Quasigroups and Related Systems **13** (2005), 157 – 174

Conjugate invariant quasigroups

Zoran Stojaković and Wieslaw A. Dudek

Abstract

Some properties of conjugate invariant quasigroups and their relations to various combinatorial and algebraic structures are described.

1. Introduction

The theory of quasigroups, although older than the theory of groups, is often considered as a minor offshoot of the later (which can be witnessed by AMS Subject Classification 20N05 where quasigroups and loops are considered as just one of "other generalizations of groups"). What is neglected in this consideration are numerous applications of quasigroups in other branches of mathematics and not only mathematics. This paper aims to give a brief presentation of some applications of quasigroups in combinatorics, namely the connection of so called conjugate (parastrophy) invariant quasigroups and some combinatorial structures and also to describe some algebraic properties of such quasigroups.

2. Preliminaries

Although we shall consider binary and n-ary quasigroups, we shall give basic definition and notions for n-ary case, which for $n = 2$ give the usual definitions in the binary case.

The sequence $x_m, x_{m+1}, \ldots, x_n$ we denote by x_m^n or $\{x_i\}_{i=m}^n$. If $m > n$ then x_m^n will be considered empty.

2000 Mathematics Subject Classification: 20N05, 20N15, 05B07

Keywords: n-groupoid, n-quasigroup, n-group, conjugate, H-permutable, Steiner system, Mendelsohn system, quadruple system, identity

An n-ary groupoid (n-groupoid) (Q,f) is called an *n-quasigroup* if the equation $A(a_1^{i-1},x,a_{i+1}^n)=a_{n+1}$ has a unique solution x for every $a_1^{n+1}\in Q$ and every $i\in\{1,\dots,n\}$. An n-quasigroup (Q,f) is called *idempotent* if for every $x\in Q$ $f(x,x,\dots,x)=x$. An element $x\in Q$ is called an *idempotent* if $f(x,x,\dots,x)=x$.

An n-quasigroup (Q,f) is called *(i,j)-associative* iff the following identity holds

$$f(x_1^{i-1},f(x_i^{i+n-1}),x_{i+n}^{2n-1})=f(x_1^{j-1},f(x_j^{j+n-1}),x_{j+n}^{2n-1}).$$

An n-quasigroup which is (i,j)-associative for all $i,j\in\mathbb{N}_n$ is called an n-group.

By S_n we denote the symmetric group of degree n and by A_n its alternating subgroup.

If G is a group and $S\subseteq G$, by $\Gamma\{S\}$ we denote the subgroup of G generated by S.

A *Steiner system* $S(t,k,v)$ is a pair (S,T), where S is a v-set and T is a family of k-subsets of S such that every t-subset of S is contained in exactly one element of T. An $S(2,3,v)$ is called a *Steiner triple system* (STS) and an $S(3,4,v)$ is called a *Steiner quadruple system* (SQS). Ordered analogues of Steiner systems are Mendelsohn systems. A *Mendelsohn system* $M(t,k,v)$ is a pair (S,T) where S is a v-set and T is a family of cyclic k-tuples $\langle a_1,\dots,a_k\rangle$, $a_1,\dots,a_k$ distinct elements of S, such that every ordered pair of distinct elements from S belongs to exactly one element of T. A cyclic k-tuple $\langle a_1,\dots,a_k\rangle$ is the following set of k ordered pairs: $\langle a_1,\dots,a_k\rangle=\{(a_1,a_2),(a_2,a_3),\dots,(a_{k-1},a_k),(a_k,a_1)\}$. An $M(2,3,v)$ and an $M(3,4,v)$ are called a *Mendelsohn triple system* (MTS) and a *Mendelsohn quadruple system* (MQS), respectively.

3. Quasigroup conjugates

Here we give some basic properties of quasigroup conjugates [2].

If (S,f) is an n-quasigroup and $\sigma\in S_{n+1}$, then the n-quasigroup (Q,f^σ) defined by

$$f^\sigma(\{x_{\sigma(i)}\}_{i=1}^n)=x_{\sigma(n+1)}\Longleftrightarrow f(x_1^n)=x_{n+1}$$

is called a *σ-conjugate* (or simply *conjugate*) of f. A conjugate (Stein [19]) is also called *parastrophe* (after A. Sade [18]), the later is also used in Russian literature (Belousov, [1], [2], [3]).

Let f, g, h be n-ary quasigroup operations defined on the same set Q. If h is a conjugate of g and g is a conjugate of f, then h is a conjugate of f. If $f^\sigma = g$ and $h = g^\tau$, then $h = (f^\sigma)^\tau = f^{\sigma\tau}$.

If $f = f^\sigma$, then (Q, f) is called *σ-permutable.* If $H \subseteq S_{n+1}$ and $f = f^\sigma$ for all $\sigma \in H$, then (Q, f) is called *H-permutable.* H-permutable quasigroups are also called *conjugate invariant quasigroups.*

The set H of all $\sigma \in S_{n+1}$ such that $f = f^\sigma$ is a subgroup of S_{n+1} which is denoted by $\Pi(f)$. A H-permutable n-quasigroup (Q, f) such that $H = \Pi(f)$ is called *exactly H-permutable* n-quasigroup.

