Bull. Aust. Math. Soc. (First published online 2025), page 1 of 12*
doi:10.1017/S0004972725100166
*Provisional—final page numbers to be inserted when paper edition is published

SEMIGROUP CONGRUENCES AND SUBSEMIGROUPS OF THE DIRECT SQUARE

CALLUM BARBER and NIK RUŠKUC✉

(Received 8 April 2025; accepted 24 April 2025)

Abstract

We investigate semigroups S which have the property that every subsemigroup of $S \times S$ which contains the diagonal $\{(s, s) : s \in S\}$ is necessarily a congruence on S. We call such an S a DSC semigroup. It is well known that all finite groups are DSC, and easy to see that every DSC semigroup must be simple. Building on this, we show that for broad classes of semigroups, including periodic, stable, inverse and several well-known types of simple semigroups, the only DSC members are groups. However, it turns out that there exist nongroup DSC semigroups, which we obtain by utilising a construction introduced by Byleen for the purpose of constructing interesting congruence-free semigroups. Such examples can additionally be regular or bisimple.

2020 *Mathematics subject classification*: primary 20M10; secondary 08A30, 20M12.

Keywords and phrases: semigroup, congruence, subsemigroup, simple semigroup.

1. Introduction

Given an algebra A, a congruence on A is an equivalence relation that is compatible with the operations of the algebra. We can also think of ρ as a subset of the direct product $A \times A$. So instead of ρ being reflexive we can think of ρ as containing the diagonal $\Delta = \{(x, x) : x \in A\}$, and the notion of ρ respecting the operations then becomes ρ being a subalgebra of $A \times A$. Motivated by this we give the following definition.

Definition 1.1. Let A be an algebra. A *diagonal subalgebra* ρ of $A \times A$ is a subalgebra of $A \times A$ that contains the diagonal $\Delta = \{(x, x) : x \in A\}$. A *congruence* on A is a diagonal subalgebra of $A \times A$, such that for all $x, y, z \in A$,

$$(x, y) \in \rho \Rightarrow (y, x) \in \rho \quad \text{and} \quad (x, y), (y, z) \in \rho \Rightarrow (x, z) \in \rho.$$

It is a well known, easy fact that for groups, diagonal subgroups and congruences are one and the same.

PROPOSITION 1.2. *Let G be a group. Then the diagonal subgroups of $G \times G$ are precisely the congruences on G.*

PROOF. This is regarded as folklore, but we provide a short proof for completeness. By definition any congruence is a diagonal subgroup. If ρ is a diagonal subgroup, and if $(x, y), (y, z) \in \rho$, then, bearing in mind that $(x, x), (y, y), (y^{-1}, y^{-1}) \in \rho$, we have

$$(y, x) = (y, y)(x, y)^{-1}(x, x) \in \rho \quad \text{and} \quad (x, z) = (x, y)(y^{-1}, y^{-1})(y, z) \in \rho.$$

Hence, ρ is a congruence. □

The same result holds more generally for any algebras A with a Mal'cev term, that is, a term $m(x, y, z)$ in three variables such that $m(x, y, y) = x = m(y, y, x)$ holds for all $x, y \in A$ (see, for example, [5, Theorem 4.70]). In particular, the result holds for rings, associative and Lie algebras, loops and quasigroups. However, it does not hold for semigroups, as the following easy example shows.

EXAMPLE 1.3. Consider the left zero semigroup $S = \{x, y\}$ with multiplication $ab = a$ for all $a, b \in S$. The set $\rho = \{(x, x), (x, y), (y, y)\}$ is a diagonal subsemigroup of $S \times S$ but is not a congruence on S.

Motivated by this we give the following definition.

DEFINITION 1.4. We will say that a semigroup is *DSC* if every diagonal subsemigroup is a congruence.

Over the course of this paper we will see that DSC semigroups are few and far between. In fact, with any of a number of additional mild assumptions, the only DSC semigroups are groups. A further wrinkle worth keeping in mind is that, despite Proposition 1.2, not even all groups are DSC, due to the fact that a group may contain subsemigroups that are not subgroups. Here is a concrete example

EXAMPLE 1.5. Let $\mathbb{Z}$ denote the infinite cyclic group. Then $\{(x, y) \in \mathbb{Z} \times \mathbb{Z} : x \leq y\}$ is a diagonal subsemigroup of $\mathbb{Z} \times \mathbb{Z}$, but is not a congruence.

Of course, this 'anomaly' cannot arise for finite, or indeed periodic, groups.

We can prove, in full generality, that all DSC semigroups are simple (Theorem 2.1). Proceeding from there, we prove that for a semigroup S:

- supposing S is finite or periodic, S is DSC if and only if S is a group (Corollaries 2.4, 2.5);
- if S is a stable or inverse DSC semigroup then S is a group (Corollary 2.3, Theorem 2.6).

