E_k$, i.e.,

   $$\forall a_1, \ldots, a_{h-1} \in E_k \colon (a_1, \ldots, a_{h-1}, c)^T \in \rho$$

   (in other words, taking into account the second property, if an h-tuple contains a component equal to a central element then this tuple belongs to ρ).

Let $\mathfrak{C}_k = \cup_{h=1}^{k-1} \mathfrak{C}_k^h$ be the set of all central relations on E_k.

Lemma 3.9. *No quasigroup preserves a central relation of the arity greater than* 1.

Proof. Assume that a relation $\rho \in \mathfrak{C}_k^h$, $h \geqslant 2$, is preserved by a quasigroup operation f. Since ρ is non-trivial by definition, there exists an h-tuple $(a_1, \ldots, a_h)^T \notin \rho$. Let $c \in E_k$ be central.

Since f is a quasigroup operation, for any elements $a_1 \in E_k$ there exists a fixation of the variables $x_2 = b_2, \ldots, x_n = b_n$ such that $f(c, b_2, \ldots, b_n) = a_1$. Similarly, select $b_1^{(2)}, \ldots, b_1^{(h)}$ such that $f\left(b_1^{(i)}, c, \ldots, c\right) = a_i$.

Consider column vectors $(c, b_2, \ldots, b_n)^T$ and $(b_1^{(i)}, c, \ldots, c)^T$, $i = 2, \ldots, h$. Since each vector contains a central element, these vectors belong to ρ. If we apply the function f to each row of the matrix comprised by the vectors, we will obtain the column $(a_1, \ldots, a_h)^T$ that does not belong to ρ:

$$\left|\begin{array}{cccc|c} c & b_2 & \ldots & b_n & a_1 \\ b_1^{(2)} & c & \ldots & c & a_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ b_1^{(h)} & c & \ldots & c & a_h \end{array}\right|$$

Thus the relation ρ is not preserved by f by definition. □

Remark 3.10. No unary central relation is preserved by the set of all constants. It is sufficient to consider a non-central constant as a function from P_k^0 to prove this fact.

Lemma 3.11. *A quasigroup has a proper subquasigroup if and only if its operation preserves a central relation of the arity* 1.

Proof. ($\Rightarrow$) By definition the quasigroup operation preserves the central relation consisting of elements of a subquasigroup.

($\Leftarrow$) Consider a central relation ρ of the arity 1. Suppose that ρ is specified by central elements $a_1, \ldots, a_s$, $s < k$. Then by Definition 2.12 for any n-tuple α of central elements it holds that $f(\alpha)$ is also a central element, so the set of all central elements comprises a proper subquasigroup. □

Note that the presence of a proper subquasigroup makes the quasigroup non-shapeless. This property is also considered as undesirable by Artamonov et al.

Remark 3.12. The presence of a subquasigroup in an n-quasigroup of the order k with tabular operation specification can be decided with the complexity $O\left(k^{\frac{n^2+n+1}{n+1}}(\log k)^{\frac{n}{n+1}}\right)$ for fixed n and $k \to \infty$ [12]. A more efficient procedure with the complexity $O\left(k^{7/3}\right)$ for the case $n = 2$ was announced in [11], but the construction and the proof are currently not published.

Remark 3.13. In the case $n = 2$ the presence of a proper subquasigroup is a "frequent" property. I. V. Cherednik showed that the fraction of 2-quasigroups with proper subquasigroups is asymptotically greater than $1/2$ [6]. To the best of our knowledge, this result is still unpublished, and the problem for $n > 2$ is still uninvestigated.

3.4. Classes of functions which preserve h-universal relations

Suppose that $m, h \in \mathbb{N}$, $h \geqslant 3$. Consider some relation $\xi_m^h \subseteq E_{h^m}^h$. Note that the elements of E_{h^m} can be naturally decomposed into powers of h, i.e., treated as numbers in the numeric system base h:

$$a \in E_{h^m} \qquad a = a^{(0)} + a^{(1)} \cdot h + a^{(2)} \cdot h^2 + \ldots + a^{(m-1)} \cdot h^{m-1},$$

where $a^{(i)}$ denote the "digits" of this number.

Let us introduce the following relation:

$$\iota_k^h := \{(a_0, \ldots, a_{h-1}) \in E_k^h \mid \exists i, j \in E_k \colon i \neq j \wedge a_i = a_j\}$$

In other words, the criterion for belonging to this relation is the presence of at least two identical elements a_i, a_j $i \neq j$.

