*Computing and Applied Sciences Impact* (2026), 3(1-4): 35-48
ISSN: 3043-680X

Research Article

# Construction of semisymmetric entropic quasigroups

Pius Aje Onah [1]*

1 School of Mathematics, University of Science and Technology of China, Hefei, China
*Corresponding author: Pius Aje Onah (pionaj1@gmail.com)

Received: April 6, 2026; Revised: June 4, 2026; Accepted: June 4, 2026; Published: 20, 2025



## Abstract

Elliptic curves are non-singular cubic plane-curves over a field containing at least one point and naturally form a group, where the associative property is based on Cayley-Bacharach theorem. A semisymmetric entropic (medial) quasigroup (SEQ) is a non-commutative generalization of this principle. This is a magma satisfying the pair of identities: $(xy)x = y$ and $(wx)(yz) = (wy)(xz)$. Every SEQ is associated (not necessarily uniquely) with an Abelian group. In this paper, we give methods for constructing SEQs based on their corresponding Abelian groups. In particular, we show that SEQs are central quasigroups.

**Keywords:** Quasigroups; Semisymmetric; Entropic; Medial; Elliptic curves

## 1. Introduction

In this paper, we investigate the structures of semisymmetric entropic quasigroups (SEQs), especially those of the finite kind. The terms *entropic* and *medial* are used interchangeably for the algebraic property $(wx)(yz) = (wy)(xz)$ [1-4]. The commutative case is commonly referred to as a medial totally symmetric quasigroup (Medial TSQG). A medial TSQG is a generalization of elliptic curves [1, 3, 5], thus an SEQ can be seen as a not necessarily commutative generalization of an elliptic curve. The number of medial TSQG increases exponentially as the order increases; however, most of them are structure-wise equivalent [2]. The number of these isomorphism classes depends on the prime factorization of the intended order. Their construction is quite straightforward: let $(G, +)$ be an Abelian group and set $x \cdot y = k - x - y$, then $(G,\cdot)$ is a medial TSQG [1, 3]. And in fact, every medial TSQG is a consequence of such constructions.

Now, as we would see, every SEQ is isotopic to an Abelian group, however, recovering the SEQ may not be uniquely possible due to the possibility that the SEQ is not commutative. Thus, the above construction is no longer sufficient for SEQs as they are not Abelian. However, one may consider instead $x \cdot y = k + \phi(x) + \psi(y)$, for two automorphism of $G$ [2, 6, 7]. Then $(G,\cdot)$ is called a central quasigroup or a T-quasigroup. They are entropic if and only if $\phi$ and $\psi$ commute. Quasigroups correspond to Latin squares, and J. D. H. Smith has shown [8] that central quasigroups can be described abstractly as those quasigroups in which the diagonal is a normal sub-quasigroup of the square.

The main result of this paper, presented in Section 4, is as follows:

**Theorem 1.1:** Every SEQ $(G,\cdot)$ is equivalent to an Abelian group $(G,+)$ reequipped with the product law $x \cdot y = k - \phi(x) - \phi^{-1}(y)$, where $\phi$ is a group automorphism of $(G,+)$ satisfying $\phi^3(x) = x$ and $k$ is a fixed point of $\phi$.

The structure of this paper is as follows: In Section 2, we provide some basic definitions as preliminaries. In section 3, we define SEQs and present alternative formulations. We deduce their corresponding group isotopes and show that they are isomorphic as Abelian groups. In section 4, we deconstruct SEQs with particular attention to finite SEQs. Two structures are of particular interest: commutativity and the existence of idempotent elements. Every SEQ is a *crossing* of two smaller SEQs of both kinds. In many cases, this *crossing* is a direct product, in which case the SEQ is a central quasigroup. In Section 5, we present some examples.

## 2. Preliminaries

In this section, we define some basic concepts:

**Definition 2.1:** A Magma is a pair $(G,\cdot)$, of a set $G$ and a binary operation $\cdot$ that is closed on $G$. We write $xy$ for $x \cdot y$ when the operation is clear.

**Definition 2.2:** A Group is an associative magma with an identity element such that every element is invertible. That is, $(xy)z = x(yz), \forall x,y,z \in G; \exists e \in G: xe = e = ex, \forall x \in G;$ and given any $x \in G, \exists y \in G: xy = e = yx$. If it is commutative, that is $xy = yx, \forall x,y \in G$, then we call $(G,\cdot)$ an Abelian group.

**Theorem 2.1 (Fundamental Theorem of Finite Abelian Groups):** Every finite Abelian group $G$ can be expressed as the direct sum of cyclic subgroups of prime-power order.

A cyclic group of order $n$ is usually denoted by $C_n$ or the additive group of $\mathbb{Z}/n\mathbb{Z}$, the integers modulo $n$.

**Definition 2.3:** A Quasigroup $(G,\cdot)$ is a magma obeying the *Latin square* property. That is, for each $a$ and $b$ in $G$, there exist unique elements $x,y \in G$ such that $ax = b$ and $ya = b$ (In other words: Each element of the set occurs exactly once in each row and exactly once in each column of the quasigroup's multiplication table, or Cayley table. This property ensures that the Cayley table of a finite quasigroup is a Latin square). The requirement that $x$ and $y$ be unique can be replaced by the requirement that the magma be cancellative.

**Definition 2.4:** An Elliptic Curve is a smooth, projective, algebraic curve of genus one, on which there is a specified point $O$. An elliptic curve is defined over a field $k$ and describes points in $k^2$, the Cartesian product of $k$ with itself, together with points at infinity.

Let $P, Q$ be two points on the curve and let $P * Q$ denote the third point of intersection of line $PQ$ and the curve (counting multiplicities). Then the group law is given by $P + Q = (P * Q) * O$. This is indeed a group and the proof for the associative property is based on the following theorem [5]:

**Theorem 2.2 (Cayley-Bacharach Theorem):** Assume that two cubics, $C_1$ and $C_2$, in the projective plane meet in nine (different) points, as they do in general over an algebraically closed field. Then every cubic that passes through any eight of the points also passes through the ninth point.

## 3. Semisymmetric Entropic Quasigroups (SEQs)

In this section we give equivalent definitions of semisymmetric entropic quasigroups and show their connection to Abelian groups.

**Definition 3.1:** A semisymmetric entropic (medial) quasigroup (SEQ), $(G,\cdot)$, is a magma satisfying the following:

i) Left semisymmetric: $(xy)x = y, \forall x, y \in G$;
ii) Entropic (medial): $(wx)(yz) = (wy)(xz), \forall w, x, y, z \in G$.

