BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 1(53), 2007, Pages 37–45
ISSN 1024–7696

Power sets of n-ary quasigroups

G. Belyavskaya

Abstract. In the theory of latin squares and in the binary quasigroup theory the notion of a latin power set (a quasigroup power set) is known. These sets have a good property, and namely, they are orthogonal sets. Such sets were studied and methods of their construction were suggested in different articles (see, for example, [1–5]).
In this article we introduce (k)-powers of a k-invertible n-ary operation (with respect to the k-multiplication of n-ary operations) and (k)-power sets of n-ary quasigroups, $n \geq 2$, $1 \leq k \leq n$, prove pairwise orthogonality of such sets and consider distinct posibilities of their construction with the help of binary groups, in particular, using $n-T$-quasigroups and n-ary groups.

Mathematics subject classification: 20N05, 20N15, 05B07.
Keywords and phrases: Binary quasigroup, k-invertible n-ary operation, n-ary quasigroup, latin square, n-dimensional hypercube, latin power set, quasigroup power set, pairwise orthogonal set of n-ary quasigroups.

1 Introduction

In the theory of latin squares the notion of a power set of latin squares or a latin power set is known. In the articles [1–4] some properties and different methods of constructing such sets , in particular, sets based and not based on groups, were considered. In [5] an algebraic approach to the study of latin power set was used and a new method of constructing quasigroup power sets based on cyclic S-systems (such systems correspond to a particular case of latin power sets [6]) and on pairwise balanced block designs of index one (BIB(v,b,r,k,1)) [7] was suggested.

Any power set of latin squares (of quasigroups) is an orthogonal set and can be used in applications, in particular, by the construction of some codes and ciphers. Such a ciphering device whose algorithm is based on a latin power set has been patented [8]. In [4] it was noticed, " It is obvious that latin power sets based on non-group tables are more preferable to those based on group tables because the greater irregularity makes the cipher safer".

In this article we introduce and study the power sets of n-ary quasigroups, in particular, prove pairwise orthogonality of such sets, consider distinct posibilities of their construction.

2 Necessary notions and results

We recall some notations, concepts and results which are used in the article. At first remember the following denations and notes from [9]. By x_i^j we will denote

the sequence $x_i, x_{i+1}, \dots, x_j$, $i \le j$. If $j < i$, then x_i^j is the empty sequence, $\overline{1,n} = \{1, 2, \dots, n\}$. Let Q be a finite or an infinite set, $n \ge 2$ be a positive integer and let Q^n denote the Cartesian power of the set Q.

An *n-ary operation* A (briefly, an *n-operation*) on a set Q is a mapping $A : Q^n \to Q$ defined by $A(x_1^n) \to x_{n+1}$, and in this case we write $A(x_1^n) = x_{n+1}$.

A *finite n-groupoid (Q, A) of order m* is a set Q with one n-ary operation A defined on Q, where $|Q| = m$.

An *n-ary quasigroup (n-quasigroup)* is an n-groupoid such that in the equality

$$A(x_1^n) = x_{n+1}$$

each of n elements from x_1^{n+1} uniquely defines the $(n+1)$-th element. Usually a quasigroup n-operation A is itself considered as an n-quasigroup.

The n-operation E_i, $1 \le i \le n$, on Q with $E_i(x_1^n) = x_i$ is called the *i-th identity operation* (or the *i-th selector) of arity n*.

An n-operation A on Q is called *i-invertible* for some $i \in \overline{1,n}$ if the equation

$$A(a_1^{i-1}, x_i, a_{i+1}^n) = a_{n+1}$$

has a unique solution for each fixed n-tuple $(a_1^{i-1}, a_{i+1}^n, a_{n+1}) \in Q^n$.

For an i-invertible n-operation there exists the *i-inverse n-operation* ${}^{(i)}A$ defined in the following way:

$${}^{(i)}A(x_1^{i-1}, x_{n+1}, x_{i+1}^n) = x_i \Leftrightarrow A(x_1^n) = x_{n+1}$$

for all $x_1^{n+1} \in Q^{n+1}$.

