A Method for Finding New Sets of Axioms for Classes of Semigroups

João Araújo
Universidade Aberta, R. Escola Politécnica, 147
1269-001 Lisboa, Portugal
&
Centro de Álgebra, Universidade de Lisboa
1649-003 Lisboa, Portugal, mjoao@lmc.fc.ul.pt

Janusz Konieczny*
Department of Mathematics, University of Mary Washington
Fredericksburg, VA 22401, USA, jkoniecz@umw.edu

Abstract

We introduce a general technique for finding sets of axioms for a given class of semigroups. To illustrate the technique, we provide new sets of defining axioms for groups of exponent n, bands, and semilattices.

2010 *Mathematics Subject Classification.* 08B05, 03C05, 20A05, 20M20.

1 Introduction

The general aim of providing new sets of axioms that equivalently define a given mathematical structure has been the source of considerable research and progress in mathematics. About one hundred years ago Boolean algebras attracted this kind of attention in the pioneer work of Sheffer [35], but this was just the first of a vast number of papers (for example, [9], [10], [12], [17], [20], [23], [26], [28], [31], [39], [41]).

The same can be said about other theories (see, for example, [11], [16], [21], [25], [27], [32], [33], [34], [37], [42], [43]).

However, one cannot speak about the general problem of finding new sets of axioms without assigning to groups the most notable place (see the survey paper [30], and also [4], [6], [14], [18], [19], [22], [29], [36], [38], [40]).

Semigroup theory, as a topic developed under the guidance of A.H. Clifford, might be seen as a product of these kinds of axiomatic considerations (see [7], Section 6).

It is well known that groups can be defined by a single axiom (see [6]), but the analogous result for, e.g., inverse semigroups (one of the most important classes of semigroups apart from groups) does not hold (see [3]). It is clear that semigroups offer an enormous field full of challenges for mathematicians and for experts in automated reasoning willing to find new sets of axioms for the many notable sub-classes of semigroups.

*This author was supported by a University of Mary Washington professional activity grant.

The aim of this paper is to provide a general tool for finding new sets of axioms for classes of semigroups. In Section 2 we give a general explanation of the technique. This method uses the Cayley representation for semigroups, but it can be similarly used with different representations. Section 3 is a detailed illustration of the technique applied to the case of bands. In this section we show how the new defining axioms for bands are found, we prove that they really define bands, and the independence of the axioms is verified (see Theorem 3.3 and also Theorem 3.5). Finally, in Section 4 we apply the technique to the class of groups of exponent n, incidentally finding a single defining identity of these groups in the class of groupoids with 1 (see Theorem 4.2).

2 A Method Using Cayley Representation

The usual way of defining a class of semigroups is to specify some additional conditions that a semigroup must satisfy to belong to the class. For example, we say that a semigroup S is *regular* if for all $a \in S$, there is $x \in S$ such that $axa = a$ [8, page 50]. We just defined the class of regular semigroups. Note that the starting point of this definition is a semigroup S, that is, associativity is one of the explicitly given axioms: for all $a, b, c \in S$, $a(bc) = (ab)c$.

In our method of finding new axioms for a class of semigroups, we will not start with a semigroup, but rather with a groupoid or a groupoid with a (right or two-sided) identity element. The associativity axiom will not be stated explicitly but it will follow from other axioms. A way to replace the associativity axiom with equivalent axiom or axioms is given by the following observation. Suppose that we have a Cayley table for a groupoid $(S, *)$. The rows and columns of the table can be viewed as mappings from S to S. Then the multiplication $*$ is associative if and only if every row commutes with every column.

To be more precise we introduce some definitions. A *groupoid* is a pair $(S, *)$, where S is a non-empty set and $*$ is a binary operation on S. For a non-empty set X, we denote by $T(X)$ the monoid of full transformations on X. The monoid $T(X)$ consists of all functions $\alpha : X \to X$ with the function composition as multiplication (for $\alpha, \beta \in T(X)$ and $x \in X$, $(\alpha\beta)(x) = \alpha(\beta(x))$).

Let S be a groupoid. Every element $s \in S$ induces in a natural way mappings $\underline{s}$ and $\overline{s}$ from S to S defined by: $\underline{s}(x) = sx$ and $\overline{s}(x) = xs$. In other words, the mappings $\underline{s}$ and $\overline{s}$ are elements of $T(S)$ induced by the rows and columns, respectively, of the Cayley table for S.

The following lemma, well acknowledged in group theory but almost never mentioned by semigroup theorists, says that a groupoid S is a semigroup if and only if its Cayley table rows commute with its Cayley table columns.

Lemma 2.1 *Let S be a groupoid. Then S is a semigroup if and only if $\underline{s}\,\overline{t} = \overline{t}\,\underline{s}$ for all $s, t \in S$.*

Proof: For all $s, t, x \in S$

$$\begin{aligned}(\underline{s}\,\overline{t})(x) = (\overline{t}\,\underline{s})(x) \quad &\Leftrightarrow \quad \underline{s}(\overline{t}(x)) = \overline{t}(\underline{s}(x)) \\ &\Leftrightarrow \quad \underline{s}(xt) = \overline{t}(sx) \\ &\Leftrightarrow \quad s(xt) = (sx)t.\end{aligned}$$

The result follows. ■

In view of Lemma 2.1, we will be interested in the centralizers of transformations $\underline{s} \in T(S)$, where s is an element of a semigroup S.

For $\alpha \in T(X)$, the *centralizer* of α is a subset $C(\alpha)$ of $T(X)$ defined by:

$$C(\alpha) = \{\beta \in T(X) : \alpha\beta = \beta\alpha\}.$$

It is clear that $C(\alpha)$ is a submonoid of $T(X)$.

