On groupoids with identity $x(xy) = y$

Lidija Goračinova-Ilieva, Smile Markovski,
Ana Sokolova

Abstract

The groupoid identity $x(xy) = y$ appears in defining several classes of groupoids, such as Steiner's loops which are closely related to Steiner's triple systems, the class of cancellative groupoids with property $(2,5)$, Boolean groups, and groupoids which exhibit orthogonality of quasigroups. Its dual identity is one of the defining identities for the variety of quasigroups corresponding to strongly 2-perfect m-cycle systems. In this paper we consider the following varieties of groupoids: $\mathcal{V} = Var(x(xy) = y)$, $\mathcal{V}_c = Var(x(xy) = y,\ xy = yx)$, $\mathcal{V}_u = Var(x(xy) = y,\ (xy)y = xy)$, $\mathcal{V}_i = Var(x(xy) = y,\ (xy)y = yx)$. Suitable canonical constructions of free objects in each of these varieties are given and several other structural properties are presented. Some problems of enumeration of groupoids are also resolved. It is shown that each $\mathcal{V}_i$-groupoid defines a Steiner quintuple system and vice versa, implying existence of Steiner quintuple systems of enough large finite cardinality.

AMS mathematics subject classification (2000): 20N02, 20N05, 08B20, 51E10

Key words: design, groupoid, identity, free object, quasigroup, Steiner system, variety

1 Preliminaries

A groupoid is a pair $(G, \cdot)$ consisting of a nonempty set G and a binary operation $\cdot$ on G. Some well known classes of groupoids are semigroups Sem i.e. groupoids satisfying the identity $x(yz) = (xy)z$, commutative groupoids Com with the identity $xy = yx$, groupoids with unit Un (satisfying the law $(\exists x)(\forall y)yx = xy = y$), etc. We note that some of these classes are defined by identities, i.e. they are varieties of groupoids. The class Un is not a variety, but it is functionally equivalent ([10]) to the variety of groupoids determined by the identities $xe = ex = x$, where e is a nullary operation. For that reason we will think of Un as being a variety.

In this paper we are mainly interested in varieties of groupoids satisfying the identity $x(xy) = y$ and we consider the following varieties: $\mathcal{V} = Var(x(xy) = y)$, $\mathcal{V}_e = \mathcal{V} \cap Un$ (with extended signature), $\mathcal{V}_c = \mathcal{V} \cap Com$, $\mathcal{V}_u = Var(x(xy) = y,\ (xy)y = xy)$, $\mathcal{V}_i = Var(x(xy) = y,\ (xy)y = yx)$. Suitable constructions of free objects in each of these varieties and several other structural properties and properties of freeness are presented in next sections. The variety $\mathcal{V}_{cs} = Var(x(xy) = y,\ xy = yx,\ x(yz) = (xy)z)$ is the variety of Boolean groups (i.e. elementary 2-Abelian groups). Several results on this variety as well as the variety $\mathcal{V}_{sem} = Var(x(xy) = y,\ x(yz) = (xy)z)$ are presented in [8].

In the sequel $B \neq \emptyset$ will be an arbitrary set and T_B will denote the set of all groupoid terms over B in signature $\cdot$. T_B is the absolutely free groupoid with (free) base B where the operation is defined by $(u, v) \mapsto uv$. Length $|u|$ of an element $u \in T_B$ is defined inductively by:

$$u \in B \implies |u| = 1, \quad u = xy \implies |u| = |x| + |y|.$$

Let $\mathcal{B}(T_B)$ be the boolean of T_B, i.e. the set of all subsets of T_B. We define inductively a mapping $P : T_B \to \mathcal{B}(T_B)$ by:

$$t \in B \implies P(t) = \{t\}, \qquad t = t_1t_2 \implies P(t) = \{t\} \cup P(t_1) \cup P(t_2).$$

For instance, $P((xy)(xz)) = \{x, y, z, xy, xz, (xy)(xz)\}$ for $x, y, z \in B$.

The cardinal number of a base of a free groupoid F is said to be the rank of F.

2 Variety $\mathcal{V}$

Free objects in $\mathcal{V}$ are defined in [4]. Here we state another description.

Let $F = \{t \in T_B \mid (\forall u, v \in T_B)\ u \cdot uv \notin P(t)\}$. Then for all $u, v \in F$ we have $uv \notin F \Leftrightarrow (\exists w \in T_B)\ v = uw)$. Define an operation $*$ on F by

$$u * v = \begin{cases} uv & uv \in F \\ w & v = uw \text{ for some } w \in F \end{cases}$$

for each $u, v \in F$. The product $u * v$ is well defined since $v = uw_1 = uw_2$ implies $w_1 = w_2$ in the absolutely free groupoid T_B.

Theorem 1 *$(F, *)$ is a free groupoid in the variety $\mathcal{V}$ with free base B.*

□

Theorem 2 *Every subgroupoid $(G, *)$ of $(F, *)$ is free as well.*

Proof We show that the set $R = (B \cap G) \cup \{uv \in G | \{u, v\} \not\subseteq G\}$ is a free base of $(G, *)$.

First, by induction on length of terms we show that R is nonempty and generating for G. Let $t \in G$ such that $|t| = min\{|s| \mid s \in G\}$. If $t \in B$, then $t \in R$. If $t = uv$, then $|u| < |t|, |v| < |t|$, so $\{u, v\} \not\subseteq G$. Hence $t \in R$. Let $uv \in G$. If $\{u, v\} \not\subseteq G$ then $uv \in R$, else $uv = u * v$ and by inductive hypothesis is generated by R.