A subset of $G$ that is closed under the product $\cdot$, inherits the above properties and is thus referred to as a semisymmetric entropic subquasigroup or sub-SEQ for short.

As will be seen below, the left and right semisymmetric conditions are equivalent and will together be simply referred to as semisymmetric. Furthermore, assuming the semisymmetric condition, the quasi-associative condition is equivalent to the entropic condition.

The first two conditions represent the linear property: given any two points on a cubic curve, there is a unique third point on the curve that is collinear to the first two. The remaining two conditions represent the Cayley-Bacharach theorem.

**Proposition 3.1:** Based on the above definitions, let $(G,\cdot)$ be a magma have the following implications:

1. Left semisymmetric ⇔ Right semisymmetric: $x(yx) = y, \forall x, y \in G$.

2. Semisymmetric and Entropic ⇒ Quasi-associative: $[(wx)y]z = x[y(zw)], \forall w, x, y, z \in G$.

3. Semisymmetric and Quasi-associative ⇒ Entropic.

4. Semisymmetric ⇒ $(G,\cdot)$ is a quasi-group.

*Proof:*

1. Suppose $(G,\cdot)$ is left semisymmetric: Let $x, y \in G$. Then $x(yx) = [(yx)y](yx) = [zy]z = y$, where $z = yx$. Then $(G,\cdot)$ is right semisymmetric.

Suppose $(G,\cdot)$ is right semisymmetric: Let $x, y \in G$. Then $(xy)x = (xy)[y(xy)] = z[yz] = y$, where $z = xy$. Then $(G,\cdot)$ is left semisymmetric.

2. Suppose $(G,\cdot)$ is semisymmetric and entropic: Let $w, x, y, z \in G$. Then $[(wx)y]z = [(wx)y][w(zw)] = [(wx)w][y(zw)] = x[y(zw)]$. Then $(G,\cdot)$ is quasi-associative.

3. Suppose $(G,\cdot)$ is semisymmetric and quasi-associative: Let $w, x, y, z \in G$. Then $(wx)(yz) = (wx)(y[(xz)x]) = ([x(wx)]y)(xz) = (wy)(xz)$. Then $(G,\cdot)$ is entropic.

4. Suppose $(G,\cdot)$ is semisymmetric: Then $xy = z \Rightarrow yz = y(xy) = x$ , $zx = (xy)x = y$. Thus, $(G,\cdot)$ is a quasi-group since $ax = b \Rightarrow x = ba$ and $ya = b \Rightarrow y = ab$, that is, $L_a^{-1}(b) = ba, R_a^{-1}(b) = ab$. ■

The torus structure of the quasi-associative property via a 3x3 torus graph (where in both rows and columns, the product of any two consecutive cells gives the next cell) are presented in Table 1 below:

Table 1: Torus structure of the quasi-associative property

| | | | | |
|---|---|---|---|---|
| $wx$ | $w$ | $x$ | $wx$ | $w$ |
| $y$ | $zw$ | $y(zw)$ | $y$ | $zw$ |
| $(wx)y$ | $z$ | ? | $(wx)y$ | $z$ |
| $wx$ | $w$ | $x$ | $wx$ | $w$ |
| $y$ | $zw$ | $y(zw)$ | $y$ | $zw$ |

Next is the torus structure of the entropic property via a 3x3 torus graph (see Table 2 below):

Table 2: Torus structure of the entropic property

| | | | | |
|---|---|---|---|---|
| $w$ | $x$ | $wx$ | $w$ | $x$ |
| $y$ | $z$ | $yz$ | $y$ | $z$ |
| $wy$ | $xz$ | ? | $wy$ | $xz$ |
| $w$ | $x$ | $wx$ | $w$ | $x$ |
| $y$ | $z$ | $yz$ | $y$ | $z$ |

**Definition 3.2:** Given an SEQ $(G,\cdot)$ and $e \in G$, define$+_e$ on $G$ by $x+_e y = (ex)(y[ee]), \forall x, y \in G$.

**Theorem 3.1:** $(G, +_e)$ is an Abelian group with identity $e$. Furthermore, if $G$ is commutative, then the operation law can be simplified as $x+_e y = (xy)e, \forall x, y \in G$.

*Proof:*

Indeed, have $+_e$ is commutative: $x+_e\, y\, = (ex)(y[ee]) = \, (ey)(x[ee]) = \, y +_e x$.

Next, we verify that $e$ is the identity: $x+_e\, e\, = (ex)(e[ee]) \, = \, (ex)e \, = \, x$.

Next, we show that $+_e$ is invertible: $-_e x \, = (ee)(e[ex])$ and $x-_e\, y \, = (ee)(x[ey])$.

Finally, we show associativity: First, observe that $e[y+_e\, x] \, = \, e[(ey)(x\,[ee])] \, = \, [([ee]e)(ey)]x \, = \, [e(ey)]x$. This implies $[y+_e x]+_e z \, = (e[y+_e x])(z[ee]) \, = \, ([e(ey)]x)(z\,[ee]) \, = \, ([e(ey)]z)\,(x\,[e\,e]) = \, [y+_e\, z]+_e\, x$.

Thus, $[x +_e\, y]+_e\, z \, = \, [y +_e\, x]+_e\, z \, = \, [y +_e\, z]+_e\, x \, = \, x+_e\, [y+_e\, z]$ (here, we used the commutative properties for the first and last equation). ■

**Proposition 3.2:** Have $(xa)(b[xc]) \, = \, (ya)(b[yc])$. And $(a[bx])y \, = \, (a[by])x$.

*Proof:*

First, $(xa)(b[xc]) = \, (xa)(b[x([yc]y)]) = (xa)([(yb)x][yc]) = (x[(yb)x])(a[yc]) = \, (yb)(a[yc]) = \, (ya)(b[yc])$.

Next, $(a[bx])y = ([a(aa)][bx])y = (aa)([bx][ya]) = (aa)([by][xa]) = ([a(aa)][by])x = (a[by])x$. ■

**Proposition 3.3:** If $G$ is an SEQ, then $(G, +_e)$ is unique up to isomorphism. We shall call $(G, +_e)$ the group induced by $e$.

*Proof:*

Consider the map

$$\phi_{e'/e}\colon (G, +_e) \to (G, +_{e'}),$$

$$\phi_{e'/e}(x) \coloneqq (xe')e.$$

Indeed, $\phi_{e'/e}(e) = (ee')e = e'$.

