Proceedings of the Edinburgh Mathematical Society (1997) 40, 63-67 ©

ON JOINS WITH GROUP CONGRUENCES

by P. M. EDWARDS

(Received 29th November 1994)

Let $\mathscr{S}$ be an arbitrary semigroup. A congruence γ on $\mathscr{S}$ is a group congruence if $\mathscr{S}/\gamma$ is a group. The set of group congruences on $\mathscr{S}$ is non-empty since $\mathscr{S}\times\mathscr{S}$ is a group congruence. The lattice of congruences on a semigroup $\mathscr{S}$ will be denoted by $\mathscr{C}(\mathscr{S})$ and the set of group congruences on $\mathscr{S}$ will be denoted by $\mathscr{GC}(\mathscr{S})$. If $\mathscr{GC}(\mathscr{S})$ is a lattice then it is modular and $\gamma\vee\rho=\gamma\circ\rho=\rho\circ\gamma$ for all $\gamma,\rho\in\mathscr{GC}(\mathscr{S})$. The main result is that $\gamma\vee\rho=\gamma\circ\rho\circ\gamma$ for any $\gamma\in\mathscr{GC}(\mathscr{S})$ and $\rho\in\mathscr{C}(\mathscr{S})$ (whence every element of the set $\mathscr{GC}(\mathscr{S})$ is dually right modular in $\mathscr{C}(\mathscr{S})$). This result has appeared, for particular classes of semigroups, many times in the literature. Also $\gamma\vee\rho=\gamma\circ\rho\circ\gamma=\rho\circ\gamma\circ\rho$ for all $\gamma,\rho\in\mathscr{GC}(\mathscr{S})$ which is similar to the well known result for the join of congruences on a group. Furthermore, if $\gamma\cap\rho\in\mathscr{GC}(\mathscr{S})$ then $\gamma\vee\rho=\gamma\circ\rho=\rho\circ\gamma$.

1991 *Mathematics subject classification:* 20 M 10

1. Introduction and summary

Unless stated otherwise $\mathscr{S}$ will always be an arbitrary semigroup. A congruence γ on $\mathscr{S}$ is a group congruence if $\mathscr{S}/\gamma$ is a group. The set of group congruences on $\mathscr{S}$ is non-empty since $\mathscr{S}\times\mathscr{S}$ is a group congruence. The lattice of congruences on a semigroup $\mathscr{S}$ will be denoted by $\mathscr{C}(\mathscr{S})$ and the set of group congruences on $\mathscr{S}$ will be denoted by $\mathscr{GC}(\mathscr{S})$. If $\mathscr{GC}(\mathscr{S})$ is a lattice then it is modular (Corollary 4). If $\mathscr{S}$ has a minimum group congruence it will be denoted by σ. The existence of a minimum group congruence is equivalent to having a maximum homomorphic group image. If $\mathscr{S}$ has a minimum group congruence then $\mathscr{GC}(\mathscr{S})$ is a complete modular lattice.

The main result [Theorem 1] is that $\gamma\vee\rho=\gamma\circ\rho\circ\gamma$ for any $\gamma\in\mathscr{GC}(\mathscr{S})$ and $\rho\in\mathscr{C}(\mathscr{S})$ whence every element of the set $\mathscr{GC}(\mathscr{S})$ is dually right modular in $\mathscr{C}(\mathscr{S})$. Also $\gamma\vee\rho=\gamma\circ\rho\circ\gamma=\rho\circ\gamma\circ\rho$ for all $\gamma,\rho\in\mathscr{GC}(\mathscr{S})$ which is similar to the well known result for the join of congruences on a group. Theorem 1 is proved to apply to all semigroups and has appeared, for particular classes of semigroups, many times in the literature. That $\sigma\vee\rho=\sigma\circ\rho\circ\sigma$ for $\mathscr{S}$ inverse is [**3**, Theorem 3.9] and that $\gamma\vee\rho=\gamma\circ\rho\circ\gamma$ for all $\gamma=\mathscr{GC}(\mathscr{S})$ for $\mathscr{S}$ regular is [**6**, Theorem 6]. Other usage appears in [**5**, Section 3], [**6**, Section 2], [**7**, Section 6], [**8**, Lemma III.5.4] and the regular case was generalised in [**2**, Theorem 5].

