Quasigroups and Related Systems **13** (2005), 99 – 104

Amalgam of a loop over an idempotent quasigroup

Tuval Foguel

Abstract

In this paper we look at away of "gluing" n copies of a loop. This construction gives us a new loop that is a union of n copies of the original loop such that any two of this copies intersect trivially.

1. Introduction

We construct a new loop from n copies of a loop over an idempotent quasigrop of order n. This new loop is the union of n subloops that are isomorphic to the original loop such that any two of this copies intersect trivially. We will see that if we choose the idempotent quasigrop "curefully" some properties of the original loop are transferred in full or in a weaker version to the new loop. For example if the original loop was simple, then the new loop is simple, if the original loop was an n generator loop, then the new loop is $n+1$ generator.

We have used this construction in order to construct a family of loops with exactly one covering [3], and to power associative AT-loop which are not diassociative [4].

2. Preliminaries

In this section, we review a few necessary notions from loop theory, and establish some notation conventions.

A *magma* $(\mathcal{L},)$ consists of a set $\mathcal{L}$ together with a binary operation on $\mathcal{L}$. For $x \in \mathcal{L}$, define the left (resp., right) translation by x by $L(x)y = xy$ (resp., $R(x)y = yx$) for all $y \in \mathcal{L}$. A magma with all left and right

2000 Mathematics Subject Classification: 20N05
Keywords: loop, idempotent quasigroup.

translations bijective is called a *quasigroup*. A quasigroup $\mathcal{L}$ is an *idempotent quasigroup* if for any $x \in \mathcal{L}$, $xx = x$. A quasigroup $\mathcal{L}$ with a two-sided identity element 1 such that for any $x \in \mathcal{L}$, $x1 = 1x = x$ is called a *loop*. A loop $\mathcal{L}$ is *power-associative*, if for any $x \in \mathcal{L}$, the subloop generated by x is a group. A loop $\mathcal{L}$ is *diassociative*, if for any x and $y \in \mathcal{L}$, the subloop generated by x and y is a group. For basic facts about loops and quasigroups, we refer the reader to [1], [2], [5].

Notation 2.1. Given a loop $\mathcal{L}$ and $x \in \mathcal{L}$ we will denote the *left inverse* of x by x^λ (i.e. $x^\lambda x = 1$) and the *right inverse* by x^ρ (i.e. $xx^\rho = 1$) in the multiplicative notation, and in the additive notation *left inverse* of x by $(x-)$ (i.e. $(x-) + x = 1$) and the *right inverse* by $(-x)$ (i.e. $x + (-x) = 1$).

Definition 2.2. Given a loop $\mathcal{L}$, a subloop $\mathcal{K}$ is said to be *normal* if, for all $x, y \in \mathcal{L}$, $x(y\mathcal{K}) = (xy)\mathcal{K}$, $x\mathcal{K} = \mathcal{K}x$, and $(\mathcal{K}x)y = \mathcal{K}(xy)$ ([2], p. 60, IV.1).

These three conditions are clearly equivalent to the pair $x(\mathcal{K}y) = \mathcal{K}(xy)$ and $x(\mathcal{K}y) = (x\mathcal{K})y$ for all $x, y \in \mathcal{K}$.

3. The amalgam

In this section we construct the amalgam.

Definition 3.1. Given $(S, +, \cdot)$ where $(S, +)$ is a loop with identity 0 and $(S - \{0\} = S^*, \cdot)$ is a quasigroup, and an idempotent quasigroup $(Q, \odot)$. Let $\mathcal{L}^{(Q)}(S) = \{a_q(x) : x \in S^* \text{ and } q \in Q\} \cup \{\mathbf{1}\}$ (i.e. each element of the form $a_q(x)$ in this set is double indexed by q and x) and binary operations defined as follows:

i. For any $l \in \mathcal{L}^{(Q)}(S)$, $\mathbf{1}l = l\mathbf{1} = l$.

ii. For $x, y \in S^*$,

$$a_i(x)a_i(y) = \begin{cases} a_i(x+y) & \text{if } x + y \neq 0 \\ \mathbf{1} & \text{otherwise} \end{cases}$$

iii. For $x, y \in S^*$, $a_{q_1}(x)a_{q_2}(y) = a_{q_1 \odot q_2}(xy)$ for $q_1 \neq q_2$.

We will call Q the *basis* of $\mathcal{L}^{(Q)}(S)$.