It is evident that

$$A(x_1^{i-1}, {}^{(i)}A(x_1^n), x_{i+1}^n) = {}^{(i)}A(x_1^{i-1}, A(x_1^n), x_{i+1}^n) = x_i$$

and ${}^{(i)}[{}^{(i)}A] = A$ for $i \in \overline{1,n}$.

Let Ω_n be the set of all n-ary operations on a finite or infinite set Q. On Ω_n define a binary operation $\underset{i}{\oplus}$ (the i-multiplication) in the following way:

$$(A \underset{i}{\oplus} B)(x_1^n) = A(x_1^{i-1}, B(x_1^n), x_{i+1}^n),$$

$A, B \in \Omega_n, x_1^n \in Q^n$. Shortly this equality can be written as

$$A \underset{i}{\oplus} B = A(E_1^{i-1}, B, E_{i+1}^n)$$

where E_i is the i-th selector.

In [10] it was proved that $(\Omega_n; \underset{i}{\oplus})$ is a semigroup with the identity E_i. If Λ_i is the set of all i-invertible n-operations from Ω_n for some $i \in \overline{1,n}$, then $(\Lambda_i; \underset{i}{\oplus})$ is a group. In this group E_i is the identity, the inverse element of A is the operation ${}^{(i)}A \in \Lambda_i$, since $A \underset{i}{\oplus} E_i = E_i \underset{i}{\oplus} A$, $A \underset{i}{\oplus} {}^{(i)}A = {}^{(i)}A \underset{i}{\oplus} A = E_i$.

An n-ary quasigroup (Q, A) (or simply A), is an n-groupoid with an i-invertible n-operation for each $i \in \overline{1,n}$ [9].

Let $(x_1^n)_k$ denote the $(n-1)$-tuple $(x_1^{k-1}, x_{k+1}^n) \in Q^{n-1}$ and let A be an n-operation, then the $(n-1)$-operation A_a:

$$A_a(x_1^n)_k = A(x_1^{k-1}, a, x_{k+1}^n)$$

is called *the* $(n-1)$*-retract* of A, defined by position k, $k \in \overline{1,n}$, with the element a in this position (with $x_k = a$) [9].

An n-ary operation A on Q is called *complete* if there exists a permutation $\overline{\varphi}$ on Q^n such that $A = E_1\overline{\varphi}$ (that is $A(x_1^n) = E_1\overline{\varphi}(x_1^n)$). If a complete n-operation A is finite and has order m, then the equation $A(x_1^n) = a$ has exactly m^{n-1} solutions for any $a \in Q$ [10].

Any i-invertible (for some fixed i, $i \in \overline{1,n}$) n-operation A is complete, but there exist complete n-operations which are not i-invertible for each $i \in \overline{1,n}$ [10].

For $n \geq 2$, an *n-dimensional hypercube* (briefly, an *n-hypercube) of order m* is an $\underbrace{m \times m \times \cdots \times m}_{n}$ array with m^n points based upon m distinct symbols [11].

A hypercube is a generalization of a *latin square*, which in the case of squares of *order* m, is an $m \times m$ array in which m distinct symbols are arranged so that each symbol occurs once in each row and column. A latin square is a 2-dimensional hypercube of a special type.

In [12] the connection between n-hypercubes and (algebraic) n-ary operations was established. In addition we note that a k-invertible operation A_H corresponds to an n-hypercube H with the following property: whenever $n-1$ of the n coordinates, except the k-th coordinate, are fixed, each of the m symbols appears exactly one time in that subarray (in that k-th column). In this case the mapping $L_{(\overline{a})_k} = A_H(a_1^{k-1}, x, a_{k+1}^n)$ is a permutation on Q for each $(\overline{a})_k \in Q^{n-1}$ where $(\overline{a})_k = (a_1^{k-1}, a_{k+1}^n)$. In the theory of n-quasigroups this permutation is called the k-th translation of the n-quasigroup (Q, A_H) defined by the $(n-1)$-tuple $(\overline{a})_k$ [9].

In the case of n-ary operations for $n > 2$ it is possible to consider different versions of orthogonality. The weakest is the notion of the pairwise orthogonality.

