On the congruences of finite autonomous Moore automata

By A. ÁDÁM

1. Introduction

By a congruence of an automaton, a partition π of the set of its states is meant such that π is compatible both with the transition function and with the output function. The general problem of describing the congruences of finite Moore automata seems to be a very difficult question.

In the present paper, the congruences of (possibly non-connected) finite Moore automata which have *only one* input sign are presented by a recursive construction. After introducing the most important notions, the question is elucidated in three phases. (The first and third phases are almost trivial.) First, an overview of the congruences of cyclic automata[1] is given in Section 3. The second phase is the single stage of the procedure which requires labour; in this phase the congruences possessing the following property are obtained by a construction: whenever a is a cyclic state, then the congruence class containing a intersects every connected component of the automaton (Section 4). This result can easily be extended into a complete solution of the main problem of the paper (Section 5).

The considerations of Section 4 are illustrated by an example in Section 6.

The final section of the paper gives a broad survey of several problems concerning the congruences of finite Moore automata; some related earlier investigations are referred to here, too. If the reader wants first to get a comprehensive overview of a variety of problems, and thereafter to narrow down his interest to the particular question analyzed actually, then he can be recommended to begin the study of the paper with Section7.

The author wishes to express his gratitude to the referee, Dr. GY. POLLÁK, for his various suggestions which made the considerations clearer at several places of the paper, primarily in section 4.

[1] The attribute "cyclic" is used in the sense that the graph of the automaton is a (directed) cycle. (In some articles, the same attribute is used to mean that the automaton has a state which constitutes a one-element generating system.)

2. Terminology

We shall use the standard terminology of automaton theory and certain basic notions in graph theory without explicit definitions.[2] We shall consider automata so that no state is distinguished in them as an initial one, and (if not otherwise stated) we do not pose any connectivity restriction.

A finite Moore automaton $\mathbf{A}=(A, X, Y, \delta, \lambda)$ is called *autonomous* if the input set X consists of a single element x. The automata, studied in this paper, are thought to be autonomous (unless otherwise stated). The graph-theoretical structure of these automata is described by the (simple but important) well-known theorem of Ore ([8], § 4.4; [1], Chapter I). Denote the connected components of $\mathbf{A}$ by $\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_t$. Ore's theorem implies that

(i) each connected component $\mathbf{A}_i$ (where $1 \leqq i \leqq t$) contains exactly one cycle $\mathbf{Z}_i$,

(ii) $\mathbf{A}_i$ has no other circuit than $\mathbf{Z}_i$,

(iii) an edge of $\mathbf{A}_i$ which does not belong to $\mathbf{Z}_i$ is directed towards $\mathbf{Z}_i$.

A state a is called *cyclic* if a belongs to the cycle of the connected component containing a. In the contrary case, a is called an *acyclic* state.

Let a, b be two states of an automaton. Define $\chi(a, b)$ as the smallest non-negative number i such that $\delta(a, x^i)=b$. (Possibly $\chi(a, b)$ is undefined.)

Connected components and cycles are, obviously subautomata of $\mathbf{A}$. Let a be a state; we denote by $\mathbf{A}[a]$ the connected component containing a and by $\mathbf{Z}[a]$ the cycle of $\mathbf{A}[a]$.

The next evident assertion yields a recursive description of the subautomata of $\mathbf{A}$.

Proposition 1. *Let* $\mathbf{A}$ *be an (autonomous) automaton. Then*

(i) *the union of an arbitrary number* $(\geqq 1)$ *of cycles is a subautomaton of* $\mathbf{A}$,

(ii) *whenever* $\mathbf{B}=(B, \{x\}, Y, \delta, \lambda)$ *is a subautomaton and* a *is a state of* $\mathbf{A}$ *such that*

$$a \notin B \;\&\; \delta(a, x) \in B,$$

then $\mathbf{C}=(B \cup \{a\}, \{x\}, Y, \delta, \lambda)$ *is a subautomaton,*

(iii) *each subautomaton of* $\mathbf{A}$ *can be obtained by applying* (i), (ii) (*where* (ii) *is applied several — possibly zero — times*).

Let a be an arbitrary state of $\mathbf{A}$. The smallest i such that $\delta(a, x^i)$ belongs to $\mathbf{Z}[a]$ is called the *height* of a. We denote by M_i the set of all states of height i. (Hence M_0 is the set of cyclic states; $M_0 \cup M_1 \cup \ldots \cup M_j$ constitutes a subautomaton for each $j\,(\geqq 0)$.)

A partition π of the state set A of an (autonomous) automaton $\mathbf{A}$ is called a *congruence* (of $\mathbf{A}$) if $a \equiv b \pmod{\pi}$ implies

$$\delta(a, x) \equiv \delta(b, x) \pmod{\pi}$$

and

$$\lambda(a) = \lambda(b).$$

[2] In particular, "cycle" is understood as a directed graph and the word "circuit" is used if we do not take orientation into account.

For each congruence π, we can introduce the *factor automaton* $\mathbf{A}/\pi$ so that A/π is the state set of $\mathbf{A}/\pi$ and the functions δ, λ are defined in $\mathbf{A}/\pi$ in the natural manner.

The minimal partition o of A is always a congruence. The automaton $\mathbf{A}$ is called *simple* (or *reduced*) if $\mathbf{A}$ has no other congruence than the minimal partition of A. It is easy to see that, for an arbitrary automaton $\mathbf{A}$, there exists a maximal congruence[3] π_{max}, moreover, $\mathbf{A}/\pi$ is simple precisely in the case $\pi=\pi_{max}$.

An isomorphism between automata is understood as a state-isomorphism, an analogous agreement holds for homomorphisms.

Let us define a partition π_c of A such that two states a, b are in a common class modulo π exactly if they are in the same connected component. π_c fails to be a congruence in general.

A partition π of the state set of an automaton $\mathbf{A}$ is called *extensive* if each class modulo π which contains at least one cyclic state meets every connected component. (In other words, more explicitly: π is said extensive if, whenever to a pair a, b of states there exists a positive number j satisfying $\delta(a, x^j)=a$, then there is a state c which fulfils $a\equiv c \pmod{\pi}$ and $b\equiv c \pmod{\pi_c}$.)

Consider two connected components $\mathbf{A}_i$, $\mathbf{A}_j$ of $\mathbf{A}$. Denote the maximal congruences of the cycles $\mathbf{Z}_i$, $\mathbf{Z}_j$ by π_i and π_i, respectively. If Z_i/π_j and $\mathbf{Z}_j/\pi_j$ are isomorphic automata, then we call $\mathbf{A}_i$ and $\mathbf{A}_j$ *similar* components. The similarity is an equivalence relation in the set of all connected components of the automaton. An automaton $\mathbf{A}$ is called *pan-similar* if every pair of connected components of $\mathbf{A}$ is similar. (A connected automaton is trivially pan-similar.)

3. The congruences of cyclic automata

Consider an automaton $\mathbf{A}$ such that $\mathbf{A}$ is a cycle. (See Fig. 1.) Denote the number of states (i.e., the length of the cycle) by v. Suppose that the states of $\mathbf{A}$ are denoted by $a_1, a_2, \ldots, a_v$ so that

$$\delta(a_1, x) = a_2,\ \delta(a_2, x) = a_3, \ldots, \delta(a_{v-1}, x) = a_v,\quad \delta(a_v, x) = a_1.$$

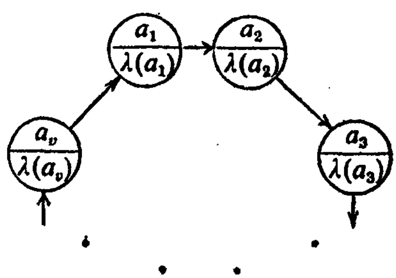

Fig. 1.

[3] The maximality means that each congruence π is a refinement of π_{max}. In general, π_{max} is not equal to the maximal partition ι of A.