Definition 3.14. A relation $\xi_m^h \subseteq E_{h^m}^h$ is called *h-ary elementary*, if it holds that

$$(a_0, \ldots, a_{h-1}) \in \xi_m^h \Leftrightarrow \forall i \in E_m \colon (a_0^{(i)}, \ldots, a_{h-1}^{(i)}) \in \iota_h^h$$

This means that among the elements $a_0, \ldots, a_{h-1}$ for any position i there are at least two elements with the same "digit" in that position.

Definition 3.15. A relation $\rho \subseteq E_k^h$ is called a *homomorphic inverse image* of a relation $\rho' \subseteq E_{k'}$ if there exists a surjective mapping q from E_k onto $E_{k'}$ such that $(a_1, \ldots, a_j) \in \rho \Leftrightarrow (q(a_1), \ldots, q(a_h)) \in \rho'$.

The set of h-universal relations $\mathfrak{B}_k$ is defined as follows.

Definition 3.16. *Let $\mathfrak{B}_k^h$ be the set of all homomorphic inverse images of the h-ary elementary relation ξ_m^h, $3 \leqslant h \leqslant k$, $m \geqslant 1$, $h^m \leqslant k$. Then $\mathfrak{B}_k = \bigcup_{h=3}^{k} \mathfrak{B}_k^h$ is the set of h-universal relations.*

D. Lau [21] obtained the following equivalent definition for functions preserving an h-universal relation.

Let q be a surjective mapping from E_k onto E_{h^m}. This mapping defines a partition on E_k in the blocks

$$\mathfrak{A}_i = \{x \in E_k : q(x) = i\}, \quad i \in E_{h^m}.$$

Next, in each block we select a representative a_i. Consider the functions $r\colon E_{h^m} \to E_k$, $g_f\colon E_k^n \to E_k$ specified by the equalities

$$r(i) = a_i, \qquad g_f(x_1, \ldots, x_n) = a_i \Leftrightarrow f(x_1, \ldots, x_n) \in \mathfrak{A}_i.$$

Note that since $g_f = r(q(f))$, it holds that

$$g_f(x_1, \ldots, x_n) = r(f'_{m-1}(x_1, \ldots, x_n) \cdot h^{m-1} + \ldots + f'_0(x_1, \ldots, x_n)), \quad (1)$$

where $f'_i(x_1, \ldots, x_n) = (q(f(x_1, \ldots, x_n)))^{(i)}$.

Since the expression can be understood in terms of "the numeric system base h", f'_i are referred to as "digits" of the representation.

Theorem 3.17 ([21, Part II, Theorem 5.2.6.1])**.** *Let ρ be a homomorphic inverse image of an h-ary elementary relation ξ_m^h. An n-ary function $f \in P_k$ belongs to the class which preserves ρ if and only if for the function g_f it holds that*

$$\forall i \in \{0, \ldots, m-1\}\colon \quad \begin{cases} \textit{either } |\operatorname{Im}(f'_i)| \leqslant h-1, \\ \textit{or} \\ \exists j \in \{1, \ldots, n\}, v \in E_m, s \in S_h\colon \\ \quad f'_i(x_1, \ldots, x_n) = s\left((q(x_j))^{(v)}\right). \end{cases}$$

This theorem asserts that each "digit" of the h-ary representation of g_f satisfies at least one of the following conditions: the image of the "digit" is incomplete or it is a function in one variable.

Lemma 3.18. *A quasigroup operation preserves no h-universal relations.*

Proof. Let (Q, f) be a quasigroup. Prove that, in the notation of the previous theorem, all functions f'_i are surjective, i.e., $|\operatorname{Im}(f'_i)| = h$ for $i = 0, \ldots, m-1$.

Indeed, since q is surjective, for any $y \in E_{h^m}$ there exists $a \in E_k$ such that $q(a) = y$. The function representing the quasigroup operation takes all values, i.e., for any $a \in E_k$ there exist $a_1, \ldots, a_n \in E_k$ such that $f(a_1, \ldots, a_n) = a$. Hence $q(f(x_1, x_2, \ldots, x_n))$ takes all h^m values. Also note that by Definition 2.1 it is sufficient to vary only one argument to iterate over all values. Hence, since $g_f = r(q(f))$, according to the representation (1), each function f'_i must also take all h possible values. This means that the first case does not hold.