Results concerning joins of congruences and group congruences for specific classes of semigroups can be found in [**3, 7, 8**] for inverse semigroups, [**5, 6**] for regular semigroups, [**5, 6**] for orthodox semigroups, and [**2**] for eventually regular semigroups.

2. Congruences on groups

Obviously when $\mathcal{S}$ is a group, G say, $\mathcal{GC}(G) = \mathcal{C}(G)$. It is well known that for $G = G_e$ there is a one to one correspondence between the normal subgroups of G and the congruences on G. Explicitly, if N is a normal subgroup of G then $\rho_N = \{(a, b) \in G \times G : ab^{-1} \in N\}$ is a congruence on G and $N = e\rho_N$. Conversely if ρ is a congruence on G then $N = e\rho$ is a normal subgroup of G. Furthermore if M and N are normal subgroups of G then $\rho_N \cap \rho_M = \rho_{N \cap M}$ and $\rho_N \circ \rho_M = \rho_{NM}$. Thus $\rho_N \circ \rho_M = \rho_{NM} = \rho_{MN} = \rho_M \circ \rho_N$ and so $\mathcal{GC}(G)$ is a modular lattice and $\gamma \vee \rho = \gamma \circ \rho = \rho \circ \gamma$ for all $\gamma, \rho \in \mathcal{GC}(G)$.

In the next section joins of congruences on an arbitrary semigroup will be considered. Results will be given for the case when one (or both) of the congruences is a group congruence.

3. Joins with group congruences

In general the join of two congruences on a semigroup $\mathcal{S}$ may be quite complicated. In fact for $\rho, \beta \in \mathcal{C}(\mathcal{S}), \rho \vee \beta$ is the transitive closure of $\rho \cup \beta$ and so $\rho \vee \beta = (\rho \circ \beta)^\infty = \bigcup_{n=1}^{\infty} (\rho \circ \beta)^n$. Example 1 below demonstrates a semigroup $\mathcal{S}$ and $\rho, \beta \in \mathcal{C}(\mathcal{S})$ for which this union must be infinite. Theorem 1 below shows that we can do much better if one of the congruences is a group congruence. The previous section mentioned how the first term of the union suffices when $\mathcal{S}$ is a group.

Theorem 1. *Let γ be a group congruence on an arbitrary semigroup $\mathcal{S}$ and let ρ be a congruence on $\mathcal{S}$. Then $\gamma \vee \rho = \gamma \circ \rho \circ \gamma$.*

Proof. It suffices to show that $\gamma \circ \rho \circ \gamma$ is transitive. Let $i\gamma$ denote the identity element of the group $\mathcal{S}/\gamma$. Take any $(x, y), (y, z) \in \gamma \circ \rho \circ \gamma$. It will be shown that $(x, z) \in \gamma \circ \rho \circ \gamma$. Then there exist $a, b, c, d \in \mathcal{S}$ such that $(x, a) \in \gamma$, $(a, b) \in \rho$, $(b, y) \in \gamma$, $(y, c) \in \gamma$, $(c, d) \in \rho$ and $(d, z) \in \gamma$. Clearly $(b, c) \in \gamma$ and so there exists $s\gamma$ in $\mathcal{S}/\gamma$ such that $s\gamma b\gamma = i\gamma$ and $c\gamma s\gamma = i\gamma$. Since $(a, b) \in \rho$ and $(c, d) \in \rho, (csa, csb) \in \rho$ and $(csb, dsb) \in \rho$ whence $(csa, dsb) \in \rho$. Therefore $x \;\gamma\; a \;\gamma\; csa \;\rho\; dsb \;\gamma\; d \;\gamma\; z$ whence $(x, z) \in \gamma \circ \rho \circ \gamma$. □

In [5] a modularity relation M was defined on a lattice L by $a M b$ if $(x \vee a) \wedge b = x \vee (a \wedge b)$ for all $x \leq b$; with its dual denoted M^*. An element d is right [left] modular if $a M d$ [$d M a$] for all $a \in L$. If L is right and left modular then it is modular. Proposition 2.3 of [5] states that if $\alpha, \beta, \xi \in \mathcal{C}(\mathcal{S})$ and $\alpha \vee \beta = \alpha \circ \beta \circ \alpha$ then $\beta M^* \alpha$ whence (i) if $\alpha \vee \xi = \alpha \circ \xi \circ \alpha$ for all $\alpha \in \mathcal{C}(\mathcal{S})$ then ξ is (dually) left modular and (ii) if $\alpha \vee \xi = \xi \circ \alpha \circ \xi$ for all $\alpha \in \mathcal{C}(\mathcal{S})$ then ξ is dually right modular.