An n-quasigroup (Q, f) is called *totally symmetric* (TS) if (Q, f) is S_{n+1}-permutable, *alternating symmetric* (AS) if it is A_{n+1}-permutable ([21], [28]) and *cyclic* if it is C_{n+1}-permutable, where C_{n+1} is a cyclic subgroup of S_{n+1} generated by the cycle $(12\dots n+1)$ ([20]). Binary quasigroups which are σ-permutable for different values of σ are commutative quasigroups, semisymmetric quasigroups (satisfying the identity $(xy)y = y$), totally symmetric quasigroups, quasigroups satisfying Sade's left "key's" law (x(xy)=y) and Sade's right "key's" law ((xy)y=x) [7].

For each subgroup H of S_{n+1} we define $\Lambda(H)$, the spectrum of H, to be the set of all positive integers q for which there exists an n-quasigroup (Q, f) of order q with $\Pi(f) = H$.

4. H-permutable n-groupoids

Although for arbitrary n-groupoids conjugates can not be always defined, the definition of σ-permutability can be extended to n-groupoids.

Definition 1. Let $\sigma \in Q_{n+1}$. An n-groupoid (Q, f) is *σ-permutable* if for all $x_{x+1} \in S$

$$f(x_1^n) = x_{n+1} \Longleftrightarrow f(\{x_{\sigma(i)}\}_{i=1}^n) = x_{\sigma(n+1)}.$$

As before, the set of all $\sigma \in S_{n+1}$ for which an n-groupoid is σ-permutable is a subgroup of S_{n+1}. If $H \subseteq S_{n+1}$, and an n-groupoid (S, f) is σ-permutable for all $\sigma \in H$, then it is H-permutable.

Let (Q, f) be an n-groupoid, H a subgroup of S_{n+1} and Γ a set of generators of H. It is not difficult to see that f is H-permutable if and only if f is σ-permutable for every $\sigma \in \Gamma$.

Theorem 1. [22] *Let H be a nontrivial subgroup of the symmetric group S_{n+1}. Every H-permutable n-groupoid is an n-quasigroup if and only if H is a transitive permutation group.*

Proof. If H is a transitive subgroup of S_{n+1}, then it is easy to see that every H-permutable n-groupoid is an n-quasigroup.

Now we assume that H is not a transitive subgroup of S_{n+1}. If for every $k \in \mathbb{N}_{n+1}$, there exists $\sigma \in H$ such that $\sigma k = n+1$, then H must be transitive. Hence there exists $k \in \mathbb{N}_{n+1}$ such that there is no permutation in H which maps k to $n+1$.

Let $P = \{\sigma(k) \mid \sigma \in H\}$ and $R = \mathbb{N}_{n+1} \backslash P$ and let $(Q,+)$ be a nontrivial commutative group. If we denote $P = \{a_1, \dots, a_i\}$, $R = \{b_1, \dots, b_m\}$, $b_m = n+1$, and if $a \in Q$ is an arbitrary element, then we define an n-groupoid (Q,f) by

$$f(x_1^n) = -x_{b_1} - \cdots - x_{b_{m-1}} + a.$$

Now we shall show that f is an H-permutable n-groupoid which is not an n-quasigroup. Since $|P| \geqslant 1$, f is not an n-quasigroup. If for some $\sigma \in H$ and some $a_j \in P$, $\sigma(a_j) = b_s$, then since there exists $\tau \in H$ such that $\tau(k) = a_j$, it follows $\sigma\tau(k) = b_s$, which is a contradiction. Hence for every $\sigma \in H$ and every $x \in P$, $\sigma(x) \in P$. Also for every $\sigma \in H$ and every $y \in R$, $\sigma(y) \in R$ (since $\sigma(b_p) = a_q$ implies $\sigma^{-1}(a_q) = b_p$, and that case was considered earlier). So, (Q,f) is an H-permutable n-groupoid. □

A question of the existence of exactly H-permutable n-quasigroups for different subgroups H of S_{n+1} is considered in [16] where the existence of such quasigroups for some composite orders is established:

Theorem 2. [16] *For every $m > n$, $p \geqslant 2$, and every subgroup H of S_{n+1} there exists a H-permutable n-quasigroups of order mp, such that $H = \Pi(f)$.*

Proof. Let M and P be finite Abelian groups of orders m and p, respectively. We construct an n-quasigroup f on $Q = M \times P$ as follows: Choose $n+1$ distinct elements $a_1, a_2, \dots, a_{n+1}$ in M, choose a pair b, c of distinct elements from P, and let $s = a_1 + a_2 + \cdots + a_{n+1}$.

Now let $x_1, x_2, \dots, x_{n+1} \in M$, $y_1, y_2, \dots, y_{n+1} \in P$. We define

$$f((x_1,y_1),(x_2,y_2),\dots,(x_n,y_n)) = (x_{n+1},y_{n+1})$$

iff the following two conditions hold:

(1) $x_1 + x_2 + \cdots + x_{n+1} = s$,

(2) if for some $\sigma \in H$, $(x_1, x_2, \dots, x_{n+1}) = (a_{\sigma(1)}, a_{\sigma(2)}, \dots, a_{\sigma(n+1)})$, then $y_1 + y_2 + \cdots + y_{n+1} = b$. Otherwise, $y_1 + y_2 + \cdots + y_{n+1} = c$. It is easy to check that (Q,f) is an n-quasigroup such that $\Pi(f) = H$. □

In [16] the following conjecture was made:

For each subgroup H of S_{n+1}, $\Lambda(H)$ consists of all but finitely many positive integers.

