ON MAXIMAL CONGRUENCES AND FINITE SEMISIMPLE SEMIGROUPS(1)

BY
ROBERT H. OEHMKE

A right congruence ρ of a semigroup S is called modular if there is an element e of S such that $ea\rho a$ for all a in S. The element e is called a left identity for ρ. A similar definition is made for modular left congruences. A two-sided congruence is called modular if it is modular both as a right and left congruence and hence has a two-sided identity.

We define $R_r[R_l, R_t]$ to be the intersection of all the maximal modular right [left, two-sided] congruences. In each case the intersection is a two-sided congruence. We shall refer to them as the r- [l-, t-] radical of S. A semigroup S is said to be x-semisimple if the x-radical is the identity relation ι on S. A semigroup modulo its x-radical is x-semisimple.

The maximal modular two-sided congruences of a finite semigroup can be described by two mutually exclusive types. This classification is then used to prove that a t-semisimple finite semigroup is t-semisimple if and only if it is a semilattice Y of groups G_α, $\alpha \in Y$ such that the structure homomorphisms $\varphi_{\alpha\beta}: G_\alpha \to G_\beta$ $(\alpha > \beta)$ [1, p. 128] are one-to-one and the group G_0 (0 the minimal element of Y) is t-semisimple, i.e., a group whose Frattini subgroup is trivial.

The maximal modular right congruences of a finite semigroup can be classified into three mutually disjoint classes. This classification is then used to prove that the kernel of a finite r-semisimple semigroup is right simple, i.e., consists of a single minimal right ideal.

A similar approach, i.e., via congruence relations, to the structure of semigroups has been initiated by Hoehnke [6]. In his paper Hoehnke gives several definitions of radicals; rad S, $(\text{rad})^- S$, $\text{rad}^\circ S$, etc., which can be related to intersections of modular congruences. (The concept of a modular congruence was also introduced in [7] and [9].) It should be pointed out that for a semigroup S, $(\text{rad})^- = r\text{-rad}$ and if S is finite $\text{rad} = t\text{-rad}$.

The author expresses his gratitude to the referee for his contributions to the revision of this paper, in particular, for the shortened versions of the proofs of Theorems 11, 13, and 28.

1. **Preliminary definitions and results.** Let σ be an equivalence relation on a semigroup S. If a is equivalent to b we shall write either $a\sigma b$ or $a \equiv b \pmod{\sigma}$. The σ-class containing a will be denoted by σ_a.

Received by the editors July 23, 1965.
(1) This work was supported in part by NSF Grant GP-3979.

An equivalence relation σ on a semigroup S is a *right (left) congruence* if $a, b, c \in S$ and $a\sigma b$ imply $(ac)\sigma(bc)((ca)\sigma(cb))$. If an equivalence relation is both a right and left congruence we shall call it a *two-sided congruence*. We shall use the generic term congruence to refer to an equivalence relation that is either a right, left or two-sided congruence.

We denote by $\mathscr{L}_r(S)$ the set of all right congruences on the semigroup S and by $\mathscr{L}_l(S)$ the set of all left congruences on the semigroup S. The set of all two-sided congruences will be, of course, $\mathscr{L}_r(S) \cap \mathscr{L}_l(S)$. The relation ι, defined by $a\iota b$ if and only if $a=b$, is trivially a two-sided congruence. So also is the relation ν defined by $a\nu b$ if and only if $a, b \in S$.

There is a natural ordering on relations which we shall use for $\mathscr{L}_r(S)$ and $\mathscr{L}_l(S)$; namely $\alpha \leqq \beta$ if and only if $a, b \in S$ and $a\alpha b$ imply $a\beta b$. Clearly for any congruence α we have $\iota \leqq \alpha \leqq \nu$.

If $\alpha \leqq \beta$ then it is easily seen that the equivalence classes of β must be unions of equivalence classes of α and conversely.

Let $\mathscr{T}$ be a set of relations on S. Then by $\bigcap \mathscr{T}$ is meant the usual intersection of the relations in $\mathscr{L}$, i.e., if $\sigma = \bigcap \mathscr{T}$ and a and b are in S then $a\sigma b$ if and only if $a\tau b$ for every $\tau \in \mathscr{T}$. If $\mathscr{T}$ is a set of right, left, or two-sided congruences then σ is respectively a right, left, or two-sided congruence.

Each right, left, or two-sided ideal I of S gives rise to a right, left, or two-sided congruence σ respectively as follows:

$$a\sigma b \Leftrightarrow a = b \qquad \text{or } a \text{ and } b \text{ are in } I.$$

This congruence has only one nontrivial equivalence class, the one equal to I. Such a congruence is called the Rees congruence defined by I [8].

LEMMA 1. *Let σ be a right congruence on the semigroup S and I be a right ideal of S. The relation τ defined by $a\tau b$ if and only if $a\sigma b$ or there exist elements a' and b' in I with $a\sigma a'$ and $b\sigma b'$ is a right congruence on S and $\sigma \leqq \tau$.*

Since τ is the *union* of σ and the right Rees congruence defined by I we refer the reader to [3] for a proof.

LEMMA 2. *If $\sigma \leqq \tau$ where σ and τ are right congruences and if σ is modular then τ is modular and a left identity for σ is also a left identity for τ.*

Proof. The conclusion follows readily from the fact that $a \equiv b \pmod{\sigma}$ implies $a \equiv b \pmod{\tau}$. For if e is a left identity for σ then $ea \equiv a \pmod{\sigma}$ and $ea \equiv a \pmod{\tau}$.

Let τ be a right congruence on S. For any a in S we define an equivalence relation τa on S by $c(\tau a)d$ if and only if $(ac)\tau(ad)$. It follows that τa is a right congruence on S. If S is a group and τ the right congruence arising from the coset decomposition

of S with respect to the subgroup H then τa is the right congruence arising from the coset decomposition of S with respect to the conjugate subgroup $a^{-1}Ha$.