Let S be a semigroup. Define $\lambda : S \to T(S)$ by: $\lambda(s) = \underline{s}$. The mapping λ is a homomorphism, called the *left regular representation* of S. For every $s \in S$, the transformation $\lambda(s) = \underline{s}$ is called a *left inner translation* of S. The image $\lambda(S)$ is a subsemigroup of $T(S)$, which is isomorphic to S if S has a right identity element. Similarly, we have an anti-homomorphism $\rho : S \to T(S)$ defined by: $\rho(t) = \overline{t}$. For every $t \in S$, the transformation $\rho(t) = \overline{t}$ is called a *right inner translation* of S.

We are now ready to describe our method. Let $\mathcal{C}$ be a class of semigroups and suppose we want to find a (new) set of axioms for this class. We proceed as follows. Let $S \in \mathcal{C}$.

(A) Find necessary conditions that the elements of $\lambda(S)$ must satisfy. For example, if $\mathcal{C}$ is a class of groups, then every $\underline{s} \in \lambda(S)$ must be a permutation of S.

(B$_1$) For all $s \in S$, characterize the centralizer $C(\underline{s})$.

(B$_2$) Use the characterization obtained in (B$_1$) to find necessary conditions that a right inner translation $\overline{t}$ must satisfy to commute with $\underline{s}$ $(s, t \in S)$.

(C) Translate the conditions obtained in (A) and (B$_2$) to abstract conditions (axioms) for S.

(D) Prove that the axioms obtained in (C) define the class $\mathcal{C}$.

If the axioms obtained in (C) do not define the class $\mathcal{C}$, we go back to (A) and (B$_2$) and try to find more conditions that transformations in $\lambda(S)$ and transformations in $C(\underline{s})$ must satisfy. If we have a set of axioms for $\mathcal{C}$, it may be possible to simplify this set. For example, the axioms may not be independent, in which case it will be possible to remove some of them. It may also happen that some axioms are not first order, in which case we may try to replace them with first-order statements (statements whose quantifiers range over elements of S).

3 Application to Bands

In this section we apply the method described in (A)–(D) of Section 2 to the class $\mathcal{C}$ of bands with a right identity element. We will obtain a set of independent axioms for this class that avoids the associativity law.

A *band* is a semigroup S that consists entirely of idempotents, that is, $aa = a$ for every $a \in S$. Let S be a band. For a function f, we denote by $\mathrm{dom}(f)$ the domain of f, by $\mathrm{im}(f) = \{f(x) : x \in \mathrm{dom}(f)\}$ the image of f, and by $\ker(f) = \{((x, y) \in \mathrm{dom}(f) \times \mathrm{dom}(f) : f(x) = f(y)\}$ the kernel of f.

(A) Find necessary conditions that the elements of $\lambda(S)$ must satisfy.

Since $\lambda : S \to T(S)$ is a homomorphism, $\underline{s} \in \lambda(S)$ is an idempotent transformation for every $s \in S$. Since every idempotent transformation fixes every element of its image, we have that for all $s, y \in S$,

$$y \in \operatorname{im}(\underline{s}) \Rightarrow \underline{s}(y) = y. \tag{3.1}$$

(B$_1$) For all $s \in S$, characterize the centralizer $C(\underline{s})$.

A description of the centralizers of idempotent transformations on an arbitrary set is provided in [1] and [2]:

Lemma 3.1 *Let $\alpha, \beta \in T(X)$ where α is an idempotent. Then $\beta \in C(\alpha)$ if and only if:*

(1) $\beta(\operatorname{im}(\alpha)) \subseteq \operatorname{im}(\alpha)$*;*

(2) *For all $x, y \in X$, if $(x, y) \in \ker(\alpha)$ then $(\beta(x), \beta(y)) \in \ker(\alpha)$.*

(B$_2$) Find necessary conditions that $\bar{t} \in C(\underline{s})$ must satisfy.

Let $s, t \in S$. Then $\bar{t} \in C(\underline{s})$ by Lemma 2.1. Thus, by Lemma 3.1, we have for all $x, y \in S$,

$$\bar{t}(\operatorname{im}(\underline{s})) \subseteq \operatorname{im}(\underline{s}), \tag{3.2}$$

$$(x, y) \in \ker(\underline{s}) \Rightarrow (\bar{t}(x), \bar{t}(y)) \in \ker(\underline{s}). \tag{3.3}$$

(C) Translate the conditions obtained in (A) and (B$_2$) to abstract conditions for S.

Conditions (3.1), (3.2) and (3.3) translate, respectively, to $y = sx \Rightarrow sy = y$, $(sS)t \subseteq sS$, and $sx = sy \Rightarrow s(xt) = s(yt)$. It is clear that the axiom $y = sx \Rightarrow sy = y$ is equivalent to the identity $s(sx) = sx$. Changing the names of the variables, we obtain for all $a, b, c, d \in S$,

$$a(ab) = ab, \tag{3.4}$$

$$(aS)b \subseteq aS, \tag{3.5}$$

$$ab = ac \Rightarrow a(bd) = a(cd). \tag{3.6}$$

(D) Prove that the axioms obtained in (C) define the class $\mathcal{C}$.