Have $\phi_{e'/e}(x)+_{e'}\phi_{e'/e}(y) = \left(e'\phi_{e'/e}(x)\right)\, \left(\phi_{e'/e}(y)[e'e']\right) = \left(e\phi_{e'/e}(x)\right)\, \left(\phi_{e'/e}(y)[ee']\right) = (xe')\, \left(\phi_{e'/e}(y)[ee']\right) = \left(x\phi_{e'/e}(y)\right)\, (e'[ee']) = \left(x\phi_{e'/e}(y)\right)e = (x[(ye')e])e = (x[(ye')([ee]e)])e = (x[(y[ee])(e'e)])e = ([(ex)(y[ee])]e')e = ([x+_e y]e')e = \phi_{e'/e}(x+_e y)$.

Thus, $\phi_{e'/e}$ is an isomorphism satisfying $\phi_{e/e''}\{\phi_{e''/e'}[\phi_{e'/e}(x)]\} = x$.

Next, consider the map

$$\psi_{e'/e}: (G, +_e) \to (G, +_{e'}),$$

$$\psi_{e'/e}(x) \coloneqq x +_e e'.$$

Indeed, $\psi_{e'/e}(e) = e +_e e' = e'$.

Have $\psi_{e'/e}(x) +_{e'} \psi_{e'/e}(y) = \left(e'\psi_{e'/e}(x)\right)\left(\psi_{e'/e}(y)[e'e']\right) = \left(e\psi_{e'/e}(x)\right)\left(\psi_{e'/e}(y)[ee']\right) = (e[x +_e e'])\left(\psi_{e'/e}(y)[ee']\right) = ([e(ex)]e')\left(\psi_{e'/e}(y)[ee']\right) = \left([e(ex)]\psi_{e'/e}(y)\right)(e'[ee']) = \left([e(ex)]\psi_{e'/e}(y)\right)e = ([e(ex)][(ey)(e'[ee])])e$, and from second part of previous proposition, $= ([e(ex)][(ey)e])(e'[ee]) = ([e(ex)]y)(e'[ee]) = [x +_e y] +_e e' = \psi_{e'/e}(x +_e y)$.

Thus, $\psi_{e'/e}$ is an isomorphism satisfying $\psi_{e''/e'}\left[\psi_{e'/e}(x)\right] = \psi_{e''/e}(x)$. Indeed, $\psi_{e''/e'}\left[\psi_{e'/e}(x)\right] = \psi_{e'/e}(x) +_{e'} e'' = \psi_{e'/e}(x) +_{e'} \psi_{e'/e}(e'' -_e e') = \psi_{e'/e}(x +_e [e'' -_e e']) = (x +_e [e'' -_e e']) +_e e' = x +_e ([e'' -_e e'] +_e e') = x +_e e'' = \psi_{e''/e}(x)$. ■

Let $G[a, b, c]$ denote the subset of $(G,\cdot)$ generated by $a, b, c \in G$. If $[(xy)(zx)]y = [(xy)(zy)]x, \forall x, y, z \in G[a, b, c]$, then $(G[a, b, c],\cdot)$ is an SEQ.

**Lemma 3.1:** Let $(G, +)$ be an Abelian group. Fix $e \in G$. Define $xy \coloneqq e - (x + y) = e - y - x$. Then $(G,\cdot)$ is a commutative SEQ. Moreover, the induced group is $(G, +)$.

*Proof:*

Indeed $(G,\cdot)$ is commutative: $xy = e - (x + y) = e - (y + x) = yx, \forall x, y \in G$;

Next, $(G,\cdot)$ is left semisymmetric: $(xy)x = e - (e - x - y) - x = y, \forall x, y \in G$;

Finally, $(G,\cdot)$ is entropic: $(wx)(yz) = e - (e - w - x) - (e - y - z) = w + x + y + z - e = (wy)(xz), \forall w, x, y, z \in G$. ■

## 4. Construction of finite SEQs

The main result of this section is as follows:

**Theorem 1.1:** Every SEQ $(G,\cdot)$ is equivalent to an Abelian group $(G, +)$ reequipped with the product law $x \cdot y = k - \phi(x) - \phi^{-1}(y)$, where $\phi$ is a group automorphism of $(G, +)$ satisfying $\phi^3(x) = x$ and $k$ is a fixed point of $\phi$.

The above theorem gives a direct method for constructing finite SEQs for both commutative and non-commutative case. The proof is presented at the end of this section, but first we establish a series of necessary or related lemmas.

Commutativity allows for much more flexible products and are easier to characterize. The following lemma gives the first framework for decomposition of SEQs:

**Lemma 4.1:** Let $(G,\cdot)$ be a finite SEQ. Then $G$ has a commutative sub-SEQ $(H,\cdot)$.

*Proof:* Let $s_1 \in G$. Consider the sequence $s_1, \cdots, s_n$, with $n \geq 1$, where $s_{k+1} = s_k s_k$ for $k = 1, 2, \cdots, n - 1$, and $s_n s_n = s_1$.

Now note that $(s_k s_m)s_m = (s_k s_m)(s_{m-1}s_{m-1}) = (s_k s_{m-1})(s_m s_{m-1}) = (s_k s_{m-1})s_{m-1}$, thus inductively, we deduce that $(s_k s_n)s_n = (s_k s_l)s_l, \forall l \Rightarrow (s_k s_m)s_m = (s_k s_k)s_k = s_k$, thus, $s_m s_k = s_m[(s_k s_m)s_m] = s_k s_m$.

Hence, $G_1 := \{s_k | k = 1, 2, \cdots, n\}$ is commutative and consequently, $G_{r+1} := G_r G_r$ (the product, $AB$, of two sets $A$ and $B$ is the set of products $ab$, where $a \in A, b \in B$), are all commutative. Indeed, assume $G_r$ is commutative and suppose $ab, cd \in G_{r+1}$, with $a, b, c, d \in G_r$. Then $(ab)(cd) = (ac)(bd) = (ca)(db) = (cd)(ab)$.

Furthermore, $G_1 \subset G_2$ and $G_r \subset G_{r+1} \Rightarrow G_{r+1} = G_r G_r \subset G_{r+1}G_{r+1} = G_{r+2}$. This follows from the definitions of $G_{r+1}$ and $G_{r+2}$ as well as the fact that if $A \subset C, B \subset D$, then $AB \subset CD$. Indeed, if $x \in AB$, then $x = ab$ for some $a \in A, b \in B$, and since $a \in C, b \in D$, have $x = ab \in CD$.