Let s be the smallest number[4] such that the v equalities

$$\lambda(a_1) = \lambda(a_{1+s}), \quad \lambda(a_2) = \lambda(a_{2+s}), \ldots, \lambda(a_{v-s}) = \lambda(a_v),$$
$$\lambda(a_{v-s+1}) = \lambda(a_1), \quad \lambda(a_{v-s+2}) = \lambda(a_2), \ldots, \lambda(a_v) = \lambda(a_s) \tag{3.1}$$

are true. s is called the *periodicity number* of **A**. We have clearly $1 \leqq s \leqq v$. The cycle is called *primitive* or *imprimitive* according as $s=v$ or $s<v$ holds.

It is obvious that the periodicity number s is a divisor of the cycle length v.

Construction I. Choose an integer d such that $s|d|v$. Introduce the partition π_d of A by

$$a_i \equiv a_j \pmod{\pi_d} \Leftrightarrow d|j-i$$

(where $1 \leqq i \leqq v$, $1 \leqq j \leqq v$).

The index of π_d is d. Each class modulo π_d has v/d elements.

Theorem 1. *A partition π of the state set A of a cyclic automaton* **A** *is a congruence of* A *if and only if there exists a number d such that ($s|d|v$ and) $\pi=\pi_d$.*

Proof. Sufficiency is evident. — Consider an arbitrary congruence π of **A**. If we define d as the smallest positive number such that $a \equiv b \pmod{\pi}$ for suitable states satisfying $\chi(a, b)=d$, then it is easy to see that $\pi=\pi_d$.

Corollary 1. *The congruence lattice of* **A** *is isomorphic to the lattice of divisors of v/s.*

Proof. Let d^* be an arbitrary divisor of v/s, let us assign to d^* the congruence π_{v/d^*}. It is easy to see that this assignment is an isomorphism.

The following assertions are immediate consequences of our former considerations:

Corollary 2. *The maximal congruence of* **A** *is π_s. Among the factor automata* $\mathbf{A}/\pi_d$ *(where d runs through the numbers fulfilling $s|d|v$) only* $\mathbf{A}/\pi_s$ *is reduced.* **A** *is reduced if and only if* **A** *is a primitive cycle.*

4. The extensive congruences of pan-similar automata

4.1. Introductory considerations

Let **A** be a pan-similar automaton. Consider an arbitrary state a of **A**, let i be the height of a. There is a state b, determined by a uniquely, such that b belongs to $\mathbf{Z}[a]$ and

$$\delta(b, x^i) = \delta(a, x^i).$$

We shall denote b by $\sigma(a)$. Thus we have defined an idempotent mapping σ of the set of all states onto the set of cyclic states. It can be seen easily that $\sigma(\delta(a, x)) = \delta(\sigma(a), x)$.

[4] The existence of s follows from the fact that the formulae (3.1) are valid for v (instead of s).

Denote by $\mathbf{D}=(D, \{x\}, Y, \delta, \lambda)$ the largest subautomaton of $\mathbf{A}$ which satisfies the implication

$$a \in D \Rightarrow \lambda(a) = \lambda(\sigma(a)).$$

The following statements are obvious.

Lemma 1.

(I) $\mathbf{D}$ *exists and includes all the cycles of* $\mathbf{A}$.

(II) D *can be obtained also as the smallest subset of* A *fulfilling the following two requirements:*

(A) *Every cyclic state belongs to* D.

(B) *If* a *is acyclic,* $\delta(a, x) \in D$ *and* $\lambda(a)=\lambda(\sigma(a))$, *then* $a \in D$.

(III) *The formulae* $a \in D$ *and* $a \equiv \sigma(a) \pmod{\pi_{\max}}$ *are equivalent (where* $a \in A$ *and* $\pi_{\max}$ *is the maximal congruence of* $\mathbf{A}$*).*

Since we have supposed that $\mathbf{A}$ is a pan-similar automaton, there exists a cyclic automaton $\mathbf{Z}$ such that $\mathbf{Z}$ is isomorphic to each $\mathbf{Z}_k/\pi_k$ where π_k is the maximal congruence of the cycle $\mathbf{Z}_k$ of the connected component $\mathbf{A}_k$ of $\mathbf{A}$. (k runs from 1 to t, where t is the number of components.) $\mathbf{Z}$ is primitive. For each choice of k, there is exactly one homomorphism τ_k from $\mathbf{Z}_k$ onto $\mathbf{Z}$.

Denote the number of states of $\mathbf{Z}$ by s and, for any choice of k, the number of states of $\mathbf{Z}_k$ by v_k. (Clearly $s|v_k$.)

Lemma 2. *Let* a, b *be two elements of* D. *Define* k *and* m *by* $\mathbf{Z}_k=\mathbf{Z}[a]$, $\mathbf{Z}_m=\mathbf{Z}[b]$. *If* $\tau_m(\sigma(a))=\tau_k(\sigma(b))$, *then* $\lambda(a)=\lambda(b)$.

Proof. We have

$$\lambda(a) = \lambda(\sigma(a)) = \lambda^*(\tau_k(\sigma(a))) = \lambda^*(\tau_m(\sigma(b))) = \lambda(\sigma(b)) = \lambda(b),$$

where λ^* is the output function of $\mathbf{Z}$. Indeed, the first and fifth equalities are valid by the definition of $\mathbf{D}$, the second and fourth ones hold because τ_k, τ_m are homomorphisms.

4.2. Recursive description of the extensive congruences

Construction II.

Step 1. Choose a subautomaton $\mathbf{G}_0=(G_0, \{x\}, Y, \delta, \lambda)$ of $\mathbf{A}$ such that $\mathbf{G}_0$ is included in $\mathbf{D}$ and each cycle $\mathbf{Z}_k$ is included in $\mathbf{G}_0$.

Step 2. Define an ascending sequence

$$\mathbf{G}_0, \mathbf{G}_1, \mathbf{G}_2, \ldots$$

of subautomata of $\mathbf{A}$ so that[5] $a \in G_{i+1}$ if and only if $\delta(a, x) \in G_i$. (The sequence is finished when $\mathbf{A}$ is entirely exhausted.)

Step 3. Choose a number d such that $s|d$ and d is a common divisor of the cycle lengths $v_1, v_2, \ldots, v_t$. Choose, furthermore, a sequence $z_1, z_2, \ldots, z_t$ of

[5] Of course, G_i is here the set of states of $\mathbf{G}_i$.

states such that z_k belongs to the cycle $\mathbf{Z}_k$ $(1 \leqq k \leqq t)$ and the equalities

$$\tau_1(z_1) = \tau_2(z_2) = \ldots = \tau_t(z_t)$$

hold.

Step 4. Introduce a sequence of partitions $\pi^{(0)}, \pi^{(1)}, \pi^{(2)}, \ldots$ in the following (recursive) manner:

(I) Each $\pi^{(i)}$ is a partition of G_i.

(II) Two elements a, b of G_0 are congruent modulo $\pi^{(0)}$ exactly if

$$\chi(a, z_k) \equiv \chi(b, z_m) \pmod{d},$$

where k and m are defined by $\mathbf{Z}_k = \mathbf{Z}[a]$ and $\mathbf{Z}_m = \mathbf{Z}[b]$.

(III) Suppose that $\pi^{(i)}$ has already been defined. Introduce $\pi^{(i+1)}$ so that the following three rules be observed:

(α) If $a \in G_i$ and $b \in G_i$, then $a \equiv b \pmod{\pi^{(i+1)}}$ holds precisely when $a \equiv b \pmod{\pi^{(i)}}$.

(β) If $a \in G_i$ and $b \in G_{i+1} - G_i$, then $a \not\equiv b \pmod{\pi^{(i+1)}}$.

