SIMPLE POWER ASSOCIATIVE LOOPS WITH EXACTLY ONE COVERING

TUVAL FOGUEL

Abstract. In this paper we look at a some results about uniquely covered power associative loops, and we construct a family of power associative loops that have exactly one covering. This gives shows that there is a wide variety of power associative loops with exactly one covering than groups.

1. Introduction

A loop $\mathcal{L}$ is said to have a covering if it is a set theoretic union of proper subloops.

Definition 1.1. A covering of a loop $\mathcal{L}$ is irredundant if each subcollection of those subloops fails to cover $\mathcal{L}$. A loop is uniquely covered if it has exactly one irredundat covering.

Similar to the group case if a finite power associative loop has a unique covering, then it is covered by maximal subloops that are cyclic subgroups. But the situation for loops is more complicated than that for groups. For example a finite group G has exactly one covering by subgroups if and only if G is isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$ for some prime p, or G is a nonabelian group of order pq for p and q distinct primes [1]. In this paper we look at a family of power associative loops this loops have exactly one covering, and some of them are simple. For basic facts about covering of group by subgroups, we refer the reader to [2], [3].

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 translations biject is called a *quasigroup*. A quasigroup $\mathcal{L}$ is an *idempotent quasigrop* 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 loop*, if for any $x \in \mathcal{L}$, the subloop generated by x is a group. For basic facts about loops and quasigroups, we refer the reader to [4], [5], [6]. The *left*, *middle*, and *right nucleus* of a loop $\mathcal{L}$ are defined, respectively, as

$$\begin{aligned} \mathrm{Nuc}_l(\mathcal{L}) &:= \{x \in \mathcal{L} : x(yz) = (xy)z \ \forall y, z \in \mathcal{L}\}, \\ \mathrm{Nuc}_m(\mathcal{L}) &:= \{y \in \mathcal{L} : x(yz) = (xy)z \ \forall x, z \in \mathcal{L}\}, \\ \mathrm{Nuc}_r(\mathcal{L}) &:= \{z \in \mathcal{L} : x(yz) = (xy)z \ \forall x, y \in \mathcal{L}\}. \end{aligned}$$

The nucleus of a loop $\mathcal{L}$ is defined as

$$\mathrm{Nuc}(\mathcal{L}) := \mathrm{Nuc}_l(\mathcal{L}) \cap \mathrm{Nuc}_m(\mathcal{L}) \cap \mathrm{Nuc}_r(\mathcal{L}).$$

Each of these is an associative subloop of $\mathcal{L}$, as follows from Theorem I.3.5 in [6]. The *centrum* and *center* of a loop $\mathcal{L}$ are defined, respectively, by

$$\begin{aligned} C(\mathcal{L}) &:= \{x \in \mathcal{L} : xy = yx \ \forall y \in \mathcal{L}\}, \\ Z(\mathcal{L}) &:= \mathrm{Nuc}(\mathcal{L}) \cap C(\mathcal{L}). \end{aligned}$$

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 $(\mathcal{K}x)y = \mathcal{K}(xy)$ ([5], p. 60, IV.1). These three conditions are clearly equivalent to the pair

2000 *Mathematics Subject Classification.* 20N05.

Key words and phrases. loop, finite covering.

$x(\mathcal{K}y) = \mathcal{K}(xy)$ and $x(\mathcal{K}y) = (x\mathcal{K})y$ for all $x, y \in \mathcal{K}$. Note that the center of a loop is a normal subloop.

3. Uniquely covered power associative loops

The following three lemmas about covering of finite power associative loops and maximal cyclic subgroups have straightforward proofs so they are omitted. By maximal cyclic subgroups we mean cyclic subgroups that are not contained in other cyclic subgroups.

Lemma 3.1. *A finite noncyclic power associative loop $\mathcal{L}$ has an irredundant covering by maximal cyclic subgroups.*

Lemma 3.2. *If $\mathcal{L}$ is a uniquely covered finite noncyclic power associative loop, then its covering by maximal cyclic subgroups is its only irredundat covering.*

Lemma 3.3. *If $\mathcal{L}$ is a finite noncyclic power associative loop with exactly one covering, then every proper cyclic subgroup of $\mathcal{L}$ is a maximal cyclic subgroups.*

The proof of the Lemma below is identical to the group theoretical case[1].

