On Bruck's prolongation and contraction maps

Tuval Foguel and Josh Hiller

Abstract. Bruck constructed the first prolongation and contraction of quasigroups in order to study Steiner triple systems. In this paper we define a new family of quasigroups: The Steiner-Bruck quasigroups (SB-quasigroups), where $aa^2 = a^2a$ and $a^2 = b^2$ for all possible a and b, which arise from Bruck's prolongation. We use Bruck's prolongation and contraction maps to explore properties of this family of quasigroups. Among other results, we show that there is a one-to-one correspondence between SB-quasigroups and uniquely 2-divisible quasigroups. As a corollary to this result we find a correspondence between idempotent quasigroups and loops of exponent 2. We then use this correspondence to study some interesting loops of exponent two and some interesting idempotent quasigroups.

1. Introduction

In [4] Bruck constructed the first prolongation and contraction of quasigroups in order to study Steiner triple systems. In this paper we use Bruck's construction to define a new family of quasigroups, the *Steiner-Bruck* quasigroups. The paper starts with a review of necessary notions from loop and quasigroup theory, and a review of prolongations and contractions.

Preliminaries. We review a few necessary notions from loop and quasigrop theory, and we establish some notation conventions.

A magma (\mathcal{L}, \cdot) consists of a set \mathcal{L} together with a binary operation \cdot 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 bijective is called a *quasigroup*. This is equivalent to saying that for each a and b in \mathcal{L} , there exist unique elements x and y in \mathcal{L} such that both

- (1) ax = b
- (2) ya = b

hold. 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*, if for any $x \in \mathcal{L}$, the subloop generated by x is a group. The *exponent* of a power-associative loop is defined as the least common multiple of the orders of all elements of the loop. If

²⁰¹⁰ Mathematics Subject Classification: 20N05.

Keywords: Finite groups of exponent 2; finite loops of exponent 2; finite idempotent quasigroups; polongation of Latin square; contraction of Latin square

there is no least common multiple, the exponent is taken to be infinity. For basic facts about loops and quasigroups, we refer the reader to [3], [5], [13].

2. Prolongation and contraction

A prolongation of a quasigroup is a process by which a quasigroup is extended to a quasigroup with one additional element. A contraction of a quasigroup is a process by which a quasigroup is shrunk to a quasigroup with one fewer element. The first construction of a prolongation and of a contraction was introduced by Bruck in [4] for his study of Steiner triple systems. For additional examples and facts about prolongation and contraction of quasigroups, we refer the reader to [1], [2], [3], [6], [7].

Classic transversal prolongation of a Latin square. In the finite case, Bruck's prolongation is a special case of the classic transversal prolongation below.

Belousov in 1967 [2] introduced the classic transversal prolongation (CT-prolongation). The CT-prolongation uses a transversal and adding a new idempotent element to the Latin square. A transversal of a Latin square of order n is a set of n cells, one in each row, one in each column such that no two of the cells contain the same symbol. The CT-prolongation works as follows:

- 1. Locate a transversal in the Latin square.
- 2. Introduce a new first row and first column to the table corresponding to the new idempotent element i.
- 3. Copy the transversal element in the (k, l)th position to (i, l) and (k, i) positions and then replace the transversal element by i.

Example 2.1. CT Prolongation of exponent two loop of order 5:

.	1	2	3	4	5		\odot	i	1	2	3	4	5
		2					i						
		2 1					1	1	i	2	3	4	5
						\implies	2	4	2	1	i	5	3
		5					3	5	3	i	1	2	4
		3									5		
5	5	4	2	3	1						2		

Bruck prolongation and contraction. In this subsection we define three families of quasigroups which will be needed in order to study Bruck's prolongation and contraction in their most generalized form.

Definition 2.2. A quasigroup Q is a *unipotent quasigroup* if for all $x, y \in Q$ we have that $x^2 = y^2$.

Definition 2.3. In a quasigroup Q an element $x \in Q$ has x^n well defined if the value of $x \cdots x$ is independent of how the *n* factors are parenthesized.

Definition 2.4. A quasigroup Q is a *Steiner-Bruck quasigroup* (SB-quasigroup) if it is a unipotent quasigroup and x^3 is well defined for all $x \in Q$.