Focusing on special classes of simple semigroups, we also have:

- if S is a completely simple DSC semigroup then S is a group (Theorem 2.2);
- for any semigroup S and any endomorphism $\theta : S \to S$, the Bruck–Reilly extension $\mathsf{BR}(S, \theta)$ is not DSC (Theorem 3.2);

https://doi.org/10.1017/S0004972725100166 Published online by Cambridge University Press

- for any two infinite cardinals $p \geq q$, the generalised Baer–Levi semigroup $\mathcal{B}(p, q)$ is not DSC (Theorem 3.3).

In Theorem 3.1 we will prove that the class of DSC semigroups is closed under quotients. Thus, one might wish to look for possible nongroup examples among simple, congruence-free semigroups. Byleen [2] gives a construction which, under certain conditions, yields such semigroups. It turns out that we can deploy this construction to show that:

- there exist nongroup DSC semigroups (Corollary 4.4(i));
- furthermore, there are such examples that are regular and bisimple (Corollary 4.4(ii)).

As a byproduct we also observe that the class of DSC semigroups is not closed under subsemigroups (Corollary 4.4(iii)).

We will require only very basic concepts from semigroup theory. They will be introduced within the text where they are needed first. For a more systematic introduction we refer the reader to any standard monograph such as [4]. We will use $\mathbb{N}$ to denote the set of all positive integers, and $\mathbb{N}_0$ for $\mathbb{N} \cup \{0\}$.

2. Completely simple, stable and inverse semigroups

In this section we will show that all DSC semigroups belonging to certain classes are in fact groups. Specifically, we will do this for completely simple, stable and inverse semigroups, in that order.

A nonempty subset I of a semigroup S is said to be an *ideal* if for all $x \in I$ and all $s \in S$ we have $sx, xs \in I$. A semigroup is said to be *simple* if it has no ideals other than itself.

THEOREM 2.1. *Any DSC semigroup is simple.*

PROOF. Suppose S is not simple. Let I be a proper ideal of S. It is easily seen that $\rho = I \times S \cup \Delta$ is a diagonal subsemigroup of $S \times S$. If we take $x \in I$ and $y \in S \setminus I$ then $(x, y) \in \rho$ but $(y, x) \notin \rho$. Hence, ρ is not a congruence and S is not a DSC semigroup. □

Let S be a semigroup, and let E be the set of idempotents of S. The relation $\leq$ on E defined by $e \leq f \iff ef = fe = e$ is a partial order. Any minimal element in this partial order is said to be *primitive*. A simple semigroup S is said to be *completely simple* if it has a primitive idempotent. All finite simple semigroups are completely simple.

There is a complete structural description of completely simple semigroups, originally due to Suschkewitsch [8]. Let G be a group, let I and J be two index sets, and let $P = (p_{ji})_{j \in J, i \in I}$ be a $J \times I$ matrix with entries from G. The *Rees matrix semigroup* $\mathcal{M}[G; I, J; P]$ is the set $I \times G \times J$ with multiplication $(i, g, j)(k, h, l) = (i, g p_{jk} h, l)$. Suschkewitsch's theorem then asserts that a semigroup S is completely simple if

https://doi.org/10.1017/S0004972725100166 Published online by Cambridge University Press

and only if it is isomorphic to some Rees matrix semigroup $\mathcal{M}[G; I, J; P]$ (see [4, Theorem 3.3.1]).

Theorem 2.2. *Let S be a completely simple semigroup. If S is DSC then S is a group.*

Proof. Let S be a completely simple semigroup. By Suschkewitsch's theorem, without loss of generality we may assume $S = \mathcal{M}[G; I, J; P]$. If $|I| > 1$ then pick $i \neq k \in I$. Now consider the set

$$\rho = \{((i, g, j), (k, h, j)) : g, h \in G,\ j \in J\} \cup \{(l, g, j), (l, h, j)) : l \in I,\ g, h \in G,\ j \in J\}.$$

It is routine to verify that ρ is a diagonal subsemigroup. For an arbitrary $j \in J$ it is easily seen that $((i, 1, j), (k, 1, j)) \in \rho$ but $((k, 1, j), (i, 1, j)) \notin \rho$. Hence, ρ is not a congruence, contradicting $\mathcal{M}[G; I, J; P]$ being DSC. Therefore, it must then be the case that $|I| = 1$ and, analogously, $|J| = 1$. It now easily follows that $S \cong G$, a group. □

We know from Theorem 2.1 that a DSC semigroup S must be simple. Whenever we can show that under some additional assumptions S must in fact be completely simple, Theorem 2.2 will force S to be a group. We deploy this strategy for stable and inverse semigroups.

In order to define stability, we need to introduce Green's equivalences $\mathcal{R}$, $\mathcal{L}$ and $\mathcal{J}$ on a semigroup S:

$$s\mathcal{R}t \Leftrightarrow sS^1 = tS^1, \quad s\mathcal{L}t \Leftrightarrow S^1s = S^1t, \quad s\mathcal{J}t \Leftrightarrow S^1sS^1 = S^1tS^1$$

(for a detailed introduction see [4, Section 2.1]). We then say that S is *stable* if the following implications hold:

$$x\mathcal{J}sx \Rightarrow x\mathcal{L}sx \quad \text{and} \quad x\mathcal{J}xs \Rightarrow x\mathcal{R}xs \quad \text{for all } s, x \in S.$$

All finite semigroups are stable [7, Theorem A.2.4]. By [7, Theorem A.4.15] every stable simple semigroup is completely simple, and so we have the following corollary.