LEMMA 3. *Let τ be a right congruence on the semigroup S. Let $\sigma = \bigcap \tau a$ where a ranges over the elements of S. Then σ is a two-sided congruence on S.*

Proof. Clearly σ is a right congruence. So let a, b, c be in S and $b\sigma c$. For any d in S we have $b \equiv c \pmod{\tau(ad)}$. Therefore by the definition of $(\tau a)d = \tau(ad)$ we have $db \equiv dc \pmod{\tau a}$ for all a in S. Hence $db \equiv dc \pmod{\sigma}$.

LEMMA 4. *Let τ be a right congruence on S and a, b in S. If $a \equiv b \pmod{\tau}$ then $\tau a = \tau b$.*

Proof. If $a \equiv b \pmod{\tau}$ and $c(\tau a)d$ we have $(ac)\tau(ad)$. But $(ad)\tau(bd)$ and $(ac)\tau(bc)$. Therefore $(bd)\tau(bc)$ and $d(\tau b)c$. Hence $\tau a \leqq \tau b$ and by symmetry $\tau a = \tau b$.

LEMMA 5. *If τ is a modular right congruence on S then $\bigcap \tau a \leqq \tau$.*

Proof. τ has a left identity e. Therefore $a\tau b$ if and only if $ea\tau eb$. Hence $\tau = \tau e$.

The following lemma [4] gives us another method of contructing new congruences from old ones.

LEMMA 6. *Let S be a semigroup, τ a right congruence on S and S^* the union of a set of equivalence classes of τ. Define $a\sigma b$ if and only if for every c in S we have $ac \in S^*$ if and only if $bc \in S^*$. Then σ is a right congruence on S such that $\tau \leqq \sigma$.*

Proof. Clearly σ is a right congruence relation. If $a\tau b$ and $c \in S$ then $(ac)\tau(bc)$. Hence $ac \in S^*$ if and only if $bc \in S^*$ since S^* is the union of equivalence classes of σ. Therefore $a\sigma b$ and $\tau \leqq \sigma$.

The above lemma also holds with "right" replaced by "left." In fact in many of the preceding and subsequent theorems on right congruences similar results can be obtained for left congruences and two-sided congruences. However, due to the natural symmetry of these results, this phenomenon will be rather obvious. Thus in most cases we will defer from any reference to it.

2. **Maximal modular congruences.** We define the word maximal for congruences of a semigroup in terms of the partial ordering on the semilattices of those congruences not equal to ν.

Let σ be a maximal right congruence and I any right ideal of S. Let $\mathscr{T}$ be the set of σ-classes that meet I. Let τ be the right congruence of Lemma 1. Since $\sigma \leqq \tau$ and σ is maximal we must have either $\sigma = \tau$ or $\tau = \nu$. If $\sigma = \tau$ then b and d in I

imply $b\sigma d$. Therefore I is contained in some σ-class S_0. If $c \in S_0$ and $a \in I$ then $c\sigma a$. But then $(cb)\sigma(ab)$. Since $ab \in I \subseteq S_0$ we must have $cb \in S_0$ also. Therefore S_0 is a right ideal of S. On the other hand, if $\tau = \nu$ then for any two elements a and b in S we have $a\tau b$. If a and b are chosen to be in arbitrary, but distinct, σ-classes we see from the definition of τ that σ_a and σ_b are in $\mathscr{T}$. Therefore any equivalence class of σ contains an element of I. Thus we have

LEMMA 7. *If σ is a maximal right congruence and I any right ideal of S then either I is contained in a σ-class S_0 (which is also a right ideal of S) or I contains an element of each σ-class.*

We shall also give a strengthened version of Lemma 6 for maximal right congruences.

LEMMA 8. *Let τ be a maximal right congruence on the semigroup S. Let S^* be the union of a set of τ-classes. Then if $a \not\equiv b \pmod{\tau}$ there is a c in S such that exactly one of the pair ac and bc is in S^* or there is a subset T of S such that for any a in S we have $ac \in S^*$ if and only if $c \in T$.*

Proof. Let σ be the congruence defined by S^* in Lemma 6. Then either $\sigma = \tau$ or $\sigma = \nu$. For each element a of S define $T_a = \{c: ac \in S^*\}$. Then $a\sigma b$ if and only if $T_a = T_b$. If $d \not\equiv e \pmod{\tau}$ and $\sigma = \tau$ then $d \not\equiv e \pmod{\sigma}$. Hence $T_d \neq T_e$. Assume $c \in T_e$ and $c \notin T_d$. Then $dc \notin S^*$ and $ec \in S^*$. Hence the first alternative of the conclusion of the Lemma holds. If $\sigma = \nu$ then $a\sigma b$ for all a and b in S. Hence $T_a = T_b = T$ for all a and b in S. Therefore for any a in S, $ac \in S^*$ if and only if $c \in T$.

Let τ be a right congruence on S. For any a in S we have defined the right congruence τa. If τ is maximal and modular the next two theorems show that in several important instances τ and τa have essentially the same nature.

THEOREM 9. *If τ is a maximal, modular right congruence on the semigroup S then either τa is a maximal, modular right congruence on S or σ_a is a right ideal and $\tau a = \nu$.*

Proof. If τ_a is a right ideal of S then $\tau a = \nu$. For ab and ac are in τ_a for all b and c in S. Hence $(ab)\tau(ac)$ and $b(\tau a)c$ for all b and c in S.