Remark 2.5. Note that in any commutative quasigroup x^3 is well defined, so a commutative unipotent quasigroup is an SB-quasigroups. In this paper we will see examples of non-comutative SB-quasigroups.

The next example shows that not all unipotent quasigroups are SB-quasigroups.

Example 2.6. $(\mathbb{Z}_4, -)$ (see multiplication table below) is a unipotent quasigroup that is not an SB-quasigroup.

—	0	1	2	3
0	0	3	2	1
1	1	0	3	2
2	2	1	0	3
3	3	2	1	0

Remark 2.7. Note that starting with any loop (L, \cdot) we can create a unipotent quasigroup with a one sided identity via the operation $a \odot b = a \cdot b^{-1}$. However, these new quasigroups will only be SB-quasigroups if L is of exponent 2, in which case $a \cdot b^{-1} = a \cdot b$.

Remark 2.8. The Theorem below shows that given any n one can find a loop that has an element x such that x^n is well defined, but $\langle x \rangle$ is not associative.

Theorem 2.9 (Theorem 5.5 [11]). If n > 5 and n is neither a power of two or a prime, then there is a Jordan loop Q containing a generating element $x \in Q$ such that x^k is well defined for $0 \leq k < n$ but x^n is not well-defined.

Remark 2.10. Note that by [14] in any Jordan loop Q and for any $x \in Q$, x^3 , x^4 , and x^5 are well-defined.

Proposition 2.11. Assume that Q is a quasigroup with $x \in Q$. Then if x^n is not well defined then x^{n+1} is not well defined.

Proof. Assume that x^n is not well defined, then there exist two distinct products $(x^n)_1 \neq (x^n)_2$. Now assume that x^{n+1} is well defined then $x(x^n)_1 = x(x^n)_2$ but the left multiplication map is bijective thus $(x^n)_1 = (x^n)_2$ contradicting the assumption that the two products are distinct.

Remark 2.12. A loop is of exponent 2 if and only if it is unipotent, so a natural question that one may ask is: given unipotency, what is required in order for a quasigroup to be a loop? The following theorem will provide an answer.

Theorem 2.13. Let Q be a unipotent quasigroup. Q is a loop if and only if x^4 is well defined for all $x \in Q$.

Proof. If Q is a unipotent loop (i.e. exponent 2 loop), then by definition Q is power associative so x^4 is well defined.

If on the other hand x^4 is well defined for all $x \in Q$, then by Proposition 2.11 x^3 is also well defined for all $x \in Q$. Let b = xi (where *i* is the unique square of Q), then we have that $xb = x(xi) = x(x(x^2)) = (x^2)(x^2) = i$ then b = x so x = xi, similarly x = ix so *i* is the identity, and Q is a loop.

Remark 2.14. In light of Theorem 2.13, it is evident that one reason SB-quasigroups are of interest is that they are as close to power associative as a unipotent quasigroup can be without becoming a loop. However, one could still ask if every SB-quasigroup is actually a loop. Put another way: can Theorem 2.13 be improved to say that a unipotent quasigroup is power associative if and only if x^3 is well defined for every x? The fundamental tool in answering this question, in the negative, is the prolongation of the following family of quasigroups.

Definition 2.15. We say that a quasigroup Q is a uniquely 2-divisible quasigroup (U2D-quasigroup) if the map $x \mapsto x^2$ is bijective.

We now define Bruck's prolongation, a special case of CT-prolongation. The key to this construction in the finite case is that the diagonal of the Latin square is a transversal, so to define Bruck's prolongation we need U2D-quasigroup.

Definition 2.16 (Bruck's prolongation). Given (Q, \odot) a U2D-quasigroup we will denote by $Q_P = Q \cup \{i\}$ as a set with binary operation for $x, y \in Q_P - \{i\}$,

$$x \bullet y = \begin{cases} x \odot y & \text{if } x \neq y \\ \text{i} & \text{otherwise} \end{cases}$$

For $x \in Q_P - \{i\}$, $i \bullet x = x \bullet i = x \odot x$ and $i \bullet i = i$.