Therefore, by induction on $r$, have a bounded infinite chain of commutative subsets: $G_1 \subset G_2 \subset G_3 \subset \cdots$, with $G_r \subset G$. So, have some $r_0 \geq 1$ such that $G_{r_0} = G_{r_0+1} = G_{r_0+2} = \cdots = H \subset G$, with $HH = G_{r_0}G_{r_0} = G_{r_0+1} = H$. Thus, $\cdot$ is closed in $H$ so that $(H, \cdot)$ is the desired commutative sub-SEQ of $G$. ■

**Corollary 4.1:** Let $(G, \cdot)$ be a finite non-commutative SEQ. If $G$ does not contain a nontrivial commutative sub-SEQ, then $|G| \equiv 1 \ (mod\ 3)$.

*Proof:*

From lemma 4.1, $G$ contains a commutative sub-SEQ, thus it must be trivial, that is $\{e\}$, some $e \in G$. Observe that $e$ is necessarily idempotent. For every $x \in G$, define $f(x) := ex$. We shall establish a few facts:

First, observe that $f(x) = e \Leftrightarrow x = e$.

Next, given any $e \neq x \in G$, cannot have $f(x) = x$ else $\{e, x\}$ would be a sub-SEQ. Thus, we must have $f(x) \neq x$.

Next, $f^{-1}(x) = xe$ from semisymmetric property and $f^3(x) = e[e(ex)] = [(xe)e]e = f^{-3}(x)$ from the quasi-associative property. So, $f^6(x) = x$. Let $m$ be the least positive integer such that $f^m(x) = x$. We shall call $m$ the cyclic order of $x$. It follows that $m|6$. Denote the set $\{f^k(x) | k \in \mathbb{N}\}$ by $< x >$.

Finally, $f(x)f(y) = (ex)(ey) = (ee)(xy) = e(xy) = f(xy)$. So $f$ is an automorphism of $(G, \cdot)$.

Now, suppose $x$ and $y$ are both of cyclic order at most 2. Then they commute, that is, $xy = yx$. Indeed, $xy = f^2(x)y = f[f(x)f^{-1}(y)] = f[(ex)(ye)] = f[(ey)(xe)] = f[f(y)f^{-1}(x)] = f^2(y)x = yx$. Moreover, $xy$ is also of order at most 2 since $f^2(xy) = f[f(x)f(y)] = f^2(x)f^2(y) = xy$. Thus, $\{x \in G | f^2(x) = x\}$ is a commutative sub-SEQ of $G$ and is thus trivial and not equal to $G$. Therefore, $f^2(x) = x \Leftrightarrow x = e$.

Hence, besides $e$, every element of $G$ are in classes of 3's or 6's and so $|G| \equiv 1 \ (mod\ 3)$. ■

Next, we characterize commutative SEQs. This is the converse of Lemma 3.1.

**Lemma 4.2:** Let $(G, \cdot)$ be a commutative SEQ. Then there is an Abelian group $(G, +)$ and $s \in G$ such that $x \cdot y = s - x - y$.

*Proof:*

Let $e \in G$. Set $x + y = (xy)e, s = ee$, then $(G, +)$ is an Abelian group with $x - y = y(ex)$. Therefore, $s - x - y = s - (x + y) = [(xy)e][es] = [(xy)e]e = [e(xy)]e = xy$. ■

The next lemma is an analogue of quotient groups. In what follows, the subset $H$ need not be special beyond the closure property. In some sense, it is naturally "normal" perhaps due to the semisymmetric property.

**Lemma 4.3:** Let $(G,\cdot)$ be an SEQ and let $H$ be a sub-SEQ with same product law. The set $G/H := \{xH | x \in G\}$ together with the operation $*$, defined on $G/H$ by $(xH) * (yH) := (xy)H$. Then $(G/H, *)$ is an SEQ with idempotent element $H$, and satisfies $|G| = |H| \cdot |G/H|$ (possibly infinite).

*Proof:*

First, we show well-definedness of $G/H$ as a collection of equivalent classes, where the equivalence relation is given by $x \sim y$ if $xs = ys'$ for some $s, s' \in H$. This is a well-defined equivalence relation since it is reflexive, symmetric and transitive. Reflexivity: $x \sim x$, holds by taking $s' = s = h$ for any choice of $h \in H$. Symmetry: $x \sim y \Rightarrow y \sim x$, holds since $xs = ys'ys' = xs$. Finally, transitivity: $x \sim y, y \sim z \Rightarrow x \sim z$, also holds since if $xs = ys'$ and $yt = zt''$ some $s, s', t, t' \in H$, then $z = t'[yt]$ and $(xs)z = (ys')(t'[yt]) = (ts')(t'[tt])$ by proposition 3.2. Let $s'' := (ts')(t'[tt])$, then, $s'' \in H$ and $(xs)z = s'' = (zs'')z$ implies $xs = zs''$ by cancellation property.

Now, let $x \sim y$. Then $xs = ys'$, with $s, s' \in H$. It follows that $(xs'')y \in H$ for all $s'' \in H$. That is $(xs'')(s'[xs]) \in H$. Indeed, $(xs'')(s'[xs]) = (ss'')(s'[ss]) \in H$. Thus, $xH = yH$. Conversely, if $xH = yH$, then $x \sim y$. Consequently, $|G| = |H| \cdot |G/H|$.

Next, we show well-definedness of $*$: if $xs_1 = x's_1', ys_2 = y's_2'$, with $s_i, s_i' \in H$, then $s \in H \Rightarrow (xy)s = (x'y')s'$, for some $s' \in H$. In particular,

$$
\begin{aligned}
s' &= [(xy)s][x'y'] \\
&= [(xy)s][(s_1'[xs_1])(s_2'[ys_2])] \\
&= [(xy)(s_1'[xs_1])][s(s_2'[ys_2])] \\
&= [(sy)(s_1'[ss_1])][s(s_2'[ys_2])] \\
&= [(ss_1')(y[ss_1])][s(s_2'[ys_2])] \\
&= [(ss_1')s][(y[ss_1])(s_2'[ys_2])] \\
&= s_1'[(y[ss_1])(s_2'[ys_2])] \\
&= s_1'[(s_1[ss_1])(s_2'[s_1s_2])] \\
&= s_1'[s(s_2'[s_1s_2])] \in H.
\end{aligned}
$$

$H$ is an element of $G/H$ since $H = sH$ for any $s \in H$. Moreover, $H * H = sH * sH = (ss)H = H$.

Finally, $(G/H, *)$ is an SEQ since it inherits the semisymmetric and entropic properties of $(G,\cdot)$: $(xH * yH) * xH = (xy)H * xH = [(xy)x]H = yH$ and $(wH * xH) * (yH * zH) = (wx)H * (yz)H = [(wx)(yz)]H = [(wy)(xz)]H = (wy)H * (xz)H = (wH * yH) * (xH * zH)$. ■

It is important to note that, like the case of groups, it is not necessarily the case that one can always *uniquely* recover the original SEQ, $G$, just from a sub-SEQ $H$, and the corresponding quotient $G/H$.

