MINIMAL CONGRUENCES ON AUTOMATA

R. H. OEHMKE

The University of Iowa, U.S.A.

Received July 7, 1988

1. Introduction

In this paper we study some of the relationships between the minimal congruences on an automaton and the structure of the automaton. In Section 2 we show there are three different types of minimal congruences that could exist on an automaton. Analogously to the study of modules over a ring [3] we have made assumptions that the universal congruence on the automaton is the least upper bound of certain classes of minimal congruences. We examine some of the implications of these assumptions.

2. Preliminaries

Let S be a semigroup and A a set such that there is a composition mapping

$$\theta : A \times S \to A$$

denoted by

$$(a, s) \to \theta(a, s) = as.$$

The mapping θ has the property that

$$(as)t = a(st)$$

for all a in A and s and t in S. We shall call the triple (A, S, θ) an S-automaton, or, more simply, an automaton. Generally, when there is no cause for confusion we shall refer to the automaton by the symbol A.

A congruence τ on A is an equivalence relation on A such that if $(a, a') \in \tau$ and $s \in S$ then $(as, a's) \in \tau$.

The set of all congruences on A will be denoted by $R(A)$ and considered as a subset of the lattice $E(A)$ of all equivalence relations on A. We shall use the same ordering on $R(A)$ that is commonly used on $E(A)$, namely, set inclusion. The set $R(A)$ is closed under the two operations $\cap$ and $\cup$. For two congruences α and β in $R(A)$ these operators are defined, respectively, as the largest element of $R(A)$ contained in both α and β and the smallest element of $R(A)$ containing both α and β.

There is a smallest congruence ι in $R(A)$ that is defined by

$$(a, a') \in \iota \Leftrightarrow a = a' \text{ and } a, a' \in A$$

and a largest congruence v in $R(A)$ that is defined by

$$(a, a') \in \nu \Leftrightarrow a, a' \in A.$$

If B is a subset of A that is also an S-automaton using the operation θ then B is called subautomaton of A. The relation μ defined by

$$(a, a') \in \mu \Leftrightarrow a, a' \in B \text{ or } a = a'$$

is a congruence relation on A.

A congruence τ is said to be minimal if $\iota \neq \tau$ and if $\iota < \sigma < \tau$ implies $\iota = \sigma$ or $\sigma = \tau$.

Let τ be a congruence on A. Let U be an equivalence class of τ containing the element e. If for every $d \in S$ such that $Ud \subseteq U$ we have $ed = e$, then e is called a zero of τ. If $U = \{e\}$ then e is called a trivial zero of τ; otherwise, e is called a nontrivial zero of τ.

Theorem 1. [1]. If τ is a minimal congruence on A then either

1. Every nontrivial equivalence class of τ has exactly two distinct elements in it, $\{a, b\}$ such that $a \notin bS$ and $b \notin aS$. All the nontrivial equivalence classes are of the form $\{a, b\}c$ for $c \in S^1$. For every c, d in S we have $ac = ad$ if and only if $bc = bd$. Finally, if $ac \neq bc \neq b$ then there is a $d \in S$ such that $acd = a$ and $bcd = b$.
2. Every nontrivial equivalence class has exactly one zero. If a is a nonzero of τ then every nontrivial equivalence class of τ is contained in aS^1. If e is a nontrivial zero of τ then every nontrivial zero of τ is in eS^1.
3. There are no nontrivial zeros of τ. If a is a nonzero of τ then every nontrivial equivalence class of τ is contained in aS^1.

[We use S^1 to represent S with an identity element 1 adjoined and such that 1 behaves unitarily on A.]

3. Type 1 congruences

If Ω is a set of congruences on A then $\bigcup \Omega$ will denote the least upper bound of Ω in the lattice of congruences on A. In this section we shall assume that Ω is the set of all congruences of Type 1 and that $\bigcup \Omega = \nu$.

We give a generalization of a previous result, [Theorem 1, 2].

An automaton A is strongly connected if for each a in A we have $A = aS$. An automaton is cancellative if for $a, b \in A$ and $s \in S$ we have $as = bs$ implies $a = b$.

Theorem 2. A is an automaton such that $\nu = \cup \Omega$ if and only if A is the disjoint union of two or more strongly connected, cancellative subautomata and A has the additional property that for any two elements a and b in A we have $as = at$ implies $bs = bt$ for all s and t in S.