Let $(H, \circ) \in \mathcal{V}$ and let $f : R \longrightarrow H$ be a mapping. Define a mapping $\hat{f} : G \longrightarrow H$ by

$$\hat{f}(t) = \begin{cases} f(t) & t \in R \\ \hat{f}(u) \circ \hat{f}(v) & t = uv,\ u, v \in G \end{cases}$$

Let $u, v \in G$. If $uv \in G$, then $\hat{f}(u * v) = \hat{f}(uv) = \hat{f}(u) \circ \hat{f}(v)$. Otherwise, if $v = uw$, then $\hat{f}(u * v) = \hat{f}(w) = \hat{f}(u) \circ (\hat{f}(u) \circ \hat{f}(w)) = \hat{f}(u) \circ \hat{f}(uw) = \hat{f}(u) \circ \hat{f}(v)$. □

Hence, the class of free objects in $\mathcal{V}$ is hereditary.

We next give two simple properties concerning the rank of a subgroupoid of a free $\mathcal{V}$-groupoid and the number of all $\mathcal{V}$-groupoids on a finite set.

Proposition 1 *Every free $\mathcal{V}$-groupoid F contains a subgroupoid with an infinite rank.*

Proof Let b be an arbitrary element of the free base of F. Then the subgroupoid G of F generated by the set $\{c_i \mid i \in \mathbb{N}\}$, where $c_0 = bb, c_{i+1} = (c_i b)b$ has an infinite rank. □

Further on we will use the following lemma.

Lemma 1 *The number of permutations whose disjoint cycles representation consists of cycles of length at most 2 on a set with n elements is*

$$\sum_{k=0}^{[\frac{n}{2}]} \frac{n!}{2^k k!(n-2k)!}$$

Proof Consider a permutation of the wanted type with f fixed elements and k disjoint cycles of length 2. Then $n = f + 2k$ and $0 \leq k \leq [\frac{n}{2}]$. The fixed elements can be chosen on $\binom{n}{n-2k}$ ways. It can be proved by induction that the number of different disjoint cycles of length 2 that can be made over a set with $2k$ elements is $(2k-1)!!$. So, given k, there are $\binom{n}{n-2k}(2k-1)!! = \frac{n!}{2^k k!(n-2k)!}$ such permutations. □

Proposition 2 *The number of different $\mathcal{V}$-groupoids on a set with n elements is* $\left(\sum_{k=0}^{[\frac{n}{2}]} \frac{n!}{2^k k!(n-2k)!}\right)^n$.

Proof Let G be a $\mathcal{V}$-groupoid of cardinality n. Note that $xy = z \implies xz = y$ holds in G and G is left-cancellative, so each row in the multiplication table of G can be considered as a permutation on the set G whose disjoint cycles representation consists of cycles of length at most 2. The number of such permutations is ordered by Lemma 1, and there are n rows in the multiplication table of G. $\square$

For example, there are 64 $\mathcal{V}$-groupoids on the set $\{1, 2, 3\}$, and they can be obtained by suitable arrangements of the strings 123, 132, 321 and 213 as rows of their multiplication tables. Here we have that the corresponding permutations are (1)(2)(3), (1)(23), (13)(2) and (12)(3).

3 Variety $\mathcal{V}_e$

The variety $\mathcal{V}_e$ consists of all $\mathcal{V}$-groupoids with unit. Note that each groupoid in this variety is involutory i.e. $x^2 = e$ is its identity. So, we can use the free object F from $\mathcal{V}$ to obtain a free object in $\mathcal{V}_e$. Namely, let $e \notin F$ and let $F_e = \{t \in F \mid (\forall u \in T_B)\ u^2 \notin P(t)\} \cup \{e\}$. Define an operation $*$ on F_e by

$$e * u = u * e = u, \quad e * e = e,$$

$$u * v = \begin{cases} uv & uv \in F_e \\ e & u = v \\ w & v = uw,\ w \in F_e \end{cases}$$

where $u, v \in F_e \setminus \{e\}$.

Theorem 3 *$(F_e, *, e)$ is a free groupoid in $\mathcal{V}_e$ with a free base B.*

Proof One can check that $F_e \in \mathcal{V}_e$. B is a generating set of F_e since B generates F and $b * b = e$, for each $b \in B \neq \emptyset$. Given $(G, \circ, 1) \in \mathcal{V}_e$ and a mapping $f : B \to G$, in an inductive way we extend it to a homomorphism $\hat{f} : F_e \to G$ as follows: $\hat{f}(e) = 1$, $\hat{f}(b) = f(b)$ for $b \in B$, and $\hat{f}(xy) = \hat{f}(x) \circ \hat{f}(y)$. $\square$

Theorem 4 *Every subgroupoid of $(F_e, *, e)$ is free as well.* $\square$

The proof of this theorem is similar to the proof of Theorem 2. Namely, given a subgroupoid $(G, *, e)$ of $(F_e, *, e)$, if $|G| = 1$ then $G = \{e\}$ is free with empty base, and if $|G| > 1$ then we define the set R as before. $R \neq \emptyset$ since it contains the elements t such that $|t| = min\{|s| \mid s \in G,\ s \neq e\}$. Now, the proof follows the same lines as the proof of Theorem 2.

If the rank of F_e is 1, then F_e is a two-element groupoid. Therefore, the corresponding property of Theorem 3 for the variety $\mathcal{V}_e$ can be stated as follows.