However, we at least have the following:

**Proposition 4.1:** The direct product of two SEQs $(G,\cdot)$ and $(G',\circ)$, together with operation $*$ defined by $(x,x')*(y,y') \coloneqq (x\cdot y, x'\circ y')$, is also an SEQ. Furthermore, given $e\in G, e'\in G'$, have isomorphism of groups $\left(G\times G', +_{(e,e')}\right) \equiv (G,+_e)\times(G',+_{e'})$.

**Lemma 4.4:** Let $(G,\cdot)$ be a finite commutative SEQ containing no idempotent element. Then there is an isomorphism $G\equiv T\times H$, for some commutative SEQ, $H$, containing an idempotent point, and some SEQ, $T=\mathbb{Z}_{3^{m_1}}\times\cdots\times\mathbb{Z}_{3^{m_N}}, N\geq 1$, with product law on $\mathbb{Z}_{3^{m_i}}$ satisfying $xy=s_i-x-y$ some $s_i$ coprime to 3 (where '$-$' is the usual subtraction on $\mathbb{Z}_{3^{m_i}}$).

*Proof:*

From Theorem 3.1, WLOG, let $G=\mathbb{Z}_{3^{m_1}}\times\cdots\times\mathbb{Z}_{3^{m_l}}\times\mathbb{Z}_{p_1^{n_1}}\times\cdots\times\mathbb{Z}_{p_k^{n_k}}, p_i\neq 3$. Let $+$ be the natural addition law on $G$. Then Lemma 4.2 implies $(x_1,\cdots,x_{l+k})\cdot(y_1,\cdots,y_{l+k})=(s_1-x_1-y_1,\cdots,s_{l+k}-x_{l+k}-y_{l+k})$, where WLOG, for $1\leq i\leq l$, have $3|s_i$ if and only if $i>N$, some $N\geq 1$. Let $T=\mathbb{Z}_{3^{m_1}}\times\cdots\times\mathbb{Z}_{3^{m_N}}, H=\mathbb{Z}_{3^{m_{N+1}}}\times\cdots\times\mathbb{Z}_{3^{m_l}}\times\mathbb{Z}_{p_1^{n_1}}\times\cdots\times\mathbb{Z}_{p_k^{n_k}}$ so that $G=T\times H$. Then $H$ has an idempotent element since $s_i=3x_i$ is solvable for $i>N$. ■

**Corollary 4.3:** Let $(G,\cdot)$ be a finite SEQ such that $|G|$ is not divisible by 3. Then $G$ contains an idempotent element.

*Proof:*

From Lemma 4.1, $G$ has a commutative sub-SEQ, $H$. Thus, it is enough to show that $H$ contains an idempotent element. The rest follows Lemma 4.4. ■

Now, indeed, besides commutative SEQs, there is another class of SEQs with a relatively straight forward characterization in relation to Abelian groups:

**Lemma 4.5:** $(G,\cdot)$ is an SEQ with an idempotent element $e$ if and only if there is an Abelian group $(G,+)$ with identity $e$ and a group automorphism $\phi: G\longrightarrow G$ with $\phi^3(x)=x$, such that $x\cdot y=-\phi(x)-\phi^{-1}(y)$.

*Proof:*

Suppose $(G,\cdot)$ is an SEQ with an idempotent element $e$. Let $\phi(x)\coloneqq e(ex)$, then $\phi^{-1}(x)=(xe)e, \phi^2(x)=e(e[e(ex)])=([(ex)e]e)e=(xe)e=\phi^{-1}(x)$. Let $x+y\coloneqq x+_e y=(ex)(ye)$, then $(G,+)$ is Abelian group with identity $e$. Next, we show that $\phi$ is an automorphism. It is enough to verify $\phi(x)+\phi(y)=\phi(x+y)$. Indeed, $\phi(x)+\phi(y)=(e[e(ex)])([e(ey)]e)=(e[e(ex)])(ey)=(ee)([e(ex)]y)=e([e(ex)]y)=e([(ee)(ex)]y)=e(e[(ex)(ye)])=\phi[(ex)(ye)]=\phi(x+y)$.

Finally, $e\phi(x)=-x$, so $-\phi(x)-\phi^{-1}(y)=[e\phi^2(x)]+[ey]=(e[e\phi^2(x)])([ey]e)=\phi^3(x)y=xy$.

Conversely, suppose $(G,+)$ is an Abelian group with identity $e$ and a group automorphism $\phi: G\longrightarrow G$ with $\phi^3(x)=x$. Let $x\cdot y=-\phi(x)-\phi^{-1}(y)$. Then $ee=e$ and $(wx)(yz)=-\phi(wx)-\phi^{-1}(yz)=-\phi\big(-\phi(w)-\phi^{-1}(x)\big)-\phi^{-1}\big(-\phi(y)-\phi^{-1}(z)\big)=\phi^2(w)+x+y+\phi(z)=\phi^2(w)+y+x+\phi(z)=(wy)(xz)$, so $(G,\cdot)$ is entropic. Finally, $(G,\cdot)$ is semisymmetric since $(xy)x=-\phi\big(-\phi(x)-\phi^{-1}(y)\big)-\phi^{-1}(x)=\phi^2(x)+y-\phi^{-1}(x)=y$. ■

This completes the proof of Theorem 4.1.

**Corollary 4.2:** Let $(G,\cdot)$ be an SEQ with an idempotent element $e$. Suppose $e$ does not commute with any other element, then $(G,\cdot)$ is idempotent. In this case, $(G,\cdot)$ corresponds to a Mendelsohn triple system [9].

*Proof:*

Suppose $e$ does not commute with any other element $(G,\cdot)$. Then $\phi(x) \coloneqq e(ex)$ implies $\phi(x) \neq x$ for $x \neq e$. Now $\phi[\phi^2(x) + \phi(x) + x] = x + \phi^2(x) + \phi(x)$, thus $\phi^2(x) + \phi(x) + x = e$. In particular, $xx = -\phi(x) - \phi^{-1}(x) = -\phi(x) - \phi^2(x) = x$.

**Proposition 4.2:** Let $(G,\cdot)$ be an SEQ. Suppose $e, e' \in G$ with $ee' = e'e$. Define $*$ on $G$ by $x * y \coloneqq [(ex)e']y = x[e'(ye)]$. Then $(G,*)$ is an SEQ. Moreover, $e * e = ee' = e'e, e' * e = e * e' = e'e'$.