Corollary 2.3. *Let S be a stable semigroup. If S is DSC then S is a group.*

A semigroup S is said to be *periodic* if for every $s \in S$ there exist distinct $m, n \in \mathbb{N}$ such that $s^m = s^n$. Every finite semigroup is periodic.

Corollary 2.4. *Let S be a periodic semigroup. Then S is DSC if and only if S is a group.*

Proof. ($\Rightarrow$) By [7, Theorem A.2.4], every finite semigroup is stable. In fact, the proof is valid under the weaker assumption of periodicity (see also the proof of [1, Corollary 3.1]). This direction now follows from Corollary 2.3.

($\Leftarrow$) Suppose S is a group. Let ρ be a diagonal subsemigroup of $S \times S$. We claim that ρ is also a diagonal subgroup of $S \times S$, and the result then follows from Proposition 1.2. Let $(x, y) \in \rho$. As S is periodic, $x^a = 1 = y^b$ for some $a, b \in \mathbb{N}$. Then $(x, y)^{-1} = (x^{-1}, y^{-1}) = (x^{ab-1}, y^{ab-1}) = (x, y)^{ab-1} \in \rho$. □

Corollary 2.5. *Let S be a finite semigroup. Then S is DSC if and only if S is a group.*

https://doi.org/10.1017/S0004972725100166 Published online by Cambridge University Press

We finish this section with a discussion of inverse semigroups. An element $s \in S$ is said to be *regular* if $sts = s$ for some $t \in S$. If in addition $tst = t$ we say that s and t are (semigroup) inverses of each other. It is known that an element is regular if and only if it has an inverse (see [4, page 51]). The semigroup S is *regular* if every element is regular, and it is *inverse* if every element has a unique inverse.

THEOREM 2.6. *Let S be an inverse semigroup. If S is DSC then S is a group.*

PROOF. Let S be an inverse DSC semigroup. There is a natural partial order on S given by $x \le y \iff x = ey$ for some idempotent e (see [4, Section 5.2]). It is also true that this partial order is compatible with the multiplication and restricts to the natural partial order on the idempotents. So $\rho = \{(x, y) \in S \times S\colon x \le y\}$ is a diagonal subsemigroup and by assumption is a congruence. Hence, $\le$ is both symmetric and antisymmetric, and therefore there exists a primitive idempotent. □

We started this paper by introducing the concept of diagonal subalgebra for general algebras and we have looked at the cases when the algebra is a group or semigroup. At this point we have enough theory to answer this question for inverse semigroups as well.

THEOREM 2.7. *Let S be an inverse semigroup. Then every diagonal inverse subsemigroup of $S \times S$ is a congruence if and only if S is a group.*

PROOF. The proof of the reverse direction is identical to the proof of Proposition 1.2. The proof of the forward direction is similar to the proof of Theorem 2.6. The only difference is that we need to show ρ is a diagonal inverse subsemigroup, which follows from the fact that $x \le y \Rightarrow x^{-1} \le y^{-1}$. □

3. Some further infinite non-DSC semigroups

As we have seen in the previous section, there exist no nongroup completely simple, stable or inverse DSC semigroups. So if we want to find a non-DSC semigroup we will have to look a bit harder. We know that any DSC semigroup is simple, and we will explore different constructions leading to examples of simple semigroups.

One such is the Rees matrix semigroup construction, which we have already encountered, but which can be deployed in greater generality. Specifically, instead of starting with a group G, we can start with an arbitrary semigroup S. Keeping the remainder of the definition from Section 2 unchanged, we obtain the Rees matrix semigroup $\mathcal{M}[S; I, J; P]$. It is easy to check (for example, by using [4, Corollary 3.1.2]), that $\mathcal{M}[S; I, J; P]$ is simple if and only if S is simple. By an analogous proof to that of Theorem 2.2, we can see that if $S' = \mathcal{M}[S; I, J; P]$ is DSC then $|I| = |J| = 1$. Hence, S' has multiplication $x \cdot y = xay$ for some $a \in S$. We claim that if S' is DSC then S must also be DSC. Let ρ be a diagonal subsemigroup of S and define $\rho' \subseteq S' \times S'$ by $(x, y) \in \rho' \iff (x, y) \in \rho$. As ρ contains the diagonal, so does ρ'. And if we have $(x, y), (z, t) \in \rho'$ then $(x, y), (z, t) \in \rho$, which gives $(xaz, yat) \in \rho$ and hence

https://doi.org/10.1017/S0004972725100166 Published online by Cambridge University Press

$(x \cdot z, y \cdot t) \in \rho'$. Hence, ρ' is a diagonal subsemigroup and, as S' is DSC, a congruence on S'. It follows that ρ is also a congruence on S, and therefore S must be DSC.