We prove that, in the class of groupoids, (3.4)–(3.6) define the class of semigroups satisfying the identity $a(ab) = ab$. In the class of groupoids with a right identity element, (3.4)–(3.6) define the class of bands. A right identity element is needed for bands since when we pass from a semigroup S to $\lambda(S)$, we cannot tell the difference between the axioms $aa = a$ and $a(ab) = ab$. Both axioms translate to $\lambda(a)$ being an idempotent for all $a \in S$. Indeed, if $aa = a$, then $\lambda(a) = \lambda(aa) = \lambda(a)\lambda(a)$; and if $a(ab) = ab$, then for all $b \in S$, $\lambda(a)(b) = ab = a(ab) = (aa)b = \lambda(aa)(b)$, and so $\lambda(a) = \lambda(aa) = \lambda(a)\lambda(a)$.

Theorem 3.2 *Let S be a groupoid. Then S is a semigroup satisfying the identity $a(ab) = ab$ if and only if* (3.4)–(3.6) *hold for all $a, b, c, d \in S$. In particular, if S has a right identity element, the S is a band if and only if* (3.4)–(3.6) *hold for all $a, b, c, d \in S$.*

Proof: It is clear that (3.4)–(3.6) hold for every semigroup satisfying the identity $a(ab) = ab$. Conversely, suppose that the groupoid S satisfies (3.4)–(3.6).

For all $s, x \in S$, we have $s(sx) = sx$ by (3.4), and so $\underline{s}(\underline{s}(x)) = s(sx) = sx = \underline{s}(x)$. Thus every element of $\lambda(S)$ is an idempotent. Let $s, t \in S$. We will prove that $\bar{t} \in C(\underline{s})$. First, by (3.5), $(sS)t \subseteq sS$, and so

$$\bar{t}(\mathrm{im}(\underline{s})) = \bar{t}(sS) = (sS)t \subseteq sS = \mathrm{im}(\underline{s}).$$

Second, suppose $(x, y) \in \ker(s)$, that is, $\underline{s}(x) = \underline{s}(y)$. Then $sx = sy$, and so, by (3.6), $s(xt) = s(yt)$. Thus

$$\underline{s}(\bar{t}(x)) = \underline{s}(xt) = s(xt) = s(yt) = s(\bar{t}(y)) = \underline{s}(\bar{t}(y)),$$

and so $(\bar{t}(x), \bar{t}(y)) \in \ker(\underline{s})$. Hence $\bar{t} \in C(\underline{s})$ by Lemma 3.1, and so S is a semigroup by Lemma 2.1. Of course, S satisfies the identity $a(ab) = ab$ by (3.4).

Now, suppose a groupoid S has a right identity element. It is clear that (3.4)–(3.6) hold for every band. Conversely, suppose that S satisfies (3.4)–(3.6). We have already established that S is a semigroup and that every element of $\lambda(S)$ is an idempotent. Since S has a right identity element, S is isomorphic to $\lambda(S)$, and so S is a band. ■

Note that (3.5) can be expressed as a first-order proposition:

$$\forall(a, b, x \in S)\, \exists(y \in S)\, ((ax)b = ay).$$

This proposition contains the existential quantifier, but it is possible to replace it with the following universally quantified proposition: for all $a, b, c, d \in S$,

$$a((ab)c) = (ab)c. \tag{3.7}$$

We note that (3.7) implies (3.5): Let $(ax)b \in (aS)b$. By (3.7), we have $(ax)b = a((ax)b) \in aS$. Therefore $(aS)b \subseteq aS$. Clearly every band S satisfies (3.7), and so Theorem 3.2 gives:

Theorem 3.3 *Let S be a groupoid with a right identity element. Then S is a band if and only if* (3.4), (3.6), *and* (3.7) *hold for all $a, b, c, d \in S$:*

Observe that (3.5) does not imply (3.7), but (3.4) and (3.5) together do imply (3.7). Hence we have:

Corollary 3.4 *Let S be a groupoid with a right identity element. Then the following are equivalent:*

(a) *S is a band.*

(b) *S satisfies* (3.4), (3.5), *and* (3.6).

(c) *S satisfies* (3.4), (3.6), *and* (3.7).

*	1	a	b	c
1	1	a	b	c
a	a	a	a	c
b	b	a	b	c
c	c	a	b	c

*	1	a	b	c
1	1	a	b	c
a	a	a	a	c
b	b	c	c	c
c	c	c	c	c

Figure 1: Independence of (3.4), (3.5), and (3.6).

*	1	a	b	c
1	1	a	b	c
a	a	c	c	c
b	b	c	a	c
c	c	c	c	c

*	1	a	b	c
1	1	a	b	c
a	a	a	a	c
b	b	a	c	c
c	c	a	a	c

Figure 2: Independence of (3.4), (3.6), and (3.7).

We will prove that the axioms (3.4), (3.5), and (3.6) are independent. First observe that a group with at least two elements satisfies (3.5) and (3.6) but it does not satisfy (3.4). Thus (3.4) is independent from (3.5) and (3.6).

To prove that (3.5) is independent from (3.4) and (3.6), let S be the groupoid on the left in Figure 1. It is straightforward to verify that S satisfies (3.4) and (3.6). However, $(aS)b = \{ab, cb\} = \{a, b\}$ and $aS = \{a, c\}$, so S does not satisfy (3.5).

Finally, it is easy to verify that the groupoid on the right in Figure 1 satisfies (3.4) and (3.5), but it does not satisfy (3.6) because $aa = ab$ but $a(ab) \neq a(bb)$. We have proved that the axioms (3.4)–(3.6) are independent.