Corollary 2. *For any semigroup $\mathcal{S}$, every group congruence on $\mathcal{S}$ is a dually right modular element of the lattice of congruences on $\mathcal{S}$.*

Corollary 3. *Let γ and ρ be a group congruences on an arbitrary semigroup $\mathcal{S}$. Then $\gamma \vee \rho = \gamma \circ \rho \circ \gamma = \rho \circ \gamma \circ \rho$. Furthermore if $\gamma \cap \rho \in \mathcal{GC}(\mathcal{S})$ then $\gamma \vee \rho = \gamma \circ \rho = \rho \circ \gamma$.*

Proof. The first assertion follows from Theorem 1. Suppose $\beta = \gamma \cap \rho \in \mathcal{GC}(\mathcal{S})$ and put $L = [\beta, \mathcal{S} \times \mathcal{S}]$. Then $L \cong \mathcal{C}(\mathcal{S}/\beta)$ which is a modular lattice of commuting congruences since $\mathcal{S}/\beta$ is a group. Thus γ and ρ commute. □

Corollary 4. *If $\mathcal{GC}(\mathcal{S})$ is a sublattice of $\mathcal{C}(\mathcal{S})$ then $\mathcal{GC}(\mathcal{S})$ is a modular lattice and $\gamma \vee \rho = \gamma \circ \rho = \rho \circ \gamma$ for all $\gamma, \rho \in \mathcal{GC}(\mathcal{S})$.*

The kernel of $\rho \in \mathcal{C}(\mathcal{S})$ is defined by, $\ker(\rho) = \{a \in \mathcal{S} : a\rho \in E(\mathcal{S}/\rho)\}$. It is well known that if two group congruences have the same kernel then they are equal. For a subset H of $\mathcal{S}$, define $H\omega = \{x \in \mathcal{S} : hx \in H \text{ for some } h \in H\}$, define ωH dually and put $H' = \omega H \cup H\omega$. If H is a subsemigroup then $H \subseteq H\omega$ and $H \subseteq \omega H$. The subset H is called closed if $H = H'$. It is straightforward to show that $H = \ker(\gamma)$ is always a closed subsemigroup for $\gamma \in \mathcal{GC}(\mathcal{S})$.

After proving the following preliminary result some applications of Theorem 1 will be given.

Theorem 5. *Let γ be a group congruence on an arbitrary semigroup with $H = \ker(\gamma)$. Then the following are equivalent:*

(1) $a \,\gamma\, b$,
(2) $xa = by$ *for some* $x, y \in H$,
(3) $ax = yb$ *for some* $x, y \in H$,
(4) $HaH \cap HbH \neq \emptyset$.

Proof. Suppose $a\gamma b$. Let z be the group inverse of $a\gamma = b\gamma$ in $\mathcal{S}/\gamma$ and put $x = bz$, $y = za$, $s = zb$ and $t = az$. Then $xa = bza = by$ and $as = azb = tb$ and $x, y, s, t \in \ker(\gamma)$ whence (1) implies (2) and (3). It also follows that for any $h \in H$, $hbzah = (hbz)ah = hb(zah) \in HaH \cap HbH$ so (1) implies (4). That (2), (3) and (4) each imply (1) is trivial, whence the four statements are equivalent. □

Theorem 6. *For any congruence ρ and any group congruence γ on an arbitrary semigroup, $a(\gamma \vee \rho)b$ if and only if $xa \,\rho\, by$ for some $x, y \in \ker(\gamma)$.*