Some constructions of exactly H-permutable n-quasigroups of prime orders were given in [22], which can be easily extended to some composite orders.

Theorem 3. [22] *Let H be a subgroup of S_{n+1}. If there exist disjoint sets $R_1, \dots, R_k \in \mathbb{N}_{n+1}$ such that for every $\sigma \in H$, $\sigma(R_i) = R_i$, $i = 1, \dots, k$, for every $x \in \mathbb{N}_{n+1} \setminus (R_1 \cup \dots \cup R_k)$, $\sigma(x) = x$, and H contains all permutations from S_{n+1} with the given properties, then there exists an H-permutable n-quasigroup (Q, f) of order p, where $p > n+1$ is any prime, such that $\Pi(f) = H$.*

In [22] the spectrum of cyclic n-quasigroups (Q, f) ([20]) with the property that $\Pi(f) = C_{n+1}$, where C_{n+1} a subgroup of S_{n+1} generated by the cycle $(12 \dots n+1)$, was investigated.

5. Steiner and Mendelsohn systems

H-permutable n-quasigroups are closely related to some combinatorial structures. First we shall consider binary case. It is well known that finite idempotent TS and semisymmetric quasigroups are equivalent to STSs and MTSs, respectively ([6], [14]).

Let $(Q, *)$ be a finite idempotent TS quasigroup. If we define

$$T = \{\{x, y, x * y\} \mid x, y \in Q,\ x \neq y\},$$

then (Q, T) is a STS, Conversely, if (Q, T) is a STS, then if we define a binary operation * on Q for all $x, y \in Q$, $x \neq y$, by

$$x * y = z \iff \{x, y, z\} \in T,$$

and

$$x * x = x,$$

then $(Q, *)$ is an idempotent TS quasigroup.

This is not the only way of turning quasigroups into STSs and vice versa. It can be shown analogously that idempotent TS loops of order $v+1$ are equivalent to STS of order v.

MTS are also equivalent to a class of H-permutable quasigroups. If (Q,T) is a MTS, and if we define a binary operation * on Q by

$$x * y = z \iff (x,y) \in \langle x,y,z\rangle,\ x \neq y,$$

and $x * x = x$ for all $x \in Q$, we get an idempotent quasigroup $(Q,*)$ such that $* = *^{(123)}$. Conversely, if $(Q,*)$ is a finite idempotent quasigroup and $* = *^{(123)}$, then (Q,T) where

$$T = \{\langle x,y,x*y\rangle \mid x,y \in Q,\ x \neq y\}$$

is a MTS. Here the quasigroup $(Q,*)$ is H-permutable, where H is a cyclic subgroup of S_3 generated by (123) (semisymmetric quasigroup).

Previous results can be naturally generalized to ternary case.

If (Q,f) is a finite ternary TS quasigroup, then by

$$T = \{\{x,y,z,f(x,y,z)\} \mid x,y,z \in Q, x \neq y \neq z \neq x\},$$

a SQS (Q,T) is defined.

If (Q,T) is an SQS and a ternary operation f is defined on Q for distinct elements $x,y,z \in Q$ by

$$f(x,y,z) = u \iff \{x,y,z,u\} \in T,$$

and $f(x,x,y) = f(x,y,x) = f(y,x,x) = y$ (*generalized idempotence* (GI)) otherwise, then (Q,f) is a GITS quasigroup.

MQS are also equivalent to a class of ternary quasigroups. If (Q,T) is a MQS, then if for distinct elements $x,y,z \in Q$ we define

$$f(x,y,z) = u \iff \langle x,y,z,u\rangle \in T$$

and $f(x,x,y) = f(x,y,x) = f(y,x,x) = y$ otherwise, we obtain a GI H-permutable ternary quasigroup (Q,f), where $H = \Gamma\{(1234)\}$. Conversely, if (Q,f) is a finite GI ternary H-quasigroup, where $H = \Gamma\{(1234)\}$, then by

$$T = \{\{x,y,z,f(x,y,z)\} \mid x,y,z \in Q, x \neq y \neq z \neq x\},$$

a MQS (Q,T) is defined.

6. Other quadruple systems

We have seen that finite idempotent S_3-permutable (TS) quasigroups and C_3-permutable (semisymmetric) quasigroups are equivalent to STSs and MTSs, respectively. This was naturally generalized to the ternary case, where finite GI S_4-permutable 3-quasigroups and GI C_4-permutable 3-quasigroups are equivalent to SQSs and MQSs, respectively. But in the ternary case besides these two classes of GI H-permutable 3-quasigroups, there exist many other GI H-permutable 3-quasigroups and to each such class of GI H-permutable 3-quasigroups a class of quadruple systems can be associated, analogously as it is done for Steiner and Mendelsohn quadruple systems.

Among these quadruple systems so called *tetrahedral quadruple systems* were first introduced and studied in [28] and they represent another generalization of MTSs.

Definition 2. Let Q be a finite set of v elements. A *directed quadruple* $\langle abcd\rangle$, where a, b, c, d are distinct elements of Q, is the following set of 12 ordered triples

$$\begin{array}{rcllll} \langle abcd\rangle & = & \{(abc), & (adb), & (acd), & (bdc), \\ & & (bca), & (dba), & (cda), & (dcb), \\ & & (cab), & (bad), & (dac), & (cbd)\}. \end{array}$$

Definition 3. A *tetrahedral quadruple system* (TQS) of order v is a pair (Q, T) where T is a collection of directed quadruples of elements of Q, such that every ordered triple of distinct elements of Q belongs to exactly one directed quadruple from Q.