Definition 1 [12]. *Two n-ary operations ($n \geq 2$) A and B given on a set Q of order m are called orthogonal (shortly, $A \perp B$) if the system $\{A(x_1^n) = a, B(x_1^n) = b\}$ has exactly m^{n-2} solutions for any $a, b \in Q$.*

This concept corresponds to two orthogonal n-dimensional hypercubes [12]. Two n-hypercubes H_1 and H_2 of order m are *orthogonal* if when superimposed, each of the m^2 ordered pairs appears m^{n-2} times [15],[11].

Definition 2 [12]. *A set $\Sigma = \{A_1^t\}$, $t \geq 2$, of n-operations is called pairwise orthogonal if any pair of distinct n-operations from Σ is orthogonal.*

In [13] the following criterion of orthogonality of two finite k-invertible n-operations was established.

Theorem 1 [13]. *Let k be a fixed number from $\overline{1,n}$. Two finite k-invertible n-operations A and B on a set Q are orthogonal if and only if the $(n-1)$-retract C_a of the n-operation $C = B \underset{k}{\oplus}\, {}^{(k)}A$, defined by $x_k = a$, is complete for every $a \in Q$.*

Definition 3. *We shall say that an n-operation C, given on a set Q, has the k-property if its $(n-1)$-retract C_a, defined by $x_k = a$, is complete for every $a \in Q$.*

Note that any n-quasigroup has the k-property for each $k \in \overline{1,n}$ since any its $(n-1)$-retract is an $(n-1)$-quasigroup.

3 Power sets of n-ary quasigroups and pairwise orthogonality

Let L be a latin square of order m, given on a set Q by its rows $\alpha_1, \alpha_2, \ldots, \alpha_m$ (which are permutations of Q). Then power l of L is defined as

$$L^l = (\alpha_1^l, \alpha_2^l, \ldots, \alpha_m^l).$$

If $L, L^2, \ldots, L^s$ are all latin squares, then the set $\{L, L^2, \ldots, L^s\}$ is called a *latin power set of size s*.

It is known that a binary quasigroup (Q, A) corresponds to every latin square L given on a set Q and if $\{L, L^2, \ldots, L^s\}$ is a latin power set, then $\{A, A^2, \ldots, A^s\}$ is the corresponding quasigroup power set where $A^l = A \cdot A \cdot \ldots \cdot A$ (l times), $1 \le l \le s$, $(A \cdot A)(x, y) = A^2(x, y) = A(x, A(x, y))$ [5].

Consider an analog of powers for n-operations. Let k be a fixed number of $\overline{1,n}$, A be a k-invertible n-operation.

The power $A^l = A \underset{k}{\oplus} A \underset{k}{\oplus} \ldots \underset{k}{\oplus} A$ (l times) with respect to the k-multiplication of n-ary operations is called the *(k)-power l of A*.

Note that if all (k)-powers $A, A^2, \ldots, A^s$ are n-quasigroups, then they are different, that is form a set, since the equality $A^t = A^r$, $t, r \in \overline{1,s}$, $t > r$, implies $A^{t-r} = E_k$ for $t - r < s$.

Definition 4. *A set $\Sigma_k = \{A, A^2, \ldots, A^s\}_k$, $s \ge 2$, is called a (k)-power set of n-quasigroups if all (k)-powers of A from Σ_k are n-quasigroups.*

Note that index k after a set shows additionally that the powers in this set are taken with respect to the k-multiplication of operations.

Using Theorem 1 it is easy to prove the following statement for any k-invertible n-operations, in particular, for n-quasigroups.