Remark 3.2. For convenience we will also denote $\mathbf{1}$ by $a_q(0)$, and thus if $x + (-x) = 0$ we get $a_q(x)a_q((-x)) = a_q(0) = \mathbf{1}$.

Remark 3.3. $|Q| \geq 3$ since Q is an idempotent quasigroup.

Remark 3.4. Given a finite loop $\mathcal{L}$ with binary operation $+$ and identity 0, we can form $(S, +, \cdot)$ by letting $S = \mathcal{L}$ as a set, setting $(S, +) = (\mathcal{L}, +)$ and enumerating S^* and giving it a binary operation $\cdot$ of a cyclic group of order $|S^*|$.

Lemma 3.5. *$\mathcal{L}^{(Q)}(S)$ is a loop with identity* $\mathbf{1}$.

Proof. See Lemma 4.3 [3]. □

Remark 3.6. $\mathcal{L}^{(Q)}(S)$ is a union of proper subloops

$$A_q = \{a_q(x) : x \in S\} \cong (S, +),$$

where $q \in Q$, with $A_{q_1} \cap A_{q_2} = \{\mathbf{1}\}$ for $q_1 \neq q_2$.

Remark 3.7. If Q and S are finite, then $|\mathcal{L}^{(Q)}(S)| = |Q|(|S| - 1) + 1$.

Lemma 3.8. *If $(S, +)$ is a group, then $\mathcal{L}^{(Q)}(S)$ is a power associative loop with identity* $\mathbf{1}$.

Proof. See Lemma 4.6 [3]. □

Definition 3.9. ([4]) A loop $\mathcal{L}$ is an *associative transitive loop* (*AT-loop*), if given $x, y, z \in \mathcal{L} - \{1\}$ such that $\langle x, y\rangle$ and $\langle y, z\rangle$ are groups, then $\langle x, z\rangle$ is a group.

Remark 3.10. Every diassociative loop is an AT-loop.

Definition 3.11. ([4]) Given a loop $\mathcal{L}$ and a non-empty subset X of $\mathcal{L}$, then

$$DA_{\mathcal{L}}(X) = \{b \in \mathcal{L} : \langle x, b\rangle \text{ is a group for all } x \in X\}$$

Theorem 3.12. *$\mathcal{L}$ is an AT-loop if and only if $DA_{\mathcal{L}}(a)$ is a diassociative loop or empty for all $a \in \mathcal{L} - \{1\}$.*

Proof. See Theorem 3.4 [4]. □

Definition 3.13. Given a power associative loop $\mathcal{L}$ the exponent of $\mathcal{L}$ is the smallest non-negative integer n (if one exists) such that $x^n = 1$ for all $x \in \mathcal{L}$.

Theorem 3.14. *If $(S, +)$ is a diassociative loop of exponent $\neq 2$, then $\mathcal{L}^{(Q)}(S)$ is an AT-loop which is not diassociative.*

Proof. Let $\mathcal{L}^{(Q)}(S) = \mathcal{L}$. Given $a_i(x) \in \mathcal{L} - \{\mathbf{1}\}$, since $(S, +)$ is a diassociative loop, $A_i \subseteq DA_{\mathcal{L}}(a_i(x))$. Let $y \in S$ such that $y + y \neq 0$ and $j \in Q$, $j \neq i$, then

$$a_i(x)(a_j(y)a_j(y)) \neq (a_i(x)a_j(y))a_j(y).$$

So $A_i = DA_{\mathcal{L}}(a_i(x))$, and since $DA_{\mathcal{L}}(a_i(x)) \neq \mathcal{L}^{(Q)}(S)$, $\mathcal{L}^{(Q)}(S)$ is an AT-loop which is not diassociative. □

Definition 3.15. ([4]) A loop $\mathcal{L}$ is a *strong associative transitive loop* (*SAT-loop*), if $DA_{\mathcal{L}}(a)$ is a group or empty for all $a \in \mathcal{L} - \{1\}$. A loop $\mathcal{L}$ is a *weak associative transitive loop* (*WAT-loop*), if $DA_{\mathcal{L}}(a)$ is a loop or empty for all $a \in \mathcal{L} - \{1\}$.

Corollary 3.16. *If $(S, +)$ is a group of exponent $\neq 2$, then $\mathcal{L}^{(Q)}(S)$ is an SAT-loop which is not a group.*

4. The amalgam over a two-quasigroup basis

Definition 4.1. A quasigroup is *homogeneous* if its automorphism group is transitive. A quasigroup is *doubly homogeneous* if its automorphism group is doubly transitive. A *two-quasigroup* is a nontrivial two generated doubly homogeneous quasigroup.