*Proof:*

First observe that $(xe')e' = (xe')(e[e'e]) = (xe')(e[ee']) = (xe)(e'[ee']) = (xe)e$.

Left semisymmetric $(x * y)e = ([(ex)e']y)e = e'(y[e(ex)]) = e'(y[([e'e]e')(ex)]) = e'(y[([ee']e')(ex)]) = e'(y[([ee']e)(e'x)]) = e'(y[e'(e'x)]) = ([(e'x)e']y)e' = (xy)e'$

$\Rightarrow y * (x * y) = y(e'[(x * y)e]) = y(e'[(xy)e']) = y(xy) = x$;

Entropic: $(w * x) * (y * z) = (e'[(wx)e]) * (e'[(yz)e]) = e'([(e'[(wx)e])(e'[(yz)e])]e) = e'([(e'e')([(wx)e][(yz)e])]e) = e'([(e'e')([(wx)(yz)][ee])]e) = e'([(e'e')([(wy)(xz)][ee])]e) = (w * y) * (x * z), \forall w, x, y, z \in S$. ■

**Proposition 4.3:** Let $(G,\cdot)$ be an SEQ. Suppose $e, e' \in G$ with $ee' = e'e$. Define $*$ on $G$ by $x * y \coloneqq [(ex)e']y = x[e'(ye)]$. Then $\cdot$ can be recovered via $xy = [(e' * x) * e] * y = x * [e * (y * e')]$.

*Proof:*

Observe that $e' * x = [(ee')e']x = [(e'e)e']x = ex$. Therefore, $[(e' * x) * e] * y = [(ex) * e] * y = [(ex)(e'[ee])] * y = [([e(ex)]e')e] * y = [(e[([e(ex)]e')e])e']y = [([e(ex)]e')e']y = [(ex)(e'[e'e])]y = [(ex)(e'[ee'])]y = [(ex)e]y = xy$. ■

In fact, have:

**Theorem 4.2:** Let $(G,\cdot)$, be the direct product of two Abelian groups $(A,+_A) \times (B,+_B)$ together with the product law $(x_1,x_2) \cdot (y_1,y_2) = \big(s - x_1 - y_1, -\phi(x_2) - \phi^{-1}(y_2)\big)$, where $s \in A$ and $\phi$ is a group automorphism of $(B,+_B)$ satisfying $\phi^3(x) = x$. Then $(G,\cdot)$ is an SEQ.

*Proof:*

We need to show that $(G,\cdot)$ is both left semisymmetric and entropic.

Left semisymmetric: $[(x_1,x_2)(y_1,y_2)](x_1,x_2) = \big(s - x_1 - y_1, -\phi(x_2) - \phi^{-1}(y_2)\big)(x_1,x_2) = \Big(s - [s - x_1 - y_1] - x_1, -\phi\big(-\phi(x_2) - \phi^{-1}(y_2)\big) - \phi^{-1}(x_2)\Big) = \big(y_1, \phi^2(x_2) + y_2 - \phi^{-1}(x_2)\big) = (y_1,y_2)$.

Entropic: $[(x_1,x_2)(y_1,y_2)][(z_1,z_2)(w_1,w_2)] = \big(s - x_1 - y_1, -\phi(x_2) - \phi^{-1}(y_2)\big)\big(s - z_1 - w_1, -\phi(z_2) - \phi^{-1}(w_2)\big) = \Big(x_1 + y_1 + z_1 + w_1 - s, -\phi\big(-\phi(x_2) - \phi^{-1}(y_2)\big) - \phi^{-1}\big(-\phi(z_2) - \phi^{-1}(w_2)\big)\Big) = \big(x_1 + y_1 + z_1 + w_1 - s, \phi^2(x_2) + y_2 + z_2 + \phi^{-2}(w_2)\big)$ is symmetric in $(y_1,y_2)$, $(z_1,z_2)$, so that $[(x_1,x_2)(y_1,y_2)][(z_1,z_2)(w_1,w_2)] = [(x_1,x_2)(z_1,z_2)][(y_1,y_2)(w_1,w_2)]$ as desired. ■

*Proof of Theorem 1.1:*

(⇒)

Let $(G,\cdot)$ be an SEQ as usual. Let $e \in G$. Then $e$ and $ee$ commute. Thus, from proposition 4.2, set $x * y = [([ee]x)e]y$ on $G$. Then $(G,*)$ is an SEQ satisfying $e * e = e$. That is, $e$ is idempotent. Applying lemma 4.5, have Abelian group $(G,+)$ with identity $e$ and a group automorphism $\phi: G \longrightarrow G$ with $\phi^3(x) = x$, such that $x * y = -\phi(x) - \phi^{-1}(y)$. From proposition 4.3, we recover $(G,\cdot)$ by via $x \cdot y = [(e * x) * (ee)] * y = -\phi(-\phi[-\phi(e) - \phi^{-1}(x)] - \phi^{-1}[ee]) - \phi^{-1}(y) = [ee] - \phi(x) - \phi^{-1}(y)$. Setting $x = ee, y = e$, have $e = xy = [ee] - \phi[ee]$ and so $\phi[ee] = ee$, that is, $ee$ is a fixed point of $\phi$.

(⇐)

Conversely, suppose $(G,+)$ is an Abelian group reequipped with the product law $x \cdot y = k - \phi(x) - \phi^{-1}(y)$, where $\phi$ is a group automorphism of $(G,+)$ satisfying $\phi^3(x) = x$ and $k$ is a fixed point of $\phi$. Then $(G,\cdot)$ is semisymmetric since $(xy)x = k - \phi\big(k - \phi(x) - \phi^{-1}(y)\big) - \phi^{-1}(x) = y$ and it is also entropic since $(wx)(yz) = k - \phi\big(k - \phi(w) - \phi^{-1}(x)\big) - \phi^{-1}\big(k - \phi(y) - \phi^{-1}(z)\big) = -k + \phi^{-1}(w) - x - y + \phi(z) = (wy)(xz)$.

## 5. Conclusion

In conclusion, SEQs form a special class of central quasigroups as presented in Theorem 1.1. Theorem 1.1 gives an efficient method for constructing SEQs. This is contingent on finding a corresponding group automorphism, $\phi$, of order 1 or 3. This approach is relatively straight forward for finite groups especially those of prime order [see appendix]. We present explicit examples in the appendix for all the possible cases (up to isomorphism) where the order is at most 6.

Now by considering the identity element, it is easy to see that $\phi$ is of order 3 precisely when the target SEQ is non-commutative. Future research can investigate the existence and distribution of all such SEQs up to isomorphism.