We have just seen that in order for $\mathcal{M}[S; I, J; P]$ to be DSC, S must also be DSC. So for finding more DSC semigroups, taking a Rees matrix semigroup will not be much help as we would have to know whether our original semigroup was DSC to begin with.

Another way to construct simple semigroups is the Bruck–Reilly extension [4, Section 5.6]. Here we take a semigroup S and an endomorphism θ of S. The *Bruck–Reilly extension* $\mathsf{BR}(S,\theta)$ is the set $\mathbb{N}_0 \times S \times \mathbb{N}_0$ with multiplication

$$(m, s, n)(p, t, q) = (m - n + k, (s\theta^{k-n})(t\theta^{k-p}), q - p + k) \quad \text{where } k = \max(n, p).$$

Under certain conditions the semigroup $\mathsf{BR}(S,\theta)$ is simple. The conditions themselves will not concern us, but the reader can consult Proposition 5.6.6 and Exercise 5.25 in [4] for two examples. Unfortunately, again, this construction will not work for us. One can show directly that *no* Bruck–Reilly extension is DSC, but it is easier to use some of the theory we have built up in the previous section. Additionally, we will need the following result.

THEOREM 3.1. *Let S be a DSC semigroup and let σ be a congruence on S. Then the quotient S/σ is also DSC.*

PROOF. Let ρ be a diagonal subsemigroup of $S/\sigma \times S/\sigma$. Define $\rho' \subseteq S \times S$ by

$$(x, y) \in \rho' \iff (x\sigma, y\sigma) \in \rho.$$

For each $x \in S$, $(x\sigma, x\sigma) \in \rho$ so $(x, x) \in \rho'$. If $(x, y), (z, t) \in \rho'$ then $(x\sigma, y\sigma)$, $(z\sigma, t\sigma) \in \rho$. This implies $(xz\sigma, yt\sigma) \in \rho$ and so $(xz, yt) \in \rho'$. Hence, ρ' is a diagonal subsemigroup of $S \times S$ which by assumption is also a congruence. Now

$$(x\sigma, y\sigma) \in \rho \Rightarrow (x, y) \in \rho' \Rightarrow (y, x) \in \rho' \Rightarrow (y\sigma, x\sigma) \in \rho,$$
$$(x\sigma, y\sigma), (y\sigma, z\sigma) \in \rho \Rightarrow (x, y), (y, z) \in \rho' \Rightarrow (x, z) \in \rho' \Rightarrow (x\sigma, z\sigma) \in \rho.$$

Hence, ρ is a congruence and S/σ is DSC. □

In particular, the homomorphic image of a DSC semigroup is DSC. This result makes it much easier to check if a semigroup is not DSC.

THEOREM 3.2. *For any semigroup S and endomorphism θ of S, the Bruck–Reilly extension $\mathsf{BR}(S,\theta)$ is not DSC.*

PROOF. Let B denote the *bicyclic monoid*, the semigroup with underlying set $\mathbb{N}_0 \times \mathbb{N}_0$ and multiplication $(m, n)(p, q) = (m - n + k, q - p + k)$, where $k = \max(n, p)$ (see [4, Section 1.6]). The bicyclic monoid is a homomorphic image of $\mathsf{BR}(S,\theta)$ via the projection onto the first and third coordinates. It is known that B is an inverse semigroup but not a group (for example, see [4, Section 5.4]). So, by Theorem 2.6, B is not DSC. Hence, $\mathsf{BR}(S,\theta)$ is not DSC either, by Theorem 3.1. □

https://doi.org/10.1017/S0004972725100166 Published online by Cambridge University Press

The final kind of simple semigroups we will look at in this section are the generalised *Baer–Levi semigroups* (see [3, Section 8.1]). Here we take two infinite cardinals p and q with $p \geq q$. Let X be a set of cardinality p and consider the set

$$B(p,q) = \{f\colon X \to X : f \text{ is injective and } |X \setminus Xf| = q\}.$$

Under the usual composition of functions $B(p,q)$ forms a semigroup. This semigroup is always simple (even right simple) and contains no idempotents [3, Theorem 8.2], so potentially makes a good candidate for a nongroup DSC semigroup. Unfortunately, this hope too turns out to be unjustified.

THEOREM 3.3. *For any two infinite cardinals $p \geq q$, the generalised Baer–Levi semigroup $B(p,q)$ is not DSC.*

PROOF. Let $B = B(p,q)$. Consider the set

$$\rho = \{(f,g) \in B \times B\colon (X \setminus Xf) \cap (X \setminus Xg) \neq \emptyset\}.$$

It is easy to check that ρ is a diagonal subsemigroup of $B \times B$. It is also clear that ρ is symmetric, so we will show that ρ is not transitive. Partition X into two sets A and B with cardinality p. Let A' and B' be subsets of A and B respectively, both with cardinality q. Let $x \in A'$. The sets $X \setminus A', X \setminus (B' \cup x)$ and $X \setminus B'$ all have cardinality p. So there are bijections

$$f'\colon X \to X \setminus A', \quad g'\colon X \to X \setminus (B' \cup x) \quad \text{and} \quad h'\colon X \to X \setminus B'.$$