Proof: The proof follows closely to the proof in the more special case except for minor changes in the language. Therefore we shall refer the reader to [2].

4. Type 2 congruences

In this section we let Ω be the set of all minimal congruences of Type 2. We assume $\nu = \cup \Omega$. We also assume A is cyclic, i.e., there exists a $c \in A$ such that $cS^1 = A$.

Let U_1 be the set of generators of A, and I_1 the set of nongenerators of A. Clearly, I_1 is a subautomaton of A. Now there must be a $\mu \in \Omega$ such that

$$(a, b) \in \mu, \quad a \in U_1, \text{ and } b \in I_1.$$

If $\omega \in I_1$ then since a is a generator of A we must have some $t \in S$ such that $at = \omega$. But then $(\omega, bt) \in \mu$. By [Theorem 1, 1] it follows that $\omega = bt$. Therefore b is a generator of I_1 and I_1 is cyclic.

We can continue the process, letting U_2 be all the generators of I_1, and I_2 all the nongenerators. The same argument as above applies, so by an induction argument we have sequences

$$\begin{gathered} U_1, U_2, \ldots, U_n, \ldots \\ I_1, I_2, \ldots, I_n, \ldots \end{gathered} \tag{1}$$

such that U_i is a nonempty set of generators of I_{i-1}.

Lemma 3. Every subautomaton of A is cyclic.

Proof: Let $\mathfrak{J}$ be the set of all subautomata of A that are not cyclic and assume $\mathfrak{J}$ is not empty. We can partially order $\mathfrak{J}$ by inclusion. If $\mathfrak{S}$ is a simply ordered subset of $\mathfrak{J}$ we let $\cup \mathfrak{S}$ be the union of all the elements of $\mathfrak{S}$. Call it M^*. If M^* is cyclic then it has a generator c. But for c to be in M^* there must be an $M \in \mathfrak{S}$ such that $c \in M$. But then since $cS^1 = M^* \supseteq M$ we must have $cS^1 = M$ an M is cyclic. Since this is a contradiction, $M^* \in \mathfrak{J}$. Therefore with the assumption that $\mathfrak{J}$ is not empty we have maximal elements in $\mathfrak{J}$. Let M be one of them.

Define an equivalence relation ϱ by $(u, v) \in \varrho$ if $u, v \in A$ and

$$\{s | s \in S^1 \text{ and } us \in M\} = \{s | s \in S^1 \text{ and } vs \in M\}.$$

It follows readily that ϱ is a congruence on A. If ϱ intersects any minimal congruence nontrivially then that congruence is contained in ϱ. If ϱ contains every minimal congruence then $\nu \leq \varrho$ and $\nu = \varrho$. But if c is a generator of A and v is in M then $(c, v) \notin \varrho$. Therefore there must be a minimal congruence μ such that $\mu \cap \varrho = \iota$. Now let $(a, b) \notin \mu$ where $a \neq b$. Since $(a, b) \notin \mu$ there is an $s \in S$ such that at most one of the pair as, bs is in M. Say $bs \in M$ and $as \notin M$. But then $(as)S^1 \cup M$ is a subautomaton that properly contains M. Therefore $(as)S^1 \cup M$ is not in $\mathfrak{J}$ and hence it must have a generator ω. Then $\omega \in (as)S^1$ or $\omega \in M$. In either case we have a contradiction. Therefore we must have $\mathfrak{J}$ empty and the lemma holds.

Lemma 4. The subautomata of A are simply ordered by inclusion.

Proof. Let M and M' be two subautomata. Then $M \cup M'$ is a subautomaton which must have a generator u. But then $u \in M$ or $u \in M'$; i.e., $M' \subseteq M$ or $M \subseteq M'$.

Lemma 5. Let K be the intersection of all the nonzero I_i that appear in (1). Then $K = \Phi$ or the sequence of U_i's is finite and K is the last of the sequence.

Proof. We first assume the sequences terminate at U_n. This means that $I_n = \Phi$ and every element of I_{n-1} is a generator of I_{n-1}. Therefore $U_n = I_{n-1} = K$. So assume that the sequence does not terminate and that K is not empty. If $k \in K$ and $ks \notin K$ for some $s \in S$ then $ks \notin I_i$ for some i. But then $ks \in U_i$ and is a generator for I_{i-1}. It is immediate that k is in I_{i-1} and a generator of I_{i-1}. But then $k \in U_i$ which is a contradiction. Hence K is a subautomaton of A.