Lemma 3.4. *Let $\mathcal{L}$ be a finite power associative noncyclic loop. $\mathcal{L}$ is a uniquely covered if and only if every maximal cyclic subgroup of $\mathcal{L}$ is a maximal subloop of $\mathcal{L}$.*

Proof. Assume that $\mathcal{L}$ is a uniquely covered and $< h >$ is maximal cyclic but not maximal in $\mathcal{L}$. Then $< h >$ is properly contained in a proper subloop $\mathcal{H}$ which is not cyclic, and $\mathcal{L} = \mathcal{H} \cup \bigcup < g >$ where $g \notin \mathcal{H}$ and $< g >$ is maximal cyclic, is an irredundat covering contradicting Lemma 3.2.

Assume that every maximal cyclic subgroup of $\mathcal{L}$ is a maximal subloop of $\mathcal{L}$,With out loss of generality $\mathcal{L}$ is not cyclic. Then if $< g >$ is maximal cyclic the only proper subloop of $\mathcal{L}$ containing $< g >$ is $< g >$, thus it is a member of any covering of $\mathcal{L}$. So if $\{< g_1 >, \cdots < g_n >\}$ is the set of maximal cyclic subgroups of $\mathcal{L}$, then they are part of any covering of $\mathcal{L}$. And $\mathcal{L} = \bigcup_{i=1}^{n} < g_i >$ which is an irredundat covering, thus $\mathcal{L}$ is a uniquely covered. □

4. Family

In this section we construct a family of loops with exactly one covering.

Definition 4.1. Given a $(S, +, \cdot)$ 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 4.2. For convenience we will also denote $\mathbf{1}$ by $a_q(0)$, and thus get $a_q(x)a_q(-x) = a_q(0) = \mathbf{1}$.

Lemma 4.3. *$\mathcal{L}^{(Q)}(S)$ is a loop with identity $\mathbf{1}$.*

Proof. By definition $\mathbf{1}$ is a two sided identity. Given $a_{q_1}(x)b = a_{q_2}(y)$ if $q_1 = q_2$ then the unique solution is $b = a_{q_1}(z)$ where z is the unique solution to $z + x = y$. If $q_1 \neq q_2$ there is a unique q_3 such that $q_1 \odot q_2 = q_3$ then the unique solution is $b = a_{q_3}(t)$ where t is the unique solution to $tx = y$. Similarly we can find unique solutions for $ba_{q_1}(x) = a_{q_2}(y)$, thus $\mathcal{L}^{(Q)}(S)$ is a loop. □

Remark 4.4. $\mathcal{L}^{(Q)}(S)$ is a union of proper subloops $A_q = \{a_q(x) : x \in S\}$, where $q \in Q$, with $A_{q_1} \cap A_{q_2} = \{\mathbf{1}\}$ for $q_1 \neq q_2$.

Remark 4.5. If Q and S are finite, then $|\mathcal{L}^{(Q)}(S)| = |Q|(|S|-1)+1$.

Lemma 4.6. *If $(S,+)$ is a group, then $\mathcal{L}^{(Q)}(S)$ is a power associative loop with identity* $\mathbf{1}$.

Proof. By Lemma 4.3 $\mathcal{L}^{(Q)}(S)$ loop with identity $\mathbf{1}$. Given $a_q(x) \in \mathcal{L}^{(Q)}(S)$,

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

a group. Thus $\mathcal{L}^{(Q)}(S)$ is a power associative loop. □

Remark 4.7. In this paper we will look at $\mathcal{L}^{(Q)}(S)$ where $S = \mathbb{F}$ a field, so A_q is an abelian group.

Remark 4.8. $|Q| \geq 3$ since Q is an idempotent quasigroup.