Assume τ_a is not a right ideal. Then every τ-class contains an element of the right ideal $a \cup aS$. Let $(ab)\tau e$ where e is a left identity of τ. (If $a\tau e$ then $(ae)\tau e^2 \tau e$.) Then $\tau(ab) = \tau$. Now if $\tau a = \nu$ then $\tau = \tau(ab) = (\tau a)b = \nu b = \nu$. Therefore $\tau a \neq \nu$. Assume σ is a right congruence such that $\tau a \leqq \sigma$. But then $\tau = \tau ab \leqq \sigma b$. Therefore $\tau = \sigma b$ or $\sigma b = \nu$. Let $c \in S$ then $(abac)\tau(ac)$ and $(ba)c(\tau a)c$. Hence ba is a left identity for τa and for σ. If $\tau = \sigma b$ then $\tau a = \sigma ba = \sigma$. If $\sigma b = \nu$ then $\sigma ba = \nu a$ and

$\sigma=\nu$. In any case there is no right congruence properly between τa and ν. Hence τa is maximal.

A right congruence is said to be right cancellative if for every a, b, c in S we have $(ab)\tau(cb)$ implies $a\tau c$. Similar definitions of cancellativity can be made for left congruences and two-sided congruences.

THEOREM 10. *Let τ be a maximal, modular right congruence and $\tau a\neq\nu$. Then τ is a right cancellative right congruence if and only if τa is a right cancellative right congruence.*

Proof. First assume that τ is a right cancellative right congruence and that $cb\equiv db \pmod{\tau a}$. Then $acb\equiv adb \pmod{\tau}$. Since τ is right cancellative we have $ac\equiv ad \pmod{\tau}$ and $c\equiv d \pmod{\tau a}$. Hence τa is right cancellative.

Assume that τa is right cancellative. Since $\tau a\neq\nu$ we have from the previous proof there is a $b\in S$ such that $(ab)\tau e$ where e is a left identity for τ. But then $\tau=\tau(ab)=(\tau a)b$. By the first half of this proof τ is right cancellative.

Consider a commutative semigroup S. Then of course the definitions of right, left, and two-sided congruences and left and right cancellativity are the same. The following theorem gives a classification of the maximal modular congruences of S. They turn out to be exactly of the types examined in the preceding two theorems.

THEOREM 11. *If τ is a maximal modular congruence on a commutative semigroup S then either τ is cancellative or τ has two equivalence classes; one of which is an ideal and the other a semigroup.*

Proof. If τ is a maximal modular congruence then S/τ has no nontrivial congruences. Hence either S/τ is the semigroup $\{0, 1\}$ or S/τ is simple [1, p. 5]. But in the latter case S/τ is both left and right simple. Therefore S/τ is a group [1, p. 6]. Since τ is maximal S/τ has no nontrivial homomorphisms. Hence it is a simple group and cyclic of prime order.

COROLLARY 12. *If τ is a maximal modular cancellative congruence on a commutative semigroup S then there exists a prime p such that if g is any element that is not an identity element of τ then the equivalence classes of τ are*

$$\tau_g, \tau_{g^2}, \ldots, \tau_{g^p}$$

and g^p is an identity element of τ.

Without the assumption of commutativity our results are somewhat more restricted. However partial results have been obtained by assuming the semigroup is finite.

THEOREM 13. *Let S be a finite semigroup. Let σ be a maximal modular two-sided congruence with an equivalence class I that is a two-sided ideal. Then σ has exactly two equivalence classes, I and E, where E is the set of identity elements of σ. Consequently, σ is both a maximal right and maximal left modular congruence.*

Proof. The semigroup S/σ has an identity element 1 and a zero element 0. Since S/σ is finite every right or left unit of S/σ is also a two-sided unit [1, p. 23]. Now if a is a nonunit of S/σ and b an element of S/σ such that ab is a unit then there is a $c \in S/\sigma$ such that $abc=1$. Hence a is a right unit and therefore a unit. Therefore the set of nonunits is a right ideal of S/σ. In the same way we see that the nonunits form a left ideal and hence a two-sided ideal of S/σ. However, S/σ is completely 0-simple [1, p. 67] and the ideal of nonunits must be 0. Therefore $S/\sigma = G \cup \{0\}$ where G is a group. Since $G \cup \{0\}$ is a decomposition of S/σ that gives rise to a modular congruence, S has a nontrivial congruence unless $G=\{1\}$. Hence we have the conclusion of the theorem.

We continue to assume that S is a finite semigroup. Then S contains minimal right ideals. Let I be such a minimal right ideal of S. For any element i in I we have $iI=I$ since iI is a right ideal contained in I. Therefore I is a right group and can be written in the form $G \times K$ where G is a group, K is a set of idempotents and $(a, e)(b, f)=(ab, f)$ for a, b in G and e, f in K [1, p. 38]. Since I is a right ideal, for every c in S and every e in K we have

$$(1, e)c = (\theta(c, e), \psi(c, e))$$

where $\theta(c, e) \in G$ and $\psi(c, e) \in K$.

If $e \in K$ then define the relation $\sigma^{(e)}$ on S by

$$a\sigma^{(e)}b \Leftrightarrow \psi(a, e) = \psi(b, e). \tag{1}$$

Clearly $\sigma^{(e)}$ is a right congruence. In fact since $(1, e)c=(1, e)(1, e)c$ where 1 is the identity element of G we have $(1, e)c \equiv c \pmod{\sigma^{(e)}}$ for all c in S. Therefore $\sigma^{(e)}$ is a modular congruence with a left identity $(1, e)$. The set of all $\sigma^{(e)}$ are conjugates in the sense that $\sigma^{(g)}=\sigma^{(e)}(1, g)$ for any pair of idempotents e and g in K. For $c\sigma^{(g)}b$ if and only if $\psi(c, g)=\psi(b, g)$ and $c \equiv b \pmod{\sigma^{(e)}(1, g)}$ if and only if $\psi(c, g)=\psi((1, g)c, e)=\psi((1, g)b, e)=\psi(b, g)$.

