Quasigroups and Related Systems **16** (2008), 31 – 36

# Direct product of quasigroups and generalized diagonal subquasigroup

*Tuval Foguel*

**Abstract**

In this paper we look at when the direct product $\mathcal{P} \times \mathcal{Q}$ of two quasigroups contains a subquasigroup isomorphic to $\mathcal{P}$.

## 1. Introduction

The direct product $\mathcal{P} \times \mathcal{Q}$ of two groups (loops) clearly contains at least one subgroup (subloop) isomorphic to $\mathcal{P}$, namely $\mathcal{P} \times \{\mathbf{1}\}$. This is not the case for a direct product of two quasigroups. Bruck in [4] gives examples of finite nontrivial quasigroups $\mathcal{P}$ and $\mathcal{Q}$ whose direct product has no proper subquasigroups.

In this paper we will look at what we can say about the quasigroups $\mathcal{P}$ and $\mathcal{Q}$ if their direct product contains a subquasigroup isomorphic to $\mathcal{P}$.

## 2. Preliminaries

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

A *magma* $(\mathcal{Q}, \cdot)$ consists of a set $\mathcal{Q}$ together with a binary operation on $\mathcal{Q}$. For $x \in \mathcal{Q}$, define the left (resp., right) translation by $x$ by $L(x)y = xy$ (resp., $R(x)y = yx$) for all $y \in \mathcal{Q}$. A magma with all left and right translations bijective is called a *quasigroup*. A quasigroup $\mathcal{Q}$ is an *idempotent quasigrop* if for all $x \in \mathcal{Q}$, $xx = x$. A quasigroup $\mathcal{L}$ with a two-sided identity element $\mathbf{1}$ such that for any $x \in \mathcal{L}$, $x\mathbf{1} = \mathbf{1}x = x$ 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

2000 Mathematics Subject Classification: 20N05
Keywords: loop, quasigroup, direct product, covering.

group. For basic facts about loops and quasigroups, we refer the reader to [2], [3] and [7].

**Notation 2.1.** Given the direct product $\mathcal{P} \times \mathcal{Q}$ of two quasigroups, we will denote the $i^{th}$ *projection homomorpishm* by $\pi_i$.

**Notation 2.2.** Given two quasigroups $\mathcal{K}$ and $\mathcal{Q}$, we will denote that $\mathcal{K}$ is a subquasigroup of $\mathcal{Q}$ by $\mathcal{K} \leq \mathcal{Q}$, and that $\mathcal{K}$ is a subquasigroup of $\mathcal{Q}$ but not equal to $\mathcal{Q}$ by $\mathcal{K} \lneq \mathcal{Q}$.

## 3. Generalized diagonal subquasigroup

**Lemma 3.1.** *If $\hat{\mathcal{Q}}$ is a homomorphic image of a quasigroup $\mathcal{P}$ and $\hat{\mathcal{Q}} \subseteq \mathcal{Q}$ a quasigroup, then $\hat{\mathcal{Q}}$ is a quasigroup.*

*Proof.* See [3]. □

**Lemma 3.2.** *$\mathcal{P} \cong \mathcal{K} \leq \mathcal{P} \times \mathcal{Q}$ where $\mathcal{P}$ and $\mathcal{Q}$ are quasigroups if and only if there exists a homomorphism $f : \mathcal{P} \to \mathcal{Q}$.*

*Proof.* Assume $\mathcal{P} \cong \mathcal{K} \leq \mathcal{P} \times \mathcal{Q}$. Then $\pi_2$ is a homomorphism from $\mathcal{K} \to \mathcal{Q}$ and since $\mathcal{P} \cong \mathcal{K}$ there exists a homomorphism $f : \mathcal{P} \to \mathcal{Q}$. Conversely, if there exists a homomorphism $f : \mathcal{P} \to \mathcal{Q}$, then $\mathcal{P} \cong \{(p, f(p)) | p \in \mathcal{P}\} \leq \mathcal{P} \times \mathcal{Q}$. □