Each can be extended to an injection from X to itself; call these functions f, g and h, respectively. Note that $X \setminus Xf = A'$, $X \setminus Xg = B' \cup \{x\}$ and $X \setminus Xh = B'$. So $f, g, h \in B$ and $(f,g), (g,h) \in \rho$, but $(f,h) \notin \rho$. Hence, ρ is not transitive. □

4. Nongroup DSC semigroups

In Theorem 3.1 we saw that any quotient of a DSC semigroup must be DSC. So if we have a semigroup S with congruence σ, for S to be DSC so must S/σ. This gives us an extra constraint on being DSC. So we will try looking at congruence-free semigroups. One rather general such construction was introduced by Byleen in [2]. The construction uses the notions of monoid actions and presentations, which we now briefly review.

Let S be a monoid with identity 1 and let A be a set. A *right action* of S on A is a function $A \times S \to A$, $(a,s) \mapsto a \triangleright s$ such that $(a \triangleright s) \triangleright t = a \triangleright (st)$ and $a \triangleright 1 = a$ for all $a \in A$ and all $s, t \in S$. The action is said to be *faithful* if for any two distinct $s, t \in S$ there exists $a \in A$ such that $a \triangleright s \neq a \triangleright t$. A *left action* of S on a set B is defined analogously. For more details, see [4, Section 8.1].

Now suppose that X is an alphabet and denote by X^* the *free monoid* on X; it consists of all words over X, including the empty word ϵ, and the operation is concatenation. A *monoid presentation* is a pair of the form $\langle X \mid R\rangle$, where $R \subseteq X^* \times X^*$. The *monoid defined* by this presentation is $S = X^*/\rho$, where ρ is the congruence generated by R. The elements of this semigroup are the ρ-classes $[u]$, $u \in X^*$. An *elementary sequence*

https://doi.org/10.1017/S0004972725100166 Published online by Cambridge University Press

with respect to $\langle X \mid R\rangle$ is any sequence $w_1, w_2, \dots, w_n$ $(n \geq 1)$ of words from X^* such that for every $i = 1, \dots, n-1$ we have $w_i = w'uw''$, $w_{i+1} = w'vw''$ for some $w', w'' \in X^*$ and some $(u, v) \in R$ or $(v, u) \in R$. For two words $u, v \in X^*$ we have $[u] = [v]$ if and only if there exists an elementary sequence starting at u and ending in v. We will abuse notation and write u instead of $[u]$ for a typical element of S, and $u = v$ instead of (u, v) for a typical element of R. For a more detailed basic introduction to presentations see [4, Section 1.6].

Definition 4.1. Let S be a monoid with identity 1, and let A and B be sets that are disjoint from each other and from S. Let $\alpha\colon A \times S \to A, (a, s) \mapsto a \triangleright s$ be a right action, and let $\beta\colon S \times B \to B, (s, b) \mapsto s \triangleleft b$ be a left action. Let $W = A \cup B \cup S$ and let P be an $A \times B$ matrix with entries in W. Let $C^1(S; \alpha, \beta; P)$ denote the monoid with monoid presentation

$$\langle W \mid ab = p_{a,b},\ as = a \triangleright s,\ sb = s \triangleleft b,\ st = s \cdot t,\ 1 = \epsilon\ (a \in A,\ b \in B,\ s, t \in S)\rangle.$$

In the above presentation, the relation $st = s \cdot t$ should be interpreted as a word of length 2, namely st, being equal to a word of length 1, the product of s and t in S. In other words, those relations represent the inclusion of the Cayley table of S in the defining presentation for $C^1(S; \alpha, \beta; P)$.

In [2] it is shown that any element of $C^1(S; \alpha, \beta; P)$ can be written uniquely in the form vsu where $v \in B^*, s \in S$ and $u \in A^*$. The monoid $C^1(S; \alpha, \beta; P)$ has identity $1 = \epsilon$. Calculations are easy in $C^1(S; \alpha, \beta; P)$ as each relation (other than $1 = \epsilon$) replaces a word of length 2 with a word of length 1. In general, this semigroup need not be DSC. We now introduce some additional conditions which will then imply DSC.

Definition 4.2. Let A, B and C be nonempty sets and let $P = (p_{ab})_{a\in A, b\in B}$ be an $A \times B$ matrix with entries from C. We say that P is 2-*transitive* if the following hold:

(1) for every $a_1 \neq a_2 \in A$ and $c_1, c_2 \in C$, there exists $b \in B$ such that $p_{a_1,b} = c_1$ and $p_{a_2,b} = c_2$;
(2) for every $b_1 \neq b_2 \in B$ and $c_1, c_2 \in C$, there exists $a \in A$ such that $p_{a,b_1} = c_1$ and $p_{a,b_2} = c_2$.

We will be interested in 2-transitive $A \times B$ matrices with entries in $W = A \cup B \cup S$. As $|W| \geq |A|, |B|$, the sets A and B will of necessity be infinite. For an explicit construction when A and B are countably infinite see [6].