Since $\sigma^{(e)}$ is a modular right congruence either it is contained in a maximal modular right congruence or $\sigma^{(e)}=\nu$. If $\sigma^{(e)}=\nu$ then K must contain only a single idempotent e. For if $e, g \in K$ and $e \neq g$ then $\psi((1, e), e)=e \neq g=\psi((1, g), e)$. If K contains only a single idempotent then the minimal right ideal is a group. On the other hand if I is not a group there is a maximal, modular right congruence τ that contains $\sigma^{(e)}$.

THEOREM 14. *The maximal modular right congruence τ is neither right cancellative nor does it have an equivalence class that is a right ideal of S.*

Proof. Let c be any element of S. If $f=\psi(c, e)$ than by (1) we see that $(1, f)\sigma^{(e)}c$. Hence every equivalence class of $\sigma^{(e)}$ contains an element of the form $(1, f)$. Since each τ-class is a union of $\sigma^{(e)}$-classes we also have that every τ-class contains an element of the form $(1, f)$. If J is a τ-class that is a right ideal and $(1, f)$ is an element of J then $(1, f)S=G\times K$ is in J. Therefore τ is the trivial right congruence ν. Hence no τ-class is a right ideal.

Assume that τ is right cancellative. Since $(1, g)(1, e)=(1, e)(1, e)$ it follows that $(1, g)(1, e)\equiv(1, e)(1, e) \pmod{\tau}$ and $(1, g)\tau(1, e)$ by the right cancellativity of τ for all g in K. But then τ is ν since every τ-class contains an element of the form $(1, f)$.

The following theorem gives us a characterization of the maximal, modular right congruences of a finite semigroup similar to the corresponding theorem for commutative semigroups. However, if any minimal right ideal of the semigroup contains more than one idempotent then we have seen from the above theorem that there must be a third type of maximal, modular right congruence.

We first prove the following lemma.

LEMMA 15. *Let S be a finite semigroup, $G\times K$ a minimal right ideal of S and τ a maximal modular right congruence on S that does not have an equivalence class that is a right ideal. Let τ_x be any equivalence class of τ. Then $(G\times K)\cap\tau_x=Ha\times K_x$ where K_x is a subset of K and Ha is a coset of G with respect to the subgroup H of G and a depends on x.*

Proof. The right ideal $G\times K$ must intersect every τ-class nontrivially. Let τ_e be an equivalence class of τ consisting of left identity elements of τ. Then there is an element (a, g) of $G\times K$ such that $(a, g)\in\tau_e$. Since G is finite there is an integer n such that $a^n=1$, where 1 is the identity element of G. But τ_e is a subsemigroup of S; therefore $(1, g)=(a^n, g)=(a, g)^n\in\tau_e$. In the same manner we have $(a^{-1}, g)\in\tau_e$. Also if (a, g) and (b, g) are in τ_e then $(ab, g)=(a, g)(b, g)\in\tau_e$. Hence the set $H=\{a\in G: (a, g)\in\tau_e\}$ is a subgroup of G. Now let $(c, f)\in\tau_e$. Then $(c, g)=(c, f)(1, g)\in\tau_e$. Hence $c\in H$. Thus we have $(G\times K)\cap\tau_e=H\times K_e$ where H is a subgroup of G and K_e is a subset of K. Next, we examine the intersection of $G\times K$ with an arbitrary equivalence class τ_x. Let (a, f) and (b, k) be in τ_x where $a, b\in G$ and $f, k\in K$. Then $(a, f)(a^{-1}, g)=(1, g)\in\tau_e$. Since $(a, f)\tau(b, k)$ we have also $(b, k)(a^{-1}, g)=(ba^{-1}, g)\in\tau_e$. Therefore $ba^{-1}\in H$, $b\in Ha$ and $(G\times K)\cap\tau_x\subseteq Ha\times K_x$ where K_x is a subset of K. Conversely, if $(a, f)\in\tau_x$ and $h\in H$ then $(ha, f)=(h, g)(a, f)$ in τ_x since (h, g) is a left identity of τ. Hence $(G\times K)\cap\tau_x=Ha\times K_x$.

COROLLARY 16. *If τ is right cancellative then $(G\times K)\cap\tau_x=Ha\times K$ for some a depending on x.*

Proof. If τ is right cancellative then for $\tau_x\neq\tau_y$ we have $\tau_{xc}\neq\tau_{yc}$ for any element c in S. Since S is finite, for any c and d in S there is a solution τ_x to the equation

$\tau_{xc}=\tau_d$. In particular there is a solution to the equation $\tau_{x(1,f)}=\tau_d$. The only elements of $G\times K$ in $S(1,f)$ are the elements (a,f). Therefore K_d contains f for every f in K and every d in S. Therefore $K_d=K$ for every d in S.

THEOREM 17. *Let S be a finite semigroup and let τ be a maximal, modular right congruence on S. Then*

(1) *τ is right cancellative*;

(2) *τ has an equivalence class that is a right ideal or*

(3) *τ contains $\sigma^{(g)}$ defined in* (1) *for some idempotent* $(1, g)$ *in the minimal right ideal $G\times K$.*

Proof. Assume that neither of the first two alternatives hold. Then each τ-class contains an element of $G\times K$. Let $(1, g)\in\tau_e$, the τ-class of left identities of τ, and $f=\psi(x, g)$ for some x in S. Let $(G\times K)\cap\tau_e=H\times K_e$. Assume $H\neq G$ and $b\in G$ such that $b\notin H$. Then $(1, g)\not\equiv(b, g)\pmod{\tau}$. Let $S^*=S^*(f)$ be the union of all those τ-classes containing an element of the form (a,f) for $a\in G$. By Lemma 8 either there is a y in S such that exactly one of the pair $(1, g)y$ and $(b, g)y$ is in S^* or there is a nonempty subset T of S such that for every z in S we have $zc\in S^*$ if and only if $c\in T$. The first of these alternatives cannot hold. For if $h=\psi(y, g)$ then $(1, g)y=(\theta(y, g), h)\in S^*(h)$ if and only if $(b, g)y=(b, g)(1, g)y=(b\theta(y, g), h)\in S^*(h)$. Therefore the second alternative must hold. Thus for any d such that $\psi(d, g)=f$ and any z in S we have $zd\in S^*$. In particular, for any $k\in K$ we have $(\theta(d, k), \psi(d, k))\in S^*$.