Directed quadruples are obtained from 4-element subsets of Q by an orientation which can be represented by the following diagram (Figure 1). If the elements a, b, c, d of a directed quadruple $\langle abcd\rangle$ are represented as the vertices of the tetrahedron as in Figure 1, then the vertices of each face of the tetrahedron are cyclically ordered in positive direction observed from the interior of the tetrahedron.

So, TQSs can be considered as a 3-dimensional analogue of MTSs. If $\langle abc\rangle$ is a directed triple from an MTS, then the orientation of the pairs which belong to that triple is shown in Figure 2.

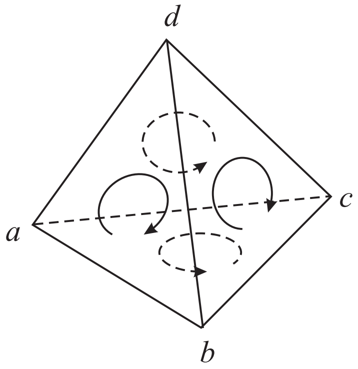

Figure 1.

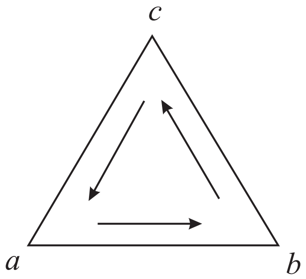

Figure 2.

That TQSs are a generalization of MTSs will follow from the algebraic characterization of TQS which will be given later.

Let (Q,T) be a TQS of order v. We define a ternary operation f on Q. If (abc) is an ordered triple of distinct elements from Q, then it belongs to exactly one directed quadruple from T. If d is the fourth element in that quadruple, then we define $f(a,b,c)=d$. If for all $x,y\in Q$ $f(x,x,y)=f(x,y,x)=f(y,x,x)=y$ then (Q,f) is a GIAS-3-quasigroup.

Now let (Q,f) be a finite GIAS-3-quasigroup. Let (abc) be an ordered triple of distinct elements of Q and $f(a,b,c)=d$. Suppose $d\in\{a,b,c\}$, say $d=a$, then since (Q,f) is AS, $f(a,b,c)=d$ implies $f(a,a,b)=c$ and since (Q,f) is GI we get $c=a$ which is a contradiction. Hence $d\notin\{a,b,c\}$.

Now, for every ordered triple (abc) of distinct elements from Q, we define a directed quadruple $\langle abcf(a,b,c)\rangle$ and denote by T the family of such directed quadruples. Since (Q,f) is AS, it follows that for every four distinct elements $a,b,c,d\in Q$ such that $\langle abcd\rangle\in T$

$$\begin{aligned}&\langle abcd\rangle=\langle bcad\rangle=\langle cabd\rangle=\\=&\langle adbc\rangle=\langle dbac\rangle=\langle badc\rangle=\\=&\langle acdb\rangle=\langle cdab\rangle=\langle dacb\rangle=\\=&\langle bdca\rangle=\langle dcba\rangle=\langle cbda\rangle.\end{aligned}$$

This means that every ordered triple of distinct elements from Q belongs to exactly one directed quadruple from T, hence (Q,T) is a TQS.

We have seen that TQSs are equivalent to GIAS-3-quasigroups, but since in the binary case the alternating subgroup A_3 of the symmetric group S_3 is in fact cyclic group C_3, it follows that TQSs are a generalization of MTSs.

The spectrum of TQSs was determined in [28], [15] where it was proved that the spectrum consists of all $n \equiv 1, 2, 4, 5, 8, 10 \pmod{12}$.

Similarly, we can define quadruple systems for other subgroups H of S_4. In [30] the spectrum of GI H-permutable 3-quasigroups where H is D_4 (the dihedral group), K_4 (Klein group) and $\Gamma\{(13)(24)\}$ was determined. The spectrum $\Lambda(D_4) = \{1\} \cup \{2n \mid n \in \mathbb{N}\}$ and $\Lambda(K_4)$ consists of all $n \equiv 0, 1, 2$ (mod 4).

7. Identities

It is easy to see that Definition 1 can be given in another equivalent form.

Definition 4. Let $\sigma \in Q_{n+1}$. If $\sigma(k) = n+1$ for some $k \in \mathbb{N}_n$, then an n-groupoid (Q, f) is *σ-permutable* if for all $x_1^{n+1} \in Q$

$$f(\{x_{\sigma(i)}\}_{i=1}^{k-1}, f(x_1^n), \{x_{\sigma(i)}\}_{i=k+1}^{n}) = x_{\sigma(n+1)}.$$

If $\sigma(n+1) = n+1$, then (Q, f) is *σ-permutable* if for all $x_1^{n+1} \in S$

$$f(\{x_{\sigma(i)}\}_{i=1}^{n}) = f(x_1^n).$$

We see that the class of all H-permutable n-groupoids is a variety.

When applied to n-quasigroups, this definition is equivalent to the previously given definition of σ-permutability.

Consequently, every H-permutable n-quasigroup can be defined as an n-quasigroup satisfying a system of identities.