Proposition 3 *Every free $\mathcal{V}_e$-groupoid F_e with a rank greater than one, contains a subgroupoid with an infinite rank.*

Proof Let B be the free base of F_e, $a, b \in B,\ a \neq b$. Then the subgroupoid of F_e generated by the set $\{c_i \mid i \in \mathbb{N}\}$, where $c_0 = ab,\ c_{i+1} = (c_i b)b$ has an infinite rank. □

Proposition 4 *The number of different $\mathcal{V}_e$-groupoids on a set with n elements, $n > 1$, is* $$n\left(\sum_{k=0}^{[\frac{n}{2}]-1} \frac{(n-2)!}{2^k k!(n-2-2k)!}\right)^{n-1}.$$

Proof If G is a $\mathcal{V}_e$-groupoid with unit e, then $x \cdot x = e$ and $x \cdot e = x$, for each $x \in G$. So, in the multiplication table of G, the row for the unit e is uniquely defined, and in the row of any other element $x \neq e$ there are two fixed elements, obtained from $x \cdot x = e$ and $x \cdot e = x$. The remaining $n-2$ elements in the row of x correspond to a permutation of order $n-2$ whose disjoint cycles representation consists of cycles of length at most 2. The total number of such permutations is ordered by Lemma 1, there are $n-1$ rows that should be suitably fulfilled, and there are n ways a unit to be chosen. □

For example, exactly 32 distinct $\mathcal{V}_e$-groupoids can be constructed over the set $\{1, 2, 3, 4\}$. Fix a unit, for instance 1. Then, in the multiplication table of the groupoid, the row and the column for 1 are determined, and on the main diagonal it is only 1. The row for 2 can be completed by choosing the elements 3 and 4 in two different ways (corresponding to the permutation (3)(4) or the permutation (34)), and so on.

4 Variety $\mathcal{V}_c$

In this section we focus on the variety $\mathcal{V}_c$ containing all $\mathcal{V}$ commutative groupoids.

Proposition 5 *Any two of the identities* $x \cdot xy = y,\ yx \cdot x = y,\ xy = yx$ *imply the third one.*

Proof Let $x{\cdot}xy = y$ and $yx{\cdot}x = y$ hold. Then $xy = y(y{\cdot}xy) = y((x{\cdot}xy){\cdot}xy) = yx$. $\square$

Hence, $\mathcal{V}_c$ can be defined by any two of the preceding three identities, and we have that the groupoids in $\mathcal{V}_c$ are TS-quasigroups (totally symmetric quasigroups [3]). Further on we describe the free objects in this variety with base B.

Let $(G, \cdot)$ be a groupoid. For $x, y, z = xy \in G$, we say that x and y are divisors of z. An element is prime if it has no divisors.

Proposition 6 ([2]) *A groupoid* $(C, \cdot)$ *is a free commutative groupoid with free base* B *if and only if*

- (i) $(\forall x, y, t, u \in C)(xy = tu \implies \{x, y\} = \{t, u\})$;
- (ii) B *is the set of primes in* $(C, \cdot)$ *and it generates* $(C, \cdot)$. $\square$

Let $(C, \cdot)$ denote the free commutative groupoid with base B and $F_c = \{t \in C \mid (\forall u, v \in C)\ u(uv) \notin P_c(t)\}$, where the mapping $P_c : C \to \mathcal{B}(C)$ is defined inductively by: $t \in B \Rightarrow P_c(t) = \{t\},\quad t = uv \Rightarrow P_c(t) = \{t\} \cup P_c(u) \cup P_c(v)$. P_c is well defined by Proposition 6(i). Define an operation $*$ on F_c in the following way:

$$u * v = \begin{cases} uv & uv \in F_c \\ w & v = uw \text{ or } u = vw \text{ in } (C, \cdot) \end{cases}$$

Theorem 5 $(F_c, *)$ *is a free groupoid in the variety* $\mathcal{V}_c$ *with a free base* B.

Proof Let $u, v \in F_c$ and $u{\cdot}v \notin F_c$. Then $u{*}v = w$ for some $w \in P_c(u) \cup P_c(v)$ and since $y \in P_c(x) \wedge x \in F_c \implies y \in F_c$, we get $u{*}v \in F_c$. Therefore $(F_c, *)$ is a groupoid and it is commutative by construction. Also, for $u, v \in F_c$, if $u * v = uv$ then $u * (u * v) = v$. If $u * v = w,\ v = uw$ (or $u = vw$) in $(C, \cdot)$ then $u * (u * v) = u * w = uw = v$ (or $u * (u * v) = vw * (vw * v) = vw * w = v$). Hence, $(F_c, *) \in \mathcal{V}_c$.

If $(G, \circ)$ is a $\mathcal{V}_c$-groupoid and $f : B \to G$ a mapping, let $\hat{f} : C \to G$ be the homomorphism that extends f, i.e. $\hat{f}|_B = f$. Then $\hat{f}|_{F_c}$ is a homomorphism from F_c to G that extends f. $\square$

By using similar ideas as in the proofs of Theorem 2 and Theorem 4, it can be proved that the property of freeness in $\mathcal{V}_c$ is hereditary too:

Theorem 6 *Each subgroupoid of a free* $\mathcal{V}_c$*-groupoid is free as well.* $\square$

Proposition 7 *Every free $\mathcal{V}_c$-groupoid contains a subgroupoid with infinite rank.*

Proof Define terms $b^{<n>}$ inductively in the following way: $b^{<0>} = b,\ b^{<k+1>} = b^{<k>} \cdot b^{<k>}$. If b is a base element of a free $\mathcal{V}_c$-groupoid, then the subgroupoid generated by the set $\{c_i \mid i \in \mathbb{N}\}$, where $c_0 = b^{<1>},\ c_{i+1} = b^{<i+1>} \cdot b$ has an infinite rank. $\square$

Let G be a subgroupoid of a free $\mathcal{V}_c$-groupoid and let t be one of its elements with minimal length. Since $\{t^{<n>} \mid n \in \mathbb{N}\}$ is an infinite set, we conclude that every subgroupoid of a free groupoid in $\mathcal{V}_c$ is infinite as well. The same construction can be applied for $\mathcal{V}$ too, i.e. every subgroupoid of a free $\mathcal{V}$-groupoid is not finite.