Example 2.17. Bruck prolongation of the integers mod 3:

\bigcirc	0	1	2					1	
								2	
	0			\implies	0	0	i	1	2
1	1	2	0		1	2	1	i	0
2	2	0	1		2	1	2	0	i

Definition 2.18 (Bruck's contraction). Given (Q, \bullet) an SB-quasigroup we will denote by $Q_C = Q - \{a^2\}$ as a set with binary operation for $x, y \in Q_C$,

$$x \odot y = \begin{cases} x \bullet y & \text{if } x \neq y \\ x \bullet x^2 & \text{otherwise} \end{cases}$$

Example 2.19. Bruck contraction of an order 4 nongroup SB-quasigroup:

٠						\odot	b	c	d
a	a	d	h	C					
,	, a	a	0	,		b	$\begin{vmatrix} d \\ c \end{vmatrix}$	c	b
b	d	a	c	b	\Rightarrow			L	.1
		c				c	c	0	a
C	0	C	u	u		d	b	d	c
d	c	b	d	a		a		a	C

Remark 2.20. An idempotent quasigroup is a special case of a U2D-quasigroups. A loop of exponent 2 is a special case of an SB-quasigroup. When Q is an idempotent quasigroup then Q_P is a loop of exponent 2 and, conversely, when Q is a loop of exponent 2 then Q_C is an idempotent quasigroup.

3. SB-quasigrous and U2D-quasigroups

In this section we will see that Bruck's prolongation and contraction gives us a one-to-one correspondence between SB-quasigrous and U2D-quasigroups. Most of these results have immediate corollaries for idempotent quasigroups and loops of exponent 2.

Theorem 3.1. If Q is SB-quasigroup with unique square i, then $Q = Q_{C_P}$.

Proof. By definition they have the identical multiplication tables.

Theorem 3.2. If Q is a U2D-quasigroup, then $Q = Q_{P_C}$.

Proof. By definition they have the identical multiplication tables. \Box

Corollary 3.3. There is a one-to-one correspondence between SB-quasigrous and U2D-quasigroups.

Proof. The facts from Theorems 3.1 and 3.2 that $Q = Q_{C_P}$ and $Q = Q_{P_C}$ give us a one-to-one correspondence between SB-quasigrous and U2D-quasigroups. \Box

Corollary 3.4. There is a one-to-one correspondence between idempotent quasigroup and loops of exponent 2.

Lemma 3.5. If Q is an SB-quasigroup, then there is a one-to-one homomorphism $\tau : \operatorname{Aut}(Q) \to \operatorname{Aut}(Q_C)$.

Proof. Let *i* be the unique square in *Q* note that for any $f \in Aut(Q)$ we have $f(i) = f(i \bullet i) = f(i) \bullet f(i) = i$.

Define τ : Aut $(Q) \to$ Aut (Q_C) by $\tau(f) = \hat{f} = f|_{Q_C}$. We first show that \hat{f} is a quasigroup homomorphism. Given $x, y \in Q_C$

CASE 1: $x \neq y$, note that the preimage of the product $x \bullet y$ under the contraction map is not the square element *i*, so we get that

$$\hat{f}(x \odot y) = f(x \bullet y) = f(x) \bullet f(y) = \hat{f}(x) \odot \hat{f}(y).$$

CASE 2: when x = y, then

$$\hat{f}(x \odot y) = \hat{f}(x \odot x) = f(x \bullet x^2) = f(x) \bullet f(x)^2 = f(x) \bullet i = \hat{f}(x) \odot \hat{f}(x) = \hat{f}(x) \odot \hat{f}(y).$$

Proving the claim that \hat{f} is a homomorphism.

To see that τ is injective, it suffices to observe that if $\tau(f) = \tau(g)$ then for every non-square element $x \in Q$ we have f(x) = g(x) and f(i) = g(i) = i, thus f = g. **Lemma 3.6.** If Q is a U2D-quasigroup, then there is a one-to-one homomorphism $\rho : \operatorname{Aut}(Q) \to \operatorname{Aut}(Q_P)$.