It remains to prove the impossibility of the second condition of Theorem 3.17. Assume the opposite, i.e., $f'_i = s_i((q(x_{j_i}))^{(v_i)})$ for $i = 0, \ldots, m-1$. Let x_t be the variable of the function f'_0. Consider another index $t' \neq t$ and vary the variable $x_{t'}$. According to the above, g_f should range over all possible h^m values. But according to (1), the digit in the last position (that is f'_0), cannot change, so g_f takes at most h^{m-1} values. The contradiction obtained completes the proof. □

3.5. Classes of functions which preserve equivalence relations

Denote by $\mathfrak{U}_k$ the set of all non-trivial equivalence relations.

It can be easily seen that preserving a non-trivial equivalence relation is equivalent to having a non-trivial congruence. Thus the function f of a non-simple quasigroup (E_k, f) belongs to a maximal class specified by a relation from $\mathfrak{U}_k$, and vise versa.

Remark 3.19. For the case $n = 2$ it is known that simplicity is a typical quasigroup property, namely, almost all 2-quasigroups are not isotopic to non-simple quasigroups (see [10, Lemma 1]). To the best of our knowledge, the case $n > 2$ is unexplored.

Remark 3.20. The paper [12] proposes an algorithm for deciding simplicity of an n-quasigroup of the order k with the complexity $O\left(k^{n+1}\right)$ for fixed n and $k \to \infty$.

3.6. Classes of quasi-linear functions

Suppose that $k = p^m$, where p is prime, $m \in \mathbb{N}$, $G = (E_k, \oplus)$ is an elementary p-group. Consider the following relation λ_G of the arity 4:

$$\lambda_G := \{(a, b, c, d)^T \in E_k^4 \mid a \oplus b = c \oplus d\}.$$

The set of all such relations is denoted by $\mathfrak{L}_k$.

Definition 3.21. A function is quasi-linear if it preserves a relation $\rho \in \mathfrak{L}_k$.

According to [21, Part II, Lemma 5.2.4.1], quasi-linear functions can be equivalently defined in two other ways. First, one can endow the group G with multiplication $\odot$ so that $(E_k, \oplus, \odot)$ is a field. Any function from P_k can be uniquely specified by its algebraic normal form (ANF), i.e., a polynomial over this field of the form

$$f(x_1, \ldots, x_n) = \bigoplus_{i_1, \ldots, i_n \in E_k^n} a_{i_1 i_2 \ldots i_n} x_1^{i_1} \odot x_2^{i_2} \odot \ldots \odot x_n^{i_n},$$

where $a_{i_1 i_2 \ldots i_m} \in E_k$, x^0 is the neutral element with respect to $\odot$ (see, e.g., [21, Part II, Theorem 1.4.3]). A function is quasi-linear if and only if its ANF has the form

$$f(x_1, \ldots, x_n) = a_0 \oplus \bigoplus_{i=1}^{n} \bigoplus_{j=1}^{m-1} a_{ij} \odot x_i^{p^j}.$$

Second, a function f is quasi-linear if and only the following identity holds:

$$f(x_1 \oplus y_1, \ldots, x_n \oplus y_n) + f(o, \ldots, o) = f(x_1, \ldots, x_n) \oplus f(y_1, \ldots, y_n), \quad (2)$$

where o is the neutral element with respect to $\oplus$.

Note that for any j, $1 \leqslant j \leqslant m-1$, the function x^{p^j} is an automorphism of the group G. Thus if (Q, f) is a quasigroup and f is quasi-linear, then the quasigroup is affine. For the case $n = 2$ this fact was noticed by V. L. Yugay in [27].

The definition of a quasi-linear function in terms of relation preserving can be extended to the case of arbitrary values of k and arbitrary group G; however the classes specified by relations from the extension will not be

maximal. Assume that $G' = (E_k, +)$ is an Abelian group, $\lambda_{G'}$ is the relation of the arity 4 specified by the relation

$$\lambda_{G'} := \{(a, b, c, d)^T \in E_k^4 \mid a + b = c + d\}.$$

A function preserving $\lambda_{G'}$ will be referred to as weakly quasi-linear. It can be easily seen that a function is weakly quasi-linear if and only if it satisfies the identity (2) for the operation $+$. The proof literally repeats the proof of the second equivalence in [21, Part II, Lemma 5.2.4.1]. Use this fact to establish the following.