The problem concerning the enumeration of all TS-quasigroups defined on n-element set remains open.

Example 1 Let $(G, \cdot)$ be a commutative group and define an operation $*$ on G by $\quad x * y = cx^{-1}y^{-1},\ c \in G$. Then $(G, *) \in \mathcal{V}_c$.

Example 2 The following 5-element quasigroup is a TS-quasigroup which can not be obtained by the construction given in example 1.

	0	1	2	3	4
0	0	2	1	4	3
1	2	3	0	1	4
2	1	0	4	3	2
3	4	1	3	2	0
4	3	4	2	0	1

Note that $\mathcal{V}_c \cap Un$ is in fact the variety of Steiner's loops. For constructions of free objects in that variety and some related topics the reader is referred to [5, 6].

5 Variety $\mathcal{V}_u$

We now consider the variety $\mathcal{V}_u$ defined by the identities $x(xy) = y,\ (xy)y = xy$. As it will soon become clear, its groupoids have very simple structure.

Proposition 8 $\mathcal{V}_u = Var(xy = y^2,\ x^2 \cdot x^2 = x)$

Proof By definition $\mathcal{V}_u = Var(x \cdot xy = y,\ xy \cdot y = xy)$ so we get first (1) $xy \cdot xy = xy \cdot (xy \cdot y) = y$ and then (2) $y \cdot xy = (xy \cdot xy) \cdot xy = xy \cdot xy = y$. Now (1) and (2) give $xy = (y \cdot xy)(y \cdot xy) = y^2$, and (1) gives $x^2 \cdot x^2 = x$.

On the other hand, $xy = y^2,\ x^2 \cdot x^2 = x$ first imply $x \cdot xy = x \cdot y^2 = y^2 \cdot y^2 = y$ and after that $yx = yx \cdot (yx \cdot yx) = yx \cdot (x^2 \cdot x^2) = yx \cdot x$. □

As a consequence of the previous proposition we get that in the variety $\mathcal{V}_u$ despite of $xy = y^2$ and $x^2 \cdot x^2 = x$, the following identities hold: $x^2 \cdot y = y^2,\ x \cdot y^2 = y,\ x^2 \cdot y^2 = y$. (Namely, $x \cdot y^2 = x \cdot xy = y \implies x^2 \cdot y^2 = y \implies x^2 \cdot y = x^2 \cdot (x^2 \cdot y^2) = y^2$.)

Note that $x^2 = x$ is not an identity, since $(\{0,1\}, *) \in \mathcal{V}_u$ where $0 * 0 = 1 * 0 = 1,\ 0 * 1 = 1 * 1 = 0$.

Let $F_u = \{b, b^2 \mid b \in B\}$ and define an operation $*$ on F_u by $u * b = b^2,\ u * b^2 = b$ for all $b \in B, u \in F_u$. Then we have:

Theorem 7 *$(F_u, *)$ is a free groupoid with free base B in $\mathcal{V}_u$.* □

As a result from the last theorem we get that any free groupoid in $\mathcal{V}_u$ with finite base of cardinality n is itself finite and of order $2n$.

Theorem 8 *Every subgroupoid of a free groupoid in $\mathcal{V}_u$ is free too.*

Proof Let G be a subgroupoid of a free $\mathcal{V}_u$-groupoid F_u and $B_1 = B \cap G$, where B is the free base of F_u. Since $a \in G \subseteq F_u$ imply either $a = b$ or $a = b^2$ for some $b \in B$, and $y^2 \cdot y^2 = y$ is an identity in $\mathcal{V}_u$, it follows that $G \setminus B_1 = \{b^2 \mid b \in B_1\}$. Hence, G is free in $\mathcal{V}_u$ with free base B_1. □

Hence, any subgroupoid of the free groupoid with base B coincides with the free groupoid with some base $B_1 \subseteq B$ and we get the following corollary.

Corollary 1 *Let $|B| = n$. Then the number of all subgroupoids of a free groupoid of $\mathcal{V}_u$ with base B is $2^n - 1$.* □

Since finite $\mathcal{V}_u$-groupoids are exactly those $\mathcal{V}$-groupoids which rows in its multiplication tables are identical and all elements in a row are different ($x^2 = y^2 \Rightarrow x = y$ in $\mathcal{V}_u$), by Lemma 1 we get that the number of different $\mathcal{V}_u$-groupoids defined on a set with n elements is $\displaystyle\sum_{k=0}^{[\frac{n}{2}]} \frac{n!}{2^k k!(n-2k)!}$.

6 Variety $\mathcal{V}_i$

The variety $\mathcal{V}_i$ is an interesting one, because its finite members are closely connected with the Steiner quintuple systems. Here firstly we give a description of the free objects in $\mathcal{V}_i$, and after that we discuss some aspects of the mentioned connection with Steiner quintuple systems.

Proposition 9 *Besides the defining identities*
(1) $x \cdot xy = y$ *and* *(2)* $yx \cdot x = xy$
the following identities hold in $\mathcal{V}_i$*:*

$$\begin{array}{llll}
(3) & xy \cdot x = x \cdot yx & (8) & x(yx \cdot y) = yx \\
(4) & xx = x & (9) & yx \cdot y = x \cdot yx \\
(5) & xy \cdot yx = y & (10) & xy \cdot (x \cdot yx) = x \\
(6) & (xy \cdot x)x = y & (11) & (xy \cdot x) \cdot xy = yx \\
(7) & (xy \cdot x)y = x & (12) & (xy \cdot x) \cdot yx = xy
\end{array}$$

as well as the cancellation laws and anticommutativity.