Proof. Define for ρ : Aut $(Q) \rightarrow$ Aut (Q_P)

$$\rho(g) = \hat{g} \text{ where } \hat{g}(x) = \begin{cases} g(x) & \text{if } x \neq i \\ i & \text{otherwise} \end{cases}$$

To see that \hat{g} is a homomorphism we will consider several cases.

CASE 1: $x \neq y$ and $x, y \in Q$, then

$$\hat{g}(x \bullet y) = g(x \odot y) = g(x) \odot g(y) = \hat{g}(x) \bullet \hat{g}(y)$$

CASE 2: x = y and $x, y \in Q$, then $x \bullet y = i$ so

$$\hat{g}(x \bullet y) = \hat{g}(x \bullet x) = \hat{g}(i) = i = \hat{g}(x) \bullet \hat{g}(x) = \hat{g}(x) \bullet \hat{g}(y)$$

CASE 3: x = y = i

$$\hat{g}(x \bullet y) = \hat{g}(i \bullet i) = \hat{g}(i) = i = i \bullet i = \hat{g}(i) \bullet \hat{g}(i) = \hat{g}(x) \bullet \hat{g}(y).$$

CASE 4: $x \in Q$ and y = i (and similarly if x = i and $y \in Q$)

$$\begin{split} \hat{g}(x \bullet y) &= \hat{g}(x \bullet i) = \hat{g}(x \odot x) = g(x \odot x) = g(x) \odot g(x) = \hat{g}(x) \odot \hat{g}(x) \\ &= \hat{g}(x) \bullet i = \hat{g}(x) \bullet \hat{g}(i) = \hat{g}(x) \bullet \hat{g}(y). \end{split}$$

Observe then that $\rho(f) = \rho(g)$ implies that for every element $x \in Q$ we have that f(x) = g(x) thus f = g. So ρ is an injective homomorphism.

Theorem 3.7. If Q is an SB-quasigroup, then $\operatorname{Aut}(Q) \cong \operatorname{Aut}(Q_C)$.

Proof. Note that the maps constructed in Lemma 3.5 and Lemma 3.6 are inverses of each other. $\hfill \Box$

The proofs for the following two Lemmas are obvious.

Lemma 3.8. If $\{i\} \neq K$ is a subquasigroup of an SB-quasigroup Q, then $K_C \leq Q_C$. **Lemma 3.9.** If K is a subquasigroup of a U2D-quasigroup Q, then $K_P \leq Q_P$.

4. Action of the automorphism group

Lemma 4.1. If \mathcal{L} is a finite power associative loop and $Aut(\mathcal{L})$ acts transitively on $\mathcal{L} - \{1\}$, then \mathcal{L} is an exponent p loop for some prime p.

Proof. If $a, b \in \mathcal{L} - \{\mathbf{1}\}$, then |a| = |b| since there is an $f \in Aut(\mathcal{L})$ with f(a) = b.

Lemma 4.2. If \mathcal{L} is a finite power associative loop and $Aut(\mathcal{L})$ acts double transitively on $\mathcal{L} - \{1\}$, then \mathcal{L} is an exponent 2 loop or $\mathcal{L} \cong \mathbb{Z}_3$.

Proof. By Lemma 4.1 \mathcal{L} is an exponent p loop for some prime p. If \mathcal{L} is cyclic, then $\mathcal{L} \cong \mathbb{Z}_p$ for some prime. Thus an automorphism of \mathcal{L} that fixes a non-zero element fixes all elements, so by double transitivity we see that there are at most two non-zero elements and p = 2 or p = 3.

Assume that \mathcal{L} is noncyclic. If p > 2 then let $a, b \in \mathcal{L} - \{1\}$ with $b \notin \langle a \rangle$, then there exist an $f \in \operatorname{Aut}(\mathcal{L})$ with f(a) = a and $f(b) = a^2$ contradicting that f is one-to-one. Thus \mathcal{L} is an exponent 2 loop.

Lemma 4.3. G is a finite group and Aut(G) acts double transitively on $G - \{0\}$, if and only if G is an elementary abelian 2 group or $G \cong \mathbb{Z}_3$.