## Acknowledgements

This research is based on results obtained by the author in his master's thesis and was sponsored by the People's Republic of China under the Alliance of International Science Organizations Scholarship. I am immensely grateful for their continued and unwavering support of natural sciences. The author is immensely grateful for the guidance and continual support of his supervisor Prof. Li Jiayu.

**Funding:** This research was sponsored by the People's Republic of China under the Alliance of International Science Organizations Scholarship via the Alliance of International Science Organizations (ANSO Series No. 2021 - Master - USTC - 010).

**Conflict of Interests:** The author declares no conflict of interest.

## References

[1] I. M. H. Etherington, "Quasigroups and cubic curves," *Proceedings of the Edinburgh Mathematical Society*, 14(2), 273–291, **1965**.

[2] D. Stanovský and P. Vojtěchovský, "Central and medial quasigroups of small order," *Buletinul Academiei de Ştiinţe a Republicii Moldova Matematica*, 80(1), 24–40, **2016**.
[3] B. Young, "Totally symmetric and medial quasigroups and their applications," Master's Thesis, Case Western Reserve University, May **2021**.
[4] V. A. Shcherbacov, "On the structure of finite medial quasigroups," *Buletinul Academiei de Ştiinţe a Republicii Moldova Matematica*, 47(1), 11–18, **2005**.
[5] J. H. Silverman and J. T. Tate, Rational points on elliptic curves, 2nd ed. Cham, Switzerland: Springer, **2015**.
[6] O. U. Kirnasovsky, "Linear isotopes of small order groups," *Quasigroups and Related Systems*, 2(1), 51–82, **1995**.
[7] A. Drápal, "Group isotopes and a holomorphic action," *Resultate der Mathematik*, 54(3–4), 253–272, **2009**.
[8] J. D. H. Smith, "Centrality," Chapter III in *Quasigroups and Loops: Theory and Applications*, O. Chein, H. O. Pflugfelder, and J. D. H. Smith, Eds. Berlin: Heldermann, **1990**.
[9] F. E. Bennett, "Self-orthogonal semisymmetric quasigroups," *Journal of Combinatorial Theory, Series A*, 33, 117–119, **1982**.

***Supplementary Information**

We conclude by presenting the first few examples via their Cayley graphs. They are complete and distinct up to isomorphism. Let $|G| = n$.

For non-commutative cases, following from Lemma 4.1, we start with a smaller commutative case (whose order must divide $n$) and build upwards. The most straightforward constructions are direct products.

**The case $n = 1$:**

| · | **0** |
|---|---|
| **0** | 0 |

*Table 2-Order 1 SEQ.*

Table 3 shows a representation of the case $n = 1$. This is commutative and induces $C_1$.

**The case $n = 2$:**

| · | **0** | **1** |
|---|---|---|
| **0** | 0 | 1 |
| **1** | 1 | 0 |

*Table 3- Order 2 SEQ.*

Table 4 shows a representation of the case $n = 2$, with idempotent element $0$. This is commutative and induces $C_2$.

**The case $n = 3$:**

| · | **0** | **1** | **2** |
|---|---|---|---|
| **0** | 0 | 2 | 1 |
| **1** | 2 | 1 | 0 |
| **2** | 1 | 0 | 2 |

*Table 4- Order 3 SEQ with idempotent elements.*

Table 5 shows a representation of the case $n = 3$, where all elements are idempotent. This is commutative and induces $C_3$.

| · | **0** | **1** | **2** |
|---|---|---|---|
| **0** | 1 | 0 | 2 |
| **1** | 0 | 2 | 1 |
| **2** | 2 | 1 | 0 |

*Table 5- Order 3 SEQ with no idempotent element.*

Table 6 shows a representation of the case $n = 3$, with no idempotent element. This is commutative and induces $C_3$.

**The case $n = 4$:**

| · | **0** | **1** | **2** | **3** |
|---|---|---|---|---|
| **0** | 0 | 1 | 2 | 3 |
| **1** | 1 | 0 | 3 | 2 |
| **2** | 2 | 3 | 0 | 1 |
| **3** | 3 | 2 | 1 | 0 |

*Table 6- Order 4 SEQ with one idempotent element 0 and all elements, x, satisfying xx=0.*

Table 7 shows a representation of the case $n = 4$, with $xx = 0$. This is commutative and induces $C_2 \times C_2$.

| · | **0** | **1** | **2** | **3** |
|---|---|---|---|---|
| **0** | 0 | 3 | 2 | 1 |
| **1** | 3 | 2 | 1 | 0 |
| **2** | 2 | 1 | 0 | 3 |
| **3** | 1 | 0 | 3 | 2 |

*Table 7- Order 4 SEQ given by xy=-x-y.*

Table 8 shows a representation of the case $n = 4$, via the most trivial formulation: $xy = -x - y$. This is commutative and induces $C_4$.

| · | **0** | **1** | **2** | **3** |
|---|---|---|---|---|
| **0** | 0 | 2 | 3 | 1 |
| **1** | 3 | 1 | 0 | 2 |
| **2** | 1 | 3 | 2 | 0 |
| **3** | 2 | 0 | 1 | 3 |

*Table 8- Order 4 SEQ with idempotent elements.*

Table 9 shows a representation of the case $n = 4$, that is idempotent and also non-commutative. It induces $C_2 \times C_2$.

**The case $n = 5$:**

| · | **0** | **1** | **2** | **3** | **4** |
|---|---|---|---|---|---|
| **0** | 0 | 4 | 3 | 2 | 1 |
| **1** | 4 | 3 | 2 | 1 | 0 |
| **2** | 3 | 2 | 1 | 0 | 4 |
| **3** | 2 | 1 | 0 | 4 | 3 |
| **4** | 1 | 0 | 4 | 3 | 2 |

*Table 9- The unique (up to isomorphism) order 5 SEQ.*

Table 10 shows a representation for the case $n = 5$, This is commutative and induces $C_5$.

**The case $n = 6$:**

| · | **0** | **1** | **2** | **3** | **4** | **5** |
|---|---|---|---|---|---|---|
| **0** | 0 | 5 | 4 | 3 | 2 | 1 |
| **1** | 5 | 4 | 3 | 2 | 1 | 0 |
| **2** | 4 | 3 | 2 | 1 | 0 | 5 |
| **3** | 3 | 2 | 1 | 0 | 5 | 4 |
| **4** | 2 | 1 | 0 | 5 | 4 | 3 |
| **5** | 1 | 0 | 5 | 4 | 3 | 2 |

*Table 10- Order 6 SEQ containing some idempotent elements.*

This is commutative and induces $C_2 \times C_3$.

| · | **0** | **1** | **2** | **3** | **4** | **5** |
|---|---|---|---|---|---|---|
| **0** | 2 | 1 | 0 | 5 | 4 | 3 |
| **1** | 1 | 0 | 5 | 4 | 3 | 2 |
| **2** | 0 | 5 | 4 | 3 | 2 | 1 |
| **3** | 5 | 4 | 3 | 2 | 1 | 0 |
| **4** | 4 | 3 | 2 | 1 | 0 | 5 |
| **5** | 3 | 2 | 1 | 0 | 5 | 4 |

*Table 11- Order 6 SEQ containing no idempotent element.*

Tables 11 and 12 are the order 6 SEQs, but which are commutative and induce $C_2 \times C_3$.