(γ) If a and b belong to $G_{i+1} - G_i$ and $a \equiv b \pmod{\pi^{(i+1)}}$, then $\lambda(a) = \lambda(b)$ and $\delta(\mathrm{a}, x) \equiv \delta(b, x) \pmod{\pi^{(i)}}$.

(It is clear that (γ) admits a certain liberty in partitioning the elements of $G_{i+1} - G_i$ into classes.)

Step 5. Denote by π the partition $\pi^{(i^*)}$ with the largest possible superscript i^*. (Obviously, π is a partition of $G_{i^*} = A$.)

Lemma 3. *If* $a \equiv b \pmod{\pi}$, *then* $\lambda(a) = \lambda(b)$.

Proof. Suppose $a \equiv b \pmod{\pi}$. There exists a subscript i such that a, b belong to G_i but (if $i > 0$) they are not contained in G_{i-1}. The proof proceeds by induction on i.

Let a, b be elements of $G_0 (\subseteqq D)$, recall (II) in Step 4 of Construction II. We have

$$\chi(\sigma(a), z_k) \equiv \chi(a, z_k) \equiv \chi(b, z_m) \equiv \chi(\sigma(b), z_m) \pmod{d}$$

(the first and third congruences are clearly true modulo v_k, v_m, resp., this implies their validity modulo d), hence $\tau_k(\sigma(a)) = \tau_m(\sigma(b))$, thus $\lambda(a) = \lambda(b)$ by Lemma 2.

Assume that the lemma is valid for i. Let a, b be elements of $G_{i+1} - G_i$ such that they are congruent modulo π. Then they are congruent also modulo $\pi^{(i+1)}$. $\lambda(a) = \lambda(b)$ follows from the rule (γ) in the item (III) of Step 4 of Construction II.

Lemma 4. π *is a congruence.*

Proof. After the preceding lemma, it suffices to show that $a \equiv b \pmod{\pi}$ implies $\delta(a, x) \equiv \delta(b, x) \pmod{\pi}$.

Let $a \equiv b \pmod{\pi}$ hold. There is an i as in the previous proof. Again, we use induction. First we consider the case $i = 0$. Use the short notations $a' = \delta(a, x)$ and $b' = \delta(b, x)$, recall item (II) of Step 4 of Construction II. We have

$$\chi(a', z_k) \equiv \chi(a, z_k) - 1 \equiv \chi(b, z_m) - 1 \equiv \chi(b', z_m) \pmod{d},$$

where the second congruence follows from $a \equiv b \pmod{\pi}$, the first and third congruences are valid[6] because d is a divisor of the lengths of the cycles containing z_k and z_m. Hence $a' \equiv b'$ (mod π).

If i is positive, then the inference

$$a \equiv b \,(\mathrm{mod}\ \pi) \Rightarrow a \equiv b \ (\mathrm{mod}\ \pi^{(i)}) \Rightarrow \delta(a, x) \equiv \delta(b, x) \ (\mathrm{mod}\ \pi^{(i-1)}) \Rightarrow$$

$$\Rightarrow \delta(a, x) \equiv \delta(b, x) \ (\mathrm{mod}\ \pi)$$

is valid according to item (III) of Step 4 of the construction.

Theorem 2. *A partition* π *of* A *is an extensive congruence of* $\mathbf{A}$ *if and only if* π *can be obtained by Construction II.*

Proof.

Sufficiency. Having Lemma 4, we are going to show the extensivity of a congruence π obtained by the construction. Assume that a belongs to $\mathbf{Z}_k$ and b belongs to $\mathbf{A}_m$, we want to find a $c(\in A_m)$ with $a \equiv c$ (mod π). The choice $c = \delta(z_m, x^\chi)$ is convenient, where χ stands shortly for $\chi(z_k, a)$.

Necessity. Let an extensive congruence π of $\mathbf{A}$ be considered. Our next aim is to determine the circumstances (more precisely: the choices of $d, z_1, z_2, \ldots, z_t$, $G_0, \pi^{(0)}, G_1, \pi^{(1)}, G_2, \pi^{(2)}, \ldots$) under which just the prescribed π is obtained by Construction II.

Let G_0 be the set of states $a(\in A)$ for which there is a cyclic state c such that $a \equiv c$ (mod π). Let G_{i+1} (where i can be $0, 1, 2, \ldots$) be the set of states a satisfying $\delta(a, x) \in G_i$. Let $\pi^{(i)}$ be the restriction of π to the set G_i.

Let $z_1, z_2, \ldots, z_t$ be arbitrary states in the cycles $\mathbf{Z}_1, \mathbf{Z}_2, \ldots, \mathbf{Z}_t$, respectively, such that they are pairwise congruent modulo π.

Choose a cyclic state z and denote by d the smallest positive number which satisfies $z \equiv \delta(z, x^d)$ (mod π). It can be seen that d does not depend on the choice of z.

Let π^* be the congruence which is yielded by Construction II with the parameters introduced above and with a suitable application of (III/γ) in Step 4. We want to show $\pi^* = \pi$. Consider two states a, b; we are going to get that they are congruent modulo π^* exactly when they are congruent modulo π.

Suppose first $a \in G_0$ and $b \in G_0$. Consider the three statements

$$a \equiv b \quad (\mathrm{mod}\ \pi^*),$$

$$\chi(a, z_a) \equiv \chi(b, z_b) \quad (\mathrm{mod}\ d),$$

$$a \equiv b \ (\mathrm{mod}\ \pi).$$

It can be seen that the second statement is equivalent both to the first and the third one.

We turn to the case $a \in G_i$, $b \in G_{i+1} - G_i$. With this choice of a and b, we have $a \not\equiv b$ (mod π^*). On the other hand, $a \equiv b$ (mod π) would imply

$$\delta(b, x^{i+d}) \equiv \delta(a, x^{i+d}) \equiv \delta(a, x^i) \equiv \delta(b, x^i) \ (\mathrm{mod}\ \pi)$$

[6] Except the possibility $a = z_k$, the equality $\chi(a', z_k) = \chi(a, z_k) - 1$ is also true (and analogously for b).

(the second congruence follows from $\delta(a, x^i)\in G_0$), and this is impossible since

$$\delta(b, x^i)\in G_1 - G_0.$$

By getting a contradiction, $a \not\equiv b \pmod{\pi}$ is verified.

Finally, assume that a and b belong to the same $G_{i+1} - G_i$. The equivalence of $a \equiv b \pmod{\pi}$ and $a \equiv b \pmod{\pi^*}$ follows from the fact that we have defined $\pi^{(i+1)}$ as the restriction of π. It remained still dubious whether or not the sequence

$$\pi^{(0)}, \pi^{(1)}, \pi^{(2)}, \ldots, \pi^{(i*)}$$

(as we have derived it from π) satisfies (III/γ) in Step 4 of Construction II. This holds, however, because π is a congruence.

By analyzing Construction II and Theorem 2, we get the following result:

Corollary 3. *The maximal congruence $\pi_{\max}$ of* **A** *is extensive, and just $\pi_{\max}$ is obtained when we apply Construction II in the following manner: d is chosen as equal to s;* $\mathbf{G}_0$ *is chosen as equal to* **D**; *for each possible value of i, let $a \equiv b$ (mod $\pi^{(i+1)}$) hold precisely when both $\lambda(a) = \lambda(b)$ and*

$$\delta(a, x) \equiv \delta(b, x) \pmod{\pi^{(i)}}$$

are true (where a and b belong to $G_{i+1} - G_i$).

4.3. The question of unicity

Construction I has yielded uniquely the congruences of cycles. (Also Constructions III, IV will prove to be unique.) It may happen, however, that two *different* applications of Construction II lead to the *same* extensive congruence. More nearly: if we modify either G_0 or d or the $\pi^{(i)}$'s, then the obtained congruence π is necessarily altered; but it is possible that two different systems of form $z_1, z_2, \ldots, z_t$ give the same congruence.