Proof. By Lemma 4.2 if Aut(G) acts double transitively on $G - \{0\}$, then G is an elementary abelian 2 group or $G \cong \mathbb{Z}_3$. The cyclic case is obvious.

Assume that G is a noncyclic elementary abelian 2 group, we can view G as a vector space over \mathbb{Z}_2 , so given two sets of two distinct non zero elements $a, b \in G - \{0\}$ and $c, d \in G - \{0\}$ each set is composed of linearly independent vectors and there exist an $A \in \operatorname{Aut}(G) = GL_n(\mathbb{Z}_2)$ with A(a) = c and A(b) = d. \Box

Lemma 4.4. G is a finite group and Aut(G) acts sharply double transitively on $G - \{0\}$, if and only if $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, $G \cong \mathbb{Z}_2$ or $G \cong \mathbb{Z}_3$.

Proof. The cyclic case and $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ are obvious. Assume that $G \cong \mathbb{Z}_2^n$ where n > 2, let $a, b, \text{and } c \in G$ be linearly independent vectors, we can find matrices $A, B \in \text{Aut}(G) = GL_n(\mathbb{Z}_2)$ with A(a) = b, A(b) = a, and A(c) = c while B(a) = b, B(b) = a, and B(c) = a + c showing that the action is not sharp. \Box

Definition 4.5. (cf. [15]) A quasigroup is *homogeneous* if its automorphism group is transitive. A quasigroup is *doubly homogeneous* if its automorphism group acts double transitively. A *two-quasigroup* is a nontrivial two generated doubly homogeneous quasigroup.

Remark 4.6. If Q is a two-quasigroup, then it is idempotent and is generated as a quasigroup by any two distinct elements and Q_P is a loop of exponent 2.

Lemma 4.7 (Lemma 5.3 of [8]). If p is a prime and n a positive integer, then there is a two-quasigroup $|Q| = p^n > 2$.

Lemma 4.8. If Q is a two-quasigroup, then $Aut(Q_P)$ acts sharply double transitively on $Q_P - \{0\}$ (where 0 is the identity in Q_P) and Q_P is two generated.

Proof. Since by definition Aut(Q), acts sharply double-transitively on Q.

Lemma 4.9. If \mathcal{L} is a finite power associative loop and $Aut(\mathcal{L})$ acts sharply double transitively on $\mathcal{L} - \{1\}$ (where 1 is the identity in \mathcal{L}) and \mathcal{L} is two generated, then \mathcal{L}_C is a two-quasigroup,

Proof. By Theorem 3.7 $Aut(\mathcal{L}_C)$, acts sharply double transitively on \mathcal{L}_C .

5. Finite Tarski Property Loops

Definition 5.1. A noncyclic simple power associative loop is a *Tarski Property* Loop if every nontrivial proper subloop is cyclic of order a fixed prime p.

The Tarski monster [12] and the Bruck-Tarski monster [9] are examples of infinite Tarski Property Loops.

Lemma 5.2. If Q is a two-quasigroup of order greater than 3, then Q_P is a Tarski Property Loop of exponent 2.

Proof. Corollary 5.6 and Theorem 5.13 of [8].

By Theorem 2.7 [10] for n > 2 there exists an idempotent quasigroup Q[n] of order n that is generated by any two distinct elements.

Theorem 5.3. If Q[n] is generated by any two distinct elements and n > 3, then $Q[n]_P$ is a Tarski Property Loop of order n + 1 > 4 and exponent 2.

Proof. By Theorem 3.2 of [10] the nontrivial proper subloops of $Q[n]_P$ are $A_i = \{0, i\}$ (where $i \in Q[n]$ and 0 is the identity) which are cyclic of order 2. Let $\{0\} \neq N$ be a normal subgroup of $Q[n]_P$ and $A_i \subseteq N$, if $A_i = N$ is a normal subloop, then for $j \neq i$, A_iA_j is a subloop. But $|A_iA_j| = 4 < |Q[n]_P|$, a contradiction. Therefore the only normal subloops of $Q[n]_P$ are trivial, and so $Q[n]_P$ is a simple loop and a Tarski Property Loop.