**Corollary 3.3.** *$\mathcal{P} \cong \mathcal{K} \leq \mathcal{P} \times \mathcal{Q}$ where $\mathcal{P}$ and $\mathcal{Q}$ are quasigroups if and only if $\mathcal{Q}$ contains a subquasigroup that is a homomorphic image of $\mathcal{P}$.*

*Proof.* See Lemma 3.1 and Lemma 3.2. □

**Corollary 3.4.** *$\mathcal{P} \cong \mathcal{K} \leq \mathcal{P} \times \mathcal{Q}$ where $\mathcal{P}$ and $\mathcal{Q}$ are quasigroups with $\mathcal{Q}$ containing no subquasigroups except for itself if and only if $\mathcal{Q}$ is a homomorphic image of $\mathcal{P}$.*

**Definition 3.5.** Given $\mathcal{P} \times \mathcal{Q}$ where $\mathcal{P}$ and $\mathcal{Q}$ are quasigroups, we will call a subquasigroup $\mathcal{K}$ a *generalized diagonal subquasigroup* (*gd-subquasigroup*) if $\mathcal{K} = \{(p, f(p)) | p \in \mathcal{P}\} \leq \mathcal{P} \times \mathcal{Q}$ where $f$ is a homomorphism from $\mathcal{P}$ to $\mathcal{Q}$.

**Example 3.6.** If $\mathcal{P}$ and $\mathcal{Q}$ are loops, then $\mathcal{K} = \mathcal{P} \times \{\mathbf{1}\} \leq \mathcal{P} \times \mathcal{Q}$ is a gd-subquasigroup.

**Example 3.7.** The diagonal-subquasigroup $\{(p, p) | p \in \mathcal{P}\}$ is a gd-subquasigroup of $\mathcal{P} \times \mathcal{P}$.

**Theorem 3.8.** *$\mathcal{P} \cong \mathcal{K} \leq \mathcal{P} \times \mathcal{Q}$ where $\mathcal{P}$ and $\mathcal{Q}$ are quasigroups if and only if $\mathcal{P} \times \mathcal{Q}$ contains a gd-subquasigroup.*

*Proof.* By the definition of a gd-subquasigroup, it is isomorphic to $\mathcal{P}$.

If $\mathcal{P} \cong \mathcal{K} \leq \mathcal{P} \times \mathcal{Q}$, then by Lemma 3.2 there is a homomorphism $f : \mathcal{P} \to \mathcal{Q}$. Thus $\{(p, f(p)) | p \in \mathcal{P}\} \leq \mathcal{P} \times \mathcal{Q}$ is a gd-subquasigroup of $\mathcal{P} \times \mathcal{Q}$. □

**Definition 3.9.** A quasigroup is said to have a *covering* by subquasibgroups if it is the set-theoretic union of proper subquasigroups, and, if the set of subquasigroups is finite, we say the covering is finite. Such coverings have been widely studied in groups, and recently, analogous coverings for rings, semigroups, and loops have been discussed in [1], [6], and [5], respectively. A covering is disjoint if any two distinct subquasigroups in the covering are disjoint.

**Lemma 3.10.** *If $\mathcal{P}$ is a quasigroup and $\mathcal{Q}$ is an idempotent quasigroup, then $\mathcal{P} \times \mathcal{Q}$ has a disjoint covering $\mathcal{P} \times \mathcal{Q} = \bigcup_{i \in \mathcal{Q}} (\mathcal{P} \times \{i\})$ where $\mathcal{P} \times \{i\} \cong \mathcal{P}$ for all $i \in \mathcal{Q}$.*

*Proof.* $\mathcal{P} \times \{i\} \cong \mathcal{P}$ since $i$ is an idempotent for all $i \in \mathcal{Q}$. If $i, j \in \mathcal{Q}$ and $i \neq j$, then $\mathcal{P} \times \{i\} \bigcap \mathcal{P} \times \{j\} = \emptyset$ and if $h \in \mathcal{P} \times \mathcal{Q}$, then $h = (p, i)$ where $p \in \mathcal{P}$ and $i \in \{i\} \leq \mathcal{Q}$. □

**Definition 3.11.** 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 3.12.** If $\mathcal{Q}$ is a two-quasigroup, then it is generated as a quasigroup by any two distinct elements, and by [8] $\mathcal{Q}$ is an idempotent quasigroup.