For example, a 3-groupoid (Q, f) is a GIAS-3-quasigroups if and only if the following identities hold

$$\begin{cases} f(x, y, y) = x, \\ f(x, y, z) = f(y, z, x), \\ f(y, f(x, y, z), z) = x. \end{cases}$$

The second of the given identities is equivalent to $f = f^{(123)}$, and the third is equivalent to $f = f^{(124)}$. $\Gamma\{(123), (124)\}$ is a generating set of the group A_4, hence (Q, f) is a GIAS-3-quasigroup.

Besides identities obtained from the equality of conjugates $f = f^{\sigma}$, some other identities can be also used to define varieties of H-permutable n-groupoids. A question is what is the minimal set of identities in a base of such variety. It can be shown that many of these varieties are single based [8], [9], [27], [24].

For example, the following two theorems ([24]) show that the varieties of GI-C_4-permutable 3-groupiods and GI-S_4-permutable 3-groupoids (which are necessarily 3-quasigroups and in the finte case are equivalent to MQSs and STQs, respectively) are single based.

Theorem 4. *A* 3*-groupoid* (Q,f) *is a GI-*C_4*-permutable* 3*-groupoid iff the following identity is satisfied*

$$f(f(x,y,f(u,f(v,v,f(p,q,f(f(z,t,t),p,q))),u)),x,y)=z. \tag{1}$$

Proof. The following notation will be used. If (Q,f) is a 3-groupoid, then the translation maps $T_1(a,b)$, $T_2(a,b)$, $T_3(a,b)$ are defined by

$$T_1(y,z)(x)=T_2(x,z)(y)=T_3(x,y)(z)=f(x,y,z).$$

If (Q,f) is a GI-C_4-permutable 3-groupoid, then it is easy to see that (1) is satisfied.

Now, let (Q,f) be a 3-groupoid such that (1) is valid. Since a 3-groupoid (Q,f) is a GI-C_4-permutable iff the following identities are satisfied

$$f(f(x,y,z),x,y)=z, \tag{2}$$

$$f(x,x,y)=y, \tag{3}$$

we shall prove that (1) implies (2) and (3).

(1) can be written by

$$T_1(x,y)T_3(x,y)T_2(u,u)T_3(v,v)T_3(p,q)T_1(p,q)T_1(t,t)=I, \tag{4}$$

where I is the identity mapping of Q. From (4) we get that $T_1(t,t)$ is $1-1$ and $T_1(x,y)$ is onto, hence for all $t\in Q$ $T_1(t,t)$ is a bijection, which implies

$$T_1(x,y)T_3(x,y)T_2(u,u)T_3(v,v)T_3(p,q)T_1(p,q)=T_1^{-1}(t,t).$$

The last equality implies that $T_1(x,y)$ is a bijection and

$$T_3(x,y)T_2(u,u)T_3(v,v)T_3(p,q)=T_1^{-1}(x,y)T_1^{-1}(t,t)T_1^{-1}(p,q).$$

By the similar argument we obtain that $T_3(x,y)$ is a bijection for all $x,y\in Q$, which gives

$$T_2(u,u)=T_3^{-1}(x,y)T_1^{-1}(x,y)T_1^{-1}(t,t)T_1^{-1}(p,q)T_3^{-1}(p,q)T_3^{-1}(v,v).$$

Hence $T_2(u,u)$ is a bijection for all $u \in Q$.

From (4) we get that for all $x,y,u,v,p,q,t,r,s \in Q$

$$T_1(x,y)T_3(x,y)T_2(u,u)T_3(v,v)T_3(p,q)T_1(p,q)T_1(t,t) =$$

$$= T_1(r,s)T_3(r,s)T_2(u,u)T_3(v,v)T_3(p,q)T_1(p,q)T_1(t,t),$$

and

$$T_1(x,y)T_3(x,y) = T_1(r,s)T_3(r,s),$$

that is,

$$f(f(x,y,z),x,y) = f(f(r,s,z),r,s). \tag{5}$$

By an analogous procedure it follows that for all $x,y \in Q$

$$T_i(x,x) = T_i(y,y), \quad i = 1,2,3,$$

that is,

$$f(z,x,x) = f(z,y,y), \;\; f(x,z,x) = f(y,z,y), \;\; f(x,x,z) = f(y,y,z). \tag{6}$$

Putting in (6) $y = z$, one gets

$$f(z,x,x) = f(x,z,x) = f(x,x,z) = f(z,z,z). \tag{7}$$

If in (5) we put $x = f(z,z,z), \; y = r = s = z$, using (7) it follows

$$f(f(f(z,z,z),z,z),f(z,z,z),z) = f(f(z,z,z),z,z) = f(z,f(z,z,z),z).$$

Since $T_1(x,y)$ is a bijection from the preceding equality we get

$$f(f(z,z,z),z,z) = z. \tag{8}$$

If now we put in (5) $r = s = z$, it follows

$$f(f(x,y,z),x,y) = f(f(z,z,z),z,z) = z,$$

hence identity (2) is valid. So we have proved that for all $x,y \in Q$ $T_1(x,y)T_3(x,y) = I$. But identity (2) is equivalent to

$$f(x,y,f(z,x,y)) = z,$$

which means that for all $x,y \in Q \quad T_3(x,y)T_1(x,y) = I$. Therefore, (4) becomes