By Lemma 15 there are precisely $[G : H]$, the index of H in G, τ-classes in S^*. There are also precisely $[G : H]$ τ-classes containing an element of the form $(c, \psi(dk, k))$ in S^* since $(c\theta(d, k)^{-1}, k)d=(c, \psi(d, k))\in S^*$ for any c in G. Hence each τ-class in S^* contains an element of the form $(c, \psi(d, k))$. We see that if $\tau_x\subseteq S^*$ and if $K^*=\{\psi(d, k) : \psi(d, g)=f \text{ and } k\in K\}$ then by Lemma 15 we have $\tau_x\cap(G\times K)\supseteq Ha\times K^*$ for some a in G. Now let $(c, k)\in\tau_x\cap(G\times K)$. Then $(1, g)(c, k)=(c, k)\in S^*$. Hence $(yc^{-1}, k)(c, k)=(y, k)\in S^*$ for any y in G. This follows from the fact that $(c, k)\in T$. Therefore $G\times\{k\}\subseteq S^*$ and each τ-class in S^* contains an element of $G\times\{k\}$. Therefore $S^*\cap(G\times K)=G\times\bar{K}$ where $\bar{K}$ is a subset of K that contains K^*.

Now we see that each idempotent f in K gives rise to a set $S^*=S^*(f)$ of τ-classes. If $(c, k)S^*(f)\cap S^*(e)$ for some e, f in K then by the above remarks every equivalence class of $S^*(f)$ and every equivalence class of $S^*(e)$ contains an element of the form (a, k). Hence $S^*(f)=S^*(e)$. Therefore the set of all $S^*(f)$ form a decomposition of S. Clearly the corresponding equivalence relation σ is a right congruence. For if d is any element such that for some element c in S we have $cd\in S^*(f)$ for some f then $d\in T(f)$ and $Sd\subseteq S^*(f)$. Also since the σ-classes are unions of τ-classes we must have $\tau\leqq\sigma$. But τ is maximal. Hence $\sigma=\nu$ or $\sigma=\tau$. If $\sigma=\nu$ then there is only one distinct S^* and for any equivalence class τ_x of τ

we have $\tau_x \cap (G \times K) = Ha \times K$. However, if d is any element of S and $(1, g)d = (c, k)$ then $(ac^{-1}, g)d = (ac^{-1}, g)(1, g)d = (ac^{-1}, g)(c, k) = (a, k) \in \tau_x$. For any x and d we can always find a y such that $\tau_{yd} = \tau_x$. Hence since S is finite τ is right cancellative. By our assumptions we must have $\sigma = \tau$. Then $S^*(f)$ is a single τ-class and $H = G$. Therefore in any case we have $H = G$. It then follows that $\tau \geqq \sigma^{(g)}$ since if $\psi(d, g) = \psi(c, g)$ then $(1, g)c \equiv (1, g)d \pmod{\tau}$ and $c \tau d$.

Finally we shall prove a result which together with Theorem 13 shows that the maximal, modular two-sided congruences in a finite semigroup are of essentially the same types as those in a commutative semigroup.

THEOREM 18. *Let σ be a maximal, modular two-sided congruence on a finite semigroup S. Let σ have no equivalence classes that are two-sided ideals. Then σ is cancellative.*

Proof. Since σ is a maximal, modular congruence S/σ is a simple group with an identity element. Since S is finite the nonunits of S/σ form an ideal. But S/σ is simple therefore S/σ is a group. In fact, it is a simple group. Therefore σ is cancellative.

3. **Radical of a semigroup.** If we attempt to arrive at a structure theory of semigroups by means of the various congruence relations on a semigroup one course of action that is open to us is an examination of the analogies we can make to ring theory. In examining the Jacobson radical in a ring with minimal condition we are faced with a multitude of equivalent characterizations each having an analogue in semigroup theory.

We shall confine our attention to only three of these analogues in this paper: R, the intersection of all the maximal, modular two-sided congruences on S; R_r, the intersection of all the maximal, modular right congruences on S; and R_l, the intersection of all the maximal, modular left congruences on S.

LEMMA 19. *R, R_r and R_l are two-sided congruences on S.*

Proof. Clearly R is a two-sided congruence since it is the intersection of two-sided congruences. If τ is a maximal, modular right congruence then τa is either a maximal, modular right congruence or ν. In any event, $\bigcap \tau a \leqq \tau$ since there is a left identity e such that $\tau = \tau e$ and $\bigcap \tau a$ is two-sided. Therefore the intersection of all the maximal, modular right congruences is equal to an intersection of two-sided congruences. Hence R_r is two-sided. Similarly R_l is two-sided.

THEOREM 20. *If S is finite then $R_r \leqq R$ and $R_l \leqq R$.*

Proof. Let σ be a maximal, modular two-sided congruence on S. Then σ is contained in a maximal, modular right congruence τ. As we have seen in the previous section $\sigma = \bigcap \tau a$. Therefore $R_r \leqq R$. Similarly $R_l \leqq R$.

If every maximal, modular right or left congruence contained a modular two-sided congruence then, of course, $R=R_l=R_r$. However, as seen in the following example, this need not be the case.

Let $n\geqq 1$ be a fixed positive integer. Let S be a set of $n\times n$ matrix units e_{ij}; $i,j=1,\ldots,n$ and a zero element 0.

This is a trivial type of Rees matrix semigroup [6].