Theorem 2. *Let A be a finite k-invertible n-operation and the (k)-powers $A, A^2, \ldots, A^s$, $s \ge 2$, of A be different. Then the set $\Sigma_k = \{A, A^2, \ldots, A^s\}_k$ is a pairwise orthogonal if and only if each of the n-operations $A, A^2, \ldots, A^{s-1}$ has the k-property.*

Proof. At first we remember that all k-invertible n-operations, given on a set Q, form a group with the identity E_k with respect to the k-multiplication, ${}^{(k)}A$ is the

inverse element of A in this group and $({}^{(k)}A)^l = {}^{(k)}(A^l)$. Let $1 \le i \le s-1$, $i < j \le s$. By Theorem 1 $A^j \perp A^i$ if and only if the n-operation $A^j \underset{k}{\oplus} ({}^{(k)}A)^i = A^{j-i}$ has the k-property for any $1 \le j - i \le s - 1$. □

For a binary operation A on a set Q 2-invertibility means that the equation $A(a, y) = b$ has a unique solution for any $a, b \in Q$. If A has the 2-property, then the equation $A(x, a) = b$ has a unique solution for any $a, b \in Q$, that is A is 1-invertible also. Thus, in Theorem 2 all (2)-powers $A, A^2, \dots, A^{s-1}$ of a binary (2)-invertible operation A must be quasigroups, A^s can be only (2)-invertible and is true the following

Corollary 1. *Let A be a finite 2-invertible binary operation and the (2)-powers $A, A^2, \dots, A^s$, $s \ge 2$, of A are different. Then the set $\Sigma_2 = \{A, A^2, \dots, A^s\}_2$ is orthogonal if and only if $A, A^2, \dots, A^{s-1}$ are quasigroups.*

In [1] the following result (Corollary 5a) with respect to latin power sets which we shall formulate in the language of quasigroups was proved, where $A^{-1} = {}^{(2)}A$ is the right inverse quasigroup for A ($A^{-1}(x, y) = z \Leftrightarrow A(x, z) = y$).

Proposition 1 [1]. *If $A, A^2, \dots, A^s$, $s \ge 2$, are finite quasigroups, then any s successive quasigroups from $(A^{-1})^s, (A^{-1})^{s-1}, \dots, A^{-1}, A, A^2, \dots, A^s$ form an orthogonal set of quasigroups.*

Now we prove that for n-ary case, $n \ge 2$, an analogous situation takes place.

Theorem 3. *If a set $\Sigma_k = \{A, A^2, \dots, A^s\}_k$ is a (k)-power set of finite quasigroups, then in the sequence*

$$({}^{(k)}A)^s, ({}^{(k)}A)^{s-1}, \dots, ({}^{(k)}A)^2, {}^{(k)}A, A, A^2, \dots, A^s$$

every s-tuple of successive n-quasigroups is a pairwise orthogonal set.

Proof. Let $1 \le i, j \le s$, $i < j$, then $A^j \underset{k}{\oplus} ({}^{(k)}A)^i = A^j \underset{k}{\oplus}^{(k)} (A^i) = A^{j-i} \in \Sigma_k$, so the n-operation A^{j-i} is an n-quasigroup, all its $(n-1)$-retracts are $(n-1)$-quasigroups too, so they have the k-property and by Theorem 2 we have $A^i \perp A^j$. On the other hand, by the same restrictions on i, j we obtain ${}^{(k)}(A^i) \underset{k}{\oplus} A^j = A^{j-i} \in \Sigma_k$, so ${}^{(k)}(A^i) \perp^{(k)} (A^j)$ by Theorem 2.

Let $1 \le i \le s-1$, $1 \le j \le s-i$, then $A^i \underset{k}{\oplus}^{(k)} ({}^{(k)}(A^j)) = A^i \underset{k}{\oplus} A^j = A^{i+j} \in \Sigma_k$, so $A^i \perp^{(k)} (A^j)$ by Theorem 2 (see the previous case). □

Corollary 2. *If in Theorem 3, in addition, $s+1$ is the smallest exponent such that $A^{s+1} = E_k$, then the sequence from the theorem is $A, A^2, \dots, A^s$.*

Proof. Indeed, by these conditions $({}^{(k)}A)^i = A^{s+1-i}$ for all $i \in \overline{1, s}$. □

Theorem 4. *Let (Q, A) be a finite n-quasigroup of the form*

$$A(x_1^n) = \alpha_1 x_1 \cdot \ldots \cdot \alpha_{k-1} x_{k-1} \cdot x_k \cdot \alpha_{k+1} x_{k+1} \cdot \ldots \cdot \alpha_n x_n$$

for some fixed $k \in \overline{1,n}$, where α_i is a permutation of Q for every $i \in \overline{1,n}$, $i \neq k$, $(Q,\cdot)$ is a binary group. Then $\Sigma_k = \{A, A^2, \ldots, A^s\}_k$ is a (k)-power set of n-quasigroups if and only if in the group $(Q,\cdot)$ the mapping $x \to x^l$ is a permutation for each $l \in \overline{2,s}$.