Remark 5.4. Since $Q[n]_P$ is generated by any two nontrivial distinct elements, every $f \in \operatorname{Aut}(Q[n]_P)$ is uniquely determined by its action on any two nontrivial distinct elements.

Corollary 5.5. For any n > 4 there is a Tarski Property Loop of order n and exponent 2.

6. Conclusion and future directions

As mentioned in Section 2 of this paper, SB-quasigroups are as close to being power associative as a non loop unipotent quasigroup can be. However, this idea and the proof of Theorem 2.13 hint at a possible generalization which we make explicit through the following two definitions.

Definition 6.1. Let Q be a quasigroup with the property that for all $x, y \in Q, x^n$ and y^n are well defined and $x^n = y^n$, then we say that Q is an *n*-power unipotent quasigroup or npu-quasigroup

Definition 6.2. An *nSB-quasigroup* is an *n*pu-quasigroup where x^{2n-1} is well defined.

By mimicking the proof of Theorem 2.13 we can easily prove the following generalization.

Theorem 6.3. Let Q be an npu-quasigroup with the property that x^{2n} is well defined for every $x \in Q$. Then Q is a power associative loop with identity x^n .

Remark 6.4. A power associative loop of exponent n is a nSB-quasigroups.

In light of this last remark, we close with two related conjectures.

Conjecture 1. For every n > 1 there is a quasigroup Q where x^n is well defined for all $x \in Q$ and there is at least one $y \in Q$ such that y^{n+1} is not well defined.

Conjecture 2. For every n > 1 there is a nonloop nSB-quasigroups.

Acknowledgments. The authors are indebted to an anonymous referee of this paper for providing insightful comments which has resulted in improvements to this paper.

References

- G.B. Beljavskaja, Contraction of quasigroups. I, (Russian), Bul. Akad. Štiince RSS Moldoven, 1 (1970), 6 - 12.
- [2] V.D. Belousov, Extensions of quasigroups, (Russian), Bul. Akad. Štiince RSS Moldoven, 8 (1967), 3 – 24.
- [3] V.D. Belousov, Foundations of the Theory of Quasigroups and Loops, (Russian), Izdat. Nauka, Moscow, (1967).
- [4] R.H. Bruck, Some results in the theory of quasigroups, Trans. Amer. Math. Soc., 55 (1944), 19 52.
- [5] R.H. Bruck, A Survey of Binary Systems, Springer Verlag, Berlin, (1971).
- [6] I.I. Deriyenko and W.A. Dudek, On prolongations of quasigroups, Quasigroups and Related Systems, 16 (2008), 187 - 198.
- [7] I.I. Deriyenko and W.A. Dudek, Contractions of quasigroups and Latin squares, Quasigroups and Related Systems, 21 (2013), 165 - 174.
- [8] T. Foguel, Simple power associative loops with exactly one covering, Results Math., 45 (2004), 241 - 245.
- [9] T. Foguel and M. K. Kinyon, Uniquely 2-divisible Bol loops, J. Algebra Appl., 9 (2010), 591-601.
- [10] S.M. Gagola III and L,-Ch. Kappe, On the covering number of loops, Expo. Math., 34 (2016), 436-447.
- M.K. Kinyon, K. Pula and P. Vojtěchovský, Admissible orders of Jordan loops, J. Combin. Designs, 17 (2009), 103 - 118.
- [12] A.Yu. Ol'sanskii, An infinite group with subgroups of prime order, (Russian), Izv. Akad. Nauk SSSR Ser. Mat., 44 (1980), 309 - 321.

- [13] H.O. Pflugfelder, Quasigroups and Loops: Introduction, Sigma Series in Pure Math., 7, Heldermann Verlag, Berlin, (1990).
- [14] K. Pula, Powers of elements in Jordan loops, Comment. Math. Univ. Carolin., 49 (2008), no. 2, 291 – 299.
- [15] S.K. Stein, Homogeneous quasigroups, Pacific J. Math., 14 91964), 1091-1102.

Received June 18, 2018 Revised April 18, 2019

Department of Mathematics and Computer Science Adelphi University Garden City, NY 11010 USA E-mails: tfoguel@adelphi.edu, johiller@adelphi.edu