Proposition 2. *Let two realizations of Construction II be considered. Suppose that $d, G_0, \pi^{(0)}, G_1, \pi^{(1)}, G_2, \pi^{(2)}, \ldots$ are common in them. Denote the states which represent the cycles by $z_1, z_2, \ldots, z_t$ in the first execution, and by $z_1', z_2', \ldots, z_t'$ in the second one. Denote the obtained congruences by π and π', respectively. Then $\pi = \pi'$ if and only if the numbers*

$$\chi(z_1, z_1'), \chi(z_2, z_2'), \ldots, \chi(z_t, z_t')$$

are congruent to each other modulo d.

Next we show two lemmas.

Lemma 5. *First apply Construction II with the system $z_1, z_2, \ldots, z_t$, and then modify the application in such a way that the system of the z_i's is replaced by the system*

$$z_1^* = \delta(z_1, x), \quad z_2^* = \delta(z_2, x), \ldots, z_t^* = \delta(z_t, x).$$

Both realizations of Construction II give the same congruence.

Proof. The statement is implied by the construction (especially, item (II) of Step 4) and the deduction

$$\chi(a, z_k^*) \equiv \chi(a, z_k)+1 \equiv \chi(b, z_m)+1 \equiv \chi(b, z_m^*) \pmod d.$$

Lemma 6. *Apply Construction II with the system* $z_1, z_2, \ldots, z_t$, *select a number* i $(1 \leqq i \leqq t)$ *and modify the application in such a way that* z_i *is replaced by* $z_i^+ = \delta(z_i, x^d)$. *Both realizations give the same congruence.*

Proof. It is easy to see that

$$\chi(a, z_i^+) \equiv \chi(a, z_i) \pmod d$$

for each state a of $\mathbf{A}_i$; hence the statement follows immediately.

Proof of Proposition 2.

Sufficiency. Consider the system $z_1, z_2, \ldots, z_t$. First apply Lemma 5 $\chi(z_1, z_1')$ times, thus we get a system $z_1^*, z_2^*, \ldots, z_t^*$ such that $z_1^* = z_1'$ and $d \mid \chi(z_i^*, z_i')$ for each i $(2 \leqq i \leqq t)$. We can obtain the system $z_1', z_2', \ldots, z_t'$ by applying Lemma 6 (several times, in a straightforward manner).

Necessity. Suppose

$$\chi(z_i, z_i') \not\equiv \chi(z_j, z_j') \pmod d$$

for a suitable pair i, j $(1 \leqq i \leqq t,\ 1 \leqq j \leqq t)$. Then z_i and z_j are congruent modulo π, and it is easy to see that they are incongruent modulo π'. Hence $\pi \neq \pi'$.

4.4. *Considerations on how certain subautomata can be generated*

Construction II relies upon the subautomata of $\mathbf{D}$ containing all the cyclic states. From a theoretical point of view, Proposition 1 gives a good survey of these subautomata.

This survey has the practical disadvantage that a subautomaton is handled as the set of *all* states of it. It would be more useful, to characterize the subautomata in terms of certain sets which consist of a relatively *small* number of states. The present subsection is devoted to this subject.

Let $\mathbf{B} = (B, \{x\}, Y, \delta, \lambda)$ be a subautomaton of $\mathbf{A}$ such that $\mathbf{B}$ includes each cycle. Denote by $R(\mathbf{B})$ the set of states a satisfying the condition

$$a \in B \;\&\; (\forall b)[b \in B \Rightarrow \delta(b, x) \neq a].$$

$R(\mathbf{B})$ is called the *minimal generating system* of $\mathbf{B}$. Each element of $R(\mathbf{B})$ is an acyclic state. (If, in particular, $\mathbf{B}$ is the union of all cycles, then $R(\mathbf{B}) = \emptyset$.)

It is evident that a state b belongs to B if and only if either b is cyclic or there is an $a(\in R(\mathbf{B}))$ and a number $i(\geqq 0)$ such that $\delta(a, x^i) = b$.

Proposition 3. *If* $\mathbf{B}_1$ *and* $\mathbf{B}_2$ *are different subautomata of* $\mathbf{A}$ *which contain all the cyclic states, then* $R(\mathbf{B}_1) \neq R(\mathbf{B}_2)$.

Proof. If $R(\mathbf{B}_1) = R(\mathbf{B}_2)$, then $\mathbf{B}_1$ equals $\mathbf{B}_2$ in consequence of the sentence before the proposition.

Proposition 4. *Let R be a (possibly empty) set of acyclic states. The following statements* (A), (B) *are equivalent:*

(A) *There exists a subautomaton* $\mathbf{B}$ *of* $\mathbf{A}$ *such that* $\mathbf{B}$ *contains all the cyclic states,* $\mathbf{B}$ *is a subautomaton of* $\mathbf{D}$ *and* $R(\mathbf{B})=R$.

(B) R *is a subset of* D *and whenever* $a\in R$ *and* i *is a positive number, then* $\delta(a, x^i)\notin R$.

Proof. (A)$\Rightarrow$(B) is evident. — If a set R satisfies (B), then it is easy to see that a is acyclic and $R=R(\mathbf{B})$ holds for the subautomaton $\mathbf{B}$ which is defined by the following rule: $b\in B$ if and only if either b is cyclic or there is an $a(\in R)$ and a non-negative number i such that $\delta(a, x^i)=b$.

Construction III. The construction consists of an initial step and an arbitrary number ($\geqq 0$) of general steps.

Initial step. Let R_1 be an arbitrary non-empty subset of $M_1\cap D$.

General step. Consider a set R_i such that R_i has been obtained by the preceding step of the construction, $R_i\subseteqq M_1\cup M_2\cup\ldots\cup M_i$ and $R_i\cap M_i\neq\emptyset$. Choose a non-empty subset Q of $R_i\cap M_i$ such that $\delta^{-1}(q)\cap D\neq\emptyset$ for each choice of $q\in Q$, where $\delta^{-1}(q)$ is the set of states a satisfying $\delta(a, x)=q$. Choose for each $q(\in Q)$ a non-empty subset $\theta(q)$ of $\delta^{-1}(q)\cap D$. Let us form the set

$$R_{i+1}=(R_i-Q)\cup\Big(\bigcup_{q\in Q}\theta(q)\Big).$$

Construction III can be finished after an arbitrary step. It breaks up necessarily when there is no possibility for the non-empty choice of Q.

Proposition 5. *The realizations of Construction III give pairwise different sets. A set R is obtainable by Construction III if and only if* $R=R(\mathbf{B})$ *with some subautomaton* $\mathbf{B}$ *such that* $\mathbf{B}$ *contains all the cyclic states,* $\mathbf{B}$ *is included in* $\mathbf{D}$, *and* $\mathbf{B}$ *has at least one acyclic state.*

Proof. The first assertion follows from the requirements that certain sets must be non-empty in Construction III. The second assertion is an easy consequence of the characterization of the sets $R(\mathbf{B})$ stated in Proposition 4.

5. Overview of the congruences in the general case

Let $\mathbf{A}$ be an arbitrary finite autonomous Moore automaton. Denote by π_h the partition of A such that $a\equiv b \pmod{\pi_h}$ holds precisely if the connected components which contain a and b are similar. Evidently, $\pi_c\subseteqq\pi_h$.

Construction IV.

Step 1. Let a partition π^* of A be chosen such that $\pi_c\subseteqq\pi^*\subseteqq\pi_h$. Denote by $\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_q$ the (pan-similar) subautomata of $\mathbf{A}$ which are determined by the classes $A_1, A_2, \ldots, A_q$ modulo π^*, respectively. (q is the index of π^*.)

Step 2. For each choice of i ($1\leqq i\leqq q$), let us consider a partition π_i of A which satisfies the following assertions:

(i) $A_1 \cup A_2 \cup \ldots \cup A_{i-1} \cup A_{i+1} \cup \ldots \cup A_q$ is (precisely) one class modulo π_i.
(ii) The restriction of π_i to A_i is an extensive congruence of $\mathbf{A}_i$.