Now we prove that (3.4), (3.6) and (3.7) ((1), (2), and (3) of Theorem 3.3) are independent. First, (3.4) and (3.6) do not imply (3.7) since they do not imply (3.5) and (3.7) implies (3.5). The left groupoid in Figure 2 satisfies (3.6) and (3.7) but it does not satisfy (3.4) since $bb = a$ and $ba = c$. Finally, the groupoid on the right in Figure 2 satisfies (3.4) and (3.7) but it does not satisfy (3.6) since $ab = a = aa$ and $a(bb) = c \neq a = a(ab)$.

Observe that every semigroup satisfies conditions (3.5) and (3.6). However, the converse does not hold as the groupoid in Figure 3 shows. That groupoid satisfies (3.5) and (3.6), but it is not a semigroup since it does not have an idempotent whereas every finite semigroup has an idempotent. Thus we propose the following problem:

Problem. Is it possible to find a set P of independent axioms containing (3.5) and (3.6) such that a groupoid is a semigroup if and only if it satisfies the axioms in P?

*	a	b	c
a	b	a	c
b	a	c	b
c	c	b	a

Figure 3: Groupoid satisfying (3.5) and (3.6) that is not a semigroup.

The axioms of Theorem 3.3 can be easily modified to obtain the following result about semilattices (commutative bands).

Theorem 3.5 *Let S be a groupoid with a left identity element. Then S is a semilattice if and only if it satisfies the following axioms:*

(1) $a(ab) = ab$;

(2) $ab = ac \Rightarrow a(bd) = a(dc)$;

(3) $a((ab)c) = (ab)c$.

Proof: It is clear that every semilattice satisfies (1)–(3). Conversely, suppose that a groupoid S with a left identity element, say f, satisfies (1)–(3). Taking $a = f$ and $b = c$ in (2), we obtain $bd = db$ for all $b, d \in S$. Thus S is commutative and f is also a right identity element. But then (2) implies (3.6), and so S is a band by Theorem 3.3. Therefore, S is a semilattice. ■

We point out that axioms (1)–(3) do not work if we do not assume that a groupoid S has a left identity element. Indeed, suppose S is a left zero semigroup, that is, $xy = x$ for all $x, y \in S$. Then (1)–(3) are clearly satisfied (and every element of S is a right identity element) but S is not a semilattice (if S has more than one element).

4 Application to Groups of Exponent n

In this section we apply the method described in (A)–(D) of Section 2 to the class $\mathcal{C}$ of groups of exponent n. We will obtain a single axiom that defines this class in the class of groupoids with a right identity element.

Let $n \geq 1$ be an integer. We say that a group G is a *group of exponent* n if $x^n = 1$ for every $x \in G$. Let G be a group of exponent n.

(A) Find necessary conditions that the elements of $\lambda(G)$ must satisfy.

For an integer $k \geq 0$ and $\alpha \in T(X)$, we denote by α^k the composition of α with itself k times, where it is understood that $\alpha^0 = \mathrm{id}_X$ (the identity transformation on X).

Since $\lambda : G \to T(G)$ is a homomorphism, we have $\underline{s}^n = \mathrm{id}_X$ for every $s \in G$. Thus, for every $x \in G$,

$$\underline{s}^n(x) = x. \tag{4.1}$$

(B$_1$) For all $s \in G$, characterize the centralizer $C(\underline{s})$.

Let $\delta \in T(X)$ be one-to-one. Denote by $S(\delta)$ and $F(\delta)$ the following subsets of X:

$$S(\delta) = \{x \in X : \delta(x) \neq x\} \quad \text{and} \quad F(\delta) = \{x \in X : \delta(x) = x\}.$$

Let $\delta, \sigma \in T(X)$ be one-to-one. We say that δ *included* in σ, and write $\delta \sqsubseteq \sigma$, if $\delta(x) = \sigma(x)$ for every $x \in S(\delta)$. We say that δ and σ are *disjoint* if $S(\delta) \cap S(\sigma) = \emptyset$.

Let A be a set of pairwise disjoint one-to-one elements of $T(X)$. The *formal product* $\prod_{\delta\in A}\delta$ of elements of A is a one-to-one element of $T(X)$ defined by

$$\left(\prod_{\delta\in A}\delta\right)(x)=\begin{cases}\delta(x) & \text{if } x\in S(\delta) \text{ for some } \delta\in A\\ x & \text{otherwise.}\end{cases}$$

If $A=\emptyset$, we agree that $\prod_{\delta\in A}\delta$ is the identity transformation. The following lemma follows from [13, Theorem 4]. (This theorem has been proved for a finite set X. However, for a one-to-one $\alpha\in T(X)$, the proof of the theorem carries over to the infinite case.)

Lemma 4.1 *Let S be a semigroup, and let $\alpha,\beta\in T(S)$ such that $\alpha=\underline{s}$ for some $s\in S$ and $\alpha=\prod_{\delta\in A}\delta$ is a formal product of cycles $\delta\in A$. Then $\beta\in C(\alpha)$ if and only if:*

(1) *$\beta(F(\alpha))\subseteq F(\alpha)$;*

(2) *For every cycle $(x_0\,x_1\ldots x_{k-1})\in A$, either $\beta(\{x_0,x_1,\ldots,x_{k-1}\})=\{y\}$ for some $y\in F(\alpha)$ or there is a cycle $(y_0\,y_1\ldots y_{m-1})\in A$ such that m divides k and $\beta(x_i)=y_i$ for every $0\le i\le k-1$, where the subscripts on the y_i are calculated modulo m.*

(B$_2$) Find necessary conditions that $\bar{t}\in C(\underline{s})$ must satisfy.