Assume σ is a maximal, modular two-sided congruence on S. Let e_{ij} be an identity element of S. Since 0 behaves like a zero element of S, σ_0 is a two-sided ideal. Hence by Theorem 13 σ has precisely two equivalence classes; one containing 0 and the other containing e_{ij}. The equivalence class containing e_{ij} is a subsemigroup. Therefore $e_{ij}e_{ij}\neq 0$ and $i=j$. Hence for any element e_{ij} with $i\neq j$ we have $e_{ij}\equiv 0 \pmod{\sigma}$. But then $e_{ij}e_{ji}\equiv 0 \pmod{\sigma}$ and $e_{ii}\equiv 0 \pmod{\sigma}$. Hence there are no maximal, modular two-sided congruences on S and $R=\nu$. Consider the partition

$$\{e_{i1}\},\{e_{i2}\},\ldots,\{e_{in}\},\{e_{jk}: j\neq i\}\cup\{0\}$$

of S. It is easily seen that this partition gives rise to a maximal modular right congruence τ_i which has e_{ii} as a left identity element.

The following theorem shows that R has one of the essential properties of a radical.

THEOREM 21. *If S is a semigroup then the semigroup S/R has ι for its radical.*

Proof. It follows from the standard isomorphism theorems (see for example [2; p. 61]) that there is a one-to-one order-preserving correspondence between the two-sided congruences of S that contains R and the two-sided congruences of S/R. Let R_x be the equivalence class of R containing x. If $\bar{\sigma}$ is the two-sided congruence of S/R corresponding to the two-sided congruence σ of S then $x\equiv y \pmod{\sigma}$ for any x and y in S if and only if $R_x\equiv R_y \pmod{\bar{\sigma}}$. If σ is modular with identity element a then $ax\equiv x \pmod{\sigma}$. Hence $R_aR_x\equiv R_x \pmod{\bar{\sigma}}$ and $\bar{\sigma}$ is modular. Similarly the modularity of $\bar{\sigma}$ implies the modularity of σ. Therefore there is a one-to-one correspondence between the maximal, modular two-sided congruences of S and those of S/R. It follows readily that since the intersection of the maximal, modular two-sided congruences of S is R the corresponding two-sided congruences of S/R has an intersection equal to ι.

Substantially the same proof can be given to show that both R_r and R_l also have this essential property of a radical.

Let σ be an equivalence relation on a semigroup S. Let T be a subset of S. We shall say T is *separated* by σ if not every element of T is in the same σ-class. We shall say T is *completely separated* by σ if every element of T is in a distinct σ-class.

Assume that S is a finite semigroup for which $R_r=\iota$. Let $G\times K$ be a minimal right ideal of S. We shall refer to maximal, modular right congruences as given in

Theorem 17 as right congruences of Types 1, 2, and 3. $G\times K$ is not separated by any congruence of Type 2 and $G\times\{e\}$ is not separated by any congruence of Type 3 for any e in K. Hence $G\times\{e\}$ is separated by a right cancellative right congruence and completely separated by the intersection of all the right cancellative maximal, modular right congruences on S. Recall that any maximal, modular right congruence τ that is right cancellative is determined by a subgroup H of G. Each τ-class is defined by an element a of G and is the set of elements d such that $(1, e)d=(ha, f)$ where $h\in H$ and e is any element of K. Let σ and σ' be two such right congruences determined by the subgroups H and H'. The intersection of σ and σ' is determined by the intersection $H\cap H'$; i.e., $d\equiv(c, f)\pmod{\sigma\cap\sigma'}$ if and only if for any e in K we have $(1, e)d=(\theta(d, e), \psi(d, e))$ and c and $\theta(d, e)$ are in the same coset of G with respect to $H\cap H'$. Similarly the intersection α of all the maximal, modular, right cancellative, right congruences is determined by the cosets of a subgroup M of G. However, α must completely separate $G\times\{e\}$ for any e in K.

Therefore M is the identity subgroup of G. Thus every α-class is determined by a single element a of G; i.e., $d\equiv(a, f)\pmod{\alpha}$ if and only if for every e in K we have $(1, e)d=(a, \psi(d, e))$. Thus we have

LEMMA 22. *If S is a finite semigroup for which $R_r=\iota$ and $G\times K$ is a minimal right ideal then for any d in S we have $(1\times K)d\subseteq a\times K$ for some a depending on d. Also if for any idempotent e in K we have $\theta(d, e)=\theta(c, e)$ then d and c are not separated by any right cancellative maximal, modular right congruence of S.*

COROLLARY 23. *A right cancellative maximal modular right congruence does not separate a pair of distinct idempotents.*

Proof. Let x be any idempotent of S and $x\equiv(a, e)\pmod{\alpha}$ where α is the intersection of all the right cancellative maximal, modular right congruences on S. Then by the lemma we must have $(1, e)x=(a, \psi(x, e))$. But then $(1, e)x=(1, e)x^2=(a, \psi(x, e))x=(a^2, g)$ for some g in K. We must have $a^2=a$. Thus $a=1$ and any two idempotents are congruent modulo α.

COROLLARY 24. *Every maximal subgroup of G determines a right cancellative maximal, modular right congruence.*

Proof. Let H be a maximal subgroup of G. Define the relation τ by $c\equiv d\pmod{\tau}$ if and only if $\theta(c, e)\theta(d, e)^{-1}\in H$. By the results of the lemma, τ is independent of the choice of e. Clearly τ is an equivalence relation. To see that it is a right congruence we take $a\in S$ and note that $\theta(ca, e)=\theta(c, e)\theta(a, \psi(c, e))$ and $\theta(da, e)=\theta(d, e)\theta(a, \psi(d, e))$. Since $\theta(a, \psi(c, e))=\theta(a, \psi(d, e))$ we have

$$\theta(ca, e)\theta(da, e)^{-1} = \theta(c, e)\theta(d, e)^{-1}\in H.$$

Hence $c \equiv d \pmod{\tau}$ implies $ca \equiv da \pmod{\tau}$. It follows from the definition of τ that each τ-class intersects $G \times K$ in precisely the subset $Ha \times K$ for some a of G and that $H \times K$ forms a set of left identity elements of τ. If $\sigma \neq \nu$ is any right congruence that contains τ then every σ-class contains a subset of the form $Ha \times K$. Hence σ must be right cancellative. Therefore σ is defined by a proper subgroup H' of G that must contain H. Hence $H = H'$ and $\tau = \sigma$.