Proof. Let an n-quasigroup (Q,A) have the form of the theorem, then

$$A^2(x_1^n) = A(x_1^{k-1}, A(x_1^n), x_{k+1}^n) = \alpha_1 x_1 \cdot \ldots \cdot \alpha_{k-1}x_{k-1}\cdot$$

$$(\alpha_1 x_1 \cdot \ldots \cdot \alpha_{k-1}x_{k-1} \cdot x_k \cdot \alpha_{k+1}x_{k+1} \cdot \ldots \cdot \alpha_n x_n) \cdot \alpha_{k+1}x_{k+1} \cdot \ldots \cdot \alpha_n x_n =$$

$$(\alpha_1 x_1 \cdot \ldots \cdot \alpha_{k-1}x_{k-1})^2 \cdot x_k \cdot (\alpha_{k+1}x_{k+1} \cdot \ldots \cdot \alpha_n x_n)^2.$$

Taking into account that $A^l(x_1^n) = A^{l-1}(x_1^{k-1}, A(x_1^n), x_{k+1}^n)$ we shall obtain by the same way

$$A^l(x_1^n) = (\alpha_1 x_1 \cdot \ldots \cdot \alpha_{k-1}x_{k-1})^l \cdot x_k \cdot (\alpha_{k+1}x_{k+1} \cdot \ldots \cdot \alpha_n x_n)^l \tag{1}$$

for any $l \in \overline{1,s}$.

Let A^l be a finite n-quasigroup for some l, $2 \leq l \leq s$, then it is i-invertible for each $i \in \overline{1,n}$, that is for any $(n-1)$-tuple $(a_1^n)_i \in Q^{n-1}$,

$$A^l(a_1^{i-1}, x, a_{i+1}^n) = A^l(a_1^{i-1}, y, a_{i+1}^n) \Leftrightarrow x = y. \tag{2}$$

If $i \in \overline{1,k-1}$, then we have

$$(\alpha_1 a_1 \cdot \ldots \cdot \alpha_{i-1}a_{i-1} \cdot \alpha_i x \cdot \alpha_{i+1}a_{i+1} \cdot \ldots \cdot \alpha_{k-1}a_{k-1})^l \cdot a_k \cdot (\alpha_{k+1}a_{k+1} \cdot \ldots \cdot \alpha_n a_n)^l =$$

$$(\alpha_1 a_1 \cdot \ldots \cdot \alpha_{i-1}a_{i-1} \cdot \alpha_i y \cdot \alpha_{i+1}a_{i+1} \cdot \ldots \cdot \alpha_{k-1}a_{k-1})^l \cdot a_k \cdot (\alpha_{k+1}a_{k+1} \cdot \ldots \cdot \alpha_n a_n)^l$$

$\Leftrightarrow x = y$. Doing the respective cancelation we obtain

$$(a \cdot \alpha_i x \cdot b)^l = (a \cdot \alpha_i y \cdot b)^l \Leftrightarrow x = y, (L_a R_b \alpha_i x)^l = (L_a R_b \alpha_i y)^l \Leftrightarrow x = y,$$

where $a = \alpha_1 a_1 \cdot \ldots \cdot \alpha_{i-1}a_{i-1}$, $b = \alpha_{i+1}a_{i+1} \cdot \ldots \cdot \alpha_{k-1}a_{k-1}$, $L_a x = a \cdot x$, $R_b x = x \cdot b$. Changing x (y) with $\alpha_i^{-1}R_b^{-1}L_a^{-1}x$ $(\alpha_i^{-1}R_b^{-1}L_a^{-1}y)$, we obtained

$$x^l = y^l \Leftrightarrow \alpha_i^{-1}R_b^{-1}L_a^{-1}x = \alpha_i^{-1}R_b^{-1}L_a^{-1}y \Leftrightarrow x = y$$

by each $i \in \overline{1,k-1}$.