**Example 3.13.** Given $\mathcal{Q} = GF(p^n)$ (the Galois field of $p^n$ elements), and $\alpha$ a primitive element in $GF(p^n)$. Then $(\mathcal{Q}, \odot)$ is a two-qusigroup under the binary operation

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

for all $a, b \in \mathcal{Q}$.

**Lemma 3.14.** *If $\mathcal{P}$ is a quasigroup with no subquasigroups except for itself, and $\mathcal{Q}$ is a two-quasigroup, then every proper subquasigroup of $\mathcal{P} \times \mathcal{Q}$ is of the form $\mathcal{P} \times \{i\} \cong \mathcal{P}$ where $i \in \mathcal{Q}$.*

*Proof.* Assume $\mathcal{K} \leq \mathcal{P} \times \mathcal{Q}$. Since $\pi_1(\mathcal{K}) \leq \mathcal{P}$ and $\mathcal{P}$ is a quasigroup with no proper subquasigroups, $\pi_1(\mathcal{K}) = \mathcal{P}$.

Let $k_1 = (p_1, i), k_2 = (p_2, j) \in \mathcal{K}$. If $i \neq j$, then since $\mathcal{Q}$ is a two-quasigroup $\pi_2(\mathcal{K}) = \mathcal{Q}$. Therefore given any $(p, t) \in \mathcal{P} \times \mathcal{Q}$ there exist $k = (\hat{p}, t) \in \mathcal{K}$, but some "power" of $\hat{p}$ is equal to $p$, and thus $\mathcal{K} = \mathcal{P} \times \mathcal{Q}$. So if $\mathcal{K} \leq \mathcal{P} \times \mathcal{Q}$, then $\mathcal{K} = \mathcal{P} \times \mathcal{Q}$ or $\mathcal{K} = \mathcal{P} \times \{i\}$. □

## 4. The non gd-subquasigroup

**Lemma 3.1.** *If $\mathcal{P} \cong \mathcal{K} \leq \mathcal{P} \times \mathcal{Q}$ where $\mathcal{P}$ and $\mathcal{Q}$ are quasigroups, then $\pi_1(\mathcal{K}) \leq \mathcal{P}$ and $\pi_1(\mathcal{K})$ is a homomrphic image of $\mathcal{P}$.*

*Proof.* $\pi_1(\mathcal{K}) \leq \mathcal{P}$ by definition. Since $\pi_1(\mathcal{K})$ is a homomrphic image of $\mathcal{K}$ it is a homomrphic image of $\mathcal{P} \cong \mathcal{K}$. □

**Corollary 3.2.** *If $\mathcal{P} \cong \mathcal{K} \leq \mathcal{P} \times \mathcal{Q}$ where $\mathcal{P}$ is a simple quasigroup and $\mathcal{Q}$ is a quasigroup, then $\pi_1(\mathcal{K}) \cong \mathcal{P}$ or $\{\mathbf{1}\}$.*

**Corollary 3.3.** *If $\mathcal{P} \cong \mathcal{K} \leq \mathcal{P} \times \mathcal{Q}$ where $\mathcal{P}$ is a quasigroup with no subquasigroups except for itself, and $\mathcal{Q}$ is a quasigroup, then $\pi_1(\mathcal{K}) \cong \mathcal{P}$.*

**Example 3.4.** In $\mathbb{Z} \times \mathcal{L}$, where $\mathbb{Z}$ denotes the integers and $\mathcal{L}$ is any loop, $\mathcal{K} = 2\mathbb{Z} \times \{\mathbf{1}\} \cong \mathbb{Z} \cong \pi_1(\mathcal{K})$, but note that $\pi_1(\mathcal{K}) \neq \mathbb{Z}$.