Let $s,t\in G$. Then $\bar{t}\in C(\underline{s})$ by Lemma 2.1. Since G is a group of exponent n, $\underline{s}\in T(G)$ is a formal product of cycles, each of length $\le n$. (We will call them cycles in $\underline{s}$.) Let $(x\ \underline{s}(x)\ldots\underline{s}^{n-1}(x))$ be a cycle of length n in $\underline{s}$. Let $y=\bar{t}(x)$. Since $\bar{t}\in T(G)$ is a permutation, it follows from Lemma 4.1 that there is a cycle $(y_0\,y_1\ldots y_{n-1})$ of length n in $\underline{s}$ such that $\bar{t}(\underline{s}^i(x))=y_i$ for every $0\le i\le n-1$. Then $\bar{t}(x)=y_0$ and $\bar{t}(\underline{s}^{n-1}(x))=y_{n-1}$. Thus $y=\bar{t}(x)=y_0$, and so $\bar{t}(\underline{s}^{n-1}(x))=y_{n-1}=\underline{s}^{n-1}(y_0)=\underline{s}^{n-1}(y)$. The latter implies

$$\underline{s}(\bar{t}(\underline{s}^{n-1}(x)))=\underline{s}(\underline{s}^{n-1}(y))=\underline{s}^n(y)=y=\bar{t}(x).$$

We have proved that for all $s,t,x,y\in G$,

$$\underline{s}(\bar{t}(\underline{s}^{n-1}(x)))=\bar{t}(x). \tag{4.2}$$

(C) Translate the conditions obtained in (A) and (B$_2$) to abstract conditions for G.

Let S be a groupoid. For all $a,b\in S$ and every integer $n\ge 0$, we define $a^{(n)}b$ recursively by

$$a^{(0)}b=b \text{ and } a^{(n)}b=a(a^{(n-1)}b) \text{ for } n\ge 1.$$

For example, $a^{(1)}b=ab$, $a^{(2)}b=a(ab)$, and $a^{(3)}b=a(a(ab))$. Note that for all $m,n\ge 0$, $a^{(m)}(a^{(n)}b)=a^{(m+n)}b$.

Now, conditions (4.1) and (4.2) translate, respectively, to

$$s^{(n)}x=x, \tag{4.3}$$

$$s((s^{(n-1)}x)t)=xt. \tag{4.4}$$

If S is a groupoid with right identity element, then (4.4) clearly implies (4.3). Thus we are left with one axiom, namely (4.4). Changing the names of the variables, we obtain for all $a,b,c,d\in G$,

$$a((a^{(n-1)}b)c)=bc. \tag{4.5}$$

(D) Prove that the axioms obtained in (C) define the class $\mathcal{C}$.

We prove that (4.5) defines the class of groups of exponent n in the class of groupoids with a right identity element.

Theorem 4.2 *Let S be a groupoid with a right identity element and let $n \geq 1$ be an integer. Then S is a group of exponent n if and only if for all $a, b, c \in S$,*

$$a((a^{(n-1)}b)c) = bc. \tag{4.6}$$

Proof: It is clear that every group of exponent n satisfies (4.6). Conversely, suppose that a groupoid S with a right identity element, say e, satisfies (4.6). Taking $c = e$ in (4.6), we obtain

$$a^{(n)}b = b \tag{4.7}$$

for all $a, b \in S$. Let $a, b, c, d \in S$ and suppose $ab = cd$. We have $a((a^{(n-1)}c)d) = cd$ by (4.6), and so

$$\begin{aligned} a((a^{(n-1)}c)d) = cd &\Rightarrow a((a^{(n-1)}c)d) = ab \quad (\text{since } ab = cd) \\ &\Rightarrow a^{(n-1)}(a((a^{(n-1)}c)d)) = a^{(n-1)}(ab) \\ &\Rightarrow a^{(n)}((a^{(n-1)}c)d) = a^{(n)}b \\ &\Rightarrow (a^{(n-1)}c)d = b \quad (\text{by } (4.7)). \end{aligned}$$

We have proved that for all $a, b, c, d \in S$,

$$ab = cd \Rightarrow (a^{(n-1)}c)d = b. \tag{4.8}$$

Let $s, u, t \in S$. We want to prove that $(su)t = s(ut)$. Let $x = su$, $z = xt$ and $y = s^{(n-1)}z$. Then, by (4.7),

$$s^{(n-1)}x = s^{(n-1)}(su) = s^{(n)}u = u \quad \text{and} \quad sy = s(s^{(n-1)}z) = s^{(n)}z = z.$$

Thus $sy = xt$ and so, by (4.8), $(s^{(n-1)}x)t = y$. Hence $ut = y$ and so $s(ut) = sy$. On the other hand, $sy = xt = (su)t$, and so $s(ut) = (su)t$.

We have proved that S is a semigroup. It is clear that in a semigroup, $a^{(n)}b = a^n b$ for all elements a and b. Thus, by (4.7), we have that for all $a \in S$,

$$a^n = a^n e = a^{(n)}e = e. \tag{4.9}$$

Thus, S is a semigroup with a right identity e such that every $a \in S$ has a right inverse (namely, a^{n-1}). It is well known that such a semigroup is a group with identity e. It follows by (4.9) that S is a group of exponent n. ■

Axiom (4.6) is of the form $\alpha = bc$, where α is a term constructed from multiplication and variables. For example, for $n = 3$, the axiom is $a(a(a(bc))) = bc$, so $\alpha = a(a(a(bc)))$. Denoting by $V(\alpha)$ the number of variable occurrences in α, we have $V(\alpha) = n + 2$ (n occurrences of a and one occurrence of b and c each). We point out that axiom (4.6) does not work if we do not assume that a groupoid S has a right identity element. Indeed, suppose S is a right zero semigroup, that is, $xy = y$ for all $x, y \in S$. Then (4.6) is clearly satisfied but S is not a group (if S has more than one element).