Proof For any x, y in a $\mathcal{V}_i$ - groupoid we have

(3) $xy \cdot x \overset{(2)}{=} (yx \cdot x)x \overset{(2)}{=} x \cdot yx$;
(4) $xx \overset{(2)}{=} xx \cdot x \overset{(3)}{=} x \cdot xx \overset{(1)}{=} x$;
(5) $xy \cdot yx \overset{(2)}{=} xy \cdot (xy \cdot y) \overset{(1)}{=} y$;
(6) $(xy \cdot x)x \overset{(2)}{=} x \cdot xy \overset{(1)}{=} y$;
(7) $(xy \cdot x)y \overset{(6)}{=} (xy \cdot x)((xy \cdot x)x) \overset{(1)}{=} x$;
(8) $x(yx \cdot y) \overset{(1)}{=} (y \cdot yx)(yx \cdot y) \overset{(5)}{=} yx$;
(9) $yx \cdot y \overset{(1)}{=} x(x(yx \cdot y)) \overset{(8)}{=} x \cdot yx$;
(10) $xy \cdot (x \cdot yx) \overset{(3)}{=} xy \cdot (xy \cdot x) \overset{(1)}{=} x$;
(11) $(xy \cdot x) \cdot xy \overset{(3)}{=} xy \cdot (x \cdot xy) \overset{(1)}{=} xy \cdot y \overset{(2)}{=} yx$;
(12) $(xy \cdot x) \cdot yx \overset{(3,9)}{=} (yx \cdot y) \cdot yx \overset{(3)}{=} yx \cdot (y \cdot yx) \overset{(1)}{=} yx \cdot x \overset{(2)}{=} xy$.

Also

$$\begin{array}{lll}
xy = xz & \Longrightarrow & y = x \cdot xy = x \cdot xz = z, \\
yx = zx & \Longrightarrow & xy = yx \cdot x = zx \cdot x = xz, \\
xy = yx & \Longrightarrow & y = x \cdot xy = x \cdot yx \overset{(3,9)}{=} y \cdot xy = y \cdot yx = x.
\end{array}$$ □

From (1), (6) and the cancellation laws we have:

Corollary 2 *Any groupoid in* $\mathcal{V}_i$ *is a quasigroup.* □

Note that in any groupoid of $\mathcal{V}_i$ we have $x \cdot yx = xy \cdot x = yx \cdot y = y \cdot xy$ by (3) and (9). Let α be the congruence on T_B generated by the preceding equalities. We denote by uvu the class $u(vu)/\alpha$ and use the same operation symbol for T_B/α as we did for T_B. Also, we shall sometimes continue using the notions "term" and "subterm" for the elements of T_B/α.

Let $F_i \subseteq T_B/\alpha$ be the set of all terms that do not contain as a subterm a left-hand side of $(i) - (viii)$:

(i)	$ss = s$	(v)	$s \cdot sts = ts$
(ii)	$s \cdot st = t$	(vi)	$st \cdot sts = s$
(iii)	$st \cdot t = ts$	(vii)	$sts \cdot s = t$
(iv)	$st \cdot ts = t$	$(viii)$	$sts \cdot st = ts$

where $s, t \in T_B$.

The next proposition justifies the definition of the set F_i as well as the use of the notions "term" and "subterm".

Proposition 10 *If the term $u(vu) \in T_B$ for some $u, v \in T_B$ does not contain as a subterm a term of the following forms: ss, $s \cdot st$, $st \cdot t$, $st \cdot ts$, $s \cdot s(ts)$, $s \cdot (st)s$, $s \cdot (ts)t$, $s \cdot t(st)$, $st \cdot s(ts)$, $st \cdot (st)s$, $st \cdot (ts)t$, $st \cdot t(st)$, $(st)s \cdot s$, $s(ts) \cdot s$, $t(st) \cdot s$, $(ts)t \cdot s$, $(st)s \cdot st$, $s(ts) \cdot st$, $t(st) \cdot st$, $(ts)t \cdot st$, then the same holds for the terms $(uv)u$, $(vu)v$ and $v(uv)$.*

Proof By checking all the possibilities it is easy to see that $(vu)v$ does not contain such a subterm. Namely, each assumption that the term has such a subterm, means that the term is of the given form (having in mind that the statement holds for u, v and vu) which always leads to contradiction for u, v, vu or $u(vu)$. For instance, $(vu)v = (st)s \cdot st \implies u(vu) = s \cdot (st)s$. In the same way, it can be shown in all the cases for uv and then finally for $v(uv)$ as well. $\square$

Define an operation $*$ on F_i in the following way. For $u, v \in F_i$, if $uv \in F_i$ then $u * v = uv$. Otherwise, if uv has the form of a left-hand side of some of (i) - $(viii)$ define $u * v$ to be the corresponding right-hand side of the identity, except in the case of (iii) i.e. when $u = wv$, then we put $u * v = v * w$. It can be shown, by induction on length of terms, that $*$ is well defined. Note that, by the previous proposition if $sts \in F_i$ then also $ts \in F_i$.

Theorem 9 *$(F_i, *)$ is free in $\mathcal{V}_i$ with free base B.*

Proof First, we show that $(F_i, *)$ satisfies (1). Let $u, v \in F_i$. If $uv \in F_i$ then $u * (u * v) = u * (uv) \overset{(ii)}{=} v$. Otherwise, we consider several cases.

(i') $u = v : u * (u * v) = u * (u * u) \overset{(i)}{=} u * u \overset{(i)}{=} u = v$;

(ii') $v = ut : u * (u * v) = u * (u * ut) \overset{(ii)}{=} u * t = ut = v$;

(iii') $u = tv$ and

0. $vt \in F_i : u * (u * v) = tv * (tv * v) \overset{(iii)}{=} tv * (v * t) = tv * vt \overset{(iv)}{=} v$;

1. $v = t$ is impossible case since we would have $u = tv = tt \notin F_i$;

2. $t = vp : u * (u * v) = tv * (v * t) = vpv * (v * vp) \overset{(ii)}{=} pvp * p \overset{(vii)}{=} v$;

3. $v = pt : u*(u*v) = tv*(v*t) = tpt*(pt*t) = tpt*(t*p) = tpt*tp \overset{(viii)}{=} pt = v$;

4. $v = qs,\ t = sq$; 5. $t = vpv$; 6. $v = pq,\ t = pqp$; 7. $v = tpt$; 8. $v = pqp,\ t = pq$.