Proof. The following proof is a slight modification of the proof of Theorem 7 of LaTorre [**6**]. Put $H = \ker(\gamma)$. Suppose $(a, b) \in \gamma \vee \rho$. By Theorem 1 there exist $c, d \in \mathcal{S}$ such that $a \gamma c$, $c \rho d$ and $d \gamma b$. Since $a \gamma c$, by Theorem 5 there exist $h, k \in H$ such that $ha = ck$ and similarly there exist $p, q \in H$ such that $pd = bq$. Put $x = ph$ and $y = qk$ so $x, y \in H$. Then $xa = pha = p(ha) = p(ck) \,\rho\, p(dk) = (pd)k = (bq)k = by$ so $xa \,\rho\, by$ with $x, y \in H$. Conversely, if $xa \,\rho\, by$ with $x, y \in H$ then since $xa \,\gamma\, a$ and $by \,\gamma\, a$, $a \,\gamma\, xa \,\rho\, by \,\gamma\, b$ so $(a, b) \in \gamma \vee \rho$. □

Theorem 7. *For any congruence ρ and any group congruence γ on an arbitrary semigroup,* $\ker(\gamma \vee \rho) = ((\ker(\gamma))\rho)\omega$.

Proof. Take $x \in \ker(\gamma \vee \rho)$. For any $e \in E, (x, e) \in \gamma \vee \rho$ so from Theorem 6 there exist $p, q \in \ker(\gamma)$ such that $xp \, \rho \, qe$. Now $qe \in \ker(\gamma)$ so $xp \in (\ker(\gamma))\rho$. Since $p \in \ker(\gamma) \subseteq (\ker(\gamma))\rho$, we have that $x \in ((\ker(\gamma))\rho)\omega$. Conversely, if $x \in ((\ker(\gamma))\rho)\omega$, then $hx \in (\ker(\gamma))\rho$ for some $h \in (\ker(\gamma))\rho$ so $(hx, y) \in \rho$ for some $y \in \ker(\gamma)$ and $(h, z) \in \rho$ for some $z \in \ker(\gamma)$. Since $(y, e) \in \gamma$, it follows that $(hx, e) \in \gamma \vee \rho$ so $hx \in \ker(\gamma \vee \rho)$. Similarly, $h \in \ker(\gamma \vee \rho)$ whence $x \in \ker(\gamma \vee \rho)$ since $\ker(\gamma \vee \rho)$ is closed. Therefore $\ker(\gamma \vee \rho) = ((\ker(\gamma))\rho)\omega$.

Theorems 1, 6 and 7 above generalise the corresponding results for regular semigroups given in [**6**].

Example 1. Let $\mathscr{S} = \mathbb{Z}^+$ with left zero multiplication and let ρ and β be congruences on $\mathscr{S}$ given respectively by the partitions $\{\{1\}, \{2,3\}, \{4,5\}, \{6,7\}, \ldots\}$ and $\{\{1,2\}, \{3,4\}, \{5,6\}, \ldots\}$. Then $\rho \vee \beta = \mathscr{S} \times \mathscr{S}$ and clearly $\rho \vee \beta \neq \bigcup_{n=1}^{m} (\rho \circ \beta)^n$ for any finite m.

Example 2. A congruence γ on $\mathscr{S}$ is a cancellative congruence if $\mathscr{S}/\gamma$ is a cancellative semigroup. Any semigroup has a minimum cancellative congruence, namely the intersection of all the cancellative congruences. Denote the set of idempotent elements in $\mathscr{S}$ by $E = E(\mathscr{S})$. A semigroup $\mathscr{S}$ is *E-inversive* if for all $x \in \mathscr{S}$, there exists $y \in \mathscr{S}$ such that $xy \in E$. A semigroup is *eventually regular* [*group-bound*] if every element has some power that is regular [in a subgroup]. The class of E-inversive semigroups includes eventually regular semigroups, regular semigroups, group-bound semigroups, finite semigroups and semigroups with a zero element. If $\mathscr{S}$ is an E-inversive semigroup then the group congruences coincide with the cancellative congruences, whence $\mathscr{S}$ has a minimum group congruence σ equal to the intersection of all cancellative congruences on $\mathscr{S}$, [**1**]. Let $\mathscr{S}$ be any semigroup that possesses a minimum group congruence σ. Then $\mathscr{GC}(\mathscr{S}) = [\sigma, \mathscr{S} \times \mathscr{S}]$ is a complete modular lattice. The mapping $\phi : \mathscr{C}(\mathscr{S}) \to \mathscr{GC}(\mathscr{S})$ defined by $\phi(\rho) = \sigma \vee \rho$ is a surjection of $\mathscr{C}(\mathscr{S})$ onto $\mathscr{GC}(\mathscr{S})$ and the elements of $\mathscr{GC}(\mathscr{S})$ are invariant under ϕ. If $\mathscr{S}$ is orthodox then the mapping ϕ is a homomorphism, [**6**, Theorem 11].