Lemma 4.9. *If $|\mathbb{F}| > 2$, then $\mathcal{L}^{(Q)}(\mathbb{F})$ is not a group. And if $|\mathbb{F}| = 2$ and $|Q| = 3$ then it is the Klein 4-group.*

Proof. If $\mathbb{F} = GF(2)$ and $|Q| = 3$, then $|\mathcal{L}^{(Q)}(\mathbb{F})| = 4$ and for any $x \in \mathcal{L}^{(Q)}(\mathbb{F})$, $x^2 = \mathbf{1}$ so $\mathcal{L}^{(Q)}(\mathbb{F})$ is the Klein 4-group. If $|\mathbb{F}| > 2$ then there exists $x \in \mathbb{F}^*$ with $-x^2 \neq 1$.Let $q_1, q_2 \in Q$ where $q_1 \neq q_2$, look at

$$a_{q_1}(-x)(a_{q_1}(x)a_{q_2}(1)) = a_{q_3}(-x^2) \neq a_{q_2}(1) = (a_{q_1}(-x)a_{q_1}(x))a_{q_2}(1)$$

not even in the case that $q_2 = q_3$ so $\mathcal{L}^{(Q)}(\mathbb{F})$ does not have the left inverse property and $\mathcal{L}^{(Q)}(\mathbb{F})$ is not a group. □

Remark 4.10. If Q is finite then every subset of $\mathcal{L}^{(Q)}(\mathbb{F})$ with more than $2|Q|$ elements has a triplet of elements that commute and generate a group, but $Z(\mathcal{L}^{(Q)}(\mathbb{F}))$ is trivial when $|\mathbb{F}| > 2$.

5. Two-quasigroup basis

Definition 5.1. 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 5.2. If Q is a two-quasigroup, then it is generated as a quasigroup by any two distinct elements.

Lemma 5.3. *If p is a prime and n a positive integer, then there is a two-quasigroup $|Q| = p^n$.*

Proof. By Theorem 2.5 [7], given $Q = GF(p^n)$ (the Galois field of p^n elements), 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 5.4. Given a two-quasigroup Q we will denote its elements by $\{0, 1, \dots\}$.

Theorem 5.5. *If $\mathbb{F}$ is a finite field and $(Q, \odot)$ is a two-quasigroup, then $\mathcal{L}^{(Q)}(\mathbb{F}) =< a_i(x), a_j(y) >$ for any $a_i(x), a_j(y) \in \mathcal{L}^{(Q)}(\mathbb{F}) - \{\mathbf{1}\}$ such that $i \neq j$ and $< x >$ or $< y >= \mathbb{F}$.*

Proof. Let $K =< a_i(x), a_j(y) >$ since $< a_i(x) >$ and $< a_j(y) >\subseteq K$ we may assume with out loss of generality that $x = 1$. Let $k = i \odot j$, then $a_k(1) = a_i(y^{-1})a_j(y) \in K$. Given $q \in Q$ it is a word in i and k so $< a_q(1) >\subseteq K$, thus $K = \mathcal{L}^{(Q)}(\mathbb{F})$. □

Corollary 5.6. *If $\mathbb{F}$ is a field of prime order and $(Q, \odot)$ is a two-quasigroup, then $\mathcal{L}^{(Q)}(\mathbb{F}) =< a_i(x), a_j(y) >$ for any $a_i(x), a_j(y) \in \mathcal{L}^{(Q)}(\mathbb{F}) - \{\mathbf{1}\}$ such that $i \neq j$.*

Theorem 5.7. *If $\mathbb{F}$ is a finite field and $(Q, \odot)$ is a two-quasigroup, then $\mathcal{L}^{(Q)}(\mathbb{F})$ is uniquely covered.*

Proof. By Lemma 3.4 all we need to show is that A_j is a maximal subloop for all j. Assume that C is a subloop of $\mathcal{L}^{(Q)}(\mathbb{F})$ with $A_j \subsetneq C$ for some j, then there is a $a_i(x) \in C - \{A_j\}$, so by Theorem 5.5 $C = \mathcal{L}^{(Q)}(\mathbb{F})$. □

Corollary 5.8. *If $\mathbb{F}$ is a field of prime order and $(Q, \odot)$ is a two-quasigroup, then $\mathcal{L}^{(Q)}(\mathbb{F})$ has exactly one covering by proper subloops.*

Lemma 5.9. *If $\mathbb{F}$ is a field of order 2 and $(Q, \odot)$ is a two-quasigroup with more than three element, then $\mathcal{L}^{(Q)}(\mathbb{F})$ is not a group.*