Step 3. Let us form the partition

$$\pi = \pi_1 \cap \pi_2 \cap \ldots \cap \pi_q$$

of A.

Theorem 3. *A partition π of A is a congruence of $\mathbf{A}$ if and only if π can be obtained by Construction IV.*

Proof. Sufficiency is evident. — Consider a congruence π of $\mathbf{A}$. If we take π^* as $\pi \cup \pi_c$ and define each π_i so that π_i coincides with π on A_i, then it is clear that Construction IV gives π.

An easy consequence of the previous considerations of Section 5 is:

Corollary 4. *The maximal congruence of $\mathbf{A}$ is obtained when we choose (in Construction IV) π^* as equal to π_h and we determine each π_i so that its restriction to A_i should be the maximal congruence of $\mathbf{A}_i$.*

Proposition 6. *An automaton $\mathbf{A}$ is reduced if and only if the following three assertions hold:*
(i) *Each cycle of $\mathbf{A}$ is primitive.*
(ii) *The cycles of $\mathbf{A}$ are pairwise non-isomorphic.*
(iii) *There is no pair of different states a, b in $\mathbf{A}$ such that $\delta(a,x)=\delta(b,x)$ and $\lambda(a)=\lambda(b)$.*

Proof.

Necessity. If (i) does not hold, then we get a nontrivial congruence so that we select an imprimitive cycle $\mathbf{Z}$ and we define π so that $a \equiv b \pmod{\pi}$ if either $a=b$ or a, b are states of $\mathbf{Z}$ which satisfy $s|\chi(a,b)$.

If (ii) is not true, then we can choose two different cycles and an isomorphism α between them; the following partition π is a nontrivial congruence: $a \equiv b \pmod{\pi}$ is either $a=b$ or one of a, b is the image of the other under α.

If (iii) is not valid, then let us choose a pair a, b fulfilling $\lambda(a)=\lambda(b)$ and $\delta(a,x)=\delta(b,x)$; the following partition is a nontrivial congruence: $\{a, b\}$ is one of the classes and all other classes consist of one element.

Sufficiency. Suppose that (i), (ii), (iii) are fulfilled. It is clear that $\pi_c=\pi_h$. Let us recall the considerations of Section 4 in case of an arbitrary connected component $\mathbf{A}_i$ of $\mathbf{A}$. D consists of the cyclic states only. Corollary 3 and the last sentence of Corollary 2 imply that the maximal congruence of $\mathbf{A}_i$ equals its minimal congruence, i.e., $\mathbf{A}_i$ is simple. Taking Corollary 4 into account, we get that also $\mathbf{A}$ is reduced.

Remark 1. Consider the conditions (i), (ii) in Proposition 6. (i) & (ii) can be formulated in the following manner (equivalently):
(iv) Whenever $\mathbf{Z}_1, \mathbf{Z}_2$ are cyclic subautomata of $\mathbf{A}$ and there is an isomorphism α of $\mathbf{Z}_1$ onto $\mathbf{Z}_2$, then ($\mathbf{Z}_1=\mathbf{Z}_2$ and) α is the identical automorphism of $\mathbf{Z}_1$.

Remark 2. The sufficiency of the conditions in Proposition 6 can be proved also by using the following idea (without any reference to the previous results):

we start with a congruence π and two different states such that $a \equiv b \pmod{\pi}$, and we strive to show by studying the sequences

$$a,\ \delta(a, x),\ \delta(a, x^2), \ldots$$

and

$$b,\ \delta(b, x),\ \delta(b, x^2), \ldots$$

that either (i) or (ii) or (iii) is violated.

The question may arise when two congruences, obtained either by Construction II or by Construction IV, are related in such a way that one is a refinement of the other. The answer is given in the next results which can be verified by routine inferences.

Proposition 7. *Consider two realizations of Construction II (concerning the same automaton* **A***). Distinguish them from each other by the sub- or superscripts* α *and* β*; in particular, let the obtained congruences be* π_α *and* π_β*, respectively. The relation* $\pi_\alpha \leqq \pi_\beta$ *holds if and only if the following four conditions are satisfied:*

(A) $G_0^\alpha \leqq G_0^\beta$.

(B) $d_\beta \mid d_\alpha$.

(C) *The numbers*

$$\chi(z_1^\alpha, z_1^\beta),\ \chi(z_2^\alpha, z_2^\beta), \ldots, \chi(z_t^\alpha, z_t^\beta)$$

are congruent to each other modulo d_β.

(D) *Whenever two different states* a *and* b *are congruent* mod π_α *in consequence of* (III/γ) *in Step 4 of the (first execution of) Construction II and they are not contained in* G_0^β, *then* a *and* b *belong to the same* $\mathbf{G}_{j+1}^\beta$ *and they are in a common class* mod $\pi_\beta^{(j+1)}$ *(in course of Step 4 of the second realization).*

Proposition 8. *Consider two realizations of Construction IV (concerning the same automaton* **A***). Distinguish them from each other as in the preceding proposition. The relation* $\pi_\alpha \leqq \pi_\beta$ *holds if and only if the following conditions* (I), (II) *are fulfilled:*

(I) $\pi_\alpha^* \leqq \pi_\beta^*$.

(II) *The implication*

$$a \equiv b \pmod{\pi_i^\alpha} \Rightarrow a \equiv b \pmod{\pi_j^\beta}$$

is valid for every i $(1 \leqq i \leqq q_\alpha)$, *where* j $(1 \leqq j \leqq q_\beta)$ *is the number determined by* $\mathbf{A}_i^\alpha \leqq \mathbf{A}_j^\beta$.

6. Example 1

6.1. Exposition of the example

In Section 6 we give an example to demonstrate how the extensive congruences of a pan-similar automaton can be constructed.

Fig. 2 shows the graph of an autonomous automaton **A** (with $|A|=33$ and $|Y|=3$). **A** has two connected components and is pan-similar. The simple homomorphic image of the cycles of **A** can be seen in Fig. 3. For the sake of brevity, we

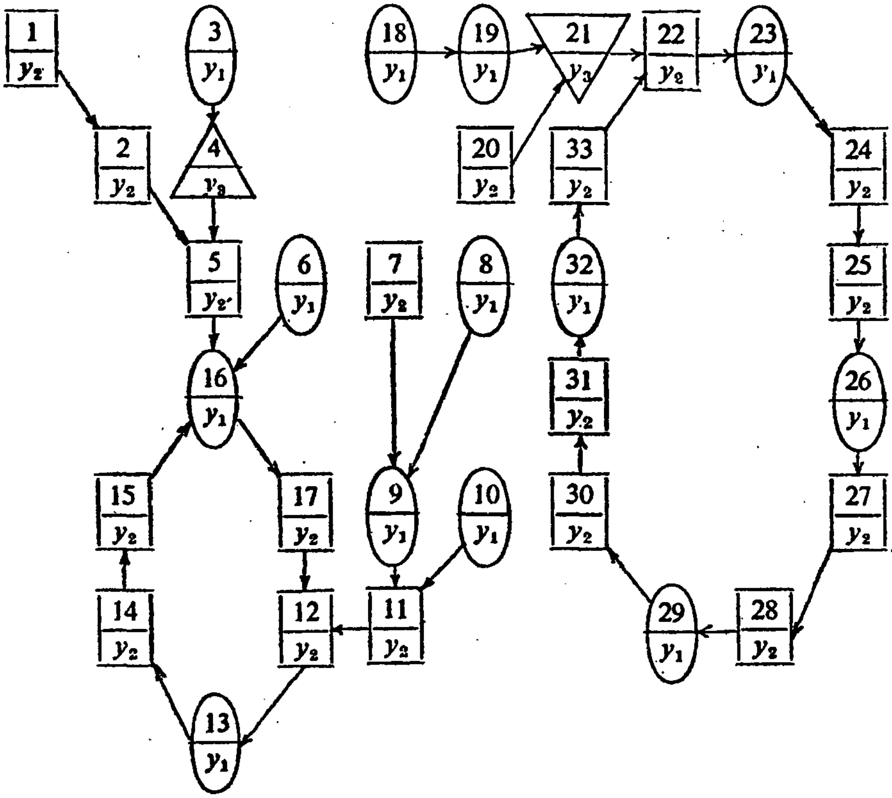

Fig. 2.