There must be a $\mu \in \Omega$ such that $(a, b) \in \mu$ where $a \notin K$ and $b \in K$. We can assume $a \in U_j$ for some j. Since $b \in I_{j-1}$ there is an $s \in S^1$ such that $as = b$. Therefore a cannot be a zero of μ and it follows that b must be the zero of μ. Now if $t > j$ we can find a $u \in S$ such that $au \in I_t$. So also is $bu \in I_t$. By [Theorem 1, 1] we have a contradiction. Therefore there must be no $t > j$ and the sequence of U_i' s terminates. This is a contradiction. Therefore $K = \Phi$.

We will now examine the situation in which the sequence of U_i' s terminate. This can be guaranteed by placing a minimal chain condition on subautomata of A. Therefore we shall assume

$$A = U_1 \cup \ldots \cup U_n.$$

In the next three results we relate minimal congruences in Ω to certain types of functions on A.

Lemma 6. Assume $i \neq n$ and f is a mapping $U_i \to U_{i+1}$ such that

1. If $as \in U_i$ then $f(as) = f(a)s$;

2. If $as \in I_i = U_{i+1} \cup \ldots \cup U_n$ then $as = f(a)s$;

3. If $f(a) = f(b)$ then $a = b$ or there exists an s in S such that exactly one of bs and as is in U_{i+1}.

Let $\mu_a = \{a\} \cup \{f(a)\} \cup \{c | f(a) = f(c)\}$ for all $a \in U_i$. Then the μ_a and all necessary singletons form a decomposition of A that relates to a minimal congruence on A.

Proof: First assume $b \in \mu_a$. We wish to show if $b \in U_i$ then $\mu_b = \mu_a$. Clearly, if $a = b$ then $\mu_a = \mu_b$. So assume $b \in U_i$ and that $f(a) = f(b)$. Then $a \in \{c | f(c) = f(b)\}$ and $a \in \mu_b$. Therefore it follows that $\mu_a = \mu_b$. Now let $s \in S$. Again, if $a = b$ we have $as = bs$ and $bs \in \mu_{as}$. If $a \in U_i$ and $b = f(a)$ then either $as \in U_i$ or $as \in I_i$. If the former, then $bs = f(a)s = f(as)$ and $bs \in \mu_{as}$. If $as \notin U_i$ then $as = f(a)s = bs$ and again $bs \in \mu_{as}$. If we still assume $b \in \mu_a$ but assume in addition that $f(a) = f(b)$, then $as, bs \notin U_i$ implies $as = f(a)s = f(b)s = bs$. If $as \notin U_i$ and $bs \in U_i$, then $as = f(a)s = f(b)s = f(bs)$ and $as \in \mu_{bs}$, which implies $bs \in \mu_{as}$. Finally, if both as and bs are in U_i then $f(as) = f(a)s = f(b)s = f(bs)$. This shows that our chosen decomposition is compatible with the operators on A given by S. Therefore it corresponds to a congruence μ on A.

Next assume δ is a congruence not equal to ι and such that $\delta \leq \mu$. Assume $(a, b) \in \delta$ and $a \neq b$. If both a and b are in U_i then select an s such that $as \in U_i$ and $bs \notin U_i$ (or vice versa). We still have $(as, bs) \in \delta$. Also, there is an m such that $asm = a$. Therefore $(a, bsm) \in \delta$ where $bsm \in U_{i+1}$ and hence equal to $f(a)$. Now if $d \in \{c | f(c) = f(a)\}$ and $at = d$ then

$$bsmt = f(a)t = f(at) = f(d) = f(a) = bsm.$$

Therefore $(at, bsmt) \in \delta$ and $(d, a) \in \delta$. This means $\delta_a = \mu_a$ and $\delta = \mu$.

Lemma 7. Let μ be a minimal congruence on A. Then there exists an i such that the nonzeros of μ are in U_i and the nontrivial zeros of μ are in U_{i+1}.