All the cases 4.-8. are impossible since they lead to $u = sq \cdot qs,\ u = vpv \cdot v,\ u = pqp \cdot pq,\ u = t \cdot tpt,\ u = pq \cdot pqp$, respectively, contradicting $u \in F_i$.

$(iv')\ u = tp, v = pt : u * (u * v) = tp * (tp * pt) \overset{(ii)}{=} tp * p \overset{(iv)}{=} p * t = pt = v$;

$(v')\ v = utu : u * (u * v) = u * (u * utu) \overset{(v)}{=} u * tu = utu = v$;

$(vi')\ u = tp, v = tpt : u * (u * v) = tp * (tp * tpt) \overset{(vi)}{=} tp * t = tpt = v$;

$(vii')\ u = vtv : u * (u * v) = vtv * (vtv * v) \overset{(vii)}{=} vtv * t = v$;

$(viii')\ u = tpt, v = tp : u * (u * v) = tpt * (tpt * pt) = tpt * pt = tp = v$.

So we have shown that $(F_i, *)$ satisfies (1) and continue for (2). If $u, v \in F_i$ and $u * v = uv \in F_i$, then $(u * v) * v = uv * v = v * u$. Otherwise, we have the cases:

$(i'')\ u = v : (u * v) * v = (u * u) * u = u * u = v * u$;

$(ii'')\ v = ut$, and in this case $tut \in F_i$ i.e. no other case is possible and we get $(u * v) * v = (u * ut) * ut = t * ut = tut = utu = ut * u = v * u$;

$(iii'')\ u = tv : (u * v) * v = (tv * v) * v = (v * t) * v$ and there are several possibilities:

0. $vt \in F_i (vtv \in F_i) : (u * v) * v = vt * v = vtv = v * u$;

1. $v = t$ is impossible case;

2. $t = vp : (u * v) * v = (v * t) * v = (v * vp) * v = p * v = pv$ since $u = tv = vpv \in F_i$, so $pv \in F_i$, and on the other hand $v * u = v * vpv = pv$;

3. $v = pt : (u * v) * v = (v * t) * v = (pt * t) * pt = (t * p) * pt$ and since $u = tv = tpt \in F_i$ also $tp \in F_i$ and $(t * p) * pt = tp * pt = p$ and $v * u = pt * tpt = p$;

4. $v = pq,\ t = qp$; 5. $t = vpv$; 6. $v = pq,\ t = pqp$; 7. $v = tpt$; 8. $v = pqp,\ t = pq$.

All the cases 4.-8. are impossible.

$(iv'')\ u = pt, v = tp : (u * v) * v = (pt * tp) * tp = t * tp = p = tp * pt = v * u$;

$(v'')\ v = upu : (u * v) * v = (u * upu) * upu = pu * upu = p = upu * u = v * u$;

$(vi'')\ u = pt, v = ptp : (u*v)*v = (pt*ptp)*ptp = p*ptp = tp = ptp*pt = v*u$;

$(vii'')\ u = vpv : (u * v) * v = (vpv * v) * v = p * v = pv = v * vpv = v * u$;

$(viii'')\ u = ptp, v = pt : (u*v)*v = (ptp*pt)*pt = tp*pt = p = pt*ptp = v*u$.

Thus we have shown that $F_i \in \mathcal{V}_i$.

By induction on length of terms one can show that B is a base for F_i. Namely, $B \subseteq F_i$ and if $uv \in F_i$ then $uv = u * v$ is generated by B if u and v are.

Let $(G, \circ) \in \mathcal{V}_i$ and $f : B \to G$. Define a mapping $\hat{f} : F_i \to G$ inductively by $\hat{f}(b) = f(b), b \in B$ and $\hat{f}(uv) = \hat{f}(u) \circ \hat{f}(v)$ for $uv \in F_i \setminus B$. We show that $\hat{f}$ is a homomorphism and an extension of f. If $u, v \in F_i$ and $uv \in F_i$ the statement is clear by definition of $\hat{f}$. Otherwise one of the same eight cases might occur. We check here only the third case when $u = tv$, because the others can be checked as earlier. Now, $\hat{f}(u * v) = \hat{f}(tv * v) = \hat{f}(v * t)$ which by induction on length of u equals to $\hat{f}(v) \circ \hat{f}(t) = (\hat{f}(t) \circ \hat{f}(v)) \circ \hat{f}(v) = \hat{f}(tv) \circ \hat{f}(v) = \hat{f}(u) \circ \hat{f}(v)$. $\square$

Note that $|B| = 1 \implies |F_i| = 1$ and $|B| = 2 \implies |F_i| = 5$. It is clear that in each $\mathcal{V}_i$-groupoid every two distinct elements generate a subgroupoid with five elements. In fact, $\mathcal{V}_i$ is the class of cancellative groupoids with property (2,5) ([11]). (A class K is said to have the property (k, n) if every algebra in K generated by k distinct elements has exactly n elements.)

Let $(G, \cdot)$ belongs to $\mathcal{V}_i$ and define a groupoid by $x * y = yx,\ x, y \in G$. It is easy to verify that the quasigroup $(G, *)$ is an orthogonal mate of G.