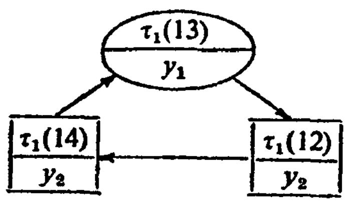

Fig. 3.

Table 1

i	1	2	3	4	5	6	7	8	9	10	11	18	19	20	21
$\sigma(i)$	13	14	13	14	15	15	15	15	16	16	17	31	32	32	33

denote a state simply by i instead of a_i. We make a perspicuous distinction between the output signs y_1, y_2, y_3 so that we draw a circle, a square or a triangle, respectively.

Table 1 shows the values of σ on the acyclic states. D consists of the states 2, 5, 7, 9, 10, 11 and the eighteen cyclic states.

6.2. The realizations of Construction III

The initial step of the construction can be applied in three different ways; we get the sets

$$R_1^{(1)} = \{5\},\quad R_1^{(2)} = \{11\},\quad R_1^{(3)} = \{5, 11\}.$$

After an initial step, we have eleven possibilities for applying a general step; the resulting sets are

$$R_2^{(1)} = \{2\},\quad R_2^{(2)} = \{9\},\quad R_2^{(3)} = \{10\},\quad R_2^{(4)} = \{9, 10\},\quad R_2^{(5)} = \{2, 11\},$$
$$R_2^{(6)} = \{5, 9\},\quad R_2^{(7)} = \{5, 10\},\quad R_2^{(8)} = \{5, 9, 10\},\quad R_2^{(9)} = \{2, 9\},$$
$$R_2^{(10)} = \{2, 10\},\quad R_2^{(11)} = \{2, 9, 10\}.$$

(If we start with $R_1^{(1)}$, we get $R_2^{(1)}$. The sets $R_2^{(3)}$, $R_2^{(4)}$, $R_2^{(5)}$ are obtained if we start with $R_1^{(2)}$. The remaining seven sets are derived from $R_1^{(3)}$.)

If one of $R_2^{(2)}$, $R_2^{(4)}$, $R_2^{(6)}$, $R_2^{(8)}$, $R_2^{(9)}$, $R_2^{(11)}$ is considered, we can execute a second general step. In this manner we arrive to the following six sets:

$$R_3^{(1)} = \{7\},\quad R_3^{(2)} = \{7, 10\},\quad R_3^{(3)} = \{5, 7\},$$
$$R_3^{(4)} = \{5, 7, 10\},\quad R_3^{(5)} = \{2, 7\},\quad R_3^{(6)} = \{2, 7, 10\}.$$

We have exhausted all possibilities for performing Construction III. We have got that there are twenty-one choices for the subautomaton occurring in Construction II. (Twenty of these are generated by the constructed sets, respectively; among them, $R_3^{(6)}$ generates the whole sub-automaton **D**. A further subautomaton consists of the cyclic states only.)

6.3. The possibilities for choosing d, z_1, z_2

Now we turn to how Construction II can be performed for the automaton **A**. We have two possibilities for choosing d: either $d=3$ or $d=6$. As we have seen earlier, B can be selected in 21 manners.

If $d=6$, then there are two essentially different[7] possibilities for the choice of the pair $\{z_1, z_2\}$. The first of these is $z_1=12$, $z_2=22$; the other is $z_1=12$, $z_2=25$. If $d=3$, then we have only one possibility (apart from non-essential changes): $z_1=12$, $z_2=22$.

In the previous considerations, we have seen that the number of possibilities for choosing the parameters B, d, z_1, z_2 is 63 $(=21.(2+1))$. In fact, **A** has more than 63 extensive congruences, because Step 4 (III/γ) of Construction II is not strictly determined.

6.4. Some notational conventions

Before dealing with the extensive congruences of **A** in a somewhat (but not fully) detailed manner, it is appropriate to introduce how the partitions of the state set of **A** can be denoted shortly. We agree that, e.g.,

$$\langle 1, 4 \mid 2, 3, 11 \mid 6, 19\rangle$$

[7] "Essentially different" is meant in sense of Proposition 2.

denotes the partition in which the three sets $\{1, 4\}$, $\{2, 3, 11\}$, $\{6, 19\}$ are classes and each one of the remaining states forms a one-element class. If it is already known that $H=\{2, 11\}$, then we can write

$$\langle 1, 4 \mid H, 3 \mid 6, 19\rangle$$

instead of the above formula, too.

Let another notation also be introduced in the following way (for sake of conciseness): the formula

$$\langle 1, 8, 11 \mid 3, 9 \parallel (2, 10), (4, 7)\rangle$$

will mean the system consisting of the four partitions

$$\langle 1, 8, 11 \mid 3, 9\rangle,$$
$$\langle 1, 8, 11 \mid 3, 9 \mid 2, 10\rangle,$$
$$\langle 1, 8, 11 \mid 3, 9 \mid 4, 7\rangle,$$
$$\langle 1, 8, 11 \mid 3, 9 \mid 2, 10 \mid 4, 7\rangle.$$

6.5. Study of the extensive congruences obtained through certain subautomata

We have seen in Subsection 6.2 that there are 21 possibilities for choosing $\mathbf{G}_0$. Among these, now we consider the subautomata generated by

$$\emptyset,\quad R_1^{(1)},\quad R_2^{(3)},\quad R_2^{(7)},\quad R_2^{(4)},$$

and we are going to discuss the congruences obtained with these $\mathbf{G}_0$'s. (The discussion of any of the remaining 16 possibilities resembles to one or another of these.)

Introduce the sets (of cyclic states)

$$\begin{aligned}
H_1 &= \{12, 15, 22, 25, 28, 31\},\\
H_2 &= \{13, 16, 23, 26, 29, 32\},\\
H_3 &= \{14, 17, 24, 27, 30, 33\},\\
K_1 &= \{12, 22, 28\},\\
K_2 &= \{13, 23, 29\},\\
K_3 &= \{14, 24, 30\},\\
K_4 &= \{15, 25, 31\},\\
K_5 &= \{16, 26, 32\},\\
K_6 &= \{17, 27, 33\},\\
L_1 &= \{12, 25, 31\},\\
L_2 &= \{13, 26, 32\},\\
L_3 &= \{14, 27, 33\},\\
L_4 &= \{15, 22, 28\},\\
L_5 &= \{16, 23, 29\},\\
L_6 &= \{17, 24, 30\}.
\end{aligned}$$

Let us study first the case when $\mathbf{G}_0$ contains the cyclic states only. If $d=3$ (and $z_1=12$, $z_2=22$), then two congruences are obtained with these parameters:

$$\langle H_1 | H_2 | H_3 \| (9, 10) \rangle.$$

Analogously, if $d=6$, $z_1=12$, $z_2=22$, then

$$\langle K_1 | K_2 | K_3 | K_4 | K_5 | K_6 \| (9, 10) \rangle$$

are got; when $d=6$, $z_1=12$, $z_2=25$, then

$$\langle L_1 | L_2 | L_3 | L_4 | L_5 | L_6 \| (9, 10) \rangle$$

are. Altogether, we have obtained six congruences for the smallest possible $\mathbf{G}_0$.