Let $i \in \overline{k+1,n}$. Then from (2) it follows

$$(\alpha_1 a_1 \cdot \ldots \cdot \alpha_{k-1}a_{k-1})^l \cdot a_k \cdot (\alpha_{k+1}a_{k+1} \cdot \ldots \cdot \alpha_{i-1}a_{i-1} \cdot \alpha_i x \cdot \alpha_{i+1}a_{i+1} \cdot \ldots \cdot \alpha_n a_n)^l =$$

$$(\alpha_1 a_1 \cdot \ldots \cdot \alpha_{k-1}a_{k-1})^l \cdot a_k \cdot (\alpha_{k+1}a_{k+1} \cdot \ldots \cdot \alpha_{i-1}a_{i-1} \cdot \alpha_i y \cdot \alpha_{i+1}a_{i+1} \cdot \ldots \cdot \alpha_n a_n)^l$$

$\Leftrightarrow x = y$,

$$(c \cdot \alpha_i x \cdot d)^l = (c \cdot \alpha_i y \cdot d)^l \Leftrightarrow x = y$$

where $c = \alpha_{k+1}a_{k+1} \cdot \ldots \cdot \alpha_{i-1}a_{i-1}, d = \alpha_{i+1}a_{i+1} \cdot \ldots \cdot \alpha_n a_n$. Then $x^l = y^l \Leftrightarrow x = y$ for all $l \in \overline{1,s}$ (see the previous case).

Thus, if all (k)-powers $A, A^2, A^3, \dots, A^s$ are n-quasigroups, then in the group $(Q, \cdot)$ the mapping $x \to x^l$ is a permutation for each $l \in \overline{1,s}$.

Conversely, let all mappings $x \to x^l$, $l \in \overline{2,s}$, be permutations in the group $(Q, \cdot)$. Then all k-powers $A, A^2, A^3, \dots, A^s$, defined by (1) are different, that is they form a set. Indeed, if $A^t(x_1^n) = A^r(x_1^n)$, $1 \le r, t \le s$ and $t > r$, then from (1) we have

$$x^t x_k y^t = x^r x_k y^r, \quad x^{t-r} x_k y^{t-r} = x_k$$

for any $x, y \in Q$. Setting $y = e$ (the identity of the group $(Q, \cdot)$) in the last equality we obtain that $x^{t-r} x_k = x_k$ and $x^{t-r} = e$ for $t - r < s$ and any $x \in Q$. But by the conditions all mappings $x \to x^l$, $l \in \overline{1,s}$, are permutations, so we have contradiction.

It remains to show that all (k)-powers are n-quasigroups. For that we can prove (2) fixing an arbitrary $(n-1)$-tuple $(a_1^n)_i$ of elements of Q and making the inverse transformations corresponding to the case $i \in \overline{1,k-1}$ ($i \in \overline{k+1,n}$). That is every (k)-power l of the finite n-quasigroup (Q, A) is i-invertible for any $i \in \overline{1,n}$, $i \ne k$. But the n-operation A^l is always k-invertible as a power with respect to the k-multiplication. Thus, (Q, A^l) is an n-quasigroup for each $l \in \overline{1,s}$ and the set $\Sigma_k = \{A, A^2, \dots A^s\}_k$ is a (k)-power set of n-ary quasigroups. □

Corollary 3. *Let $(Q, +)$ be an abelian group of order m, $m = p_1^{\beta_1} p_2^{\beta_1} \dots p_t^{\beta_t}$ be decomposition in prime multipliers, $p_1 < p_2 < \dots < p_t$, $p_1 \ge 3$, k be a fixed element, $1 \le k \le n$, (Q, A) be an n-quasigroup of the form:*

$$A(x_1^n) = \alpha_1 x_1 + \alpha_2 x_2 + \dots + \alpha_{k-1} x_{k-1} + x_k + \alpha_{k+1} x_{k+1} + \dots + \alpha_n x_n,$$

where all α_i are permutations. Then $\Sigma_k = \{A, A^2, \dots, A^{p_1-1}\}_k$ is a (k)-power set of n-quasigroups.