Let F_i be a free groupoid in $\mathcal{V}_i$, such that its free base contains three distinct elements a, b, c. Then the subgroupoid of F_i generated by the set $\{d_i \mid i \in \mathbb{N}\}$, where $d_0 = ab$ and $d_{3i+1} = (d_{3i} \cdot c)a,\ d_{3i+2} = (d_{3i+1} \cdot b)c,\ d_{3i+3} = (d_{3i+2} \cdot a)b$, for $i \in \mathbb{N}$, has an infinite rank. Hence, we get the following result.

Proposition 11 *Every free $\mathcal{V}_i$-groupoid with rank greater than two has a subgroupoid with an infinite rank.* $\square$

So, unlike the free $\mathcal{V}_i$-groupoids with rank one or two, the free $\mathcal{V}_i$-groupoids with rank greater than two are infinite. Also, apart from the groupoids of the previous varieties, there is no $\mathcal{V}_i$-groupoid with $n \leq 20$ elements, $n \neq 1, 5$. Here we present the table of a $\mathcal{V}_i$-groupoid with 21 elements.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
0	0	2	1	4	3	6	5	8	7	12	15	18	9	14	13	10	17	16	11	20	19
1	3	1	4	0	2	9	15	16	17	5	11	10	18	19	20	6	7	8	12	13	14
2	4	3	2	1	0	14	10	11	16	18	6	7	17	20	5	19	8	12	9	15	13
3	2	4	0	3	1	20	19	14	13	17	18	15	16	8	7	11	12	9	10	6	5
4	1	0	3	2	4	13	11	20	10	15	8	6	19	5	16	9	14	18	17	12	7
5	7	10	15	16	17	5	8	0	6	11	1	9	20	18	19	2	3	4	13	14	12
6	8	12	13	9	16	7	6	5	0	3	20	14	1	2	11	18	4	19	15	17	10
7	6	13	12	10	9	8	0	7	5	4	3	17	2	1	18	20	19	11	14	16	15
8	5	14	18	11	19	0	7	6	8	16	12	3	10	15	1	13	9	20	2	4	17
9	13	11	8	19	20	10	17	15	2	9	5	1	14	0	12	7	18	6	16	3	4
10	16	9	20	14	12	11	13	18	19	1	10	5	4	6	3	17	0	15	7	8	2
11	19	5	17	13	14	1	16	12	15	10	9	11	7	3	4	8	6	2	20	0	18
12	14	15	11	5	8	3	18	17	4	13	19	2	12	9	0	1	20	7	6	10	16
13	12	16	10	15	18	17	20	19	11	14	2	8	0	13	9	3	1	5	4	7	6
14	9	17	19	18	6	15	4	10	20	0	7	16	13	12	14	5	11	1	3	2	8
15	17	18	14	8	7	19	12	4	3	20	16	13	6	11	2	15	10	0	1	5	9
16	15	19	9	20	11	12	14	13	18	2	17	4	5	7	6	0	16	10	8	1	3
17	10	20	7	6	13	18	3	2	14	19	0	12	11	4	8	16	15	17	5	9	1
18	20	6	16	7	5	4	1	3	9	8	14	19	15	17	10	12	2	13	18	11	0
19	18	7	5	17	10	2	9	1	12	6	4	20	8	16	15	14	13	3	0	19	11
20	11	8	6	12	15	16	2	9	1	7	13	0	3	10	17	4	4	15	19	18	20

The most interesting characteristic of the $\mathcal{V}_i$ variety is due to its (2,5) property and reflects the connection between $\mathcal{V}_i$ and the Steiner quintuple systems.

Let $(Q,\cdot)$ be an n-element quasigroup in $\mathcal{V}_i$. Consider the set $\hat{Q} = \{K \mid (K,\cdot) \text{ is a 5-element subquasigroup of } (Q,\cdot)\}$. It follows by the (2,5) property that for any two elements $a, b \in Q$ there exists a unique K in $\hat{Q}$ such that $a, b \in K$. Hence, $\hat{Q}$ is a 2-(n,5,1) design, i.e. a Steiner quintuple system.

Example 3 From the preceding 21-element quasigroup we have the following Steiner quintuple system:

$\{0,1,2,3,4\}$,

$\{0,5,6,7,8\}$, $\{0,9,12,13,14\}$, $\{0,10,15,16,17\}$, $\{0,11,18,19,20\}$,

$\{1,5,9,10,11\}$, $\{1,6,12,15,18\}$, $\{1,7,13,16,19\}$, $\{1,8,14,17,20\}$,

$\{2,5,14,15,19\}$, $\{2,6,10,13,20\}$, $\{2,7,11,12,17\}$, $\{2,8,9,16,18\}$,

$\{3,5,12,16,20\}$, $\{3,6,9,17,19\}$, $\{3,7,10,14,18\}$, $\{3,8,11,13,15\}$,

$\{4,5,13,17,18\}$, $\{4,6,11,14,16\}$, $\{4,7,9,15,20\}$, $\{4,8,10,12,19\}$.

On the other hand, let $S = \{B_1, B_2, \ldots, B_k\}$ be a Steiner quintuple system. Clearly, for each $i \in \{1,2,\ldots,k\}$, a $\mathcal{V}_i$-quasigroup $(B_i, *_i)$ can be constructed. Now, put $Q = \bigcup B_i$ and $* = \cup *_i$. For arbitrary $a, b \in Q$ there is a unique i, such that a and b both belong to B_i. By the construction of $*$, $a * (a * b) = a *_i (a *_i b) = b$, and similarly the other identity can be checked, so $(Q, *)$ is in $\mathcal{V}_i$.