If we start with the subautomaton generated by $R_1^{(1)}$ (as $\mathbf{G}_0$), then we get fourteen congruences

$$\langle H_1, 5 | H_2 | H_3 \| (9, 10) \rangle,$$

$$\langle H_1, 5 | H_2 | H_3 | 4, 21 \| (3, 19), (9, 10) \rangle,$$

$$\langle K_1 | K_2 | K_3 | K_4, 5 | K_5 | K_6 \| (9, 10) \rangle,$$

$$\langle L_1 | L_2 | L_3 | L_4, 5 | L_5 | L_6 \| (9, 10) \rangle,$$

$$\langle L_1 | L_2 | L_3 | L_4, 5 | L_5 | L_6 | 4, 21 \| (3, 19), (9, 10) \rangle.$$

With the subautomaton generated by $R_2^{(3)}$, three congruences are obtained:

$$\langle H_1 | H_2, 10 | H_3, 11 \rangle,$$

$$\langle K_1 | K_2 | K_3 | K_4 | K_5, 10 | K_6, 11 \rangle,$$

$$\langle L_1 | L_2 | L_3 | L_4 | L_5, 10 | L_6, 11 \rangle.$$

With the subautomaton generated by $R_2^{(7)}$, we get seven congruences:

$$\langle H_1, 5 | H_2, 10 | H_3, 11 \rangle,$$

$$\langle H_1, 5 | H_2, 10 | H_3, 11 | 4, 21 \| (3, 19) \rangle,$$

$$\langle K | K_2 | K_3 | K_4, 5 | K_5, 10 | K_6, 11 \rangle,$$

$$\langle L_1 | L_2 | L_3 | L_4, 5 | L_5, 10 | L_6, 11 \rangle,$$

$$\langle L_1 | L_2 | L_3 | L_4, 5 | L_5, 10 | L_6, 11 | 4, 21 \| (3, 19) \rangle.$$

Finally, the discussion of the subautomaton generated by $R_2^{(4)}$ leads to twelve congruences:

$$\langle H_1 | H_2, 9, 10 | H_3, 11 | H_4 | H_5 | H_6 \| (5, 7), (6, 8) \rangle,$$

$$\langle K_1 | K_2 | K_3 | K_4 | K_5, 9, 10 | K_6, 11 \| (5, 7), (6, 8) \rangle,$$

$$\langle L_1 | L_2 | L_3 | L_5, 9, 10 | L_6, 11 \| (5, 7), (6, 8) \rangle.$$

6.6. *Short overview of the extensive congruences of* A

Out of the 21 basic sets, five ones were examined in Subsection 6.5. Now we cast a glance to the other 16 ones. The generating sets $R_1^{(2)}$, $R_3^{(1)}$, $R_3^{(2)}$ behave similarly to the smallest $\mathbf{G}_0$ (each of them leads to six congruences). $R_2^{(2)}$ and $R_2^{(10)}$ behave analogously to $R_2^{(4)}$ and $R_2^{(7)}$, respectively. The behaviour of the eleven generating sets not yet mentioned is analogous to $R_1^{(1)}$.

Consequently, the number of extensive congruences of **A** is

$$233 = (4.6+2.12+2.7+12.14+1.3).$$

6.7. *Maximal and minimal extensive congruences*

The maximal congruence of **A** is

$$\langle H_1, 5, 7|H_2, 9, 10|H_3, 2, 11|3, 19|4, 21|6, 8\rangle;$$

it can be obtained from $R_3^{(6)}$ and $d=3$.

The question arises whether, for an arbitrary pan-similar automaton, there exists a minimal congruence among the *extensive* ones. The analysis of **A** shows that the answer is negative (in general). Indeed, let the extensive congruences

$$\pi_K = \langle K_1|K_2|K_3|K_4|K_5|K_6\rangle,$$
$$\pi_L = \langle L_1|L_2|L_3|L_4|L_5|L_6\rangle$$

(got with the smallest $\mathbf{G}_0$ and $d=6$) be considered. The system $\{\pi_K, \pi_L\}$ is minimal in the following weak sense: each extensive congruence π satisfies at least one of the relations $\pi_K \leqq \pi$ and $\pi_L \leqq \pi$. None of π_K, π_L is a refinement of the other, their intersection is not extensive.

7. Appendix (Outlook)

7.1. *Theoretical considerations*

Let now $\mathbf{A}=(A, X, Y, \delta, \lambda)$ be an arbitrary (not necessarily autonomous) finite Moore automaton. A partition π of the state set A was called a congruence if $a\equiv b \pmod{\pi}$ implies

$$(\lambda(a) = \lambda(b)) \;\&\; (\delta(a, x) \equiv \delta(b, x) \pmod{\pi}) \tag{7.1}$$

for every choice of $a(\in A), b(\in A)$ and $x(\in X)$ (cf. Section 2). The question to which the present paper is devoted is a particular case of the following general one:

Basic problem. Describe the congruences of an arbitrary automaton **A**.

A satisfactorily explicit solution of this problem is, of course, hopeless in full generality. The importance of the basic problem (in spite of the fact that it seems to be an imaginary question) is that it can be considered as a common source of other problems. More explicitly, it admits several particularizations (into various directions) so that these particular questions are interesting and their solution lies already (more or less) within the limits of real possibilities. We can pose certain specializations of the basic problem so that one or another of the following constraints is accepted (possibly combined with each other):

(A) **A** is autonomous, i.e., $|X|=1$.

(B) **A** is initially connected, i.e., a state $a_0(\in A)$ is distinguished and it is postulated that to each $a(\in A)$ there is an input word p (depending on a) such that $\delta(a_0, p)=a$.

(C) We are not interested in obtaining all congruences of the automata but we want to separate the simple automata from the non-reduced ones. (The results in this direction are considered to be valuable in so far as the method of separation is of constructive character.)

(D) We are not interested in the output function of the automata. (This approach is, strictly spoken, the particular case of the basic problem when we restrict ourselves to the case $|Y|=1$.)

(E) The definition of congruence is strengthened by requiring $\delta(a, x_1)\equiv\delta(b, x_2)$ (mod π) in the second term of (7.1) $(x_1\in X, x_2\in X)$. (From a rigidly formal point of view, this is not a particular case of the basic problem. However, this strengthening of the definition implies that the set of congruences of an automaton becomes narrower.)

The specializations (A) and (A) & (E) are the same. If we accept both (D) and (E), we arrive at a purely graph-theoretical problem.

In the paper [4], a (natural and easy) solution of the particular case (A) & (B) & (C) of the basic problem was stated (Section 3) and the constructive aspects of the question were dealt with (Sections 4—5).

In [5], the case (A) & (D) [=(A) & (D) & (E)] was discussed (Chapter II) and these considerations were expanded into an elucidation of the case (D) & (E) for a large class of directed graphs (Chapter III).

In the present paper, a treatment of the case (A) is contained. Thus the theory elaborated now is a common generalization of Section 3 of [4] and Chapter II of [5].

Among the articles whose subject is more or less related to the present paper, let [9], [6], [10] and the most recent publication [7] be mentioned. A number of further references can be found in [10] and [5].

In the author's opinion, the most exciting subproblem of the entire domain of questions is the case (B) & (C). Unfortunately, the topic seems to become terribly more intricate when the autonomousness of the automata is abandoned.

My intention with the papers [2], [3] was that they should be the first steps towards a constructive treatment of the subproblem (B) & (C). As far as it can be predicted, each further step in this direction will require to surmount immense difficulties.

7.2. Examples 2 and 3

Let us finish our paper with two examples which show the difficulties of handling the non-autonomous case.

Statement 1. *Let* $\mathbf{A}=(A, X, Y, \delta, \lambda)$ *be an automaton, consider the* n *autonomous automata* $\mathbf{A}_i=(A, \{x_i\}, Y, \delta_i, \lambda)$ *where* $n=|X|$, x_i *runs through the elements of* X *and* δ_i *is the restriction of* δ *to the case when the second argument is* x_i.