Proof. In an abelian group of order m with the zero 0 all mappings $x \to 2x$, $x \to 3x, \dots, (p_1 - 1)x$ are permutations. Otherwise, $lx = ly \Rightarrow l(x - y) = 0$ if $x \ne y$, $2 \le l < p_1$, it means that in the group $(Q, +)$ there exists an element which has the order smaller than p_1. We have contradiction with Lagrange's Theorem stating that the order of any subgroup (and the order of any element) divides the order of a finite group [14]. Now use Theorem 4. □

For a finite elementary abelian group (that is a group which is a direct power of a group of a prime order [14]) from Corollary 3 immediately follows

Corollary 4. *If in Corollary 3 $(Q, +)$ is an elementary abelian group of order $m = p^t$, $p \ge 3$, then $\Sigma_k = \{A, A^2, \dots A^{p-1}\}_k$ is a (k)-power set of n-quasigroups.*

Corollary 5. *Let in Corollary 3 the order of an abelian group $(Q, +)$ be a prime number p, $p \ge 3$ and an n-quasigroup A have the form*

$$A(x_1^n) = x_1 + x_2 + \dots + x_n,$$

then $\Sigma_k = \{A, A^2, \dots, A^{p-1}\}_k$ is a (k)-power set of n-quasigroups for each $k \in \overline{1,n}$.

Remark. Note that in general $\Sigma_k \neq \Sigma_l$ if $k \neq l$, since powers of an n-quasigroup A, taken with respect to the k-multiplication and with respect to the l-multiplication of n-operations, can be different.

Corollary 6. *Let $\Sigma_k = \{A, A^2, \dots, A^{p-1}\}_k$ be a (k)-power set of n-quasigroups of Corollary 4 or 5, then $\Sigma'_k = \{E_k, A, A^2, \dots, A^{p-1}\}_k$ is a (cyclic) group with respect to the k-multiplication of n-operations.*

Proof. By Theorem 4 the (k)-powers of an n-quasigroup A in these sets have the form (1). By $l = p$ where p is a prime number in that case we obtain $A^p = E_k$, since $a^p = e$ in the group $(Q, \cdot)$ with the identity e for each $a \in Q$. □

Recall that an n-quasigroup (Q, A) is called an *$n - T$-quasigroup* if there exist a binary abelian group $(Q, +)$, its automorphisms $\alpha_1, \alpha_2, \dots, \alpha_n$ and an element $a \in Q$ such that

$$A(x_1^n) = \alpha_1 x_1 + \alpha_2 x_2 + ... + \alpha_{k-1} x_{k-1} + \alpha_k x_k + \alpha_{k+1} x_{k+1} + \cdots + \alpha_n x_n + a \quad (3)$$

for all $x_1^n \in Q^n$ [16].

Corollary 7. *Let (Q, A) be an $n - T$-quasigroup of (3) with $\alpha_k = \epsilon$ (the identity permutation) for some fixed k, $k \in \overline{1, n}$, where (Q, A) is an abelian group of order $m = p_1^{\beta_1} p_2^{\beta_1} \dots p_t^{\beta_t}$, $p_1 < p_2 < \cdots < p_t$, $p_1 \geq 3$. Then the set $\Sigma_k = \{A, A^2, \dots, A^{p_1-1}\}_k$ is a (k)-power set of n-quasigroups.*

Proof . Follows from Theorem 4 and Corollary 3, taking into account (with respect to the element a) that (Q, A) is an abelian group. □

Consider an *n-ary group* (Q, A) [9]. By Theorem of Gluskin-Hossu this n-group has the form

$$A(x_1^n) = x_1 \cdot \theta x_2 \cdot \theta^2 x_3 \cdot ... \cdot \theta^{n-1} x_n \cdot a, \quad (4)$$

where $(Q, \cdot)$ is a binary group, θ is its automorphism such that $\theta a = a$, $\theta^{n-1} x = axa^{-1}$. In this case we say that (Q, A) is an *n-group over the binary group* $(Q, \cdot)$.