Single axioms for groups of exponents n exist for every $n \geq 2$, without the assumption of a right identity element [15]. If such an axiom has the form $\alpha = x$, where x is a variable and α is a term constructed from multiplication and variables, then $V(\alpha) \geq 2n + 1$ [5]. Single axioms $\alpha = x$ with $V(\alpha) = 2n + 1$ have been constructed for $n = 4$ [15] and all odd $n \geq 3$ [5].

Modifying (4.6), we obtain an axiom that defines the class of abelian groups of exponent n in the class of groupoids with identity.

Theorem 4.3 *Let S be a groupoid with a right identity element and let $n \geq 1$ be an integer. Then S is an abelian group of exponent n if and only if for all $a, b, c \in S$,*

$$a((a^{(n-1)}b)c) = cb. \tag{4.10}$$

Proof: It is clear that every abelian group of exponent n satisfies (4.10).

Conversely, suppose S is a groupoid with a right identity element, say e, satisfying (4.10). We start by proving that e is also a left identity element. Indeed, using (4.10), we obtain for all $a, c \in S$,

$$c = ce = a((a^{(n-1)}e)c) = a(a^{(n-1)}c) = a((a^{(n-1)}c)e) = ec,$$

and hence e is also a left identity element. Now, taking $a = e$ in (4.10), we obtain $bc = cb$ for all $b, c \in S$. Thus S is abelian. But then (4.10) implies (4.6), and so S is a group of exponent n by Theorem 4.2. ■

Again, the example of right zero semigroups shows that axiom (4.10) does not work if we do not assume that a groupoid S has a right identity element.

It is worth observing that identity (4.10) found by our method yields, for the case of exponent 3, an identity very close to the identity (4.3) of [24] found by a computer.

5 Final Remarks and Problems

The general method explained in Section 2 is based on the Cayley representation of semigroups. Variations of the method based on other representations of classes of semigroups will lead to different sets of axioms. For example, the same idea can be used with the Vagner-Preston representation for inverse semigroups [8, Theorem 5.1.7] to find axioms that define subclasses of inverse semigroups. However, since the inner translations that occur in the Vagner-Preston representation cannot be defined for an arbitrary groupoid S, we start with a groupoid $(S, *, ^{-1})$ with an involution and such that $x = (xx^{-1})x$. (Recall that a unary operation $^{-1}$ on a groupoid S is called an *involution* if for all $a, b \in S$, $(ab)^{-1} = b^{-1}a^{-1}$ and $(a^{-1})^{-1} = a$.) For $s \in S$, we define the inner translations $s_* : s^{-1}S \to S$ and $s^* : Ss^{-1} \to S$ by $s_*(s^{-1}x) = s(s^{-1}x)$ and $s^*(xs^{-1}) = (xs^{-1})s$. (These are the equivalents of the inner translations $\underline{s}$ and $\overline{s}$ used in the Cayley representation.) If S is an inverse semigroup, then both s_* and s^* are one-to-one, that is, they are elements of the symmetric inverse semigroup $\mathcal{I}(S)$ of partial one-to-one transformations on S. The mapping $\phi : S \to \mathcal{I}(S)$ defined by $\phi(s) = s_*$ is a monomorphism from S to $\mathcal{I}(S)$ [8, Theorem 5.1.7], called the Vagner-Preston representation of S. (The monomorphism ϕ is the equivalent of the Cayley representation λ for general semigroups.)

For the sake of illustration, we will provide axioms for semilattices that we have obtained using our method with the Vagner-Preston representation, that is, axioms that follow from translating the commutativity of partial one-to-one transformations to the language of groupoids with involution.

Theorem 5.1 *Let S be a groupoid with an involution ${}^{-1}$ such that $(aa^{-1})a = a$ for all $a \in S$. Then S is a semilattice if and only if for all $x, a, b \in S$:*

(1) $x \in a^{-1}S \Rightarrow ax = x$;

(2) $x \in Sb \Rightarrow (ax)b = ax$;

(3) $aS \cap bS \subseteq (ab)S$.

Proof: That this result is true follows from the way conditions (1)-(3) were found (applying the obvious analogous of our method to the Vagner-Preston representation). Here we provide an equational proof of the result just for the sake of completeness.

Let S be a semilattice and let $a \in S$. Then $aa^{-1}a = a$ (by the assumption), and so $a^{-1} = (aa^{-1}a)^{-1} = a^{-1}(a^{-1})^{-1}a^{-1} = a^{-1}aa^{-1}$. Thus a^{-1} is an inverse of a [8, (2.3.1)]. Since S is a semilattice, a is clearly an inverse of itself, and so $a^{-1} = a$ since in an inverse semigroup every element has a unique inverse [8, Theorem 5.1.1]. Thus (1) can be rewritten as $x \in aS \Rightarrow ax = x$, which is clearly satisfied in a semilattice. It is also clear that S satisfies (2) and (3).

Conversely, let S be a groupoid with an involution ${}^{-1}$ such that $(aa^{-1})a = a$ for all $a \in S$, and suppose (1)–(3) hold for all $x, a, b \in S$. We want to prove that S is a semilattice, that is, for all $x, y, z \in S$, $xx = x$, $xy = yx$, and $x(yz) = (xy)z$. Let $x, y, z \in S$.