Example 3. Let $\mathscr{S} = \langle a \rangle$ be an infinite monogenic semigroup. Then the relation $\rho_n = \{(a^p, a^q) : p \equiv q (\operatorname{mod} n)\}$ is a group congruence on $\mathscr{S}$ and every group congruence on $\mathscr{S}$ is of this form [**4**, p. 185, Exercise 26]. If ρ_n and ρ_m are two group congruences on $\mathscr{S}$ then $\rho_n \cap \rho_m = \rho_k$ where k is the lowest common multiple of n and m. It follows that the intersection of any finite set of group congruences on $\mathscr{S}$ is a group congruence and that $\mathscr{S}$ does not possess a minimum group congruence. In fact the intersection of all group congruences on $\mathscr{S}$ equals $1_{\mathscr{S}}$ which is of course not a group congruence. Therefore $\mathscr{GC}(\mathscr{S})$ is a lattice but is not a complete lattice. It follows from Corollary 4 that $\mathscr{GC}(\mathscr{S})$ is a modular lattice.

Example 4. This example was suggested by T. E. Hall. Put $A = \langle a \rangle$ and $B = \langle b \rangle$ both infinite cyclic groups and in $A \times B$ let $\mathcal{S}$ be the subsemigroup generated by (a, b), $(a, b$ inverse) and (a inverse, b). Note that if $(a^p, b^q) \in \mathcal{S}$ then $p+q$ is even and $p+q \geq 0$. In particular, the semigroup $\mathcal{S}$ is not a group since (a, b) does not have an inverse in $\mathcal{S}$. Let ρ_A and ρ_B be the kernels of the projections of $\mathcal{S}$ onto A and B respectively. Then ρ_A and ρ_B are group congruences on $\mathcal{S}$ but their intersection is trivial and so is not a group congruence. Since $(a^2, b^{-2})\,\rho_A\,(a^2, b^0)\,\rho_B\,(a^0, b^0)$ we have that (a^2, b^{-2}) is $\rho_A \circ \rho_B$ related to (a^0, b^0). Because $(a^0, b^{-2}) \notin \mathcal{S}$, (a^2, b^{-2}) is not $\rho_B \circ \rho_A$ related to (a^0, b^0). Thus $\rho_A \circ \rho_B \neq \rho_B \circ \rho_A$ [cf. Corollary 3].

REFERENCES

1. A. H. Clifford and G. B. Preston, *The algebraic theory of semigroups*, Volume I (Mathematical Surveys, **7**, American Mathematical Society, Providence, Rhode Island, 1961).

2. S. Hanumantha Rao and P. Lakshmi, Group congruences on eventually regular semigroups, *J. Austral. Math. Soc. Ser. A* **45** (1988), 320–325.

3. J. M. Howie, The maximum idempotent-separating congruence on an inverse semigroup, *Proc. Edinburgh Math. Soc.* **14** (1964), 71–79.

4. J. M. Howie, *An introduction to semigroup theory* (London Mathematical Society Monographs, **7**, Academic Press, London, New York, San Francisco, 1976).

5. P. R. Jones, Joins and meets of congruences on a regular semigroup, *Semigroup Forum* **30** (1984), 1–16.

6. D. R. LaTorre, Group congruences on regular semigroups, *Semigroup Forum* **24** (1982), 327–340.

7. Mario Petrich, Congruences on inverse semigroups, *J. Algebra* **55** (1978), 231–256.

8. Mario Petrich, *Inverse semigroups* (John Wiley, New York, 1984).

Econometrics Department
Monash University
Clayton
Victoria 3168
Australia