For an n-group over an abelian group (it is a particular case of $n-T$-quasigroups) we have the following

Corollary 8. *Let (Q, A) be an n-group of (4) over an abelian group of order $m = p_1^{\beta_1} p_2^{\beta_1} \dots p_t^{\beta_t}$, $p_1 < p_2 < ... < p_t$, $p_1 \geq 3$. Then $\Sigma_1 = \{A, A^2, \dots, A^{p_1-1}\}_1$ is a (1)-power set of n-quasigroups, $\Sigma_n = \{A, A^2, \dots, A^{p_1-1}\}_n$ is an (n)-power set of n-quasigroups. Moreover, if the automorphism θ has order k, $2 \leq k \leq n-1$, then $\Sigma_{lk+1} = \{A, A^2, \dots, A^{p_1-1}\}_{lk+1}$ is also a $(lk+1)$-power set for each l such that $2 \leq lk \leq n-1$.*

Proof. In this case $\theta^{n-1} x_n = x_n$ and $\theta^{lk} = \epsilon$ for each l such that $1 \leq lk \leq n-1$ and all statements are true by Corollary 7. □

References

[1] Norton D.A. *Groups of orthogonal row-latin squares.* Pacific J. Math., 1952, **2**, p. 335–341.

[2] Denes J. *What is there a latin power set?* Amer.Math. Monthly, 1997, **104**, p. 563–565.

[3] Denes J., Mullen G.L., Suchower S.J. *A note on power sets of latin squares.* J. Comb. Math. Combin. Computing, 1994, **16**, p. 27–31.

[4] Denes J., Owens P.J. *Some new latin power sets not based on groups.* J. Comb. Theory, Ser. A 85, 1999, p. 69–82.

[5] Belyavskaya G.B. *Quasigroup power sets and cyclic S-systems.* Quasigroups and related systems, 2002, **9**, p. 1–17.

[6] Belyavskaya G.B., Cheban A.M. *S-systems of an arbitrary index, II.* Mat. Issled., vyp. 7, 1972, p. 3–13 (in Russian).

[7] Denes J., Keedwell A.D., *Latin Squares and Their Applications.* Academiai Kiado, Budapest, 1974.

[8] Denes J., Petroczki P. *A digital encrypting communication system.* Hungarian Patent N 201437A, 1990.

[9] Belousov V.D. *n-Ary quasigroups.* Kishinev, Shtiintsa, 1972 (in Russian).

[10] Yakubov T. *On $(2,n)$-semigroup of n-ary operations.* Izvestiya AN MSSR., Ser. fiz.-teh. i mat. nauk, 1974, N 1, p. 29–46 (in Russian).

[11] Laywine C.F., Mullen G.L., Whittle G. *D-Dimensional hypercubes and the Euler and MacNeish conjectures.* Monatsh. Math., 1995, **111**, p. 223–238.

[12] Belyavskaya G., Mullen Gary L. *Orthogonal hypercubes and n-ary operations.* Quasigroups and related systems, 2005, **13**, p. 73–86.

[13] Belyavskaya G. *Pairwise orthogonality of n-ary operations.* Buletinul Academiei de Stiinte a Republicii Moldova. Matematica, 2005, N 3(49), p. 5–18.

[14] Kostrikin A.I. *Introduction in algebra.* Moscow, Nauka, 1977.

[15] Kishen K. *On the construction of latin and hyper-graceo-latin cubes and hypercubes.* J. Ind. Soc. Agric. Statist., 1950, **2**, p. 20–48.

[16] Syrbu P.N. *On congruences of n-ary T-quasigroups.* Quasigroups and related systems, 1999, **6**, p. 71–80.

Institute of Mathematics and Computer Science
Academy of Sciences of Moldova
Academiei str. 5, MD-2028 Chişinău
Moldova

E-mail: *gbel@math.md*

Received November 11, 2006