Remark 4.2. If Q is a two-quasigroup, then it is generated as a quasigroup by any two distinct elements.

Lemma 4.3. *If p is a prime and n a positive integer, then there is a two-quasigroup with $|Q| = p^n$.*

Proof. See Lemma 5.3 [3]. □

Remark 4.4. Given $Q = GF(p^n)$ (the Galois field of p^n elements) where $p^n > 2$, and α a primitive element in $GF(p^n)$. Then $(Q, \odot)$ is a two-qusigroup under the binary operation

$$a \odot b = \alpha a + (1 - \alpha)b$$

for all $a, b \in Q$ is a two-quasigroup.

Remark 4.5. Given a two-quasigroup Q we will denote its elements by $\{0, 1, \dots\}$.

Theorem 4.6. *If $(Q, \odot)$ is a two-quasigroup and $(S^*, \cdot)$ a loop, then*

$$\mathcal{L}^{(Q)}(S) = \langle A_i, a_j(y) \rangle$$

for any $a_j(y) \in \mathcal{L}^{(Q)}(S) - \{A_i\}$.

Proof. Let $K = \langle A_i, a_j(y) \rangle$ and $k = i \odot j$, then $a_k(1) = a_i(y^\lambda)a_j(y) \in K$. Given $a_q(t) \in \mathcal{L}^{(Q)}(S)$ let $r \in Q$ be the unique element with $r \odot i = q$, r is a reduced word in i and k. Therefore $a_r(1) \in K$ and $a_r(1)a_i(t) = a_q(t) \in K$, thus $K = \mathcal{L}^{(Q)}(S)$. □

Corollary 4.7. *If $(S, +)$ an n generated loop, $(S^*, \cdot)$ a loop and $(Q, \odot)$ is a two-quasigroup, then $\mathcal{L}^{(Q)}(S)$ is an $n + 1$ generated loop.*

Theorem 4.8. *If $(S, +)$ is a simple loop, $(S^*, \cdot)$ a loop, $|S| > 2$ and $(Q, \odot)$ is a two-quasigroup, then $\mathcal{L}^{(Q)}(S)$ is simple.*

Proof. Let $\{\mathbf{1}\} \neq \mathcal{K}$ be a normal subloop of $\mathcal{L}^{(Q)}(S)$. Then there exist $a_i(1) \in \mathcal{K} - \{\mathbf{1}\}$. $A_i \cap \mathcal{K}$ is a normal subloop of $A_i \cong (S, +)$ so $A_i \subset \mathcal{K}$. Without loss of generality assume $i = 0$, and let $k = 1 \odot 0$. $a_k(1) \in a_1(1)A_0 \cap a_k(1)A_0$, but since $|A_i| > 2$, $a_1(1)A_0 \neq a_k(1)A_0$, so by Theorem I.2.16 of [5] $A_0 \neq \mathcal{K}$, thus there exist $a_j(y) \in \mathcal{K} - A_0$ and $\mathcal{K} = \mathcal{L}^{(Q)}(S)$. □

Corollary 4.9. *If $(S, +)$ a finite simple group, $(S^*, \cdot)$ a loop and $(Q, \odot)$ is a two-quasigroup, then $\mathcal{L}^{(Q)}(S)$ is a simple 3 generated loop.*

References

[1] **V. D. Belousov**: *Foundations of the Theory of Quasigroups and Loops*, (Russian), Izdat. Nauka, Moscow, 1967.

[2] **R. H. Bruck**: *A Survey of Binary Systems* Springer Verlag, Berlin, 1971.

[3] **Tuval Foguel**: *Simple Power Associative Loops with Exactly One Covering*, Results in Mathematics **45** (2004), 241 – 245.

[4] **Tuval Foguel**: *Associative transitive loops*, Algebra Colloquium, **12** no. 3 (2005), 535 – 540.

[5] **H. O. Pflugfelder**: *Quasigroups and Loops: Introduction*, Sigma Series in Pure Math. **7**, Heldermann Verlag, Berlin, 1990.

[6] **S. K. Stein**: *Homogeneous quasigroups*, Pacific J. Math. **14** (1964), 1091 – 1102.

Department of Mathematics
Auburn University Montgomery
PO Box 244023
Montgomery, AL 36124-4023
USA
e-mail: tfoguel@mail.aum.edu

Received April 8, 2005