The proof of the following result closely follows Byleen's proof showing that $C^1(S; \alpha, \beta; P)$ is congruence-free. Our proof will be divided into more cases as we have to work around the parts that use symmetry and transitivity.

Theorem 4.3. *The monoid $C^1(S; \alpha, \beta; P)$, with α, β faithful monoid actions and P a 2-transitive matrix over $W = A \cup B \cup S$, has only two diagonal subsemigroups.*

Proof. Let $T = C^1(S; \alpha, \beta; P)$. We will show that $\Delta = \{(t, t)\colon t \in T\}$ and $T \times T$ are the only diagonal subsemigroups of $T \times T$. To this end we will consider arbitrary distinct $vsu, ytx \in T$ and show that the subsemigroup ρ of $T \times T$ generated by (vsu, ytx)

https://doi.org/10.1017/S0004972725100166 Published online by Cambridge University Press

and Δ is equal to $T \times T$. Note that if $W \times W \subseteq \rho$, then for any $w = w_1 \cdots w_n$ and $w' = w'_1 \cdots w'_m \in T$ we have $(w_i, 1), (1, w'_j) \in \rho$ for all i, j, and so

$$(w, w') = (w_1, 1) \cdots (w_n, 1)(1, w'_1) \cdots (1, w'_m) \in \rho.$$

Hence, under this assumption, $\rho = T \times T$. So it suffices to show that $W \times W \subseteq \rho$. To do this we will first prove several intermediate claims.

CLAIM 1. For every $u \in A^*$ there exists $\lambda \in \Delta$ such that $(1, 1) = (u, u)\lambda$.

PROOF. The result is trivial if $u = \epsilon$ so let $u = a_1 \cdots a_n$. By 2-transitivity of P there are $b_1, \ldots, b_n \in B$ such that $a_1 b_1 = 1, a_2 b_2 = b_1, \ldots, a_n b_n = b_{n-1}$. If we let $\lambda = (b_n, b_n)$, then

$$(1, 1) = (a_1 \cdots a_n b_n, a_1 \cdots a_n b_n) = (u, u)\lambda. \qquad \square$$

CLAIM 2. Let $u, x \in A^*$ be distinct. Then there exist $\lambda \in \Delta$ and $\epsilon \neq p \in A^*$ such that $(1, p) = (u, x)\lambda$ or $(p, 1) = (u, x)\lambda$.

PROOF. First we note that if either of u or x is empty then the result follows by taking $\lambda = (1, 1)$. We will use induction on $|u| + |x|$. As u and x are distinct, the base case is when $|u| + |x| = 1$, so one of u, x is the empty word. The result then follows by the observation at the start of the proof. Let $n > 1$ and suppose for all distinct words $u', x' \in A^*$ with $|u'| + |x'| < n$ that there exists $\lambda \in \Delta$ such that $(u', x')\lambda = (1, p)$ or $(p, 1)$. Now suppose that $|u| + |x| = n$ and that neither u nor x is empty. Write $u = a_1 \cdots a_n$, $x = a'_1 \cdots a'_m$.

If $a_n = a'_m$ then from Claim 1, there is $\lambda_1 \in \Delta$ such that $(1, 1) = (a_n, a'_m)\lambda_1$. The words $a_1 \cdots a_{n-1}$ and $a'_1 \cdots a'_{m-1}$ are distinct as u, x are distinct and $a_n = a'_m$. By the inductive hypothesis there are elements $\lambda_2 \in \Delta$ and $\epsilon \neq p \in A^*$ such that $(a_1 \cdots a_{n-1}, a'_1 \cdots a'_{m-1})\lambda_2 = (1, p)$ or $(p, 1)$. Now take $\lambda = \lambda_1 \lambda_2$.

Now assume $a_n \neq a'_m$. Assume also that $|u| \geq |x|$; the case when $|u| \leq |x|$ is dual. There exists $b \in B$ such that $a_n b = a_n, a'_m b = 1$. Now $|u| > |a'_1 \cdots a'_{m-1}|$ so the words u and $a'_1 \cdots a'_{m-1}$ are distinct. So by the inductive hypothesis there exist $\lambda' \in \Delta$ and $\epsilon \neq p \in A^*$ such that $(u, a'_1 \cdots a'_{m-1})\lambda' = (1, p)$ or $(p, 1)$. Now take $\lambda = (b, b)\lambda'$. $\square$

CLAIM 3. Let $u, x \in A^*$ and $w_1, w_2 \in W$, with $u \neq x$. Then there exist $\lambda, \mu \in \Delta$ such that $(w_1, w_2) = \mu(u, x)\lambda$.