Lemma 3.22. *A quasigroup (E_k, f) is affine if and only if the function f is weakly quasi-linear.*

Poof. Suppose that $G' = (E_k, +)$ is an Abelian group, $\alpha_1, \ldots, \alpha_n \in \mathrm{Aut}(G')$, $c \in E_k$, $f(x_1, \ldots, x_n) \equiv \alpha_1(x_1) + \ldots + \alpha_n(x_n) + c$. Then for any tuples $(u_1, \ldots, u_n)$, $(x_1, \ldots, x_n)$, $(y_1, \ldots, y_n)$, $(z_1, \ldots, z_n)$ such that $u_i + x_i = y_i + z_i$, $i = 1, \ldots, n$, it holds that

$$\begin{aligned}
&f(u_1, ..., u_n) + f(x_1, ..., x_n) = \alpha_1(u_1) + ... + \alpha_n(u_n) + c + \alpha_1(x_1) + ... + \alpha_n(x_n) + c \\
&= \alpha_1(u_1 + x_1) + ... + \alpha_n(u_n + x_n) + c + c = \alpha_1(y_1 + z_1) + ... + \alpha_n(y_n + z_n) + c + c \\
&= \alpha_1(y_1) + ... + \alpha_n(y_n) + c + \alpha_1(z_1) + ... + \alpha_n(z_n) + c = f(y_1, ..., y_n) + f(z_1, ..., z_n),
\end{aligned}$$

so f is weakly quasi-linear.

Conversely, assume that f is weakly quasi-linear with respect to an Abelian group $G' = (E_k, +)$. Let $c = f(o, \ldots, o)$. For $i = 1, \ldots, n$ select $a_1^i, \ldots, a_n^i \in E_k$ so that $f(a_1^i, \ldots, a_{i-1}^i, o, a_{i+1}^i, \ldots, a_n^i) = o$ (such values exist by definition of a quasigroup) and set $\alpha_i(x) = f(a_1^i, \ldots, a_{i-1}^i, x, a_{i+1}^i, \ldots, a_n^i)$. Consider the tuples $(a_1^i, ..., a_{i-1}^i, x, a_{i+1}^i, ..., a_n^i)$, $(a_1^i, ..., a_{i-1}^i, y, a_{i+1}^i, ..., a_n^i)$, $(a_1^i, ..., a_{i-1}^i, x + y, a_{i+1}^i, ..., a_n^i)$ and $(a_1^i, ..., a_{i-1}^i, o, a_{i+1}^i, \ldots, a_n^i)$. Note that componentwise sums of the first two tuples and the last two tuples coincide. Thus

$$\begin{aligned}
&\alpha_i(x + y) \\
&= f\left(a_1^i, \ldots, a_{i-1}^i, x + y, a_{i+1}^i, \ldots, a_n^i\right) + f\left(a_1^i, \ldots, a_{i-1}^i, o, a_{i+1}^i, \ldots, a_n^i\right) \\
&= f\left(a_1^i, \ldots, a_{i-1}^i, x, a_{i+1}^i, \ldots, a_n^i\right) + f\left(a_1^i, \ldots, a_{i-1}^i, y, a_{i+1}^i, \ldots, a_n^i\right) \\
&= \alpha_i(x) + \alpha_i(y),
\end{aligned}$$

so $\alpha_i \in \mathrm{Aut}(G')$, $i = 1, \ldots, n$.

Finally show that $f(x_1, \ldots, x_n) = \alpha_1(x_1) + \ldots + \alpha_n(x_n) + c$. Indeed,

$$\begin{aligned}
&f(x_1, \ldots, x_n) = f(x_1, \ldots, x_n) + f\left(0, a_2^1, \ldots, a_n^1\right) \\
&= f\left(x_1, a_2^1, \ldots, a_n^1\right) + f(0, x_2, \ldots, x_n) = \alpha_1(x_1) + f(0, x_2, \ldots, x_n)
\end{aligned}$$

$$
\begin{aligned}
&= \alpha_1(x_1) + f(0, x_2, \ldots, x_n) + f\left(a_1^2, 0, a_3^2, \ldots, a_n^2\right) \\
&= \alpha_1(x_1) + f\left(a_1^2, x_2, a_3^2, \ldots, a_n^2\right) + f(0, 0, x_3, \ldots, x_n) \\
&= \alpha_1(x_1) + \alpha_2(x_2) + f\left(0, 0, x_3, \ldots, x_n\right) = \ldots = \\
&= \alpha_1(x_1) + \ldots + \alpha_{n-1}(x_{n-1}) + f(0, \ldots, 0, x_n) \\
&= \alpha_1(x_1) + \ldots + \alpha_{n-1}(x_{n-1}) + f(0, \ldots, 0, x_n) + f\left(a_1^n, \ldots, a_{n-1}^n, 0\right) \\
&= \alpha_1(x_1) + \ldots + \alpha_{n-1}(x_{n-1}) + f\left(a_1^n, \ldots, a_{n-1}^n, x_n\right) + f(0, \ldots, 0) \\
&= \alpha_1(x_1) + \ldots + \alpha_n(x_n) + c. \qquad \square
\end{aligned}
$$

The fact that the set of all constant functions and a quasigroup function may be contained only in classes specified by relations from the families $\mathfrak{U}_k$ or $\mathfrak{L}_k$ yields the following lemma.