COROLLARY 25. *The Frattini subgroup* [4, *p.* 156] *of G is the identity.*

Proof. Each maximal subgroup of G defines a right cancellative maximal, modular right congruence. Thus the intersection of the maximal subgroups of G must be the identity.

Now assume that $G \times K$ is a minimal right ideal. All minimal right ideals of a finite semigroup have the same cardinal number. For if I and J are two minimal right ideals and $a \in J$ then aI is a right ideal and a subset of J. Hence $aI = J$ and the cardinal number of I is greater than or equal to that of J. By symmetry the equality of the cardinalities prevails. Then $d(G \times K)$ is also a minimal right ideal.

If σ is a right congruence of Type 2 with the equivalence class S_0 that is a right ideal then both $G \times K$ and $d(G \times K)$ are contained in S_0 by Lemma 7 and the minimality of these ideals. Let $(1, e)d = (a^{-1}, f)$. Then $d(a, e)$ is an idempotent since $d(a, e)d(a, e) = d(a, e)(1, e)d(a, e) = d(a, e)(a^{-1}, f)(a, e) = d(a, e)$. By the above remark and Lemma 22, $d(a, e)$ and $(1, e)$ must be separated by a right congruence of Type 3. Since each such right congruence contains a right congruence $\sigma^{[g]}$ of (1) there must be a $g \in K$ such that

$$\psi((1, e), g) \neq \psi(d(a, e), g).$$

However, both of these elements of K are equal to e. Hence we must have $d(a, e) = (1, e)$. Therefore we have

THEOREM 26. *Under the assumptions of Lemma* 23, $G \times \{e\}$ *is a minimal left ideal of S.*

By using the assumption that $R_l = \iota$, a similar argument would show that any minimal left ideal of S contains a minimal right ideal. Since any left ideal contains elements of $G \times K$ the minimal left ideals of S must be the ideals $G \times \{e\}$, $G \times \{f\}, \ldots$ for $e, f \in K$. Hence these left ideals also have the minimal cardinality and they must contain a right ideal. But then $G \times K = G \times \{e\}$ and K consists of a single idempotent.

THEOREM 27. *If S is a finite semigroup for which* $R_r = R_l = \iota$ *then S has a subgroup G which is both the minimal right ideal of S and the minimal left ideal of S.*

4. **t-semisimple semigroups.** In this section we shall obtain a characterization of t-semisimple semigroups, namely:

THEOREM 28. *S is a finite t-semisimple semigroup if and only if S is the union of disjoint subgroups G_b where b is an element of a semilattice Y; to each pair G_b, $G_{b'}$ with $b \geqq b'$ there is a monomorphism $\varphi_{b,b'}$ on G_b into $G_{b'}$ such that for $b \geqq b' \geqq b''$*

$$\phi_{b,b'}\phi_{b',b''} = \phi_{b,b''},$$

the product in S of any two elements $x \in G_b$ and $x' \in G_{b'}$ is defined by

$$xx' = (x\phi_{b,b''})\cdot(x'\phi_{b',b''})$$

where the right hand product is taken in $G_{b''}$ and $bb' = b''$ in Y, and G_0 is t-semisimple where 0 is the minimal element of Y.

Proof. Let $\{\sigma_i : i = 1, \ldots, m\}$ be the cancellative maximal modular congruences on S and $\{\tau_j : j = 1, \ldots, n\}$ be the maximal modular right congruences having exactly two equivalence classes. Then, such as in [2], we see that S is isomorphic to a subdirect product of the simple groups $\Gamma_i = S/\sigma_i$ and the two element semigroups $B_j = S/\tau_j \cong \{0, 1\}$. Hence S can be considered as a subsemigroup of the direct product $\Gamma \times B$ where Γ is a group that is the direct product $\prod \Gamma_i$ of finite simple groups and $B = \prod B_j$ is a Boolean algebra.

We denote the elements of $\Gamma \times B$ by $(\alpha_1, \alpha_2, \ldots, \alpha_m; \beta_1, \ldots, \beta_n)$ where $\alpha_i \in \Gamma_i$ and $\beta_j \in B_j$. Define Γ_b, for $b = (\beta_1, \ldots, \beta_n)$, to be the set of all elements $(\alpha_1, \ldots, \alpha_m)$ of Γ such that $(\alpha_1, \ldots, \alpha_m; \beta_1, \ldots, \beta_n)$ is in S, and let G_b be the set of all such elements that are in S. Then G_b and Γ_b are isomorphic subgroups since Γ_b is a subsemigroup of a finite group. Let $0 = (0, \ldots, 0)$ be the zero element of B. Since

$$(\alpha_1, \ldots, \alpha_m; \beta_1, \ldots, \beta_n)(1, \ldots, 1; 0, \ldots, 0) = (\alpha_1, \ldots, \alpha_m; 0, 0, \ldots, 0)$$

Γ_0 is a subdirect product of $\prod \Gamma_i$. Hence Γ_0 is a t-semisimple group and $\Gamma_0 \supseteq \Gamma_b$. More generally, if b and b' are elements of B such that $b \geqq b'$, then $\Gamma_{b'} \supseteq \Gamma_b$.