$$T_2(u,u)T_3(v,v)T_1(t,t) = I,$$

that is,

$$f(u,f(v,v,f(z,t,t)),u)=z.$$

Putting in the preceding identity $u=v=t=z$ and using (7) and (8) we get

$$f(z,z,z)=z,$$

which by (7) gives

$$f(z,x,x)=f(x,z,x)=f(x,x,z)=z. \qquad \square$$

Theorem 5. *A* 3*-groupoid* (Q,f) *is a GI-*S_4*-permutable* 3*-groupoid iff the following identity is satisfied*

$$f(f(x,y,f(u,f(v,v,f(p,q,f(f(z,t,t),q,p))),u)),x,y)=z. \tag{9}$$

These results can be extended to other GI-H-permutable 3-groupoids. In [27] it is proved that the variety of GI-H-permutable 3-groupoids can be defined by a single identity for every subgroup H of S_4 which contains at least one permutation σ such that $\sigma(4)\neq 4$.

8. Algebraic properties

Conjugate invariant quasigroups have many combinatorial applications, but it is also interesting to consider algebraic properties of these quasigroups. We shall illustrate some of these properties on GIAS-3-quasigroups [23]. We have seen that the class of all GIAS-3-groupoids is a variety, and every GIAS-3-groupoid is necessarily a GIAS-3-quasigroup.

Theorem 6. *Let* $\mathcal{U}=(Q;f)$ *be a GIAS-*3*-groupoid and let* $C(\mathcal{U})$ *be the congruence lattice of* $\mathcal{U}$*. Then*

a) *If* $\theta\in C(\mathcal{U})$*, then each* θ*-class is a subalgebra of* $\mathcal{U}$*,*

b) $\mathcal{U}$ *has permutable congruences,*

c) $\mathcal{U}$ *has regular congruences,*

d) $\mathcal{U}$ *has uniform congruences,*

e) $\mathcal{U}$ *has coherent congruences.*

Proof. a) Obvious.

b) Follows from Mal'cev's theorem (a variety has permutable congruences iff it has a ternary polynomial $f(x,y,z)$ such that $f(x,y,y)=$

$f(y,y,x)=x$).

c) Let $[a]\theta,\ \theta\in C(\mathcal{U})$, be a θ-class. If $x\equiv y\ (\theta)$ then $f(x,y,a)\equiv f(y,y,a)\ (\theta)$, hence $a\equiv f(x,y,a)\ (\theta)$. Conversely, if $a\equiv f(x,y,a)\ (\theta)$, then $f(a,x,a)\equiv f(f(x,y,a),x,a)\ (\theta)$ and since $\mathcal{U}$ is AS $f(f(x,y,a),x,a)=y$, hence $x\equiv y\ (\theta)$. We have proved that for all $x,y\in Q$, $x\equiv y\ (\theta)$ iff $a\equiv f(x,y,a)\ (\theta)$, so one θ-class defines the whole congruence.

d) Let $\theta\in C(\mathcal{U}),\ a,b\in Q,\ a\not\equiv b\ (\theta)$. The mapping $\varphi:[a]\theta\rightarrow[b]\theta$ defined by $\varphi(x)=f(x,a,b)$ is a bijection. φ is obviously $1-1$, and if $y\in[b]\theta$, then $x=f(y,b,a)\in[a]\theta$ is such that $\varphi(x)=f(f(y,b,a),a,b)=y$.

e) Let $\mathcal{B}=(B;f)$ be a subalgebra of $\mathcal{U}$ which contains a congruence class $C=[a]\theta$. If we assume that there exist elements $p\in Q\backslash B,\quad q\in B\backslash C$, such that $p\equiv q\ (\theta)$, and if r is an arbitrary element from C, then since the mapping $f:[r]\theta\rightarrow[q]\theta$ defined by $x\mapsto f(x,r,q)$ is a bijection, it follows that there exist an element $r_1\in C$ such that $f(r_1,r,q)=p$. But, since $\mathcal{B}$ is a subalgebra, $p\in B$, which is a contradiction. Hence all elements congruent to an element of B belong to B, i.e. a subalgebra which contains a congruence class must be a union of congruence classes. □

We have proved that if a GIAS-3-groupoid has a nontrivial congruence, then that congruence is uniform and each congruence class is a subalgebra. Since factor algebra is also a GIAS-3-groupoid we have the following corollary.

Corollary 1. *A necessary condition that a finite GIAS-3-groupoid of order v has nontrivial congruences, is that $v\equiv v_1v_2$, where v_1,v_2 are integers greater than 1 such that $v_1,v_2\equiv 1,2,4,5,8,10\ (mod\ 12)$.*

In [13] Fraser and Horn studied varieties V with the property that for every $\mathcal{A},\mathcal{B}\in V$ each congruence θ of $\mathcal{A}\times\mathcal{B}$ is a product congruence $\theta_1\times\theta_2$. A variety V of algebras has the Fraser-Horn property if for every $\mathcal{A},\mathcal{B}\in V$ all congruences of $\mathcal{A}\times\mathcal{B}$ are product congruences. A congruence of a direct product which is not a product congruence is called skew.