Corollary 3.23. *If a quasigroup is affine over a group G that is not an elementary p-group, then this quasigroup is non-simple.*

This fact is a generalization of the first lemma of [2, Proposition 3.2] for the case $n > 2$.

Remark 3.24. Non-affinity is a crucial property for cryptographic applications. For the case $n = 2$ it is known that solvability of a system of equations over a quasigroup is decidable in polynomial time if and only if the quasigroup is affine; otherwise the problem is NP-complete [20, Corollary 3.17].

Remark 3.25. Similarly to the case of simplicity, almost all 2-quasigroups are not isotopic to affine quasigroups (see [10]). To the best of our knowledge the problem for $n > 2$ is uninvestigated.

Remark 3.26. Affinity of a 2-quasigroup can be decided with complexity $O\left(k^2 \log k\right)$ ([13]). In the case $n > 2$ the complexity is $O\left(k^n\right)$ for fixed n and $k \to \infty$ (see [12]).

4. Main results

The lemmas 3.2, 3.4, 3.9 and 3.18 obtained in the previous section directly imply the following statements.

Theorem 4.1. *A quasigroup (Q, f) of the arity n is polynomially complete if and only if f is not quasilinear and does not preserve any non-trivial equivalence relation, or, equivalently, if the quasigroup is simple and non-affine.*

Corollary 4.2. *Polynomial completeness of a quasigroup of the arity n can be decided with complexity $O\left(k^{n+1}\right)$ for fixed n and $k \to \infty$.*

Theorem 4.3. *A quasigroup (Q, f) of the arity n is complete if and only if f is not quasi-linear and autodual and does not preserve any central relation of the arity 1 and any non-trivial equivalence relation; equivalently, if the quasigroup is simple and non-affine, does not have proper subquasigroups and has a trivial automorphism group.*

Remark 4.4. *Efficient completeness decision can be obtained by constructing an efficient procedure for deciding whether the automorphism group is trivial.*

5. Conclusion

Polynomial completeness and completeness of n-ary quasigroups are important properties from cryptographic point of view. In our paper we have obtained criteria for polynomial completeness and completeness in terms of maximal classes of k-valued logics. We have also discussed the relationship between maximal classes and various quasigroup properties and the complexity of deciding these properties.

The goals for future research include extending results which are known only for the case $n = 2$ to the case $n > 2$ and investigating the complexity of deciding whether the automorphism group of a quasigroup is trivial.

Acknowledgments. The authors thank D.N. Zhuk and A.E. Pankratiev for fruitful discussions and valuable comments.

References

[1] **V.A. Artamonov, S. Chakrabarti, S. Gangopadhyay, S.K. Pal**, *On Latin squares of polynomially complete quasigroups and quasigroups generated by shifts*, Quasigroups Relat. Syst. **21** (2013), 117 – 130.

[2] **V.A. Artamonov, S. Chakrabarti, S.K. Pal**, *Characterizations of highly non-associative quasigroups and associative triples*, Quasigroups Relat. Syst. **25** (2017), 1 – 19.

[3] **V.A. Artamonov, S. Chakrabarti, S.K. Tiwari, V.T. Markov**, *Algebraic properties of subquasigroups and construction of finite quasigroups*, Algebra Logic **61** (2022), 251 – 270.

[4] **D. Chauhan, I. Gupta, R. Verma**, *Quasigroups and their applications in cryptography*, Cryptologia **45** (2021), 227 – 265.

[5] **Y. Cheng, Y. Xu**, *Stream cipher based on Latin cubes*, Proc. First Intern. Confer. Information Sci. and Electronic Technology, (2015), 137 – 140.

[6] **I.V. Cherednik**, *private communications.*

[7] **A.V. Cheremushkin**, *Almost all Latin squares have a trivial autostrophy group*, Prikl. Diskr. Mat. **3(5)** (2009), 29 – 32.