Now let Y be the set of all $b = (\beta_1, \ldots, \beta_n) \in B$ such that $(1, \ldots, 1; \beta_1, \ldots, \beta_n)$ is in S. Clearly Y is a subsemilattice of B. Since $G_b G_{b'} \subseteq G_{bb'}$ for $b, b' \in Y$ it is clear that S is the semilattice of groups G_b for $b \in Y$.

If we define $\phi_{bb'} : G_b \to G_{b'}$ for $b \geqq b'$ to be essentially the inclusion map of Γ_b into $\Gamma_{b'}$ the properties of the $\phi_{bb'}$ stated in the theorem are immediate. Thus the necessity of the theorem holds.

Assume S is a semilattice Y of subgroups G_b satisfying the conditions of the theorem. If $S = G_0$ then it is clear that S is t-semisimple. Therefore assume Y contains more than one element. Let $x \in G_b$ and $y \in G_a$ with $b > a$. Let $W = \{c : c \in Y$ and $c \geqq b\}$ and W', the complement in Y of W. Clearly W is a subsemigroup of

Y and W' an ideal of Y. Since $G_cG_d \subseteq G_{cd}$ it follows that $F=\bigcup_{c\in W} G_c$ is a subsemigroup of S and $J=\bigcup_{c\in W'} G_c$ is a two-sided ideal of S. The decomposition $S=F\cup J$ gives rise to a maximal modular two-sided congruence that separates x and y.

Now assume x and y are in G_b and $x\neq y$. Let 1_0 be the identity of the group G_0, $x_0=x\cdot 1_0=(x)\phi_{b,0}$ and $y_0=y\cdot 1_0=(y)\phi_{b,0}$. Since $\phi_{b,0}$ is an isomorphism $x_0\neq y_0$. If G_0 is t-semisimple there is a maximal normal subgroup H of G_0 that contains exactly one of the elements x_0 and y_0, say y_0.

Define a relation σ on S by

$$w \equiv z \pmod{\sigma}$$

where $w\in G_b$ and $z\in G_a$ if and only if $w_0z_0^{-1}\in H$ where $w\cdot 1_0=w_0$ and $z\cdot 1_0=z_0$. Clearly σ is an equivalence relation. Let $u\in G_c$. Then $(wu)_0=(wu)1_0=w(u1_0)=wu_0=(w1_0)u_0=w_0u_0$. Hence $(wu)_0(zu)_0^{-1}=(w_0u_0)(z_0u_0)^{-1}=w_0z_0^{-1}\in H$. Therefore $wu\equiv zu \pmod{\sigma}$. Similarly $uw\equiv uz \pmod{\sigma}$. Hence σ is a two-sided congruence that separates x and y. Also $1_0x\equiv x1_0\equiv x_0 \pmod{\sigma}$ so σ is modular.

If $wu\equiv zu \pmod{\sigma}$ then $(wu)_0(zu)_0\in H$. Therefore $w_0z_0^{-1}\in H$ and $w\equiv z \pmod{\sigma}$. Hence σ is right cancellative. Similarly σ is left cancellative. If τ is a two-sided congruence such that $\sigma<\tau$ then τ is modular and cancellative.

Consider the congruence $\bar{\tau}$ induced by τ on G_0. The kernel of $\bar{\tau}$ is a subgroup H' that contains H. If $x\tau y$ then $x_0y_0^{-1}\in H'$ and $H'=G_0$. But then τ has an equivalence class that is a two-sided ideal and cannot be cancellative. Therefore τ separates x and y and there is a maximal modular cancellative two-sided congruence that separates x and y.

Therefore any pair of distinct elements of S are separated by some maximal modular two-sided congruence. Hence S is t-semisimple.

COROLLARY 29. *If S is a finite t-semisimple semigroup all of whose maximal, modular two-sided congruences are cancellative then S is a group.*

COROLLARY 30. *A t-semisimple finite semigroup S with a zero element is a semilattice.*

Proof. Since S has a zero element the minimal two-sided ideal is $\{0\}$. Hence each $G_b=\{0\}$ and S is a semilattice.

We conclude with the following theorem.

THEOREM 31. *If S is a t-semisimple finite semigroup with no nontrivial modular two-sided congruences then S is either a simple group or the unique semilattice of two elements.*

Proof. If S is semisimple then S has a maximal, modular two-sided congruence. Therefore ι is a modular two-sided congruence. If ι is cancellative then S is a group.

Since S has no nontrivial congruences it has no nontrivial normal subgroups and hence is simple. If ι has two equivalence classes then S has two elements one of which forms a subsemigroup and the other forms an ideal.

References

1. A. H. Clifford and G. B. Preston, *Algebraic theory of semigroups*, Vol. 1, Math. Surveys No. 7, Amer. Math. Soc., Providence, R. I., 1961.

2. P. M. Cohn, *Universal algebra*, Harper and Row, New York, 1965.

3. R. A. Dean and R. H. Oehmke, *Idempotent semigroups with distributive right congruence lattices*, Pacific J. Math. **14** (1964), 1187–1209.

4. P. Dubreil, *Contributions à la théorie des demigroupes*. II, Univ. Roma. Ist. Naz. Alta Math. Rend. Math e Appl. (5) **10** (1951), 183–200.

5. Marshall Hall, Jr., *The theory of groups*, Macmillan, New York, 1959.

6. H. J. Hoehnke, *Structure of semigroups*, Canad. J. Math. **18** (1966), 449–491.

7. R. H. Oehmke, *On the structure of an automaton and its input semigroup*, JACM **10** (1963), 521–525.

8. D. Rees, *On semigroups*, Proc. Cambridge Philos. Soc. **36** (1940), 387–400.

9. E. J. Tully, Jr., *Representation of a semigroup by transformations acting transitively on a set*, Amer. J. Math. **83** (1961), 533–541.

University of Iowa,
Iowa City, Iowa