Proof: Let b be a nontrivial zero of μ and $b \in U_{i+1}$. Let δ be the congruence defined by the subautomata I_i. If $\mu \leq \delta$ then every nontrivial element of μ is in I_i. But b is a generator of I_i. Therefore for every nontrivial element c of μ there is an s such that $bs = c$. But this contradicts b being a nontrivial zero. Therefore we must assume μ is not less than δ and $\mu \cap \delta = \iota$. Therefore it follows that every nontrivial equivalence class of μ contains exactly one element of I_i which must be a nontrivial zero. Now every nontrivial zero is generated by any other nontrivial zero. Thus all nontrivial zeros are in U_{i+1}. Still assume b is a nontrivial zero in U_{i+1}. Assume $(c, b) \in \mu$ where $c \in I_j$ and $j \leq i$. There is an s such that $cs \in U_i$. We of course have $(cs, bs) \in \mu$ and $as \neq bs$. If β is the congruence related to the subautomaton I_{s-1} then $\mu \leq \beta$ and every nonzero of μ is in U_i.

Theorem 8. Let μ be a minimal congruence in Ω. Then μ is defined by a function f as in Lemma 6.

Proof: Let a be a nonzero of μ. Therefore there is a unique b in U_{i+1} such that $(a, b) \in \mu$ by Lemma 7. Let $f(a) = b$. Clearly, 1) and 2) of Lemma 6 hold for this choice of f. Define a relation α on A by $(c, d) \in \alpha$ if and only if

$$\{s|cs \in I_i\} = \{s|ds \in I_i\}.$$

Assume $(c, d) \in \mu$, $c \neq d$, $c, d \in U_i$ and $(c, d) \in \alpha$. Then $\mu \leq \alpha$. Therefore if b is the unique zero such that $(c, b) \in \mu$ we also have $(c, b) \in \alpha$. But this says $cS \subseteq I_i$ and c is not in U_i. This is a contradiction. Therefore we can assume there is an s in S such that $as \in U_i$ and $ds \notin U_i$. But then $ds \in U_{i+1}$ and 3) of Lemma 6 holds.

We will conclude this section with a result on the semigroup S. We will continue to assume that the universal congruence, ν, is the union of the congruence in Ω.

In addition, we shall assume that S has a minimal right ideal, J. For any a in A we have aJ a subautomaton of S. Therefore $aJ = I_i$ for some i. If $i \neq n$ then let $K = \{s|s \in \mathfrak{S}$ and $as \in U_n\}$. Clearly, K is a right ideal of S and we must have $K = J$. Therefore $aJ = U_n$ for all $a \in A$. We also have that sJ is a minimal right ideal for each $s \in S$ and $L = \bigcup sJ$ is a minimal two-sided ideal of S. Then $aL = U_n$ for every a in A. Let $a \neq b$ be two elements of A. There exist sequences $a = c_1, c_2, \ldots, c_n = b$ in A and $\mu_1, \ldots, \mu_{n-1}$ in Ω such that $(c_i, c_{i+1}) \in \mu_i$. Now let l be an element of L and consider the sequence $c_1l, c_2l, \ldots, c_nl$. All of these elements are in U_n. But by Lemma 7 no equivalence class of any μ_i contains more than one element of U_n. Therefore since $(c_il, c_{i+1}l) \in$ $\in \mu_i$ we must have $c_il = c_{i+1}l$ for all i. Therefore Al is a singleton for all l in L.

Theorem 9. If S has a minimal two-sided ideal L then Al is a singleton.

5. Type 3 congruences

In this section we assume ν is the least upper bound of the congruence of Type 3.

Theorem 10. A is a strongly connected S-automaton.

Proof: If μ is a minimal congruence of Type 3 then every nonzero of μ generates a subautomaton that contains every other nonzero of A. Now if a and b are two distinct elements of A then they are sequences $a = c_1, \ldots, c_n =$ $= b$ of elements of A and $\mu_1, \ldots, \mu_{n-1}$ of minimal congruences of Type 3 such that

$$(c_i, c_{i+1}) \in \mu_i.$$

But then c_i is in the subautomaton generated by c_{i+1} and c_{i+1} is in the subautomaton generated by c_i. Hence it follows that $a \in bS$ and $b \in aS$. Therefore A is strongly connected.

References

1. OEHMKE, R. H.: On minimal right congruences of a semigroup, Tamkang J. Math. *16* (1985) 29–35.
2. OEHMKE, R. H.: Some semisimplicity conditions for semigroups, Tamkang J. Math. *16* (1985) 105–116.
3. STENSTRÖM, B.: Rings of Quotients, Springer-Verlag, 1970, Berlin.

Robert H. OEHMKE The University of Iowa;
Iowa City, Iowa 52242