PROOF. By Claim 2, there exist $\lambda' \in \Delta$ and $\epsilon \neq p \in A^*$ such that $(u, x)\lambda' = (1, p)$ or $(p, 1)$. We will assume $(u, x)\lambda' = (1, p)$; the case when $(u, x)\lambda' = (p, 1)$ is dual. Let $p = a_1 \cdots a_n$. There exist $b_0, \ldots, b_n \in B$ with $a_1 b_1 = b_0, \ldots, a_{n-1} b_{n-1} = b_{n-2}$, $a_n b_n = b_{n-1}$ and $b_n \neq b_0$, so $p b_n = b_0$. Now we can pick $a \in A$ such that $a b_n = w_1$ and $a b_0 = w_2$. If we let $\mu = (a, a)$ and $\lambda = \lambda'(b_n, b_n)$, then

$$\mu(u, x)\lambda = (a, a)(1, p)(b_n, b_n) = (a b_n, a b_0) = (w_1, w_2). \qquad \square$$

The next three claims are dual to Claims 1, 2, 3 and we omit their proofs.

CLAIM 4. For every $v \in B^*$ there exists $\mu \in \Delta$ such that $(1, 1) = \mu(v, v)$.

https://doi.org/10.1017/S0004972725100166 Published online by Cambridge University Press

CLAIM 5. Let $v, y \in B^*$ be distinct. Then there exist $\mu \in \Delta$ and $\epsilon \neq q \in B^*$ such that $(1, q) = \mu(v, y)$ or $(q, 1) = \mu(v, y)$.

CLAIM 6. Let $v, y \in B^*$ and $w_1, w_2 \in W$, with v and y distinct. Then there exist $\lambda, \mu \in \Delta$ such that $(w_1, w_2) = \mu(v, y)\lambda$.

Now let $vsu, ytx \in T$ be distinct, and let $w_1, w_2 \in W$ be arbitrary. We will show $(w_1, w_2) \in \rho = \langle (vsu, ytx), \Delta \rangle$.

If $u = x$ and $v = y$ then it must be the case that $s \neq t$. By Claims 1 and 4 there exist $\lambda, \mu \in \Delta$ such that $(u, x)\lambda = (1, 1) = \mu(v, y)$. As the right action α is faithful, there is $a \in A$ such that $a_1 = a \triangleright s \neq a \triangleright t = a_2$. From Claim 3, there exist $\lambda', \mu' \in \Delta$ such that $\mu'(a_1, a_2)\lambda' = (w_1, w_2)$. Thus,

$$(w_1, w_2) = \mu'(a, a)\mu(vsu, ytx)\lambda\lambda' \in \rho.$$

Now suppose that $u \neq x$ and $v = y$ (the case when $u = x$ and $v \neq y$ is dual). By Claims 2 and 4 there exist $\lambda, \mu \in \Delta$ and $\epsilon \neq p \in A^*$ such that $\mu(v, y) = (1, 1)$ and $(u, x)\lambda = (p, 1)$ (again the case when $(u, x)\lambda = (1, p)$ is dual). Let a be any element of A and let $a_1 = a \triangleright s, a_2 = a \triangleright t$. As the words p and $1 = \epsilon$ are distinct, the words $a_1 p$ and a_2 are also distinct. Hence, by Claim 3, there exist $\lambda', \mu' \in \Delta$ such that $\mu'(a_1 p, a_2)\lambda' = (w_1, w_2)$. Thus,

$$(w_1, w_2) = \mu'(a, a)\mu(vsu, ytx)\lambda\lambda' \in \rho.$$

If instead we had $u \neq x$ and $v \neq y$ then, by Claims 2 and 5, there exist $\lambda, \mu \in \Delta$ and $\epsilon \neq p \in A^*, \epsilon \neq q \in B^*$ such that

$$(u, x)\lambda \in \{(1, p), (p, 1)\} \quad \text{and} \quad \mu(v, y) = \{(1, q), (q, 1)\}.$$

Here we will write $(u, x)\lambda = (p_1, p_2)$, noting that $|p_1| \neq |p_2|$. We will treat the case when $\mu(v, y) = (1, q)$; the other case $((v, y)\mu = (q, 1))$ is dual to this.

Write $q = b_1 \cdots b_n$, and let a be any element of A. There exist $a_n, \ldots, a_1 \in A$ such that

$$a_n b_n = a, \quad a_{n-1} b_{n-1} = a_n, \quad \ldots, \quad a_1 b_1 = a_2.$$

So we have $a_1 q = a$. The words $(a_1 \triangleright s)p_1$ and $(a \triangleright t)p_2$ are distinct (as p_1 and p_2 have different lengths), so, by Claim 3, there are $\lambda', \mu' \in \Delta$ such that

$$\mu'((a_1 \triangleright s)p_1, (a \triangleright t)p_2)\lambda' = (w_1, w_2).$$

Hence,

$$(w_1, w_2) = \mu'(a_1, a_1)\mu(vsu, ytx)\lambda\lambda' \in \rho.$$

So in all cases $(w_1, w_2) \in \rho$ and hence $W \times W \subseteq \rho$. □

From here on, when we refer to $C^1(S; \alpha, \beta; P)$, we will assume that α and β are faithful actions, and that P is 2-transitive over $A \cup B \cup S$.