Theorem 7. *A variety of GIAS-3-groupoids does not have the Fraser-Horn property.*

Proof. In [17] it is proved that the variety which coordinatizes Steiner quadruple systems has a skew congruence. Since this variety is a subvariety of the variety V of all GIAS-3-groupoids, it follows that V does not have the Fraser-Horn property. □

Using a theorem of Birkhoff ([5]) which states that if every algebra from a variety has permutable congruences and singleton subalgebras, then every finite algebra from that variety has a decomposition into a direct product of directly irreducible algebras which is unique up to isomorphism of the factors and up to their sequence, by Theorem 6 we get the next theorem.

Theorem 8. *Each finite GIAS-3-groupoid has a decomposition into a direct product of directly irreducible factors which is unique up to isomorphism of the factors and up to their sequence.*

9. H-permutable n-groups

Various classes of H-permutable n-groups were considered in [11], [12], [21], [29], [26]. Here we shall describe some of them.

Theorem 9. *Let (Q,f) be an n-group. (Q,f) is AS iff there exists an Abelian group $(Q,+)$ such that $x=-x$ for all $x\in Q$, and*

$$f(x_1^n)=\sum_1^n x_i+c,$$

where c is a fixed element from Q.

Proof. Let (Q,f) be an AS-n-group. Then by Hosszú-Gluskin theorem there exist a group $(Q,\cdot)$, its automorphism θ and an element $c\in Q$ such that

$$f(x_1^n)=x_1\theta x_2\theta^2x_3\dots\theta^{n-1}x_nc,$$

where $\theta c=c$ and for all $x\in Q$ $\theta^{n-1}x=cxc^{-1}$. f is AS, hence $f=f^\sigma$, where $\sigma=(1,2,n+1)$, and the following identity is valid

$$f(x_2,f(x_1^n),x_3^n)=x_1,$$

that is

$$x_2\theta(x_1\theta x_2\theta^2x_3\dots\theta^{n-1}x_nc)\theta^2x_3\dots\theta^{n-1}x_nc=x_1. \qquad (10)$$

If we put in the preceding equality $x_1=e$, $i=1,\dots,n$, where e is the unit of $(Q,\cdot)$, we get that $c^2=e$. Now putting in (10) $x_i=e$, $i=1,\dots,n$, it follows $\theta x_1=x_1$, i. e. θ is the identity mapping of Q. If in (10) we put $x_1=e$, $i=1,3,\dots,n$, we obtain $\theta^2x_2=x_2^{-1}$ which means that for all $x\in Q$, $x=x^{-1}$. Hence $(Q,\cdot)$ is an Abelian group and

$$f(x_1^n)=x_1x_2\dots x_nc.$$

The converse part of the theorem is obvious. □

Since the group $(Q,\cdot)$ such that $x = x^{-1}$ for all $x \in Q$ is of order 2^t, $t \in \mathbb{N}$, and for every $t \in \mathbb{N}$ there exists such group of order 2^t, we have the following corollary.

Corollary 2. *There exists a nontrivial finite AS-n-group (Q, f) of order q iff $q = 2^t$, $t \in \mathbb{N}$.*

Cyclic n-groups have similar structure. Some properties of such n-groups are given in the following theorems ([29]).

Theorem 10. *Let (Q, f) be an (i, j)-associative cyclic n-quasigroup, where $j - i$ is relatively prime to n. Then (Q, f) is an n-group.*

Theorem 11. *Let (Q, f) be an n-group, where $n = 2k$, $k \in \mathbb{N}$. (Q, f) is cyclic iff there exists an Abelian group $(Q, +)$ such that $x = -x$ for all $x \in Q$, and*

$$f(x_1^n) = \sum_1^n x_i + c,$$

where c is a fixed element from Q.

Theorem 12. *Let (Q, f) be an n-group, where $n = 2k + 1$, $k \in \mathbb{N}$. (Q, f) is cyclic iff there exists an Abelian group $(Q, +)$ such that*

$$f(x_1^n) = x_1 - x_2 + x_3 - \cdots + x_n + c, \tag{11}$$

where $c = -c$ is a fixed element from Q.

Corollary 3. *When n is even, there exists a nontrivial finite cyclic n-group (Q, f) of order q iff $q = 2^t$, $t \in \mathbb{N}$. When n is odd, a nontrivial finite cyclic n-group (Q, f) of order q exists for every $q \in \mathbb{N}$ and every such group is represented by* (11).

Further investigation of H-permutable n-groups is done in [26] where some necessary and sufficient conditions for an n-group to be σ-permutable are determined and several conditions under which such n-groups are derived from binary groups are given.

10. Other applications

We have described some properties of conjugate invariant quasigroups, but there are many other applications of such quasigroup which could not be presented here. For example, orthogonality of quasigroup conjugates have been extensively investigated, a survey of that research can be found in [4]. Close to that are permutable orthogonal arrays, some classes of graphs, codes and other structures.

References

[1] **V. D. Belousov**: *Fundations of the theory of quasigroups and loops*, (Russian), Nauka, Moscow, 1967.

[2] **V. D. Belousov**: *n-ary quasigroups*, (Russian), Sţiinţa, Kishinev, 1972.

[3] **V. D. Belousov**: *Parastrophic-orthogonal quasigroups*, Quasigroups and Related Systems **13** (2005), 25−72 (translation from the Russian preprint edited by Acad. Nauk Moldav. SSR, Inst. Mat. s Vychisl. Tsentrom, Kishinev, 1983).