Proof. By Theorem 5.5 $\mathcal{L}^{(Q)}(\mathbb{F}) =< a_i(1), a_j(1) >$ for any $i \neq j$. Given $y \in \mathcal{L}^{(Q)}(\mathbb{F}) - \{\mathbf{1}\}$, $y = a_i(1)$ for some i so the order of y is two. Since the order of $\mathcal{L}^{(Q)}(\mathbb{F})$ greater than four, $\mathcal{L}^{(Q)}(\mathbb{F})$ is not a group. □

Definition 5.10. A finite loop $\mathcal{L}$ satisfies the *strong Lagrange property.* If whenever $\mathcal{K}$ is a subloop of $\mathcal{H}$ which is a subloop of $\mathcal{L}$, then $|\mathcal{K}|$ divides $|\mathcal{H}|$ (see Definition I.2.15 of [6]).

Lemma 5.11. *If $\mathbb{F}$ is a field of prime order p and $(Q, \odot)$ is a two-quasigroup with $|\mathbb{F}|$ divides $|Q|-1$, then $\mathcal{L}^{(Q)}(\mathbb{F})$ has the strong Lagrange property.*

Proof. The only subloops of $\mathcal{L}^{(Q)}(\mathbb{F})$ are $\{\mathbf{1}\}, A_i$ and $\mathcal{L}^{(Q)}(\mathbb{F})$, and $|\mathcal{L}^{(Q)}(\mathbb{F})| = p|Q| + (|Q| - 1)$. □

Theorem 5.12. *If $\mathbb{F}$ is a field of odd prime order and $(Q, \odot)$ is a two-quasigroup, then $\mathcal{L}^{(Q)}(\mathbb{F})$ is simple.*

Proof. Let $\{\mathbf{1}\} \neq \mathcal{K}$ be a normal subloop of $\mathcal{L}^{(Q)}(\mathbb{F})$. Since $\{\mathbf{1}\} \neq \mathcal{K}$ there exist $a_i(x) \in \mathcal{L}^{(Q)}(\mathbb{F}) - \{\mathbf{1}\}$, such that $a_i(x) \in \mathcal{K}$, so $A_i \subset \mathcal{K}$. With out 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 $a_1(1)A_0 \neq a_k(1)A_0$, so by Theorem I.2.16 of [6] $A_0 \neq \mathcal{K}$, thus there exist $a_j(y) \in \mathcal{K} - A_0$ and $\mathcal{K} = \mathcal{L}^{(Q)}(\mathbb{F})$. □

Theorem 5.13. *If $\mathbb{F}$ is a field of order 2 and $(Q, \odot)$ is a two-quasigroup with $|Q| > 3$, then $\mathcal{L}^{(Q)}(\mathbb{F})$ is simple.*

Proof. Let $\{\mathbf{1}\} \neq \mathcal{K}$ be a normal subloop of $\mathcal{L}^{(Q)}(\mathbb{F})$. Since $\{\mathbf{1}\} \neq \mathcal{K}$ there exist $a_i(1) \in \mathcal{L}^{(Q)}(\mathbb{F}) - \{\mathbf{1}\}$, such that $a_i(1) \in \mathcal{K}$, so $A_i \subset \mathcal{K}$. Since Q is a two-quasigroup with $|Q| > 3$, there exists $j \in Q$ such that $j \odot (i \odot j) \neq i$. So look at $a_j(1)(A_i a_j(1)) = A_{j \odot (i \odot j)}$ while $A_i(a_j(1)a_j(1)) = A_i$, thus A_i is not a normal subloop. Thus there exist $a_j(1) \in \mathcal{K} - A_i$ and $\mathcal{K} = \mathcal{L}^{(Q)}(\mathbb{F})$. □

The Theorems above show that if $\mathbb{F}$ is a field of order 2 and $(Q, \odot)$ is a two-quasigroup with $|Q| > 3$, or if $\mathbb{F}$ is a field of odd prime order, then $\mathcal{L}^{(Q)}(\mathbb{F})$ is a simple power associative loop with exactly one covering.

6. The Characteristic zero case

A group with a finite covering by subgroups has a normal subgroup of finite index, also a group in which every infinite set of pairwise noncommuting elements is finite has a center of finite index [2]. The Theorem and Lemma below shows that this does not hold for power associative loops.