We will show that there are nongroup DSC semigroups that are bisimple. The Green's equivalence $\mathcal{D}$ on a semigroup S is defined to be $\mathcal{R} \circ \mathcal{L} = \mathcal{L} \circ \mathcal{R}$ (for a

https://doi.org/10.1017/S0004972725100166 Published online by Cambridge University Press

more detailed explanation see [4, Section 2.1]). We say a semigroup S is *bisimple* if $\mathcal{D} = S \times S$.

COROLLARY 4.4. *The following statements involving DSC semigroups hold:*

(i) *there exist nongroup DSC semigroups;*
(ii) *there exist nongroup DSC semigroups that are regular and bisimple;*
(iii) *subsemigroups of DSC semigroups are not necessarily DSC.*

PROOF. (i) From Theorem 4.3, we have seen that $C^1(S;\alpha,\beta;P)$ is DSC. To see that it is not a group, take any $a \in A$ and $vsu \in C^1(S;\alpha,\beta;P)$. Then $vsua \neq 1$. So, the element a has no group theoretic inverse and hence $C^1(S;\alpha,\beta;P)$ is not a group.

(ii) If S is bisimple, Byleen showed in [2] that $C^1(S;\alpha,\beta;P)$ is also bisimple. Now suppose S is regular. Let $vsu \in C^1(S;\alpha,\beta;P)$, with $v = b_1 \cdots b_m$ and $u = a_1 \cdots a_n$. There exist $s' \in S$, $a'_1, \ldots, a'_m \in A$ and $b'_1, \ldots, b'_n \in B$ such that $ss's = s$, $s'ss' = s'$ and

$$a'_1 b_1 = \cdots = a'_m b_m = a_1 b'_1 = \cdots = a_n b'_n = 1.$$

If we set

$$y = b'_n \cdots b'_1 \quad \text{and} \quad x = a'_m \cdots a'_1,$$

then $ys'x$ is an inverse of vsu. Hence, $C^1(S;\alpha,\beta;P)$ is regular. Therefore, if a monoid S is regular and bisimple (such as any group) then $C^1(S;\alpha,\beta;P)$ is regular and bisimple.

(iii) Consider the subsemigroup A^* of $C^1(S;\alpha,\beta;P)$. This semigroup is not DSC (as it is not simple). Hence, $C^1(S;\alpha,\beta;P)$ has non-DSC subsemigroups. □

5. Closing remarks and further questions

Now that we have seen that there exist DSC semigroups that are not groups, one might want to try to understand them better, and perhaps completely classify them. This seems to be out of reach at present but some seemingly easy questions remain. For example, we have seen that not even all (infinite) groups are DSC semigroups. So one may ask whether a description of DSC groups might be possible. Also, we do not know whether DSC semigroups are closed under formation of direct products.

Another direction one may take is to investigate more systematically the degree of interdependence of all four defining properties of a congruence. Specifically, a relation ρ on a semigroup S is a congruence if and only if it is reflexive, symmetric, transitive and compatible. DSC semigroups are precisely those for which reflexivity and compatibility imply symmetry and transitivity. What about other combinations of these properties?

References

[1] L. W. Anderson, R. P. Hunter and R. J. Koch, 'Some results on stability in semigroups', *Trans. Amer. Math. Soc.* **117** (1965), 521–529.

[2] K. Byleen, 'Embedding any countable semigroup in a 2-generated congruence-free semigroup', *Semigroup Forum* **41**(2) (1990), 145–153.

https://doi.org/10.1017/S0004972725100166 Published online by Cambridge University Press

[3] A. H. Clifford and G. B. Preston, *The Algebraic Theory of Semigroups. Volume II*, Mathematical Surveys and Monographs, 7 (American Mathematical Society, Providence, RI, 1967).
[4] J. M. Howie, *Fundamentals of Semigroup Theory*, London Mathematical Society Monographs New Series, 12 (Oxford University Press, New York, 1995).
[5] R. N. McKenzie, G. F. McNulty and W. F. Taylor, *Algebras, Lattices, Varieties. Volume 1*, AMS Chelsea Publishing, 383 (American Mathematical Society, Providence, RI, 2018).
[6] M. Quick and N. Ruškuc, 'Growth of generating sets for direct powers of classical algebraic structures', *J. Aust. Math. Soc.* **89**(1) (2010), 105–126.
[7] J. Rhodes and B. Steinberg, *The q-theory of Finite Semigroups*, Springer Monographs in Mathematics (Springer, New York, 2009).
[8] A. Suschkewitsch, 'Über die endlichen Gruppen ohne das Gesetz der eindeutigen Umkehrbarkeit', *Math. Ann.* **99**(1) (1928). 30–50.

CALLUM BARBER, School of Mathematics and Statistics,
University of St Andrews, St Andrews KY16 9SS, UK
e-mail: cjb38@st-andrews.ac.uk

NIK RUŠKUC, School of Mathematics and Statistics,
University of St Andrews, St Andrews KY16 9SS, UK
e-mail: nik.ruskuc@st-andrews.ac.uk

https://doi.org/10.1017/S0004972725100166 Published online by Cambridge University Press