We have shown that every $\mathcal{V}_i$-quasigroup induces a Steiner quintuple system and vice versa. Note that the first procedure was deterministic, unlike the second one. Namely, on each 5-element set six different $\mathcal{V}_i$-quasigroups can be defined, which means that for one Steiner quintuple system $\{B_1, B_2, \ldots, B_k\}$, 6^k different $\mathcal{V}_i$-quasigroups can be constructed, in the way presented above. By the preceding discussion we have proved the following result.

Theorem 10 *Each n-element $\mathcal{V}_i$-quasigroup give rise to an n-element Steiner quintuple system, i.e. $2-(n,5,1)$ design, and each n-element Steiner quintuple system give rise to 6^n different n-element $\mathcal{V}_i$-quasigroups.* □

Let $(Q,\cdot)$ and $(Q', *)$ be isomorphic $\mathcal{V}_i$-quasigroups and S and S' be their corresponding Steiner quintuple systems. Let $f : Q \longrightarrow Q'$ be an isomorphism. Since f preserves subquasigroups and for any subquasigroup $(K', *)$ of

$(Q', *)$ there is a unique subquasigroup $(K, \cdot)$ of $(Q, \cdot)$ satisfying $f(K) = K'$, f is an isomorphism from S to S'.

For the opposite, let f be an isomorphism from a Steiner quintuple system $S = \{B_1, B_2, \ldots, B_k\}$ to a Steiner quintuple system $S' = \{B'_1, B'_2, \ldots, B'_k\}$ and $Q = \bigcup B_i$, $Q' = \bigcup B'_i$. Let $(Q, \cdot)$ be one of the quasigroups arising from S. Define an operation $*$ in Q' by

$$a * b = c \iff f^{-1}(a) \cdot f^{-1}(b) = f^{-1}(c.)$$

Then $(Q', *)$ is a quasigroup arising from S' and f is an isomorphism from $(Q, \cdot)$ to $(Q', *)$.

Denote by $\mathcal{FV}_i$ the class of all finite $\mathcal{V}_i$-quasigroups, and by $\mathcal{S}$ the class of all Steiner quintuple systems. An equivalence on $\mathcal{FV}_i$ can be defined by

$$(Q, \cdot) \ \alpha \ (Q', *) \iff \hat{Q} = \hat{Q}',$$

where $\hat{Q}$ is defined as before. The reasoning above leads us to the following result.

Theorem 11 *There is one to one correspondence between $\mathcal{FV}_i/\alpha$ and $\mathcal{S}$.* □

Corollary 3 *A necessary condition for existence of n-element $\mathcal{V}_i$-quasigroup is $n = 20k + 1$ or $n = 20k + 5$ for some nonnegative integer k.*

Proof Given an n-element $\mathcal{V}_i$-quasigroup, we construct an n-element Steiner quintuple with b blocks. Since there are $x = n(n-1)/2$ different pairs of elements and each block contains $y = 5 \cdot 4/2 = 10$ such pairs, we have $b = x/y = n(n-1)/20$. On the other hand, $n = 4m + 1$ where m is the number of occurrences of fixed element in the blocks. □

We do not know whether for each n such that $n = 20k+1$ or $n = 20k+5$ there exists an n-element $\mathcal{V}_i$-quasigroup.

Since a direct product of $\mathcal{V}_i$-quasigroups is a $\mathcal{V}_i$-quasigroup, we have possibility to construct Steiner quintuple systems of enough large finite cardinality. It follows from the next property:

Corollary 4 *The existence of n-element and m-element Steiner quintuple systems implies existence of nm-element Steiner quintuple system.* □

References

[1] **D. E. Bryant, S. Oates-Williams:** *Strongly 2-perfect cycle systems and their quasigroups*, Discrete Mathematics 167/168 (1997), 167-174

[2] **Ǵ. Čupona:** *Free commutative groupoids* (personal communication)

[3] **J. Denes, A. D. Keedwell:** *Latin Squares and their Applications*, English Univ. Press Ltd., London (1974)

[4] **J. Ježek:** *Free groupoids in varieties determined by a short equation*, Acta Universitatis Carolinae - Math. et Phys. Vol.23 $N_0$1 (1982), 3-24

[5] **S. Markovski, A. Sokolova:** *Free Steiner loops*, Glasnik Matematički, Vol 36(56) (2002), 85-93

[6] **S. Markovski, A. Sokolova:** *Term rewriting system for solving the word problem for Steiner's loops,* Bulletin Mathematique 24(L), Skopje (2000), 7-18

[7] **S. Markovski, L. Goračinova Ilieva, A. Sokolova:** *Free groupoids with the identity* $(xy)y = yx$, Proceed. 10^{th} Congress of Yugoslav Math., Belgrade, 21-24.01.2001, 173-176

[8] **S. Markovski, A. Sokolova, L. Goračinova Ilieva:** *On semigroups with the identity* $xxy = y$, Publ. de l'Institut Math., Nouvelle serie, tome 70(84) (2001), 1-8

[9] **S. Markovski, A. Sokolova, L. Goračinova Ilieva:** *On groupoid functional equation* $A(x, B(x, y)) = y$, On Tribute to 65^{th} Aniversary of Prof. S. B. Presic: A Krapez Ed., Beograd (2001), 84-88

[10] **R. N. McKenzie, W. F. Taylor, G. F. McNulty:** *Algebras, Lattices, Varieties*, Wadsworth & Brooks, Monterey, California (1987)

[11] **R. Padmanabhan:** *Characterization of a class of groupoids*, Algebra Universalis Vol. 1 (1972), 374-382

Address of the authors:

S. Markovski (contact person) and A. Sokolova,

Faculty of Sciences and Mathematics, Institute of Informatics, p.f.162 Skopje, Republic of Macedonia, e-mail: {smile,anas}@ii.edu.mk

Lidija Goračinova-Ilieva,

Pedagogical Faculty, Štip, Republic of Macedonia, e-mail: fildim@mt.net.mk