Since $x = (xx^{-1})x$, we have $x^{-1} = ((xx^{-1})x)^{-1} = x^{-1}(xx^{-1})^{-1} \in x^{-1}S$. Thus, by (1), $xx^{-1} = x^{-1}$, and so $x = (x^{-1})^{-1} = (xx^{-1})^{-1} = (x^{-1})^{-1}x^{-1} = xx^{-1}$. It follows that $x = x^{-1}$ and $xx = x$. The commutativity also follows since $xy = (xy)^{-1} = y^{-1}x^{-1} = yx$. Since $a^{-1} = a$ fo all $a \in S$, (1) can be rewritten as

$$x \in aS \Rightarrow ax = x. \tag{5.11}$$

To prove associativity, we will need a series of identities. Throughout the argument, we will use commutativity implicitly.

$$\begin{align}
x(yz) &= z(x(yz)), \tag{5.12}\\
x(yz) &= (xz)(x(yz)), \tag{5.13}\\
(xy)z &= (xz)((xy)z), \tag{5.14}\\
x(yz) &= ((xz)(yz))(x(yz)), \tag{5.15}\\
x(yz) &= (xz)(yz). \tag{5.16}
\end{align}$$

- (5.12): We have $yz \in Sz$, and so by (2)

$$x(yz) = (x(yz))z = z(x(yz)).$$

- (5.13): By (5.12), $x(yz) = z(x(yz)) \in xS \cap zS$. Thus $x(yz) \in (xz)S$ by (3), and so $(xz)(x(yz)) = x(yz)$ by (5.11).
- (5.14): First, $(xy)z = z(yx) = x(z(yx)) = x((xy)z)$ by (5.12) (and commutativity). Second, $x((xy)z) = (xz)(x((xy)z))$ by (5.13). Substituting $(xy)z$ for $x((xy)z)$ in the last equality, we obtain $(xy)z = (xz)((xy)z)$.
- (5.15): Applying (5.13) twice, we obtain

  $$x(yz) = (xz)(x(yz)) \text{ and } (xz)(x(yz)) = ((xz)(yz))((xz)(x(yz))).$$

  Substituting $(xy)z$ for $(xz)(x(yz))$ in the second equality, we obtain $(xy)z = ((xz)(yz))(x(yz))$.
- (5.16): We have

  $$(xz)(yz) = (x(yz))((xz)(yz)) = ((xz)(yz))(x(yz)) = x(yz),$$

  where the first equality follows from (5.14) and the last from (5.15).

Now, applying (5.16) twice, we obtain

$$x(zy) = (xy)(zy) = (zy)(xy) = z(xy),$$

and so $x(yz) = x(zy) = z(xy) = (xy)z$. ■

In the previous result, the assumption that the unary operation satisfies $(aa^{-1})a = a$ cannot be removed. Indeed, consider the groupoid S

*	0	1	2	3
0	0	0	3	3
1	0	1	2	3
2	3	2	2	3
3	3	3	3	3

with a unary operation $^{-1}$ defined by $0^{-1} = 2$, $2^{-1} = 0$ and $1^{-1} = 1$, $3^{-1} = 3$. It is easy to see that $^{-1}$ is an involution and that S is a semilattice. We have $2 \in 0^{-1}S$ (since $0^{-1} * 1 = 2 * 1 = 2$) but $0 * 2 = 3 \neq 2$, so S does not satisfy (1) of Theorem 5.1.

We conclude with the following two problems.

Problem 1. Use the method described in this paper to find new axioms for other classes of semigroups or inverse semigroups, for example for the class of completely regular semigroups.

Problem 2. The method introduced in this paper has been used to produce new defining axioms for varieties of semigroups. Is it possible to use this method to find new systems of axioms for classes of semigroups that do not form a variety?

Acknowledgments

The authors would like to thank the referee for very helpful comments that led to expressing our results in an optimal way.

The first author was partially supported by FCT and FEDER, Project POCTI-ISFL-1-143 of Centro de Algebra da Universidade de Lisboa, by FCT and PIDDAC through the project PTDC/MAT/69514/2006, by PTDC/MAT/69514/2006 Semigroups and Languages, and by PTDC/MAT/101993/2008 Computations in groups and semigroups.

The second author was supported by a 2008-09 University of Mary Washington Professional Development Grant.

References

[1] J. Araújo and J. Konieczny, Automorphism groups of centralizers of idempotents, *J. Algebra* **269** (2003), 227–239.

[2] J. Araújo and J. Konieczny, Semigroups of transformations preserving an equivalence relation and a cross-section, *Comm. in Algebra*, **32** (2004), 1917–1935.

[3] J. Araújo and W. McCune, Axioms of inverse semigroups: a solution of some problems posed by Tamura, *to appear.*

[4] R. Croisot, Demi-groupes et axiomatique des groupes, *C. R. Acad. Sci. Paris* **237** (1953), 778–780.

[5] J. Hart and K. Kunen, Single axioms for odd exponent groups, *J. Automat. Reason.* **14** (1995), 383–412.

[6] G. Higman and B.H. Neumann, Groups as groupoids with one law, *Publ. Math. Debrecen* **2** (1952), 215–221.

[7] C. Hollings, The early development of the algebraic theory of semigroups, *Arch. Hist. Exact Sci.* **63** (2009), 497–536.

[8] J.M. Howie, *Fundamentals of Semigroup Theory*, Oxford University Press, New York, 1995.

[9] E.V. Huntington, New sets of independent postulates for the algebra of logic, with special reference to Whitehead and Russell's *Principia mathematica*, *Trans. Amer. Math. Soc.* **35** (1933), 274–304.