**Remark 3.5.** Given $\mathcal{K} \leq \mathcal{P} \times \mathcal{Q}$ where $\mathcal{P}$ and $\mathcal{Q}$ are quasigroups and $\mathcal{P}$ is finite, $\pi_1(\mathcal{K}) \cong \mathcal{P}$ if and only if $\pi_1(\mathcal{K}) = \mathcal{P}$.

**Definition 3.6.** Given nonempty subsets $A$ and $B$ of a quasigroup $\mathcal{P}$,we will denote by $AB = \{ab |\ a \in A, b \in B\}$.

The following deffinition is due to Bruck (see [4]).

**Definition 3.7.** Let $\mathcal{K} \leq \mathcal{P} \times \mathcal{Q}$ where $\mathcal{P}$ and $\mathcal{Q}$ are quasigroups. For $p \in \mathcal{P}$ denote by $\mathcal{Q}_p = \{q \in \mathcal{Q} |\ (p, q) \in \mathcal{K}\} \subseteq \mathcal{Q}$.

**Lemma 3.8.** *If $\mathcal{K} \leq \mathcal{P} \times \mathcal{Q}$ where $\mathcal{P}$ and $\mathcal{Q}$ are quasigroups, then $\mathcal{Q}_p \mathcal{Q}_{\hat{p}} = \mathcal{Q}_{p\hat{p}}$ for $p, \hat{p} \in \pi_1(\mathcal{K})$.*

*Proof.* See [4] Lemma 15. Note that finiteness is not used in this part of the proof. □

**Remark 3.9.** If $\mathcal{K} \leq \mathcal{P} \times \mathcal{Q}$ where $\mathcal{P}$ and $\mathcal{Q}$ are quasigroups and $p \in \mathcal{P} - \pi_1(\mathcal{K})$, then $\mathcal{Q}_p = \emptyset$.

**Lemma 3.10.** *If $\mathcal{P} \cong \mathcal{K} \leq \mathcal{P} \times \mathcal{Q}$ where $\mathcal{P}$ is a loop and $\mathcal{Q}$ is a quasigroup, then $\mathcal{Q}_{\mathbf{1}}$ is isomorphic to a normal subloop of $\mathcal{P}$*

*Proof.* $\mathcal{Q}_{\mathbf{1}}$ is isomorphic to the kernel of $\pi_1$. □

**Lemma 3.11.** *If $\mathcal{P} \cong \mathcal{K} \leq \mathcal{P} \times \mathcal{Q}$ where $\mathcal{P}$ is a finite power associative loop and $\mathcal{Q}$ is a quasigroup, then $\underbrace{\mathcal{Q}_p \cdots \mathcal{Q}_p}_{|p|-times} = \mathcal{Q}_{\mathbf{1}}$ for any $p \in \pi_1(\mathcal{K})$.*

*Proof.* By Lemma 3.8 $\underbrace{\mathcal{Q}_p \cdots \mathcal{Q}_p}_{|p|-\text{times}} = \mathcal{Q}_{p^{|p|}} = \mathcal{Q}_{\mathbf{1}}$. □

**Definition 3.12.** For a finite power associative loop $\mathcal{P}$, $\exp(\mathcal{P}) = n$ is the smallest positive integer such that given $p \in \mathcal{P}$ the identity $p^n = \mathbf{1}$ holds.