Remark 6.1. If $\mathcal{L}$ is a finite power associative loop of order n, then for each $a \in \mathcal{L}$, $|a| \leq n$, so $a^{n!} = 1$

Theorem 6.2. *If $\mathbb{F}$ is a field of Characteristic zero, then $\mathcal{L}^{(Q)}(\mathbb{F})$ has no normal subloops of finite index.*

Proof. Let $\mathcal{K}$ be a normal subloop of $\mathcal{L}^{(Q)}(\mathbb{F})$ of finite index. Let $n = |\mathcal{L}^{(Q)}(\mathbb{F})/\mathcal{K}|$, given $a_i(x) \in \mathcal{L}^{(Q)}(\mathbb{F})$,

$$a_i(x) = a_i(\frac{x}{n!})^{n!} \in \mathcal{K},$$

thus $\mathcal{K} = \mathcal{L}^{(Q)}(\mathbb{F})$. □

Remark 6.3. If Q is a finite two-quasigroup then every subset of $\mathcal{L}^{(Q)}(\mathbb{F})$ with more than $2|Q|$ elements has a triplet of elements that commute and generate a group, but $Z(\mathcal{L}^{(Q)}(\mathbb{F}))$ is trivial.

Lemma 6.4. *If $\mathbb{F}$ is a field of Characteristic zero and $(Q, \odot)$ is a finite quasigroup, then $\mathcal{L}^{(Q)}(\mathbb{F})$ has a finite covering by subgroups.*

Proof. $\{A_i : i \in Q\}$ is a finite covering by subgroups. □

7. Loops with a Round-Robin Basis

Robinson [8] introduction the following round-robin hospitality problem: "Seven golf clubs in North Canterbury, New Zealand, run an annual round-robin tournament. All seven teams meet at each of the courses in turn: While the home team sees to the hospitality the remaining six teams play three matches of the tournament. By [8] the assignment of matches to courses is equivalent to finding an abelian idempotent quasigroup of order seven.

Definition 7.1. A *round-robin quasigroup* is an odd order idempotent abelian quasigroup (i.e. a solution to the round-robin hospitality problem for $2n+1$ clubs).

Definition 7.2. A *two-round-robin quasigroup* is a round-robin quasigroup that is also a two-quasigroup.

Theorem 7.3. *A two-round-robin quasigroup of order p exist if and only if p is an odd prime with 2 a primitive element in $GF(p)$ the Galois field of p elements.*

Proof. Corollary 2.3 and Theorem 2.5 of [7]. □

Lemma 7.4. *If $\mathbb{F}$ is a field of prime order and $(Q, \odot)$ is finite two-round-robin quasigroup and $|Q| > 3$ or $|\mathbb{F}| > 2$, then $\mathcal{L}^{(Q)}(\mathbb{F})$ is an abelian simple loop with exactly one covering by proper subloops.*

Problem 7.5. *Are there infinitely many primes p with 2 a primitive element in $GF(p)$ the Galois field of p elements (this is a special case of a well known open problem* [9]*)?*

References

[1] M.A. Brudic, Finite n-covering of groups, *Arch. Math.* **63** (1994), 385-392.
[2] B.H. Neumann, A problem of Paul Erdős on Groups *J. Austral. Math Soc.* **21** (Series A) (1976), 467-472.
[3] B.H. Neumann, Groups covered by permutable subsets, *J.London Math. Soc.* **29** (1954), 236-248.
[4] V.D. Belousov, *Foundations of the Theory of Quasigroups and Loops*, Izdat. Nauka, Moscow, 1967 (Russian)
[5] R.H. Bruck, *A Survey of Binary Systems* Springer Verlag, Berlin, 1971
[6] H.O. Pflugfelder, *Quasigroups and Loops: Introduction*, Sigma Series in Pure Math. **7**, Heldermann Verlag, Berlin, 1990.
[7] Sherman K. Stein, Homogeneous quasigroups, *Pacific J. Math.***14** (1964), 1091-1102.
[8] D. F. Robinson, Constructing an annual round-robin tournament played on neutral grounds, *Math. Chronicle* **10** (1981/82), no. 1-2, 73-82.
[9] L. J. Goldstein, Density questions in algebraic number theory, *Amer. Math. Monthly* **78** (1971) 342-351.

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

Eingegangen am 14. Februar 2004