[4] **F. E. Bennett and L. Zhu**: *Conjugate-orthogonal Latin squares and related structures*, in: Contemporary Design Theory: A Collection of Surveys, (J.H. Dinitz and D. R. Stinson, eds.), John Wiley, New York, (1992), 41 – 96.

[5] **G. Birkhoff**: *Lattice theory*, 3rd edition, Amer. Math. Soc. Colloquium Publications, Vol. XXV, 1967.

[6] **R. H. Bruck**: *A survey of binary systems*, Berlin, 1958.

[7] **J. Dénes and A. D. Keedwell**: *Latin squares and their applications*, Akadémiai Kiado, Budapest and Academic Press, New York, 1974.

[8] **D. Donovan**: *Single laws for two subvarieties of squags*, Bull. Austral. Math. Soc. **42** (1990), 157 – 165.

[9] **D. Donovan and S. Oates-Williams**: *Single laws for sloops and squags*, Discrete Math. **92** (1991), 79 – 83.

[10] **W. A. Dudek**: *Remarks on alternating symmetric n-quasigroups*, Univ. u Novom Sadu, Zb. Rad. Prirod.-Mat. Fak. Ser. Mat. **15.2** (1985), 67 – 78.

[11] **W. A. Dudek and Z. Stojaković**: *On σ-permutable n-groupoids*, Univ. u Novom Sadu, Zb. Rad. Prirod.-Mat. Fak. Ser. Mat. **15.1** (1985), 189 – 198.

[12] **W. A. Dudek and Z. Stojakovic**: *Permutable n-groups*, Beiträge zur Algebra und Geometrie **27** (1988), 129 – 140.

[13] **G. A. Fraser and A. Horn**: *Congruence relations in direct products*, Proc. Amer. Math. Soc. **26** (1970), 390 – 394.

[14] **B. Ganter and H. Werner**: *Co-ordinatizing Steiner systems*, Annals Discr. Math. **7** (1980), 3 – 24.

[15] **A. Hartman and K. T. Phelps**: *Tetrahedral quadruple systems*, Utilitas Math. **37** (1990), 181 – 189.

[16] **D. G. Hoffman**: *On the spectrum of n-quasigroups with given conjugate invariant subgroup*, J. Combin. Theory Ser. **A 35** (1983), 98 – 99.

[17] **M. J. de Resmini**: *On congruences on Steiner ternary algebras. A class of resolvable SQS's*, Boletino U.M.I. (5) **17-A** (1980), 74 – 81.

[18] **A. Sade**: *Quasigroupes parastrophiques. Expressions et identités*, Math. Nachr. **20** (1959), 73 – 106.

[19] **S. K. Stein**: *On the foundations of quasigroups*, Trans. Amer. Math. Soc. **85** (1957), 228 – 256.

[20] **Z. Stojaković**: *Cyclic n-quasigroups*, Univ. u Novom Sadu, Zb. Rad. Prirod.-Mat. Fak. Ser. Mat. **12** (1982), 407 – 415.

[21] **Z. Stojaković**: *Alternating symmetric n-quasigroups*, Univ. u Novom Sadu, Zb. Rad. Prirod.-Mat. Fak. Ser. Mat. **18** (1983), 259 – 272.

[22] **Z. Stojaković**: *On some classes of permutable n-groupoids and n-quasigroups*, Univ. u Novom Sadu, Zb. Rad. Prirod.-Mat. Fak. Ser. Mat. **18.1** (1988), 157 – 162.

[23] **Z. Stojaković**: *On an algebraic equivalent of tetrahedral quadruple systems*, Demonstratio Math. **27** (1994), 733 – 740.

[24] **Z. Stojaković**: *Single identities for Mendelsohn and Steiner 3-quasigroups*, Bull. Austral. Math. Soc. **53** (1996), 419 – 424.

[25] **Z. Stojaković and W. A. Dudek**: *Permutable n-groupoids*, Univ. u Novom Sadu, Zb. Rad. Prirod.-Mat. Fak. Ser. Mat. **14.2** (1984), 155 – 166.

[26] **Z. Stojaković and W. A. Dudek**: *On σ-permutable n-groups*, Publ. Inst. Math **40(54)** (1986), 49 – 55.

[27] **Z. Stojaković and W. A. Dudek**: *Single identities for varieties equivalent to quadruple systems*, Discrete Math. **183** (1998), 277 – 284.

[28] **Z. Stojaković and R. Madaras**: *On tetrahedral quadruple systems*, Utilitas Math. **29** (1986), 19 – 26.

[29] **Z. Stojaković and Dj. Paunić**: *On a class of n-groups*, Univ. u Novom Sadu, Zb. Rad. Prirod.-Mat. Fak. Ser. Mat. **14.2** (1984), 147 – 154.

[30] **L. Teirlinck**: *Generalized idempotent orthogonal arrays*, in: Coding Theory and Design Theory, Part II: Design Theory , D. Ray-Chaudhury (ed.), IMA Vol.Math. Appl. 21, Springer 1990, 368 – 378.

Received September 5, 2005

W. A. Dudek
Institute of Mathematics and Computer Science, Wroclaw University of Technology,
Wyb. Wyspiańskiego 27, 50-370 Wroclaw, Poland
e-mail: dudek@im.pwr.wroc.pl

Z. Stojaković
Institute of Mathematics, University of Novi Sad, Trg. Obradovića 4,
21 000 Novi Sad, Serbia and Montenegro
e-mail: stojakov@ns.sbb.co.yu