[8] **V. Dimitrova, S. Markovski**, *Classification of quasigroups by image patterns*, Proc. Fifth Intern. Confer. Informatics and Information Technol., (2007), 152 – 160.

[9] **P. Dömösi, G. Horváth**, *A novel cryptosystem based on abstract automata and Latin cubes*, Studia Sci. Math. Hungarica **52** (2015), 221 – 232.

[10] **A.V. Galatenko, V.V. Galatenko, A.E. Pankratiev**, *Strong polynomial completeness of almost all quasigroups*, Math. Notes **111** (2022), 7 – 12.

[11] **A.V. Galatenko, A.D. Mazurin, A.E. Pankratiev, R.A. Zhigliaev**, *Efficient verification of some properties of finite quasigroups*, Proc. Third Intern. Confer. Math. in Armenia (2023), 29 – 30.

[12] **A.V. Galatenko, A.E. Pankratiev, V.M. Staroverov**, *Algorithms for checking some properties of n-quasigroups*, Program. Comput. Softw. **48** (2022), 36 – 48.

[13] **A.V. Galatenko, A.E. Pankratiev, R.A. Zhigliaev**, *An optimized procedure for deciding affinity of finite quasigroups*, Proc. Fifth Intern. Confer. Computer Algebra (2023), 67 – 70.

[14] **D. Gligoroski, S. Markovski and L. Kocarev**, *Edon-R, an infinite family of cryptographic hash functions*, Second NIST Cryptographic Hash Workshop (2006), https://csrc.nist.rip/groups/ST/hash/documents/GLIGOROSKI_NIST_Hash_06_082506.pdf, Accessed 14 December 2023.

[15] **D. Gligoroski, H. Mihajloska, D. Otte, M. El-Hadedy**, *GAGE and InGAGE*, http://gageingage.org/upload/GAGEandInGAGEv1.03.pdf, Accessed 14 December 2023.

[16] **D. Gligoroski, R. S. Ødegård., M. Mihova, S. J. Knapskog, A. Drapal, V. Klima, J. Amundsen, M. El-Hadedy**, *Cryptographic hash function EDON-R'*, Proc. First Intern. Workshop on Security and Communication Networks (2009), 1 – 9.

[17] **M.M. Glukhov**, *Some applications of quasigroups in cryptography*, Prikl. Diskr. Mat. **2(2)** (2008), 28 – 32.

[18] **J. Hagemann, C. Herrmann**, *Arithmetical locally equational classes and representation of partial functions*, Universal Algebra, Colloq. Math. Soc. J. Bolyai **29** (1982), 345 – 360.

[19] **G. Horváth, C.L. Nehaniv, Cs. Szabó**, *An lemma concerning functionally complete algebras and NP-completeness*, Theoret. Comput. Sci. **407** (2008), 591 – 595.

[20] **B. Larose, L. Zádori**, *Taylor terms, constraint satisfaction and the complexity of polynomial equations over finite algebras*, Int. J. Algebra Comput. **16** (2006), 563 – 581.

[21] **D. Lau**, *Function algebras on finite sets : a basic course on many-valued logic and clone theory*, Springer (2006).

[22] **S. Markovski, A. Mileva**, *NaSHA – family of cryptographic hash functions*, First SHA-3 Candidate Confer., Leuven, 2009.

[23] **I.G. Rosenberg**, *Über die funktionale Vollständigkeit in den mehrwertigen Logiken*, Rozpravy Československe Akad. Ved. Řada Mat. Přirod. **80** (1970), 3 – 93.

[24] **C. Shannon**, *Communication theory of secrecy systems*, Bell Syst. Tech. J. **28** (1949), 656 – 715.

[25] **V.A. Shcherbacov**, *Quasigroups in cryptology*, Comput. Sci. J. Mold. **17** (2009), 193 – 228.

[26] **M. Xu, Z. Tian**, *An image cipher based on Latin cubes*, Proc. Third Intern. Confer. Information and Computer Technologies (2020), 160 – 168.

[27] **V.L. Yugay**, *A criterion for polynomial completeness of quasigroups*, Intellektualnye Sistemy. Teoria i Prilojenia **21** (2017), 131 – 135.

Received January 17, 2024

Faculty of Mechanics and Mathematics, Lomonosov Moscow State University
Main Building, GSP-1, Leninskiye Gory, Moscow, Russia
E-mails: svetlana.chaplygina@math.msu.ru, agalat@msu.ru