The next two are **not** SEQs (see tables 13 and 14 below), they are the result of constructing non-commutative semisymmetric quasigroups of order 6, they can be verified as non-SEQs by simply finding the potential Abelian isotropic group (and confirm that they are indeed not groups):

| · | **0** | **1** | **2** | **3** | **4** | **5** |
|---|---|---|---|---|---|---|
| **0** | 2 | 1 | 0 | 3 | 4 | 5 |
| **1** | 1 | 0 | 3 | 4 | 5 | 2 |
| **2** | 0 | 5 | 4 | 1 | 2 | 3 |
| **3** | 3 | 2 | 5 | 0 | 1 | 4 |
| **4** | 4 | 3 | 2 | 5 | 0 | 1 |
| **5** | 5 | 4 | 1 | 2 | 3 | 0 |

*Table 12-An example of a non-SEQ that is semisymmetric.*

| · | **0** | **1** | **2** | **3** | **4** | **5** |
|---|---|---|---|---|---|---|
| **0** | 0 | 1 | 4 | 3 | 2 | 5 |
| **1** | 1 | 0 | 5 | 2 | 3 | 4 |
| **2** | 4 | 3 | 2 | 5 | 0 | 1 |
| **3** | 3 | 4 | 1 | 0 | 5 | 2 |
| **4** | 2 | 5 | 0 | 1 | 4 | 3 |
| **5** | 5 | 2 | 3 | 4 | 1 | 0 |

*Table 13- Another example of a non-SEQ that is semisymmetric.*

Now, let $n = p$ where $p$ is prime greater than 3. Then either $(G,\cdot)$ is commutative or it contains an idempotent element by lemma 4.1. Thus, as the case maybe, using Lemma 4.2 or a combination of corollary 4.3 and lemma 4.5, we can always find an idempotent element and have $x \cdot y = -\phi(x) - \phi^{-1}(y)$, so $\phi^3 = Id$. Also, $(G,+) = \mathbb{Z}/n\mathbb{Z}$ and thus contains a primitive root $g$, modulo $p$, so that every automorphism $\phi$, is of the form $\phi(x) \equiv ax \ (mod\ p)$ some $a^3 \equiv 1 \ (mod\ p)$.

Two cases arise:

If $p \equiv 1 \ (mod\ 3)$. Then $a = 1, g^{\frac{p-1}{3}}, g^{\frac{2(p-1)}{3}}$ . Thus, $x \cdot y \equiv -g^{\frac{p-1}{3}}x - g^{\frac{2(p-1)}{3}}y \ (mod\ p)$. These are pairwise non-isomorphic.

If $p \equiv 2\ (mod\ 3)$. Then $a = 1$ and $x \cdot y = -x - y$.

For instance, $p = 7$. Have $x \cdot y \coloneqq -x - y\ (mod\ 7)$ or $x \cdot y \coloneqq 5x + 3y\ (mod\ 7)$ or $x \cdot y \coloneqq 3x + 5y\ (mod\ 7)$.

Finally, observe that complications only arise when 3 divides $n$. This follows from corollary 4.3. In particular, let us consider powers of 3. Let $(G,\cdot)$ be a finite non-commutative SEQ such that $|G|$ is a power of 3. Then from lemma 4.1, $G$ has a commutative sub-SEQ. Let $H \subset G$ be a maximal commutative sub-SEQ of $G$, that is, if $H \subset L \subset G$ where $L$ is a commutative sub-SEQ of $G$, then $L = H$. Since $G \neq H$, have, $|G/H|$ is a power of 3 and thus, from corollary 4.1, $G/H$ has a commutative sub-SEQ of order at least 3. In fact, $G/H$ has a commutative sub-SEQ of order 3, say $\{H, aH, bH\}$. Then $(aa)H = aH, (ab)H = (ba)H = H, (bb)H = bH$. It follows that $ab, ba \in H$. Let $ab = h_1, ba = h_2$, so that $b = h_1 a = a h_2 \in aH, a \in bH$. Then,

$$(H)(H) = H,$$

$$(H)(aH) = (h_1 H)(aH) = (h_1 a)(HH) = bH,$$

$$(H)(bH) = (h_2 H)(bH) = (h_2 b)(HH) = aH,$$

$$(aH)(H) = (aH)(h_2 H) = (ah_2)(HH) = bH,$$

$$(aH)(aH) = (aa)(HH) = (aa)H = aH,$$

$$(aH)(bH) = (ab)(HH) = h_1 H = H,$$

$$(bH)(H) = (bH)(h_1 H) = (bh_1)(HH) = aH,$$

$$(bH)(aH) = (ba)(HH) = h_2 H = H,$$

$$(bH)(bH) = (bb)(HH) = (bb)H = bH.$$

Let $L = H \cup aH \cup bH$. Then $LL = L$. So $L$ is a sub-SEQ. From the maximality of $H$, $L$ cannot be commutative. Let $x \in L, x \notin H, h \in H$. Then $\phi_x(h) \coloneqq x(xh) \in H$. Indeed, WLOG, let $x \in aH$, then $x = ah', x(xh) = (ah')(xh) = (ax)(h'h) \in H$ iff $a(ah') \in H$. Now $a(ah') = (bh_1)(ah') = (ba)(h_1 h') = h_2(h_1 h') \in H$. In particular, $x(xh) = (h_2[h_1 h'])(h'h) = (h_2[h_1 h'])(hh') = (h_2 h)([h_1 h']h') = (h_2 h)h_1$ is independent of $h'$. It suffices to consider only $\phi_a$ and $\phi_b$. In fact, $\phi_a^2 = \phi_a^{-1} = \phi_b$. Suppose $x_0 h = h x_0 x_0 \in L, x_0 \notin H$, then WLOG $(h_2 h)h_1 = h$ and $h_1 = h_2$, so $ab = ba$ and $xh = hx$. This implies commutativity, thus given $x, y \in L$ with $xy = yx$, must have $x, y \in H$.