**Corollary 3.13.** *If $\mathcal{P} \cong \mathcal{K} \leq \mathcal{P} \times \mathcal{Q}$ where $\mathcal{P}$ is a finite power associative loop and $\mathcal{Q}$ is a quasigroup, then for any $q \in \pi_2(\mathcal{K})$, $q^{\exp(\mathcal{P})} \in \mathcal{Q}_{\mathbf{1}}$.*

*Proof.* $q \in \mathcal{Q}_p$ for some $p \in \pi_1(\mathcal{K})$, and thus $q^{\exp(\mathcal{P})} \in \mathcal{Q}_{p^{\exp(\mathcal{P})}} = \mathcal{Q}_{\mathbf{1}}$. □

**Remark 3.14.** If $\mathcal{K} \leq \mathcal{P} \times \mathcal{Q}$ where $\mathcal{P}$ and $\mathcal{Q}$ are quasigroups and $\mathcal{K}$ is finite, then $|\mathcal{K}| = \sum_{p \in \mathcal{P}} |\mathcal{Q}_p| = \sum_{p \in \pi_1(\mathcal{K})} |\mathcal{Q}_p|$.

**Lemma 3.15.** *If $\mathcal{K} \leq \mathcal{P} \times \mathcal{Q}$ where $\mathcal{P}$ and $\mathcal{Q}$ are quasigroups and $\mathcal{K}$ is finite, then $|\mathcal{Q}_p| = |\mathcal{Q}_{\hat{p}}|$ for $p, \hat{p} \in \pi_1(\mathcal{K})$ and $\mathcal{Q}_p$ and $\mathcal{Q}_{\hat{p}}$ are either disjoint or identical.*

*Proof.* By Remark 3.14 we see that $|\mathcal{Q}_p|$ is finite for each $p$, and thus by [4] Lemma 15, $|\mathcal{Q}_p| = |\mathcal{Q}_{\hat{p}}|$ for $p, \hat{p} \in \pi_1(\mathcal{K})$ where $\mathcal{Q}_p$ and $\mathcal{Q}_{\hat{p}}$ are either disjoint or identical. □

**Remark 3.16.** *If $\mathcal{K} \cong \mathcal{P} \leq \mathcal{P} \times \mathcal{Q}$ where $\mathcal{P}$ is a finite quasigroup and $\mathcal{Q}$ is quasigroup, then $|\mathcal{P}| = \sum_{p \in \mathcal{P}} |\mathcal{Q}_p| = \sum_{p \in \pi_1(\mathcal{K})} |\mathcal{Q}_p|$.*

**Lemma 3.17.** *If $\mathcal{K} \leq \mathcal{P} \times \mathcal{Q}$ where $\mathcal{P}$ and $\mathcal{Q}$ are quasigroups and $\mathcal{K}$ is finite, then $|\pi_1(\mathcal{K})|\,|\mathcal{Q}_p| = |\mathcal{K}|$ for any $p \in \pi_1(\mathcal{K})$.*
*Proof.* By Remarks 3.16 and Lemma 3.15 we get that

$$|\mathcal{K}| = \sum_{p \in \pi_1(\mathcal{K})} |\mathcal{Q}_p| = |\pi_1(\mathcal{K})|\,|\mathcal{Q}_p|\,. \qquad \square$$

**Corollary 3.18.** *If $\mathcal{P} \cong \mathcal{K} \leq \mathcal{P} \times \mathcal{Q}$ where $\mathcal{P}$ is a finit quasigroup and $\mathcal{Q}$ is quasigroup, then $|\pi_1(\mathcal{K})|\,|\mathcal{Q}_p| = |\mathcal{P}|$ for any $p \in \pi_1(\mathcal{K})$.*

**Lemma 3.19.** *If $\mathcal{K} \leq \mathcal{P} \times \mathcal{Q}$ where $\mathcal{P}$ and $\mathcal{Q}$ are quasigroups, $\pi_1(\mathcal{K}) \cong \mathcal{K}$ and $\mathcal{K}$ is finite, then $p \mapsto \mathcal{Q}_p$ for all $p \in \pi_1(\mathcal{K})$ is a homomorphism from $\pi_1(\mathcal{K})$ to $\mathcal{Q}$.*