[10] E.V. Huntington, Boolean algebra. A correction to: "New sets of independent postulates for the algebra of logic, with special reference to Whitehead and Russell's *Principia mathematica*," *Trans. Amer. Math. Soc.* **35** (1933), 557–558.

[11] J.A. Kalman, A shortest single axiom for the classical equivalential calculus, *Notre Dame J. Formal Logic* **19** (1978), 141–144.

[12] M.K. Kinyon, K. Kunen, and J.D. Phillips, A generalization of Moufang and Steiner loops, *Algebra Universalis* **48** (2002), 81–101.

[13] J. Konieczny and S. Lipscomb, Centralizers in the semigroup of partial transformations, *Math. Japon.* **48** (1998), 367–376.

[14] K. Kunen, Single axioms for groups, *J. Automat. Reason.* **9** (1992), 291–308.

[15] K. Kunen, The shortest single axioms for groups of exponent 4, *Comput. Math. Appl.* **29** (1995), 1–12.

[16] J. Łukasiewicz, *Selected works*, Edited by L. Borkowski, Studies in Logic and the Foundations of Mathematics, North-Holland Publishing, Amsterdam-London, 1970.

[17] W. McCune, Automated discovery of new axiomatizations of the left group and right group calculi, *J. Automat. Reason.* **9** (1992), 1–24.

[18] W. McCune, Single axioms for groups and abelian groups with various operations, *J. Automat. Reason.* **10** (1993), 1–13.

[19] W. McCune, Single axioms for the left group and right group calculi, *Notre Dame J. Formal Logic* **34** (1993), 132–139.

[20] W. McCune, Solution of the Robbins problem, *J. Automat. Reason.* **19** (1997), 263–276.

[21] W. McCune and R. Padmanabhan, Single identities for lattice theory and for weakly associative lattices, *Algebra Universalis* **36** (1996), 436–449.

[22] W. McCune and A.D. Sands, Computer and human reasoning: single implicative axioms for groups and for abelian groups, *Amer. Math. Monthly* **103** (December 1996), 888–892.

[23] W. McCune, R. Veroff, B. Fitelson, K. Harris, A. Feist, and L. Wos, Short single axioms for Boolean algebra, *J. Automat. Reason.* **29** (2002), 1–16.

[24] W. McCune and L. Wos, Applications of automated deduction to the search for single axioms for exponent groups, *Logic programming and automated reasoning (St. Petersburg, (1992)*, 131–136, Lecture Notes in Comput. Sci., 624, Springer, Berlin, 1992.

[25] C.A. Meredith, Single axioms for the systems $(C, N), (C, O)$ and (A, N) of the two-valued propositional calculus, *J. Computing Systems* **1** (1953), 155–164.

[26] C.A. Meredith, Equational postulates for the Sheffer stroke, *Notre Dame J. Formal Logic* **10** (1969), 266–270.

[27] C.A. Meredith and A.N. Prior, Notes on the axiomatics of the propositional calculus, *Notre Dame J. Formal Logic* **4** (1963), 171–187.

[28] C.A. Meredith and A.N. Prior, Equational logic, *Notre Dame J. Formal Logic* **9** (1968), 212–226.

[29] B.H. Neumann, Another single law for groups, *Bull. Austral. Math. Soc.* **23** (1981), 81–102.

[30] P. M. Neumann, What groups were: a study of the development of the axiomatics of group theory, *Bull. Austral. Math. Soc.* **60** (1999), 285–301.

[31] R. Padmanabhan and R.W. Quackenbush, Equational theories of algebras with distributive congruences, *Proc. Amer. Math. Soc.* **41** (1973), 373–377.

[32] J.G. Peterson, Shortest single axioms for the classical equivalential calculus, *Notre Dame J. Formal Logic* **17** (1976), 267–271.

[33] A. Rezus, On a theorem of Tarski, *Libertas Math.* **2** (1982), 63–97.

[34] T. W. Scharle, Axiomatization of propositional calculus with Sheffer functors, *Notre Dame J. Formal Logic* **6** (1965), 209–217.

[35] H.M. Sheffer, A set of five independent postulates for Boolean algebras, with application to logical constants, *Trans. Amer. Math. Soc.* **14** (1913), 481–488.

[36] M. Sholander, Postulates for commutative groups, *Amer. Math. Monthly* **66** (1959), 93–95.

[37] B. Sobociński, Axiomatization of a partial system of three-value calculus of propositions, *J. Computing Systems* **1** (1952), 23–055.

[38] B. Stolt, *Über Axiomensysteme die eine abstrakte Gruppe bestimmen*, (Thesis), University of Uppsala, Almqvist & Wiksells, Uppsala, 1953.

[39] A. Tarski, *Equational logic and equational theories of algebras*, Contributions to Math. Logic (Colloquium, Hannover, 1966), North-Holland, Amsterdam, 1968.

[40] V. Tasić, On single-law definitions of groups, *Bull. Austral. Math. Soc.* **37** (1988), 101–106.

[41] S. Winker, Absorption and idempotency criteria for a problem in near-Boolean algebras, *J. Algebra* **153** (1992), 414–423.

[42] L. Wos, D. Ulrich, and B. Fitelson, Vanquishing the XCB question: The methodological discovery of the last shortest single axiom for the equivalential calculus, *J. Automat. Reason.* **29** (2002), 107–124.

[43] L. Wos, S. Winker, R. Veroff, B. Smith, and L. Henschen, Questions concerning possible shortest single axioms for the equivalential calculus: an application of automated theorem proving to infinite domains, *Notre Dame J. Formal Logic* **24** (1983), 205–223.