Table 2

a_i	$\delta(a_i, x_1)$	$\delta(a_i, x_2)$	$\lambda(a_i)$
a_1	a_2	a_3	y_1
a_2	a_2	a_4	y_1
a_3	a_5	a_2	y_1
a_4	a_6	a_2	y_1
a_5	a_2	a_2	y_1
a_6	a_2	a_2	y_2

Denote by $\pi_{\max}^{(i)}$ *the maximal congruence of* $\mathbf{A}_i$. *If* $\pi_{\max}^{(1)} \cap \pi_{\max}^{(2)} \cap \ldots \cap \pi_{\max}^{(n)}$ *equals the minimal partition* o *of* A, *then* $\mathbf{A}$ *is simple.*

Statement 1 is almost trivial. It may be asked whether the conversion of (the last sentence of) Statement 1 is valid.

Example 2. Analyze the automaton $\mathbf{A}$ determined by Table 2 (see Fig. 4) (with

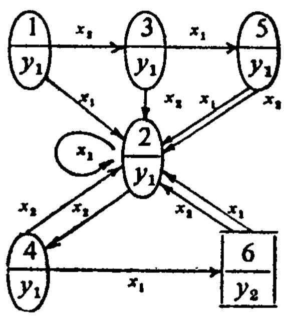

Fig. 4

$n=2$ and $v=|A|=6$). Form the autonomous automata $\mathbf{A}_1$ and $\mathbf{A}_2$. We get that the maximal congruence $\pi_{\max}^{(1)}$ of $\mathbf{A}_1$ is

$$\langle a_1, a_2, a_3, a_5 | a_4 | a_6 \rangle,$$

and the maximal congruence $\pi_{\max}^{(2)}$ of $\mathbf{A}_2$ is

$$\langle a_1, a_2, a_3, a_4, a_5 | a_6 \rangle;$$

hence $\pi_{\max}^{(1)} \cap \pi_{\max}^{(2)} = \pi_{\max}^{(1)}$. On the other hand, the automaton $\mathbf{A}$ itself is reduced.

This means that the condition in Statement 1 is (sufficient but) not necessary for the simplicity. If we take into account the connection between the distinguishability of states and the simplicity[8], then it becomes clear that whenever a pair of different states which are congruent modulo $\pi_{\max}^{(1)} \cap \pi_{\max}^{(2)}$ is considered — e.g., a_1

[8] Cf. [2], Section 5.

and a_2 —, then they are not distinguishable by any word of form x_1^m or x_2^m $(m \geqq 0)$, but there is a "mixed" input word which distinguishes them, for example,

$$\lambda(\delta(a_1, x_2x_1)) = \lambda(a_5) = y_1 \neq y_2 = \lambda(a_6) = \lambda(\delta(a_2, x_2x_1)).$$

Statement 1 has contained a sufficient condition for the *simplicity* of an automaton. The next statement asserts that another condition is sufficient for *non-simplicity*. (We shall see later that also Statement 2 does not allow a conversion.)

Statement 2. *Let* $\mathbf{A}=(A, X, Y, \delta, \lambda)$ *be an automaton, consider two sub-automata* $\mathbf{A}_1$ *and* $\mathbf{A}_2$ *of* $\mathbf{A}$.[9] *Suppose that there is an isomorphism* α *of* $\mathbf{A}_1$ *onto* $\mathbf{A}_2$ *such that* α *differs from the identical mapping of the state set of* $\mathbf{A}_1$. *Then* $\mathbf{A}$ *is not reduced.*

Table 3

a_i	$\delta(a_i, x_1)$	$\delta(a_i, x_2)$	$\lambda(a_i)$
a_1	a_2	a_3	y_1
a_2	a_4	a_4	y_2
a_3	a_5	a_5	y_2
a_4	a_6	a_6	y_3
a_5	a_7	a_7	y_3
a_6	a_2	a_1	y_4
a_7	a_3	a_1	y_4

Proof. There is a state a of $\mathbf{A}_1$ such that a and a^α are different. It is easy to see that a and a^α are undistinguishable, hence they are congruent for the maximal congruence of $\mathbf{A}$.

Example 3. Consider the automaton $\mathbf{A}$ determined by Table 3 (see Fig. 5). This automaton has neither a proper sub-automaton nor a non-trivial automorphism.

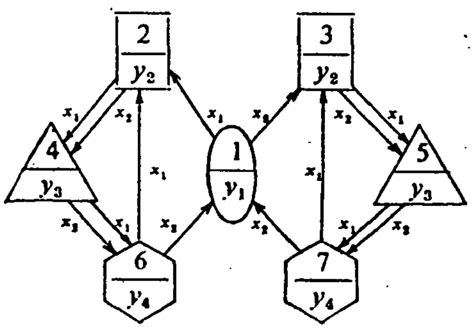

Fig. 5

[9] It is permitted that $\mathbf{A}$, $\mathbf{A}_1$, $\mathbf{A}_2$ be not pairwise different (even all of them can coincide).

Thus the condition of Statement 2 does not apply for **A**. However, **A** is not reduced, its maximal congruence $\pi_{\max}$ is

$$\langle a_1|a_2, a_3|a_4, a_5|a_6, a_7\rangle.$$

Consequently, the (sufficient) condition in Statement 2 is not necessary.

The fact that **A** is not simple but this cannot be shown by use of Statement 2 is in connection with the phenomenon that the *partial* sub-automaton over the state set $\{a_2, a_4, a_6\}$ is isomorphic to the *partial* sub-automaton over $\{a_3, a_5, a_7\}$. It can also be observed that there exists no chain

$$o = \pi_7 \subset \pi_6 \subset \pi_5 \subset \pi_4 = \pi_{\max}$$

in **A** such that $\pi_4, \pi_5, \pi_6, \pi_7$ are congruences whose indices (i.e., numbers of classes) are 4, 5, 6, 7, respectively. (Indeed, **A** has no other non-trivial congruence than $\pi_{\max}$.)

MATHEMATICAL INSTITUTE OF THE
HUNGARIAN ACADEMY OF SCIENCES
BUDAPEST 1364, HUNGARY
P.O. BOX 127.

References

[1] ÁDÁM, A., Gráfok és ciklusok (Graphs and cycles), *Mat. Lapok*, v. 22, 1971, pp. 269—282.
[2] ÁDÁM, A., On the question of description of the behaviour of finite automata, *Studia Sci. Math. Hungar.*, v. 13, 1978, pp. 105—124.
[3] ÁDÁM, A., On the complexity of codes and pre-codes assigned to finite Moore automata, *Acta Cybernet.*, v. 5, 1981, pp. 117—133.
[4] ÁDÁM, A., On the simplicity of finite autonomous Moore automata, *Studia Sci. Math. Hungar.*, v. 16, 1981, pp. 427—436.
[5] ÁDÁM, A., On certain partitions of finite directed graphs and of finite automata, *Acta Cybernet.*, v. 6, 1984, pp. 331—346.
[6] BERMAN, J., On the congruence lattices of unary algebras, *Proc. Amer. Math. Soc.*, v. 21, 1972, pp. 34—38.
[7] JAKUBÍKOVÁ-STUDENOVSKÁ, D., On congruence relations of monounary algebras, I, *Czechoslovak Math. J.*, v. 32, 1982, pp. 437—459.
[8] ORE, O., *Theory of graphs*, Amer. Math. Soc., Providence, 1962.
[9] YOELI, M. & GINZBURG, A., On homomorphic images of transition graphs, *J. Franklin Inst.*, v. 278, 1964, pp. 291—296.
[10] (СКОРНЯКОВ, Л. А.) SKORNJAKOV, L. A., Unars, *Universal Algebra, (Colloq. Math. Soc. J. Bolyai, 29, Esztergom, 1977)*, North-Holland, Amsterdam, 1982, pp. 735—743.

(Received July 15, 1984)