*Proof.* By Lemma 3.17 we see that $|\mathcal{K}| = |\pi_1(\mathcal{K})|\,|\mathcal{Q}_p| = |\mathcal{K}|\,|\mathcal{Q}_p|$, and thus we get that $|\mathcal{Q}_p| = 1$ for all $p \in \pi_1(\mathcal{K})$. Therefore by Lemma 3.8 $p \mapsto \mathcal{Q}_p$ is a homomorphism for all $p \in \pi_1(\mathcal{K})$. □

**Corollary 3.20.** *If $\mathcal{P} \cong \mathcal{K} \leq \mathcal{P} \times \mathcal{Q}$ where $\mathcal{P}$ is a finite quasigroup, $\mathcal{Q}$ is quasigroup, and $\pi_1(\mathcal{K}) \cong \mathcal{P}$, then $p \mapsto \mathcal{Q}_p$ for all $p \in \mathcal{P}$ is a homomorphism from $\mathcal{P}$ to $\mathcal{Q}$ and $\mathcal{K}$ is a gd-subquasigroup.*

*Proof.* Note that $\mathcal{K} = \{(p, \mathcal{Q}_p) | p \in \mathcal{P}\}$. □

**Theorem 3.21.** *If $\mathcal{P} \cong \mathcal{K} \leq \mathcal{P} \times \mathcal{Q}$ where $\mathcal{P}$ and $\mathcal{Q}$ are quasigroups with $\mathcal{P}$ finite, then $\pi_1(\mathcal{K}) \leq \mathcal{P}$, $\pi_1(\mathcal{K})$ is a homomrphic image of $\mathcal{P}$, $|\mathcal{Q}_p|\,|\pi_1(\mathcal{K})| = |\mathcal{P}|$ for any $p \in \pi_1(\mathcal{K})$, and if $\mathcal{P} = \pi_1(\mathcal{K})$, then $\mathcal{K}$ is a gd-subquasigroup.*

*Proof.* This follows from Lemmas 3.1, Corollary 3.18 and Corollay 3.20. □

**Example 3.22.** Let $\mathcal{Q}$ be a finite quasigroup, $\mathcal{P} = \mathcal{Q} \times \mathcal{Q}$, and $\mathcal{K} = \{(q, q, \hat{q}) |\ q, \hat{q} \in \mathcal{Q}\} \subseteq \mathcal{P} \times \mathcal{Q}$. Then $\mathcal{K} \cong \mathcal{P}$ but $\pi_1(\mathcal{K}) \ncong \mathcal{P}$ and $\pi_2(\mathcal{K}) \ncong \mathcal{P}$.

**Example 3.23.** Let $\mathcal{P} = \mathcal{L} \times \mathbb{Z}_n = \mathcal{Q}$ where $\mathcal{L}$ is a loop, $\mathbb{Z}_n$ denotes the integers mod $n$, and let $\mathcal{K} = \{(l, 0, l, i) |\ l \in \mathcal{L} \text{ and } i \in \mathbb{Z}_n\}$. Then $\mathcal{Q}_{(l,0)} = \{(l, i) |\ i \in \mathbb{Z}_n\}$ is not a quasigroup if $l \neq \mathbf{1}$ and $\left|\mathcal{Q}_{(l,0)}\right| = n$.

# References


[1] **H. Bell, A. Klein, L. C. Kappe:** *An analogue for rings of a group problem of P. Erdös and B.H. Neumann*, Acta Math. Hungar. **77** (1997), 57 – 67.

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

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

[4] **R. H. Bruck:** *Some results in the theory of quasigroups*, Trans. Amer. Math. Soc. **55** (1944), 19 – 52.

[5] **T. Foguel and L.C. Kappe:** *On loops covered by subloops*, Expositiones Math. **23**, (2005), 255 – 270.

[6] **L. C. Kappe, J.C. Lennox and J. Wiegold:** *An analogue for semigroups of a group problem of P. Erdös and B.H. Neumann*, Bull. Austral. Math. Soc. **63** (2001), 59 – 66.

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

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


Received June 25, 2007

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